

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6741559号
(P6741559)

(45) 発行日 令和2年8月19日 (2020.8.19)

(24) 登録日 令和2年7月29日 (2020.7.29)

(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 15 (全 33 頁)

(21) 出願番号	特願2016-218329 (P2016-218329)	(73) 特許権者	514136668
(22) 出願日	平成28年11月8日 (2016.11.8)		パナソニック インテレクチュアル プロ
(65) 公開番号	特開2017-130911 (P2017-130911A)		パティ コーポレーション オブ アメリ
(43) 公開日	平成29年7月27日 (2017.7.27)		カ
審査請求日	令和1年5月23日 (2019.5.23)		Panasonic Intellectual
(31) 優先権主張番号	特願2016-7481 (P2016-7481)		Property Corporation of America
(32) 優先日	平成28年1月18日 (2016.1.18)		アメリカ合衆国 90503 カリフォル
(33) 優先権主張国・地域又は機関	日本国 (JP)		ニア州, トーランス, スイート 200,
			マリナー アベニュー 20000
		(74) 代理人	100109210
			弁理士 新居 広守
		(74) 代理人	100137235
			弁理士 寺谷 英作

最終頁に続く

(54) 【発明の名称】 評価装置、評価システム及び評価方法

(57) 【特許請求の範囲】

【請求項 1】

電子制御システムを構成する複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、

前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、

前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、

前記評価装置は更に、攻撃用の複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部を備え、

前記送信部は、前記攻撃手順情報が示す送信順序に従って前記攻撃用の複数のフレームを前記バスに送信し、

前記評価装置は、前記バスからフレームを受信する受信部を備え、

前記攻撃手順情報は、無効化フレームの次に所定 ID を有する攻撃用のフレームを送信することを示し、

前記送信部は、前記受信部が前記バスから前記所定 ID を有するフレームを受信した際に前記無効化フレームを送信する

評価装置。

10

20

【請求項 2】

電子制御システムを構成する複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、
前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、
前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、
前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、
前記送信部は、無効化フレームの送信後に、当該無効化フレームで無効化したフレームと、同一のIDを有し内容の相違する攻撃用のフレームを送信する
評価装置。

10

【請求項 3】

電子制御システムを構成する複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、
前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、
前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、
前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、
前記送信部は、無効化フレームの送信後に、前記電子制御システムにおいて前記複数の電子制御ユニットのいずれかのソフトウェアの更新処理のために予め定められている更新用IDを有する攻撃用のフレームを送信し、
前記監視部は、前記更新用IDを有するフレームの受信に応じて保持しているソフトウェアの更新処理を行う機能を有する電子制御ユニット、又は、前記更新用IDを有するフレームを送信する電子制御ユニットについて、前記監視を行う
評価装置。

20

【請求項 4】

前記評価装置は更に、攻撃用の複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部を備え、
前記送信部は、前記攻撃手順情報が示す送信順序に従って前記攻撃用の複数のフレームを前記バスに送信する
請求項 2 又は 3 記載の評価装置。

30

【請求項 5】

前記攻撃手順情報は更に攻撃用の前記複数のフレームについての送信間隔を示し、
前記送信部は、前記攻撃手順情報が示す送信順序及び送信間隔に従って前記複数のフレームを前記バスに送信する
請求項 1 又は 4 に記載の評価装置。

【請求項 6】

前記複数の電子制御ユニットは、CAN (Controller Area Network) プロトコルに従って前記バスを介して通信を行い、
前記無効化フレームは、エラーフレームである
請求項 1 ～ 5 のいずれか一項に記載の評価装置。

40

【請求項 7】

前記監視部は、前記送信部により攻撃用のフレームが前記バスに送信された場合における前記複数の電子制御ユニットのうちの1つの電子制御ユニットの動作が、所定動作と一致するか否かを検出することで、前記監視を行い、
前記評価部は、前記送信部により前記攻撃用のフレームが前記バスに送信された後における前記監視部による前記検出の結果に応じて評価結果が相違するように前記評価を行う

50

請求項 1 ～ 6 のいずれか一項に記載の評価装置。

【請求項 8】

前記評価装置は、前記バスからフレームを受信する受信部を備え、

前記監視部は、前記電子制御ユニットについての前記監視として、前記受信部により特定フレームが受信されたことの検出を行い、

前記評価部は、前記送信部により前記攻撃用のフレームが前記バスに送信された後の一定期間内に、前記特定フレームが受信されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行う

請求項 1 ～ 6 のいずれか一項に記載の評価装置。

【請求項 9】

前記評価部は、評価結果として前記電子制御システムに攻撃耐性があるか否かを示す情報を出力する

請求項 1 ～ 8 のいずれか一項に記載の評価装置。

【請求項 10】

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、

前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、

前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、

前記評価システムは更に、攻撃用の複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部を備え、

前記送信部は、前記攻撃手順情報が示す送信順序に従って前記攻撃用の複数のフレームを前記バスに送信し、

前記評価システムは、前記バスからフレームを受信する受信部を備え、

前記攻撃手順情報は、無効化フレームの次に所定 ID を有する攻撃用のフレームを送信することを示し、

前記送信部は、前記受信部が前記バスから前記所定 ID を有するフレームを受信した際に前記無効化フレームを送信する

評価システム。

【請求項 11】

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、

前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、

前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、

前記送信部は、無効化フレームの送信後に、当該無効化フレームで無効化したフレームと、同一の ID を有し内容の相違する攻撃用のフレームを送信する

評価システム。

【請求項 12】

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、

前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視

10

20

30

40

50

部と、

前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備え、

前記送信部は、無効化フレームの送信後に、前記電子制御システムにおいて前記複数の電子制御ユニットのいずれかのソフトウェアの更新処理のために予め定められている更新用 I D を有する攻撃用のフレームを送信し、

前記監視部は、前記更新用 I D を有するフレームの受信に応じて保持しているソフトウェアの更新処理を行う機能を有する電子制御ユニット、又は、前記更新用 I D を有するフレームを送信する電子制御ユニットについて、前記監視を行う

評価システム。

10

【請求項 13】

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信し、

前記攻撃用のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視し、

前記監視による監視結果に基づいて前記評価を行い、

前記評価方法は更に、攻撃用の複数のフレームの内容及び送信順序を示す攻撃手順情報を保持し、

20

前記送信は、前記攻撃手順情報が示す送信順序に従って前記攻撃用の複数のフレームを前記バスに送信し、

前記評価方法は、前記バスからフレームを受信し、

前記攻撃手順情報は、無効化フレームの次に所定 I D を有する攻撃用のフレームを送信することを示し、

前記送信は、前記受信部が前記バスから前記所定 I D を有するフレームを受信した際に前記無効化フレームを送信する

評価方法。

【請求項 14】

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信し、

前記攻撃用のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視し、

前記監視による監視結果に基づいて前記評価を行い、

前記送信は、無効化フレームの送信後に、当該無効化フレームで無効化したフレームと、同一の I D を有し内容の相違する攻撃用のフレームを送信する

評価方法。

【請求項 15】

40

バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、

前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信し、

前記攻撃用のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視し、

前記監視による監視結果に基づいて前記評価を行い、

前記送信は、無効化フレームの送信後に、前記電子制御システムにおいて前記複数の電子制御ユニットのいずれかのソフトウェアの更新処理のために予め定められている更新用 I D を有する攻撃用のフレームを送信し、

50

前記監視は、前記更新用 I D を有するフレームの受信に応じて保持しているソフトウェアの更新処理を行う機能を有する電子制御ユニット、又は、前記更新用 I D を有するフレームを送信する電子制御ユニットについて、前記監視を行う

評価方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、車載ネットワークシステム等の電子制御ユニットが通信を行う電子制御システムのセキュリティ（攻撃耐性等）に関する評価を行う技術に関する。

【背景技術】

【0002】

近年、自動車には多数の電子制御ユニット（E C U : Electronic Control Unit）が配置され、E C U をつなぐ車載ネットワークには、例えば I S O 1 1 8 9 8 - 1 で規定されている C A N （Controller Area Network）規格等が用いられる。

【0003】

C A N では、通信路は 2 本のワイヤで構成されたバスであり、バスに接続されている E C U はノードと呼ばれる。バスに接続されている各ノードは、フレームと呼ばれるメッセージを送受信する。フレームを送信する送信ノードは、2 本のバスに電圧をかけ、バス間で電位差を発生させることによって、レセシブと呼ばれる「1」の値と、ドミナントと呼ばれる「0」の値を送信する。複数の送信ノードが全く同一のタイミングで、レセシブとドミナントを送信した場合は、ドミナントが優先されて送信される。受信ノードは、受け取ったフレームのフォーマットに異常がある場合には、エラーフレームと呼ばれるフレームを送信する。エラーフレームとは、ドミナントを 6 b i t 連続して送信することで、送信ノードや他の受信ノードにフレームの異常を通知するものである。

【0004】

車載ネットワークに対する攻撃としては、攻撃者が車内の情報端末に無線通信でアクセスし、情報端末のプログラムを不正に書き換えてその情報端末から車載ネットワークに対して任意の C A N メッセージを送信し、車載 E C U につながるアクチュエータを運転者の意図に反して制御するような攻撃が知られている。自動車の運転自動化等に向けて、車載 E C U 自体が V 2 X （車車間通信（V 2 V : Vehicle to Vehicle）及び路車間通信（V 2 I : Vehicle to Infrastructure））等の無線通信の機能を搭載する状況になれば、情報端末と同様に、V 2 X に対応する E C U のプログラムが不正に書き換えられ、攻撃に利用され得る。

【0005】

攻撃対策の評価手法については、現状ではまだ研究が少ないが、例えば、非特許文献 1 には、単体の車載 E C U にデータを送信してその応答に注目することで不具合（プログラミング間違いによるバグの混入等）を見つけるファジング手法が開示されている。

【先行技術文献】

【非特許文献】

【0006】

【非特許文献 1】松本勉、小林優希、土屋遊、吉田直樹、森田伸義、萱島信、「車載 E C U に対する C A N 経由のファジング手法」、S C I S 2 0 1 5、2 0 1 5 年 1 月 2 0 日

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかしながら、非特許文献 1 の手法は、単体の車載 E C U の不具合を見つけることはできても、車載ネットワークを形成する複数の E C U で構成されるシステム（電子制御システム）を評価対象としてセキュリティ（評価対象に施されたセキュリティ対策技術が攻撃を適切に防御できるか否かという攻撃耐性等）に関する評価を行えるものではない。

【0008】

そこで、本発明は、複数の ECU から構成される電子制御システムを評価対象としてセキュリティに関する評価を行い得る評価装置を提供する。また、本発明は、複数の ECU から構成される電子制御システムのセキュリティに関する評価を行い得る評価システム及びその評価のための評価方法を提供する。

【課題を解決するための手段】

【0009】

上記課題を解決するために本発明の一態様に係る評価装置は、電子制御システムを構成する複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価装置である。

10

【0010】

また、上記課題を解決するために本発明の一態様に係る評価システムは、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価システムである。

20

【0011】

また、上記課題を解決するために本発明の一態様に係る評価方法は、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信し、前記攻撃用のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視し、前記監視による監視結果に基づいて前記評価を行う評価方法である。

【発明の効果】

【0012】

30

本発明によれば、複数の ECU から構成される電子制御システムの攻撃耐性（電子制御システムに施されたセキュリティ対策技術が攻撃を適切に防御できるか否か等）について評価することが可能となる。

【図面の簡単な説明】

【0013】

【図1】実施の形態に係る評価システムの概略構成を示す構成図である。

【図2】評価システムにおける評価装置の構成図である。

【図3】評価対象の電子制御システムにおける書換（書き換え）実施 ECU の構成図である。

【図4】評価対象の電子制御システムにおける被書換 ECU の構成図である。

40

【図5】評価対象の電子制御システムにおけるセキュリティ ECU の構成図である。

【図6】評価装置の保持部が保持する攻撃手順情報の一例を示す図である。

【図7】評価装置の保持部が保持する攻撃手順情報の他の一例を示す図である。

【図8】電子制御システムにおけるソフトウェアの更新に係る動作例を示すシーケンス図である。

【図9】評価システムの動作例1を示すシーケンス図である（図10に続く）。

【図10】評価システムの動作例1を示すシーケンス図である（図9から続く）。

【図11】評価システムの動作例2を示すシーケンス図である（図12に続く）。

【図12】評価システムの動作例2を示すシーケンス図である（図11から続く）。

【図13】評価システムの動作例3を示すシーケンス図である（図14に続く）。

50

【図 1 4】評価システムの動作例 3 を示すシーケンス図である（図 1 3 から続く）。

【図 1 5】評価システムの動作例 4 を示すシーケンス図である（図 1 6 に続く）。

【図 1 6】評価システムの動作例 4 を示すシーケンス図である（図 1 5 から続く）。

【図 1 7】評価システムの動作例 5 を示すシーケンス図である（図 1 8 に続く）。

【図 1 8】評価システムの動作例 5 を示すシーケンス図である（図 1 7 から続く）。

【発明を実施するための形態】

【0014】

本発明の一態様に係る評価装置は、電子制御システムを構成する複数の電子制御ユニットが通信に用いるバスに接続され、当該電子制御システムのセキュリティに関する評価を行う評価装置であって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価装置である。監視部は、送信部により攻撃用のフレーム（例えばCANのデータフレーム、エラーフレーム等）がバスに送信される際に（例えば、送信直後に、或いは、送信直前から送信直後に亘り）、電子制御ユニット（ECU）について直接又は間接的に監視し得る。これにより、複数のECUから構成される電子制御システムを評価対象として、フレームの送信に基づくECUへの攻撃への防御機能等といったセキュリティ機能（攻撃耐性等）の評価を行い得る。

【0015】

また、例えば、前記複数の電子制御ユニットは、CAN（Controller Area Network）プロトコルに従って前記バスを介して通信を行い、前記無効化フレームは、エラーフレームであることとしても良い。これにより、ECU間でフレームの授受を行うためのCANに従うネットワークにおける、エラーフレームを含む攻撃用のフレームの送信による攻撃に対するセキュリティ機能の評価が可能となり得る。

【0016】

また、例えば、前記評価装置は更に、攻撃用の複数のフレームの内容及び送信順序を示す攻撃手順情報を保持する保持部を備え、前記送信部は、前記攻撃手順情報が示す送信順序に従って前記攻撃用の複数のフレームを前記バスに送信することとしても良い。これにより、複数のフレームの送信順序等で定まる攻撃方法に対する防御機能等の評価が可能となり得る。

【0017】

また、例えば、前記評価装置は、前記バスからフレームを受信する受信部を備え、前記攻撃手順情報は、エラーフレームの次に所定IDを有する攻撃用のフレームを送信することを示し、前記送信部は、前記受信部が前記バスから前記所定IDを有するフレームを受信した際に前記エラーフレームを送信することとしても良い。これにより、例えば、電子制御システムにおいて所定IDを有するフレームの送信元として規定されているECUになりすまして攻撃する攻撃方法に対するセキュリティ機能の評価が可能となり得る。

【0018】

また、例えば、前記攻撃手順情報は更に攻撃用の前記複数のフレームについての送信間隔を示し、前記送信部は、前記攻撃手順情報が示す送信順序及び送信間隔に従って前記複数のフレームを前記バスに送信することとしても良い。これにより、複数のフレームの送信順序及び送信間隔で定まる攻撃方法に対する防御機能等の評価が可能となり得る。

【0019】

また、例えば、前記送信部は、エラーフレームの送信後に、当該エラーフレームで無効化したフレームと、同一のIDを有し内容の相違する攻撃用のフレームを送信することとしても良い。これにより、例えば、電子制御システムにおいてバスに送信されたフレームをエラーフレームで無効化して内容を一部変更したフレームを送信するという比較的容易に実施可能な攻撃方法を用いることで効率的なセキュリティ機能の評価が可能となり得る。

。

10

20

30

40

50

【0020】

また、例えば、前記送信部は、エラーフレームの送信後に、前記電子制御システムにおいて前記複数の電子制御ユニットのいずれかのソフトウェアの更新処理のために予め定められている更新用IDを有する攻撃用のフレームを送信し、前記監視部は、前記更新用IDを有するフレームの受信に応じて保持しているソフトウェアの更新処理を行う機能を有する電子制御ユニット、又は、前記更新用IDを有するフレームを送信する電子制御ユニットについて、前記監視を行うこととしても良い。ソフトウェアの更新処理は、更新そのものであっても良いし、更新の前処理や後処理といった適切な更新のために行われる付帯処理等であっても良いし、両方を含んでいても良い。これにより、例えば、攻撃者が電子制御システムの一部のECUを支配するための攻撃の一種であるところの、ECUのファームウェア等といったソフトウェアの更新に関連した攻撃に対する電子制御システムのセキュリティ機能の評価が可能となり得る。

10

【0021】

また、例えば、前記監視部は、前記送信部により攻撃用のフレームが前記バスに送信された場合における前記複数の電子制御ユニットのうちの1つの電子制御ユニットの動作が、所定動作と一致するか否かを検出することで、前記監視を行い、前記評価部は、前記送信部により前記攻撃用のフレームが前記バスに送信された後における前記監視部による前記検出の結果に応じて評価結果が相違するように前記評価を行うこととしても良い。所定動作は、攻撃が成功した場合に予測（期待）されるECUの動作、攻撃が失敗した場合に予測されるECUの動作、正規のフレームを受信した場合におけるECUの通常の動作等であり得る。これにより、電子制御システムのセキュリティ機能の適切な評価が可能となり得る。

20

【0022】

また、例えば、前記評価装置は、前記バスからフレームを受信する受信部を備え、前記監視部は、前記電子制御ユニットについての前記監視として、前記受信部により特定フレームが受信されたことの検出を行い、前記評価部は、前記送信部により前記攻撃用のフレームが前記バスに送信された後の一定期間内に、前記特定フレームが受信されたことが前記監視部により検出されたか否かに応じて評価結果が相違するように前記評価を行うこととしても良い。特定フレームは、例えば攻撃が成功した場合或いは失敗した場合に送信されることが予測（期待）されるフレームであり、例えば、電子制御システムで規定されたフレームのIDにより識別可能である。これにより、例えばECUと直接通信する等に依らなくても、バスの監視により適切に電子制御システムを評価し得る。

30

【0023】

また、例えば、前記評価部は、評価結果として前記電子制御システムに攻撃耐性があるか否かを示す情報を出力することとしても良い。これにより、例えば、評価装置の利用者等は、電子制御システムに攻撃耐性があるか否かを知り得る。

【0024】

また、本発明の一態様に係る評価システムは、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価システムであって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、前記バスに送信する送信部と、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視する監視部と、前記送信部により前記攻撃用のフレームが前記バスに送信される際における前記監視部の監視結果に基づいて前記評価を行う評価部とを備える評価システムである。これにより、複数のECUから構成される電子制御システムにおけるECUへのフレームの送信による攻撃への防御機能等といったセキュリティ機能の評価が可能となり得る。

40

【0025】

また、本発明の一態様に係る評価方法は、バスを介して通信する複数の電子制御ユニットを備える電子制御システムのセキュリティに関する評価を行う評価方法であって、前記バス上のフレームを無効化する無効化フレームを含む、1つ以上の攻撃用のフレームを、

50

前記バスに送信し、前記攻撃用のフレームが前記バスに送信される際に、前記複数の電子制御ユニットのうち1つ以上の電子制御ユニットについて監視し、前記監視による監視結果に基づいて前記評価を行う評価方法である。これにより、複数のECUから構成される電子制御システムを評価対象として、フレームの送信による攻撃への防御機能等といったセキュリティ機能の評価が可能となり得る。

【0026】

なお、これらの全般的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なCD-ROM等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

10

【0027】

以下、実施の形態に係る評価システムについて、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本発明の一具体例を示すものである。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及びステップの順序等は、一例であって本発明を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

【0028】

（実施の形態1）

20

以下、自動車（車両）に搭載され、バスを介して通信する複数の電子制御ユニット（ECU）を含んで構成される車載ネットワークシステム（電子制御システム）のセキュリティに関する評価を行う評価装置及び評価方法、並びに、電子制御システムと評価装置とを含む評価システムについて説明する。

【0029】

〔1. 1 評価システム10の構成〕

図1は、評価システム10の概略構成を示す構成図である。評価システム10は、同図に示すように、評価装置101と、電子制御システム11とを含んで構成される。評価システム10は、電子制御システム11を評価対象として、電子制御システム11の攻撃耐性（攻撃に対して防御を行うセキュリティ対策技術が適切に作用しているか否か等）につ

30

【0030】

電子制御システム11は、車載ネットワークシステムであり、車両内の制御装置、センサ、アクチュエータ（例えば電子制御可能にされたステアリング、アクセル、ブレーキ等）、ユーザインタフェース装置等の各種機器に接続されて、車内のバス（CANバス）を介してフレームの送受信を行う複数の電子制御ユニット（ECU）を含んで構成される車載ネットワークを備える。電子制御システム11では、各ECUがフレームを授受して連携することで、例えば、先進運転者支援システム（ADAS：Advanced Driver Assistance System）の一機能である駐車支援機能、車線維持支援機能、衝突回避支援機能等の機能を実現する。各ECUは、ソフトウェアにより制御されており、ECUのソフトウェアは、ある種のフレームのCANバスでの授受を含む手順により書き換え（更新）可能である。

40

【0031】

車内には多数のECU等が含まれ得るが、ここでは説明の便宜上、一例として、電子制御システム11は、図1に示すように、書換実施ECU102、被書換ECU103、及び、セキュリティECU104を備えるものとして説明する。なお、各ECUは、CANバス20を通信路としてCAN規格（プロトコル）に従って通信を行う。CANにおいてデータの伝送に用いられるフレームであるデータフレーム（CANメッセージとも称する）は、ID（メッセージID）を格納するIDフィールド、データを格納するデータフィールド等を含むように規定されている。

50

【0032】

書換実施ECU102は、CANバス20に接続され、被書換ECU103のソフトウェアの更新処理のためのCANメッセージ（データフレーム）である更新用フレームを、CANバス20へ送信する機能（書換実施機能）を有するECUである。更新用フレームは、電子制御システム11においてソフトウェアの更新処理のために予め定められている更新用IDをメッセージIDとして有するフレームである。更新用フレームとしては、例えば、書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト（更新用のプログラムである更新ソフトウェア）、更新ソフト署名（更新ソフトウェアに対するデジタル署名）、再起動指示のそれぞれを示すフレーム等がある。書換実施ECU102は、例えば、更新用のソフトウェアを外部から電子制御システム11内に取り込む機能を有するECUである。書換実施ECU102は、具体例としては、カーナビゲーション機能を有するECU、車両外部と通信する外部通信機能を有するECU、装着された記録媒体からデータを読み取る機能を有するECU、診断ポートに接続された診断ツール（故障診断ツール）等である。診断ポートは、車載ネットワーク（CANバス）における、例えばOBD2（On-Board Diagnostics 2）等といった診断ツール等と通信するためのインタフェースである。

10

【0033】

被書換ECU103は、CANバス20に接続され、更新用フレームの受信によって、自ECU（被書換ECU103）におけるソフトウェアを更新する機能（被書換機能）を有するECUである。被書換ECU103は、例えば、アクチュエータ（例えば、ステアリング、アクセル、ブレーキ等）を制御するECU等であっても良く、更新されるソフトウェアは、例えばそのアクチュエータの制御を含む処理のためのソフトウェアであっても良い。

20

【0034】

セキュリティECU104は、CANバス20を常時監視（モニタリング）し、例えば不正なCANメッセージ（攻撃用のCANメッセージ）が流れていることを検知した場合に、そのCANメッセージを無効化する等の対処を行う。CANメッセージの無効化の方法としては、任意の方法を用いることができるが、例えば不正なCANメッセージに重畳させるように、CANプロトコルで規定されたエラーフレームを送信することで無効化し得る。

30

【0035】

評価装置101は、電子制御システム11（評価対象）に対して施されたセキュリティ対策技術の攻撃耐性を評価する装置である。評価装置101は、保持する攻撃手順情報105に基づいて、評価対象に対して攻撃（ハッキング）を仕掛け、攻撃への反応を観測するための監視（モニタリング）を行い、監視結果に応じた評価を行う。評価装置101による評価の一例としては、例えば、その攻撃に対する耐性の有無（攻撃或いは防御の成否）の判定が挙げられる。評価装置101は、監視として具体的には、CANバス20を流れるフレーム（メッセージ）の監視、書換実施ECU102及び被書換ECU103の出力信号の監視を行う。なお、評価装置101は、書換実施ECU102或いは被書換ECU103により制御されたアクチュエータ等の挙動（動作）の監視を行うこととしても良い。攻撃手順情報105は、攻撃を仕掛ける際の手順（送信すべきフレームの種類、順序、タイミング、頻度等）を示す。

40

【0036】

以下、評価システム10の各構成要素について詳細に説明する。

【0037】

〔1.2 評価装置101の構成〕

図2は、評価システム10における評価装置101の構成図である。

【0038】

評価装置101は、図2に示すように、監視部200（CANバス監視部203及び信号監視部204）と、送受信部201（送信部201a及び受信部201b）と、保持部

50

202と、評価部206と、制御部207と、記憶部208を含んで構成される。

【0039】

評価装置101は、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路、ハードディスク等を含む装置である。メモリは、ROM、RAM等であり、プロセッサにより実行される制御プログラム（ソフトウェアとしてのコンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作（各種回路の制御等）することにより、評価装置101は各種機能を実現することになる。なお、コンピュータプログラムは、所定の機能を達成するために、プロセッサに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

10

【0040】

（1）送受信部201

送受信部201は、通信回路等により実現される。送受信部201は、送信部201a及び受信部201bで構成される。送信部201aは、CANバス20に対して、CANメッセージ（例えば、書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト、更新ソフト署名等の各種情報を示す各種のフレーム等）、或いは、エラーフレームを送信する。エラーフレームは、CANバス20に流れるCANメッセージを無効化し、例えば、その無効化対象となったCANメッセージを送信したECUを、バスオフ状態やエラーアクティブ状態にし得る。受信部201bは、CANバス20を流れるCANメッセージ（例えば書換実施ECU102或いは被書換ECU103により送信された、書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト、更新ソフト署名、再起動指示、認証シード、認証結果、等の各種情報を示す各種のフレーム等）を受信する。

20

【0041】

（2）保持部202

保持部202は、メモリ、ハードディスク等の記憶媒体で実現され、評価装置101が評価対象の攻撃耐性等を評価するために仕掛ける攻撃の手順を示す攻撃手順情報105を記憶している。攻撃手順情報105は攻撃用の複数のフレーム（CANメッセージ或いはエラーフレーム）の送信順序等を示す。攻撃手順情報105の詳細については後に図6及び図7を用いて説明する。

【0042】

（3）CANバス監視部203

CANバス監視部203は、例えばプログラムを実行するプロセッサ等により実現され、評価対象の電子制御システム11で複数のECUが接続されているCANバス20を監視する。CANバス監視部203は、具体的には受信部201bを介してCANメッセージを受信して、CANメッセージに含まれるデータの中身（ペイロード）を、記憶部208に記録し、確認する。CANバス監視部203は、例えば、書換実施ECU102についての監視として、書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト、更新ソフト署名、再起動指示のそれぞれを示す更新用フレームがCANバス20に送信されたことを検出してフレームの内容を確認する。また、CANバス監視部203は、例えば、被書換ECU103についての監視として、認証シード、認証結果のそれぞれを示すフレームがCANバス20に送信されたことを検出してフレームの内容を確認する。監視部200は、CANバス監視部203により、電子制御システム11のECUについての監視として、受信部201bにより特定フレームが受信されたことの検出を行う。この特定フレームは、特定の内容を有する予め規定されたフレームであって、フレームのID、データフィールドの内容等により特定されるフレームであり得る。この特定フレームは、攻撃用のフレームの送信による攻撃に対して電子制御システム11の一部のECUが、特定フレームを送信する或いは送信しないことにより、攻撃が成功したか否か、防御が成功したか否か等が予め区別可能と想定されるフレームである。

30

40

【0043】

（4）信号監視部204

50

信号監視部 204 は、書換実施 ECU102 及び被書換 ECU103 が CAN バス 20 以外の信号線等に出力した信号を観測し、信号内容を確認する。信号監視部 204 は、例えば、書換実施 ECU102 及び被書換 ECU103 のそれぞれが信号を出力する信号線に接続する通信回路、プログラムを実行するプロセッサ等により実現される。なお、信号監視部 204 は、例えば、書換実施 ECU102 及び被書換 ECU103 のそれぞれのデバッグ用の出力信号を監視するものであっても良く、電子制御システム 11 の各 ECU は評価に際してデバッグ用の出力信号を出力し得るように構成されることとしても良い。この場合において各 ECU は、デバッグ用の出力信号として、ECU の状態を示す情報、メモリ内容を示す情報、或いは、ソフトウェアを実行するプロセッサのリセット（再起動）がなされたことを示す情報等を出力し得る構成を有していても良い。信号監視部 204 は、信号の観測により、例えば、被書換 ECU103 がソフトウェアの更新（書き換え）に係る処理を再起動の実行によって完了したか否か等を確認し得る。監視部 200 は、信号監視部 204 等により、送信部 201a により攻撃用のフレームが CAN バス 20 に送信された場合における電子制御システム 11 のいずれかの ECU の動作が、所定動作（例えば、攻撃が成功した場合に予測される動作、攻撃が失敗した場合に予測される動作、正規のフレームを受信した場合における通常の動作等）と一致するか否かを検出することで、その ECU の監視を行う。

10

【0044】

（5）評価部 206

評価部 206 は、プログラムを実行するプロセッサ等により実現される。評価部 206 は、監視部 200（CAN バス監視部 203 及び信号監視部 204）での監視による確認結果に基づいて、電子制御システム 11 のセキュリティに関する評価を行う。具体的には、評価部 206 は、監視部 200 による確認結果の全部又は一部と、攻撃手順情報 105 に基づいて CAN メッセージを送信するときの期待値とを比較し、攻撃が成功しているか否か（例えば攻撃に対する防御機能が適切に作動したか否か）等を判定する。期待値は、攻撃結果（例えば各攻撃用のフレームの送信に対する結果）として期待される書換実施 ECU102 或いは被書換 ECU103 が、送信する CAN メッセージ、或いは、送信する信号で示される情報（動作等）であり、予め規定され得る。評価部 206 は、送信部 201a により攻撃手順情報 105 に基づく攻撃用のフレームが CAN バス 20 に送信される際（例えば送信直後の一定期間、或いは送信直前から送信直後まで等）における監視部 200 の監視結果に基づいて評価を行う。評価部 206 は、例えば、送信部 201a により攻撃手順情報 105 に示される攻撃用の複数のフレームの 1 つ以上が CAN バス 20 に送信された後の一定期間内に、期待値としての特定フレームが CAN バス 20 上で送信されたことが CAN バス監視部 203 により検出されたか否かを判定し、特定フレームが検出されたか否かに応じて評価結果が相違するように評価を行い得る。また評価部 206 は、例えば、攻撃用のフレームの 1 つ以上が CAN バス 20 に送信された後の一定期間内に、書換実施 ECU102 或いは被書換 ECU103 が期待値に係る所定動作をしたことを示す信号が信号監視部 204 により検出されたか否かに応じて評価結果が相違するように評価を行い得る。

20

30

【0045】

（6）記憶部 208

記憶部 208 は、メモリ等の記憶媒体により構成され、偽の更新ソフト（更新ソフトウェア）、更新ソフトに対する偽の署名、更新手順、CAN バス 20 から受信した CAN メッセージの内容（メモリ消去命令、更新ソフト、更新ソフト署名、認証鍵、認証シード等）を保持する。

40

【0046】

（7）制御部 207

制御部 207 は、プログラムを実行するプロセッサ等により実現され、監視部 200、送受信部 201、保持部 202、記憶部 208、及び、評価部 206 を管理、制御して評価装置 101 の機能を実現する。また、制御部 207 は、認証鍵の生成、確認等のために

50

必要な演算処理を行い得る。

【0047】

[1. 3 書換実施 ECU 102 の構成]

図3は、書換実施 ECU 102 の構成図である。

【0048】

書換実施 ECU 102 は、図3に示すように、送受信部 301 と、署名記憶部 302 と、鍵記憶部 303 と、プログラム記憶部 304 と、書換手順情報記憶部 305 と、制御部 306 とを含んで構成される。

【0049】

書換実施 ECU 102 は、CANバス 20 に接続された ECU である。ECU は、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM等であり、プロセッサにより実行される制御プログラムを記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作（各種回路の制御等）することにより、書換実施 ECU 102 は機能を果たす。

【0050】

(1) 送受信部 301

送受信部 301 は、CANバス 20 に対して CAN メッセージを送信し、CANバス 20 を流れる CAN メッセージを受信する。送受信部 301 は、例えば、書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト、更新ソフト署名、再起動指示のそれぞれを示す更新用フレームを送信し、CANバス 20 に流れる認証シード、認証結果のそれぞれを示すフレームを受信する。また、送受信部 301 は、例えば、電子制御システム 11 の外部（車両外部）の装置と通信する外部通信機能を担い、更新ソフト、更新ソフト署名等を外部の装置から受信する。

【0051】

なお、書換実施 ECU 102 が被書換 ECU 103 のソフトウェアを更新するための更新処理において用いられる認証シードは、書換実施 ECU 102 と被書換 ECU 103 とが互いを認証するために用いられる情報である。また、認証鍵は、被書換 ECU 103 が送信した認証シードに基づいて、書換実施 ECU 102 が、互いに共通の秘密鍵を用いた暗号化を施すことで生成した情報である。更新処理では、書換実施 ECU 102 が、被書換 ECU 103 が送信した認証シードに基づいて共通の秘密鍵を用いた暗号化により認証鍵を生成し、認証鍵を被書換 ECU 103 へ送信し、被書換 ECU 103 が、共通の秘密鍵にて認証鍵を復号してその復号結果が先に送信した認証シードと一致すれば認証成功、一致しなければ認証不成功と判断し、判断結果である認証結果（例えば認証成功の場合に書換許可を示し認証不成功の場合に書換不許可を示す情報）を書換実施 ECU 102 に送信する。認証成功の場合において、ソフトウェアの書き換えのために、メモリ消去命令、更新ソフト、更新ソフト署名、再起動指示等が書換実施 ECU 102 から送信され、これに応じて被書換 ECU 103 ではソフトウェアの書き換え等が行われる。

【0052】

(2) 署名記憶部 302

署名記憶部 302 は、プログラム記憶部 304 で記憶している更新ソフトに対する署名を記憶する。

【0053】

(3) 鍵記憶部 303

鍵記憶部 303 は、被書換 ECU 103 から送信された認証シードを暗号化することで認証鍵を生成するときの暗号化に用いる鍵（秘密鍵）を記憶する。

【0054】

(4) プログラム記憶部 304

プログラム記憶部 304 は、被書換 ECU 103 用の更新ソフト（更新ソフトウェア）を記憶する。

【0055】

(5) 書換手順情報記憶部305

書換手順情報記憶部305は、被書換ECU103のソフトウェアの更新手順（ソフトウェアの書き換えに係る処理手順）を記憶する。

【0056】

(6) 制御部306

制御部306は、送受信部301、署名記憶部302、鍵記憶部303、プログラム記憶部304、及び、書換手順情報記憶部305を管理、制御して、書換実施ECU102の機能を実現する。即ち、制御部306は、書換手順情報記憶部305が記憶する書換手順情報（更新手順）に従って、各部を制御して、被書換ECU103のソフトウェアを、更新ソフトウェアへと更新するための更新処理（各種更新用フレームの送信、認証シード及び認証結果の受信等を含む一連の処理）等を実行し得る。

10

【0057】

[1. 4 被書換ECU103の構成]

図4は、被書換ECU103の構成図である。

【0058】

被書換ECU103は、図4に示すように、送受信部401と、署名記憶部402と、鍵記憶部403と、プログラム記憶部404と、書換手順情報記憶部405と、制御部406とを含んで構成される。

【0059】

被書換ECU103は、CANバス20に接続されたECUであり、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。例えばプロセッサが、メモリに格納された制御プログラムに従って動作することにより、被書換ECU103は機能を果たす。

20

【0060】

(1) 送受信部401

送受信部401は、CANバス20に対してCANメッセージを送信し、CANバス20を流れるCANメッセージを受信する。送受信部401は、例えば、認証シード、認証結果のそれぞれを示すフレームを送信し、CANバス20に流れる書換モード遷移指示、認証鍵、メモリ消去命令、更新ソフト、更新ソフト署名、再起動指示のそれぞれを示す更新用フレームを受信する。

30

【0061】

(2) 署名記憶部402

署名記憶部402は、プログラム記憶部404で記憶している更新ソフトに対する署名を記憶する。

【0062】

(3) 鍵記憶部403

鍵記憶部403は、被書換ECU103が送信した認証シードに基づいて書換実施ECU102が暗号化により生成した認証鍵の復号に用いる復号鍵（秘密鍵）、及び、プログラム記憶部404に記憶したプログラム（更新ソフト）の署名である署名記憶部402に記憶した署名の正当性の検証に用いる署名検証鍵を記憶する。

40

【0063】

(4) プログラム記憶部404

プログラム記憶部404は、被書換ECU103のソフトウェア（例えば書換実施ECU102から取得した更新ソフト等）を記憶する。

【0064】

(5) 書換手順情報記憶部405

書換手順情報記憶部405は、被書換ECU103のソフトウェアの更新手順を記憶する。

【0065】

50

(6) 制御部406

制御部406は、送受信部401、署名記憶部402、鍵記憶部403、プログラム記憶部404、及び、書換手順情報記憶部405を管理、制御して、被書換ECU103の機能を実現する。即ち、制御部406は、書換手順情報記憶部405が記憶する書換手順情報（更新手順）に従って、各部を制御して、被書換ECU103のソフトウェアを、更新ソフトウェアへと更新するための更新処理（各種更新用フレームの受信、認証シード及び認証結果の送信等を含む一連の処理）等を実行し得る。

【0066】

[1.5 セキュリティECU104の構成]

図5は、セキュリティECU104の構成図である。

10

【0067】

セキュリティECU104は、図5に示すように、送受信部501と、CANバス監視部502と、制御部503とを含んで構成される。

【0068】

セキュリティECU104は、CANバス20に接続され、攻撃に対処するセキュリティ機能（防御機能等）を備えたECUである。セキュリティECU104のプロセッサが、メモリに記憶された制御プログラム（コンピュータプログラム）に従って動作することにより、セキュリティECU104は機能を果たす。

【0069】

(1) 送受信部501

20

送受信部501は、CANバス20を流れるCANメッセージを受信し、CANバス監視部502の指示を受けてCANバス20に、不正なCANメッセージを無効化するためにエラーフレームを送信する。

【0070】

(2) CANバス監視部502

CANバス監視部502は、複数のECUが接続されているCANバス20から送受信部501を介して受信したCANメッセージに含まれるデータの中身（ペイロード）を確認する。CANバス監視部502は、不正なCANメッセージ（例えば電子制御システム11において予め定められたルールに準拠していないCANメッセージ）が流れていることを確認した場合に、送受信部501を介してエラーフレームを送信する。CANバス監視部502が、不正なCANメッセージを検知する方法としては、いかなる方法を用いても良い。

30

【0071】

(3) 制御部503

制御部503は、送受信部501及びCANバス監視部502を管理、制御してセキュリティECU104の機能を実現する。

【0072】

[1.6 攻撃手順情報]

評価装置101の保持部202が記憶する攻撃手順情報について説明する。図6及び図7は、それぞれ攻撃手順情報の一例を示す。

40

【0073】

図6及び図7に示すように、攻撃手順情報は、例えば、評価装置101による評価項目毎（評価対象機能毎）に、送信メッセージ（評価対象機能の評価のための攻撃として送信すべき攻撃用のフレーム）の内容及びメッセージIDと、送信メッセージの送信間隔（先行フレームとの時間間隔）と、送信順序とを含む情報である。この攻撃手順情報は、例えば、電子制御システム11に関する各種情報（仕様等）に基づいて定められる。

【0074】

例えば、図6に示す評価対象機能が「書換実施機能1」という評価項目の例では、攻撃手順は、最初（1番目）に、エラーフレームを送信することで、被書換ECU103が送信した認証シードを含むCANメッセージを無効化し、次（2番目）に、偽の認証シード

50

を含むCANメッセージを送信し、次（３番目）に、書換実施ECU102から認証シードに対応した認証鍵を受信した後に応答として、認証結果（認証応答）を含むCANメッセージを送信するという一連の手順となる。

【0075】

例えば、図7に示す評価対象機能が「被書換機能1」という評価項目の例では、攻撃手順は、最初（１番目）に、エラーフレームを送信することで、書換実施ECU102が送信したメモリ消去命令を含むCANメッセージを無効化し、次（２番目）に、メモリ消去命令を含む更新用フレーム（CANメッセージ）を送信し、次（３番目）に、偽の更新ソフトを含む更新用フレーム（CANメッセージ）を送信し、次（４番目）に、その偽の更新ソフトに対応した署名を含む更新用フレーム（CANメッセージ）を送信するという一連の手順となる。なお、図7の攻撃手順情報において、更新ソフト署名を含む更新用フレームの送信に係る情報の次に、再起動指示を示す更新用フレームの送信に係る情報を含み得る。

10

【0076】

このような攻撃手順情報に従って、評価装置101は、各評価項目について定められた攻撃用のフレームを定められた送信順序で送信することにより、電子制御システム11を攻撃して評価する。評価装置101は、例えば、攻撃手順情報で、エラーフレームの次に、所定ID（例えば認証シード用のID、認証結果である認証応答用のID等）を有する攻撃用のフレームを送信することを示す場合には、受信部201bがCANバス20から所定IDを有するCANメッセージを受信した際に、まずエラーフレームを送信し、続いて所定IDを有する攻撃用のフレームを送信する。この所定IDは、ソフトウェアの更新処理のために予め定められている更新用ID（例えば、メモリ消去命令用のID、更新ソフト用のID、更新ソフト署名用のID、再起動指示用のID等）であっても良い。

20

【0077】

〔1.7 評価システム10の動作〕

以下、上述した構成を備える評価システム10の動作について説明する。

【0078】

まず、評価システム10で評価装置101が攻撃用のフレームを送信しないときにおいて、電子制御システム11で実施されるソフトウェアの更新に係る動作例について説明する。その後に、評価装置101により評価対象の電子制御システム11を、攻撃手順情報105に従って攻撃（攻撃用のフレームの送信により攻撃）することで評価する動作について、評価項目毎の動作例（動作例1～5）を説明する。

30

【0079】

〔1.7.1 ソフトウェアの更新の動作例〕

評価装置101が攻撃用のフレームを送信しないときに、電子制御システム11で実施されるソフトウェア（被書換ECU103におけるソフトウェア）の更新について、図8のシーケンス図に即して説明する。図8の例では、ソフトウェアの更新は、書換実施ECU102が予め定められた各種の更新用フレームを主導的に送信し、これに被書換ECU103が対応することで実現される。

【0080】

40

書換実施ECU102は、書換モード遷移指示（書換モードへの遷移を指示する旨の情報）を含む更新用フレーム（CANメッセージ）をCANバス20へ送信する（ステップS601）。

【0081】

CANバス20から書換モード遷移指示を含む更新用フレームを受信した被書換ECU103は、認証シードを含むCANメッセージをCANバス20へ送信する（ステップS602）。

【0082】

認証シードを含むCANメッセージを受信した書換実施ECU102は、受信した認証シードを鍵記憶部303に記憶した鍵を用いて暗号化することで認証鍵を生成し、認証鍵

50

を含む更新用フレーム（CANメッセージ）をCANバス20へ送信する（ステップS603）。

【0083】

認証鍵を含む更新用フレームを受信した被書換ECU103は、受信した認証鍵を鍵記憶部403に記憶した鍵を用いて復号し、復号結果と送信した認証シードとの一致の確認を行う。被書換ECU103は、一致していると確認した場合は、認証結果として書換許可を意味するCANメッセージをCANバス20へ送信し、以後の更新手順の実施を許可し、一致していないと確認した場合は、認証結果として書換不許可を意味するCANメッセージをCANバス20に送信し、以後の更新手順の実施を許可しない（ステップS604）。認証結果を含むCANメッセージを受信した書換実施ECU102は、受信したCANメッセージが認証結果として書換許可を意味している場合は、以後の更新手順を実施し、書換不許可を意味している場合は、以後の更新手順を実施しない。

10

【0084】

認証結果として書換許可を意味するCANメッセージを受信した書換実施ECU102は、メモリ消去命令を含む更新用フレームをCANバス20へ送信する（ステップS605）。メモリ消去命令を含む更新用フレームを受信した被書換ECU103は、プログラム記憶部404の記憶内容（更新ソフトを格納するための領域の内容）を消去する。

【0085】

次に、書換実施ECU102は、更新ソフトを含む更新用フレームをCANバス20へ送信する（ステップS606）。なお、更新用フレームは、複数のCANメッセージで構成されていても良く、例えば、更新ソフトを含む更新用フレームは、更新ソフトのデータ量に応じて、1つ又は複数のCANメッセージで構成される。更新ソフトを含む更新用フレームを受信した被書換ECU103は、プログラム記憶部404へ、受信した更新ソフトを書き込む。

20

【0086】

次に、書換実施ECU102は、更新ソフトに対応した更新ソフト署名を含む更新用フレームをCANバス20へ送信する（ステップS607）。更新ソフト署名を含む更新用フレームを受信した被書換ECU103は、署名記憶部402に、受信した更新ソフト署名を書き込む。

【0087】

30

最後に、書換実施ECU102は、再起動指示を示す更新用フレームをCANバス20へ送信する（ステップS608）。再起動指示を示す更新用フレームを受信した被書換ECU103は、再起動（プロセッサのリセット）を実施する。再起動に際して、被書換ECU103は、例えば、プログラム記憶部404が記憶するプログラム（更新ソフト）の署名として、署名記憶部402に記憶した署名が正当か否かを、鍵記憶部403が記憶する署名検証鍵を用いて検証し、正当であった場合はプロセッサのリセットを実行する。プロセッサがリセットされると、プロセッサにより、プログラム記憶部404内の更新ソフトが実行される。被書換ECU103は、プログラムの署名の検証により、署名が正当でなかった場合は、更新ソフトを実行するための再起動を実行しない。なお、被書換ECU103は、例えば、メモリ消去命令に対応して、プログラム記憶部404の記憶内容（更新ソフトを格納するための領域の内容）を消去する際に、元の記憶内容を記憶媒体（例えば不揮発性メモリ、ハードディスク等）に保存することとしても良く、更新ソフトに係る署名が正当でなかった場合に元の記憶内容をプログラム記憶部404に復元することとしても良い。

40

【0088】

[1. 7. 2 評価システム10の動作例1]

図9及び図10は、電子制御システム11を評価する評価システム10の動作（動作例1）を示すシーケンス図である。動作例1では、評価装置101が、図6に示す書換実施機能1という評価項目に係る評価を行う例を示す。この例は、評価装置101が、被書換ECU103になりすまして書換実施ECU102に誤認識をさせる攻撃を行うことで、

50

電子制御システム 11 のセキュリティを評価する例である。以下、図 9 及び図 10 に即して、動作例 1 について説明する。

【0089】

書換実施 ECU 102 は、書換モード遷移指示を示す更新用フレーム（CAN メッセージ）を CAN バス 20 へ送信する（ステップ S601）。書換モード遷移指示を含む更新用フレームを受信した被書換 ECU 103 は、認証シードを含む CAN メッセージを CAN バス 20 へ送信する（ステップ S602）。

【0090】

評価装置 101 は、CAN バス 20 から CAN メッセージを受信することで、認証シードを含む CAN メッセージが CAN バス 20 に流れていることを検知すると、その CAN メッセージ全体が書換実施 ECU 102 に受信される前に、エラーフレームを送信し、被書換 ECU 103 が送信する認証シードを含む CAN メッセージを無効化する（ステップ S701）。CAN バス 20 上において認証シードを含む CAN メッセージは、エラーフレームにより上書きされ、正しく受信できない無効なものとなる。

【0091】

次に、評価装置 101 は、偽の認証シードを含む CAN メッセージを CAN バス 20 へ送信する（ステップ S702）。評価装置 101 の信号監視部 204 は、このステップ S702 以降の書換実施 ECU 102 の挙動の逐次監視の結果を記憶部 208 に逐次記録する。偽の認証シードを含む CAN メッセージを受信した書換実施 ECU 102 は、受信した認証シードを、鍵記憶部 303 に記憶した鍵を用いて暗号化することで認証鍵を生成する。そして、書換実施 ECU 102 は、生成した認証鍵を含む更新用フレーム（CAN メッセージ）を CAN バス 20 へ送信する（ステップ S603）。

【0092】

認証鍵を含む更新用フレームを受信した評価装置 101 は、その受信した認証鍵の正当性に拘わらず、認証結果として書換許可を意味する CAN メッセージを CAN バス 20 へ送信する（ステップ S703）。

【0093】

認証結果として書換許可を意味する CAN メッセージを受信した書換実施 ECU 102 は、メモリ消去命令を含む更新用フレームを CAN バス 20 へ送信する（ステップ S605）。メモリ消去命令を含む更新用フレームを受信した評価装置 101 は、CAN バス監視部 203 で、その受信したメモリ消去命令を含む更新用フレームの内容を記憶部 208 に記録する。

【0094】

次に、書換実施 ECU 102 は、更新ソフトを含む更新用フレームを CAN バス 20 へ送信する（ステップ S606）。更新ソフトを含む更新用フレームを受信した評価装置 101 は、CAN バス監視部 203 により、受信した更新ソフトを記憶部 208 に記録する。

【0095】

次に、書換実施 ECU 102 は、更新ソフトに対応した更新ソフト署名を含む更新用フレームを CAN バス 20 へ送信する（ステップ S607）。更新ソフト署名を含む更新用フレームを受信した被書換 ECU 103 は、CAN バス監視部 203 により、受信した更新ソフト署名を、記憶部 208 に記録する。

【0096】

次に、書換実施 ECU 102 は、再起動指示を示す更新用フレームを CAN バス 20 へ送信する（ステップ S608）。再起動指示を示す更新用フレームを受信した評価装置 101 は、CAN バス監視部 203 により、受信した再起動指示を示す更新用フレームの内容を記憶部 208 に記録する。

【0097】

最後に、評価装置 101 は、記憶部 208 に記録された、CAN バス 20 からの受信内容に係る情報、及び、ステップ S702 以降の書換実施 ECU 102 の動作に係る情報を

10

20

30

40

50

確認することで、評価を行う（ステップS801）。即ち、評価装置101は、受信内容及び書換実施ECU102の動作について、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価（攻撃の成否についての判定等）を行う。評価装置101は、例えば、確認した受信内容、及び、確認した書換実施ECU102の動作が、攻撃の期待値（被書換ECU103に対する更新用フレームの送信等の更新手順の実施と同様の動作）と同じようになっている場合に攻撃が成功していると判定する。評価装置101は、再起動指示を示す更新用フレーム等を受信しなくても、一定時間が経過した後（例えばステップS703での認証結果としてのCANメッセージの送信等から予め定められた時間が経過した後）において、ステップS801での評価を行い得る。このため、攻撃が失敗する場合（例えば、評価装置101がステップS703等で送信したCANメッセージが、セキュリティECU104によるエラーフレームの送信等により無効化された場合等）についても評価可能である。また、評価装置101は、CANバス監視部203での監視結果と、信号監視部204での監視結果とのうち一方のみを用いて攻撃の期待値に基づいて攻撃の成否についての判定等を行っても良い。また、評価装置101は、ステップS801で、評価対象である電子制御システム11のセキュリティの評価をどのように詳しく行っても良く、例えば、攻撃全体の成否の他に、攻撃用のフレームの送信という個々の攻撃の成否を判定しても良いし、各種の防御機能それぞれが作用したか否か、防御できた程度等について確認しても良い。

【0098】

〔1.7.3 評価システム10の動作例2〕

図11及び図12は、電子制御システム11を評価する評価システム10の動作（動作例2）を示すシーケンス図である。動作例2では、評価装置101が、図6に示す書換実施機能2という評価項目に係る評価を行う例を示す。この例は、評価装置101が、被書換ECU103になりすまして書換実施ECU102に誤認識をさせる攻撃を行うことで、電子制御システム11のセキュリティを評価する例である。以下、図11及び図12に即して、動作例2について説明する。

【0099】

書換実施ECU102は、書換モード遷移指示を示す更新用フレームをCANバス20へ送信する（ステップS601）。書換モード遷移指示を含む更新用フレームを受信した被書換ECU103は、認証シードを含むCANメッセージをCANバス20へ送信する（ステップS602）。認証シードを含むCANメッセージを受信した書換実施ECU102は、受信した認証シードに基づいて認証鍵を生成し、認証鍵を含む更新用フレームをCANバス20へ送信する（ステップS603）。認証鍵を含む更新用フレームを受信した被書換ECU103は、受信した認証鍵に基づく認証結果に係るCANメッセージをCANバス20へ送信する（ステップS604）。

【0100】

評価装置101は、CANバス20から認証結果に係るCANメッセージを受信することで、認証結果に係るCANメッセージがCANバス20に流れていることを検知すると、そのCANメッセージ全体が書換実施ECU102に受信される前に、エラーフレームを送信し、被書換ECU103が送信する認証結果に係るCANメッセージを無効化する（ステップS901）。CANバス20上において認証結果に係るCANメッセージは、エラーフレームにより上書きされ、正しく受信できない無効なものとなる。

【0101】

次に、評価装置101は、偽の認証結果として書換許可を意味するCANメッセージをCANバス20へ送信する（ステップS902）。評価装置101の信号監視部204は、このステップS902以降の書換実施ECU102の挙動の逐次監視の結果を記憶部208に逐次記録する。偽の認証結果に係る書換許可を意味するCANメッセージを受信した書換実施ECU102は、以後の更新手順を実施する。即ち、書換実施ECU102は、メモリ消去命令を含む更新用フレームをCANバス20へ送信する（ステップS605）。メモリ消去命令を含む更新用フレームを受信した評価装置101は、CANバス監視

部203で、その受信したメモリ消去命令を含む更新用フレームの内容を記憶部208に記録する。

【0102】

次に、書換実施ECU102は、更新ソフトを含む更新用フレームをCANバス20へ送信する（ステップS606）。更新ソフトを含む更新用フレームを受信した評価装置101は、CANバス監視部203により、受信した更新ソフトを記憶部208に記録する。

【0103】

次に、書換実施ECU102は、更新ソフトに対応した更新ソフト署名を含む更新用フレームをCANバス20へ送信する（ステップS607）。更新ソフト署名を含む更新用フレームを受信した被書換ECU103は、CANバス監視部203により、受信した更新ソフト署名を、記憶部208に記録する。

【0104】

次に、書換実施ECU102は、再起動指示を示す更新用フレームをCANバス20へ送信する（ステップS608）。再起動指示を示す更新用フレームを受信した評価装置101は、CANバス監視部203により、受信した再起動指示を示す更新用フレームの内容を記憶部208に記録する。

【0105】

最後に、評価装置101は、記憶部208に記録された、CANバス20からの受信内容に係る情報、及び、ステップS902以降の書換実施ECU102の動作に係る情報を確認することで、評価を行う（ステップS1001）。即ち、評価装置101は、上述のステップS801での評価と同様に、受信内容及び書換実施ECU102の動作について、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価（攻撃の成否についての判定等）を行う。

【0106】

[1.7.4 評価システム10の動作例3]

図13及び図14は、電子制御システム11を評価する評価システム10の動作（動作例3）を示すシーケンス図である。動作例3では、評価装置101が、図7に示す被書換機能1という評価項目に係る評価を行う例を示す。この例は、評価装置101が、書換実施ECU102になりすまして被書換ECU103に誤認識をさせる攻撃を行うことで、電子制御システム11のセキュリティを評価する例である。以下、図13及び図14に即して、動作例3について説明する。

【0107】

書換実施ECU102は、書換モード遷移指示を示す更新用フレームをCANバス20へ送信する（ステップS601）。書換モード遷移指示を含む更新用フレームを受信した被書換ECU103は、認証シードを含むCANメッセージをCANバス20へ送信する（ステップS602）。認証シードを含むCANメッセージを受信した書換実施ECU102は、受信した認証シードに基づいて認証鍵を生成し、認証鍵を含む更新用フレームをCANバス20へ送信する（ステップS603）。認証鍵を含む更新用フレームを受信した被書換ECU103は、受信した認証鍵に基づく認証結果として書換許可を意味するCANメッセージをCANバス20へ送信する（ステップS604）。認証結果として書換許可を意味するCANメッセージを受信した書換実施ECU102は、メモリ消去命令を含む更新用フレームをCANバス20へ送信する（ステップS605）。

【0108】

評価装置101は、CANバス20からメモリ消去命令を含む更新用フレームを受信することで、メモリ消去命令を含む更新用フレームがCANバス20に流れていることを検知すると、そのCANメッセージ全体が被書換ECU103に受信される前に、エラーフレームを送信し、書換実施ECU102が送信する更新用フレームを無効化する（ステップS1101）。CANバス20上においてメモリ消去命令を含む更新用フレームは、エラーフレームにより上書きされ、正しく受信できない無効なものとなる。

【0109】

次に、評価装置101は、メモリ消去命令を含む更新用フレームをCANバス20へ送信する（ステップS1102）。評価装置101のCANバス監視部203及び信号監視部204は、このステップS1102以降の被書換ECU103の動作或いは応答の逐次監視の結果を記憶部208に逐次記録する。例えば、信号監視部204は、メモリ消去命令を含む更新用フレームを受信した後の被書換ECU103の動作（例えばプログラム記憶部404の記憶内容を消去した等）等を記憶部208に記録する。

【0110】

次に、評価装置101は、更新ソフトを含む更新用フレームをCANバス20へ送信する（ステップS1103）。更新ソフトは必ずしも正規の内容である必要はなく、偽の更新ソフトであっても良い。評価装置101は、更新ソフトを含む更新用フレームを受信した後の被書換ECU103の動作或いは応答を記憶部208に記録する。

10

【0111】

次に、評価装置101は、更新ソフトに対応した更新ソフト署名を含む更新用フレームをCANバス20へ送信する（ステップS1201）。評価装置101は、更新ソフト署名を含む更新用フレームを受信した後の被書換ECU103の動作、応答等を記憶部208に記録する。なお、評価装置101は、更新ソフト、更新ソフト署名、署名生成に用いるために必要な鍵等の情報（更新処理に必要な情報）を、予め有していても良い。

【0112】

次に、評価装置101は、再起動指示を示す更新用フレームをCANバス20へ送信する（ステップS1202）。評価装置101は、再起動指示を示す更新用フレームを受信した後の被書換ECU103の動作（例えば再起動が行われたか否か等）或いは応答を記憶部208に記録する。

20

【0113】

最後に、評価装置101は、記憶部208に記録された、CANバス20からの受信内容に係る情報、及び、ステップS1102以降の被書換ECU103の動作に係る情報を確認することで、評価を行う（ステップS1203）。即ち、評価装置101は、受信内容及び被書換ECU103の動作について、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価（攻撃の成否についての判定等）を行う。評価装置101は、例えば、確認した受信内容、及び、確認した被書換ECU103の動作が、攻撃の期待値（書換実施ECU102から更新用フレームを受信した場合と同様の動作）と同じようになっている場合に攻撃が成功していると判定する。評価装置101は、CANバス監視部203での監視結果と、信号監視部204での監視結果とのうち一方のみを用いて攻撃の期待値に基づいて攻撃の成否についての判定等を行っても良い。また、評価装置101は、ステップS1203で、評価対象である電子制御システム11のセキュリティの評価をどのように詳しく行っても良く、例えば、攻撃全体の成否の他に、攻撃用のフレームの送信という個々の攻撃の成否を判定しても良いし、各種の防御機能それぞれが作用したか否か、防御できた程度等について確認しても良い。

30

【0114】

[1. 7. 5 評価システム10の動作例4]

40

図15及び図16は、電子制御システム11を評価する評価システム10の動作（動作例4）を示すシーケンス図である。動作例4では、評価装置101が、図7に示す被書換機能2という評価項目に係る評価を行う例を示す。この例は、評価装置101が、書換実施ECU102になりすまして被書換ECU103に誤認識をさせる攻撃を行うことで、電子制御システム11のセキュリティを評価する例である。以下、図15及び図16に即して、動作例4について説明する。

【0115】

書換実施ECU102は、書換モード遷移指示を示す更新用フレームをCANバス20へ送信する（ステップS601）。書換モード遷移指示を含む更新用フレームを受信した被書換ECU103は、認証シードを含むCANメッセージをCANバス20へ送信する

50

(ステップS602)。認証シードを含むCANメッセージを受信した書換実施ECU102は、受信した認証シードに基づいて認証鍵を生成し、認証鍵を含む更新用フレームをCANバス20へ送信する(ステップS603)。認証鍵を含む更新用フレームを受信した被書換ECU103は、受信した認証鍵に基づく認証結果として書換許可を意味するCANメッセージをCANバス20へ送信する(ステップS604)。認証結果として書換許可を意味するCANメッセージを受信した書換実施ECU102は、メモリ消去命令を含む更新用フレームをCANバス20へ送信する(ステップS605)。メモリ消去命令を含む更新用フレームを受信した被書換ECU103は、プログラム記憶部404の記憶内容(更新ソフトを格納するための領域の内容)を消去する。

【0116】

10

次に、書換実施ECU102は、更新ソフトを含む更新用フレームをCANバス20へ送信する(ステップS606)。

【0117】

評価装置101は、CANバス20から更新ソフトを含む更新用フレームを受信することで、更新ソフトを含む更新用フレームがCANバス20に流れていることを検知すると、そのCANメッセージ全体が被書換ECU103に受信される前に、エラーフレームを送信し、書換実施ECU102が送信する更新用フレームを無効化する(ステップS1301)。CANバス20上において更新ソフトを含む更新用フレームは、エラーフレームにより上書きされ、正しく受信できない無効なものとなる。

【0118】

20

次に、評価装置101は、偽の更新ソフトを含む更新用フレームをCANバス20へ送信する(ステップS1302)。評価装置101のCANバス監視部203及び信号監視部204は、このステップS1302以降の被書換ECU103の動作或いは応答の逐次監視の結果を記憶部208に逐次記録する。例えば、信号監視部204は、被書換ECU103のデバッグ用の出力信号等に基づき、偽の更新ソフトを含む更新用フレームを受信した後の被書換ECU103の動作(例えば、プログラム記憶部404への偽の更新ソフトの格納等)等を記憶部208に記録する。

【0119】

次に、評価装置101は、偽の更新ソフトに対応した偽の更新ソフト署名を含む更新用フレームをCANバス20へ送信する(ステップS1401)。評価装置101は、偽の更新ソフト署名を含む更新用フレームを受信した後の被書換ECU103の動作、応答等を記憶部208に記録する。

30

【0120】

次に、評価装置101は、再起動指示を示す更新用フレームをCANバス20へ送信する(ステップS1402)。評価装置101は、再起動指示を示す更新用フレームを受信した後の被書換ECU103の動作或いは応答を記憶部208に記録する。

【0121】

最後に、評価装置101は、記憶部208に記録された、CANバス20からの受信内容に係る情報、及び、ステップS1302以降の被書換ECU103の動作に係る情報を確認することで、評価を行う(ステップS1403)。即ち、評価装置101は、上述のステップS1203での評価と同様に、受信内容及び被書換ECU103の動作について、攻撃の期待値と比較することにより、電子制御システム11のセキュリティの評価(攻撃の成否についての判定等)を行う。

40

【0122】

[1.7.6 評価システム10の動作例5]

図17及び図18は、電子制御システム11を評価する評価システム10の動作(動作例5)を示すシーケンス図である。動作例5では、評価装置101が、図7に示す被書換機能3という評価項目に係る評価を行う例を示す。この例は、評価装置101が、書換実施ECU102になりすまして被書換ECU103に誤認識をさせる攻撃を行うことで、電子制御システム11のセキュリティを評価する例である。以下、図17及び図18に即

50

して、動作例 5 について説明する。

【0123】

書換実施 ECU 102 は、書換モード遷移指示を示す更新用フレームを CAN バス 20 へ送信する（ステップ S601）。書換モード遷移指示を含む更新用フレームを受信した被書換 ECU 103 は、認証シードを含む CAN メッセージを CAN バス 20 へ送信する（ステップ S602）。認証シードを含む CAN メッセージを受信した書換実施 ECU 102 は、受信した認証シードに基づいて認証鍵を生成し、認証鍵を含む更新用フレームを CAN バス 20 へ送信する（ステップ S603）。認証鍵を含む更新用フレームを受信した被書換 ECU 103 は、受信した認証鍵に基づく認証結果として書換許可を意味する CAN メッセージを CAN バス 20 へ送信する（ステップ S604）。認証結果として書換許可を意味する CAN メッセージを受信した書換実施 ECU 102 は、メモリ消去命令を含む更新用フレームを CAN バス 20 へ送信する（ステップ S605）。メモリ消去命令を含む更新用フレームを受信した被書換 ECU 103 は、プログラム記憶部 404 の記憶内容（更新ソフトを格納するための領域の内容）を消去する。次に、書換実施 ECU 102 は、更新ソフトを含む更新用フレームを CAN バス 20 へ送信する（ステップ S606）。更新ソフトを含む更新用フレームを受信した被書換 ECU 103 は、プログラム記憶部 404 へ、受信した更新ソフトを書き込む。

10

【0124】

次に、書換実施 ECU 102 は、更新ソフトに対応した更新ソフト署名を含む更新用フレームを CAN バス 20 へ送信する（ステップ S607）。

20

【0125】

評価装置 101 は、CAN バス 20 から更新ソフト署名を含む更新用フレームを受信することで、更新ソフト署名を含む更新用フレームが CAN バス 20 に流れていることを検知すると、その CAN メッセージ全体が被書換 ECU 103 に受信される前に、エラーフレームを送信し、書換実施 ECU 102 が送信する更新用フレームを無効化する（ステップ S1501）。CAN バス 20 上において更新ソフト署名を含む更新用フレームは、エラーフレームにより上書きされ、正しく受信できない無効なものとなる。

【0126】

次に、評価装置 101 は、更新ソフトに対応した偽の更新ソフト署名を含む更新用フレームを CAN バス 20 へ送信する（ステップ S1601）。評価装置 101 は、偽の更新ソフト署名を含む更新用フレームを受信した後の被書換 ECU 103 の動作、応答等を記憶部 208 に記録する。

30

【0127】

次に、評価装置 101 は、再起動指示を示す更新用フレームを CAN バス 20 へ送信する（ステップ S1602）。評価装置 101 は、再起動指示を示す更新用フレームを受信した後の被書換 ECU 103 の動作或いは応答を記憶部 208 に記録する。

【0128】

最後に、評価装置 101 は、記憶部 208 に記録された、CAN バス 20 からの受信内容に係る情報、及び、ステップ S1601 以降の被書換 ECU 103 の動作に係る情報を確認することで、評価を行う（ステップ S1603）。即ち、評価装置 101 は、上述のステップ S1203 での評価と同様に、受信内容及び被書換 ECU 103 の動作について、攻撃の期待値と比較することにより、電子制御システム 11 のセキュリティの評価（攻撃の成否についての判定等）を行う。

40

【0129】

（変形例）

以上のように、本発明に係る技術の例示として実施の形態 1 を説明した。しかしながら、本発明に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本発明の一実施態様に含まれる。

【0130】

50

(1) 上記実施の形態では、評価装置101が、電子制御システム11におけるソフトウェアの更新処理に関連して書換実施ECU102或いは被書換ECU103になりますこと攻撃する例を示したが、その他のECUになります攻撃を行っても良いし、エラーフレーム、及び、更新処理と関係ないCANメッセージの送信により、攻撃を行っても良い。

【0131】

(2) 上述の電子制御システム11では、各種ECUは、リアルな（実物としての）ECUを想定して説明した。しかし、評価システム10の評価対象としての電子制御システム11における各種ECUは、リアルなECU（例えば、評価ボード上で実装されたECU、製品としてのECU等）の代わりに、そのECUを模擬（シミュレート）する模擬ECU（例えば、そのECUの機能、挙動等を模擬するシミュレーションソフトウェアを実行するコンピュータ等）であることとしても良い。ECUが模擬ECUである場合には、評価装置101はECUの動作の監視を、コンピュータにおいてシミュレーションソフトウェアに関わる所定データ（コンピュータの所定メモリ領域の内容或いは出力内容等）の変化を観測することによって実現しても良い。

10

【0132】

(3) 上記実施の形態では、評価装置101が、CANバス20に接続された1つの装置である例を示したが、評価装置101は、攻撃手順情報105に従って攻撃用のフレームを送信する送信装置と、CANバス20を流れるCANメッセージ、CANバス20に接続されたECUの記憶内容、信号線に出力する出力信号等を監視する監視装置とに分離される等、複数の筐体に分離された構成を備えても良い。また、監視装置或いは監視部200は、CANバス20に接続されたどのECUについて監視しても良い。また、監視装置或いは監視部200は、ECUについての監視の方法としていかなる方法を用いても良く、例えば、ECUと接続された専用の信号線等による直接監視を行っても良いし、CANメッセージによる間接的な監視を行っても良いし、ECUの動作に関連して変化し得る車両の状態による間接的な監視を行っても良い。

20

【0133】

(4) 上記実施の形態では、評価システム10の評価対象として、CANバス20による車載ネットワークを備える電子制御システム11を例示したが、評価システム10で評価装置101が攻撃用のフレームを送信したり監視の対象としたりするネットワークは、必ずしも車載ネットワークでなくても良く、また、CANプロトコルによる通信が行われるCANバス20以外のネットワークであっても良い。例えば、評価システム10は、ロボット、産業機器等のネットワークその他のネットワーク通信システムを評価対象としても良い。また、CANプロトコルは、オートメーションシステム内の組み込みシステム等に用いられるCANOpen、或いは、TTCCAN（Time-Triggered CAN）、CANFD（CAN with Flexible Data Rate）等の派生的なプロトコルも包含する広義の意味のものと扱われることとしても良い。また、評価対象の電子制御システム（ネットワーク通信システム）で、CANプロトコル以外の通信プロトコル、例えば、Ethernet（登録商標）や、MOST（登録商標）、FlexRay（登録商標）、LIN（Local Interconnect Network）等を用いても良い。また、各種プロトコルに従ったネットワークを組み合わせた複合的なネットワークを含むシステムを評価対象として、評価装置101で、そのネットワークに対して攻撃及び監視を行うこととしても良い。評価装置101は、上述のネットワークで、他のノードが送信したフレームの無効化のための無効化フレーム（例えばCANではエラーフレーム）を含む攻撃用のフレームを送信することで評価を行い得る。無効化フレームは、他のノードが送信したフレームを、上書きその他の方法で無効化するフレームであれば良い。無効化は、フレームの適正な受信を妨害するために、フレームの状態を通常状態から変化させることであり、例えば上書きして1ビット以上を変化させる改変でも良いし、フレーム自体を改変せずに通信プロトコルで定められた方法で無効状態にすること（先行フレームが無効であることを示す情報の追加等）でも良い。

30

40

【0134】

50

(5) 上記実施の形態では、評価装置101が、エラーフレームの送信により、なりすまし対象とするECUが送信したCANメッセージを無効化した後に、評価装置101が、なりすまし対象のECUの更新処理の動作を全て実行する例を示したが、例えば、なりすまし対象のECUが送信するはずの複数のCANメッセージの一部のみを評価装置101が送信することとしても良い。

【0135】

(6) 上記実施の形態では、攻撃手順情報105が、エラーフレームとCANメッセージとを含む複数の攻撃用のフレームの送信順序を規定した例を示したが、攻撃手順情報105は、1つ又は複数のエラーフレームだけの送信について規定するものであっても良く、例えば、エラーフレームの送信タイミング、送信間隔、或いは、送信条件（バス上などのIDのCANメッセージが流れた時に送信すべきに係る条件等）を規定するものであっても良い。この場合でも、評価装置101は、エラーフレームの送信に対するECUの挙動等を確認することで、電子制御システム11のセキュリティに関する評価を行い得る。

【0136】

(7) 評価装置101は、評価対象のセキュリティ（攻撃耐性等）についての評価として、防御をすり抜けた不正なCANメッセージの個数や割合に基づいて、攻撃耐性の有無の判定等といった評価を行うものであっても良い。なお、評価装置101は、攻撃耐性の有無を判定するために、不正なCANメッセージの個数や割合についての上限等を規定する閾値を用い得る。この閾値は、評価装置101に対して任意に設定可能にしても良いし、評価を繰り返し実施する場合において評価結果等に応じて変化（調整）し得るようにしても良い。また、評価装置101は、攻撃の成功率（成功の頻度等）を算定しても良い。このように評価装置101は、攻撃成否或いは防御成否の択一判定の他に、例えば複数の防御機能それぞれが作動するか否か或いはどの程度有効に作用したかについて評価しても良い。また、評価装置101では、送信部201aが、攻撃手順情報105が示す送信順序で複数のフレームをCANバス20に送信する攻撃パターンを複数回繰り返し、評価部206が、攻撃パターンの繰り返しによる監視部200の監視結果の変化の有無に応じて評価結果が相違するように評価を行うこととしても良い。例えば、評価装置101が、偽の認証シードの送信、或いは、偽の認証鍵の送信を複数回繰り返した際に、一定回数以上実施して応答が受信できるか否かで攻撃の成否を判定しても良い。なお、評価装置101

【0137】

(8) 評価対象の電子制御システム11におけるセキュリティECU104を含むセキュリティ機能は、不正の検知に関するログ情報（CANメッセージの受信履歴等）を記録することとしても良く、この場合には、評価装置101は、そのログ情報と、その評価装置101が保持する、攻撃に関する期待値とを比較することで、攻撃が成功したか否かの判定或いは攻撃が成功した確率等の算出を行うことで、セキュリティについての評価を行うこととしても良い。

【0138】

(9) 上記実施の形態では電子制御システム11はセキュリティ機能として、独立したセキュリティECU104を備え得ることとしたが、バスを介して通信する複数のECUのうちの全部又は一部のECUがセキュリティ機能を備えることとしても良い。また、複数のECUがセキュリティ機能を分散して実現しても良い。

【0139】

(10) 上記実施の形態では評価装置101が評価対象の電子制御システム11におけるバスに直接接続されている例を示したが、評価装置101と評価対象との間に、ゲートウェイ等の中継装置が介在しても良い。例えば、評価装置101が、ゲートウェイとの間

で相互認証又は片方向認証を実施した上で攻撃用のCANメッセージを送信することでゲートウェイにそのCANメッセージをCANバス20へと転送させ、CANバス20からのCANメッセージを、ゲートウェイを介して取得する等により、評価対象のセキュリティ（攻撃耐性等）を評価することとしても良い。

【0140】

（11）評価装置101は、偽の認証シードを送信し、書換実施ECU102から認証鍵を得るという動作を複数回実施して、その傾向を分析することで認証鍵を類推できるかどうかでセキュリティ機能の評価を行っても良い。

【0141】

（12）上記実施の形態における評価装置101及び各種ECUは、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、ディスプレイ、キーボード、マウス等の他のハードウェア構成要素を含んでいても良い。また、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア（デジタル回路等）によりその機能を実現することとしても良い。例えば、評価装置101のCANバス監視部203、信号監視部204、送受信部201、保持部202、評価部206、記憶部208及び制御部207の各機能ブロックは、集積回路で実現され得る。また、例えば、書換実施ECU102の送受信部301、署名記憶部302、鍵記憶部303、プログラム記憶部304、書換手順情報記憶部305及び制御部306の各機能ブロックは、集積回路で実現され得る。また、例えば、被書換ECU103の送受信部401、署名記憶部402、鍵記憶部403、プログラム記憶部404、書換手順情報記憶部405及び制御部406の各機能ブロックは、集積回路で実現され得る。また、例えば、セキュリティECU104の送受信部501、CANバス監視部502及び制御部503の各機能ブロックは、集積回路で実現され得る。

【0142】

（13）上記実施の形態における各装置（評価装置101、各種ECU等）を構成する構成要素の一部又は全部は、1個のシステムLSI（Large Scale Integration：大規模集積回路）から構成されているとしても良い。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAM等を含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又は全部を含むように1チップ化されても良い。また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現しても良い。LSI製造後に、プログラムすることが可能なFPGA（Field Programmable Gate Array）や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。更には、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあり得る。

【0143】

（14）上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしても良い。前記ICカード又は前記モジュールは、マイクロプロセッサ、ROM、RAM等から構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしても良い。

【0144】

(15) 本発明の一態様としては、例えば図9～図18等に例示する処理手順の全部又は一部を含む評価方法であるとしても良い。例えば、評価方法は、バス（例えばCANバス20）を介して通信する複数のECUを備える電子制御システム11のセキュリティに関する評価を行う評価方法であって、バス上のフレームを無効化する無効化フレーム（例えばCANのエラーフレーム）を含む、1つ以上の攻撃用のフレームを、バスに送信し（例えばS701～S703、S901、S902、S1101～S1103、S1201、S1202、S1301、S1302、S1401、S1402、S1501、S1601、S1602）、攻撃用のフレームがバスに送信される際に、複数のECUのうち1つ以上のECUについて監視し、監視による監視結果に基づいて評価（例えばS801、S1001、S1203、S1403、S1603）を行う評価方法である。また、本発明の一態様としては、この評価方法に係る処理をコンピュータにより実現するコンピュータプログラムであるとしても良いし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD（Blu-ray（登録商標）Disc）、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本発明の一態様としては、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしても良い。また、前記プログラム若しくは前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム若しくは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしても良い。

【0145】

(16) 上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本発明の範囲に含まれる。

【産業上の利用可能性】

【0146】

本発明は、電子制御システムに対して施されたセキュリティ対策技術が攻撃を適切に防御できるか否か等の評価を実施するために利用可能である。

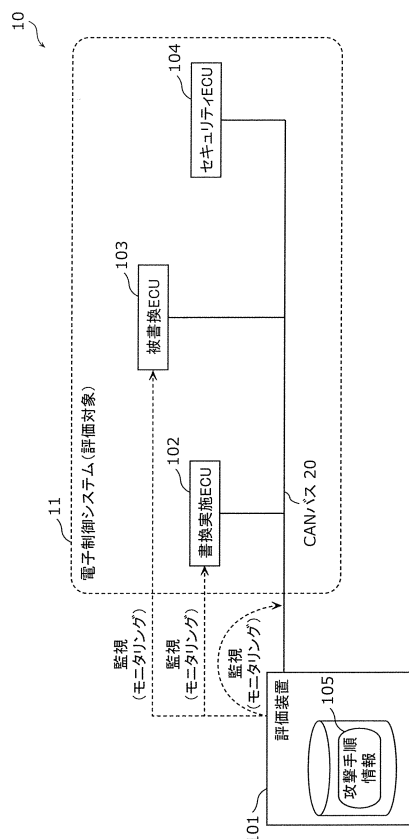
【符号の説明】

【0147】

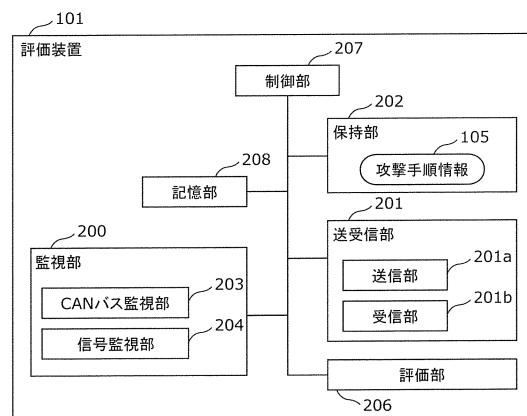
- 10 評価システム
- 11 電子制御システム
- 20 バス（CANバス）
- 101 評価装置
- 102 書換実施ECU
- 103 被書換ECU
- 104 セキュリティECU
- 105 攻撃手順情報
- 200 監視部
- 201、301、401、501 送受信部
- 201a 送信部
- 201b 受信部
- 202 保持部
- 203、502 CANバス監視部

- 204 信号監視部
- 206 評価部
- 207、306、406、503 制御部
- 208 記憶部
- 302、402 署名記憶部
- 303、403 鍵記憶部
- 304、404 プログラム記憶部
- 305、405 書換手順情報記憶部

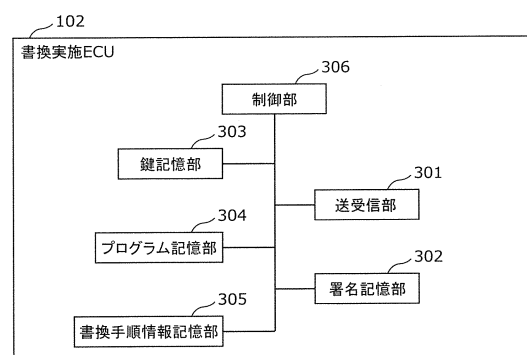
【図 1】



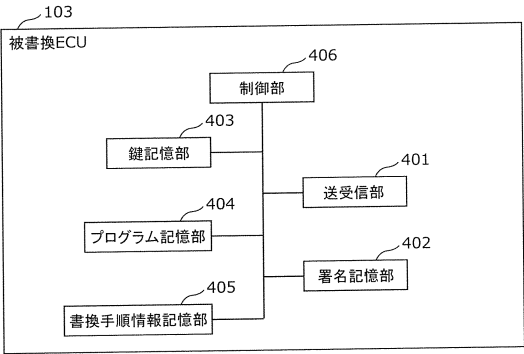
【図 2】



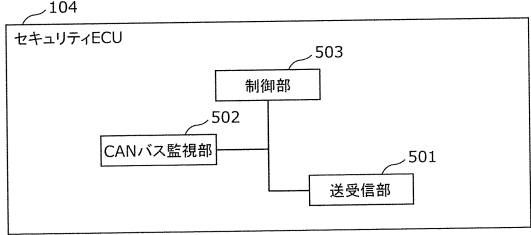
【図 3】



【図 4】



【図 5】



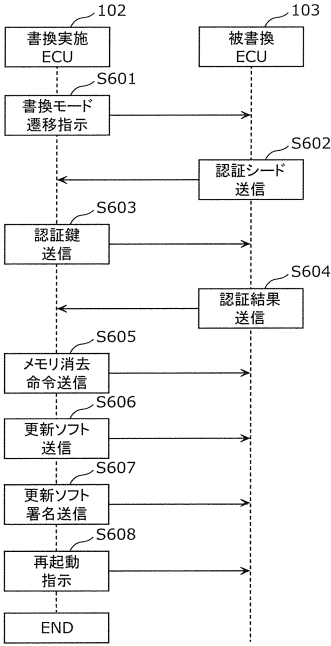
【図 6】

評価対象機能	送信メッセージ	メッセージID	送信間隔	送信順序
書換実施機能1	エラーフレーム	—	—	1
	認証シード	0x0034	20ms	2
書換実施機能2	認証応答	0x0256	20ms	3
	エラーフレーム	—	—	1
書換実施機能2	認証応答	0x0256	20ms	2

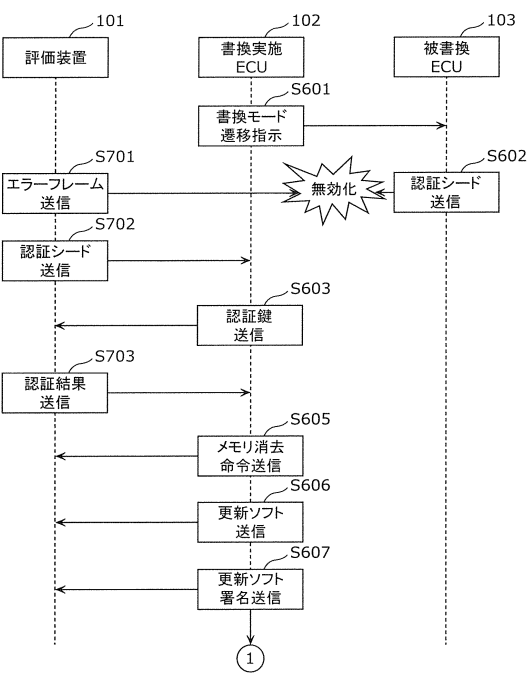
【図 7】

評価対象機能	送信メッセージ	メッセージID	送信間隔	送信順序
被書換機能1	エラーフレーム	—	—	1
	メモリ消去命令	0x0012	10ms	2
	更新ソフト	0x0056	10ms	3
	更新ソフト署名	0x0178	10ms	4
被書換機能2	エラーフレーム	—	—	1
	更新ソフト	0x0056	10ms	2
	更新ソフト署名	0x0178	10ms	3
被書換機能3	エラーフレーム	—	—	1
	更新ソフト署名	0x0178	10ms	2

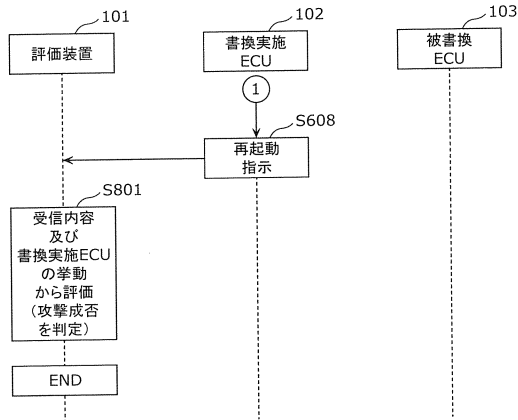
【図 8】



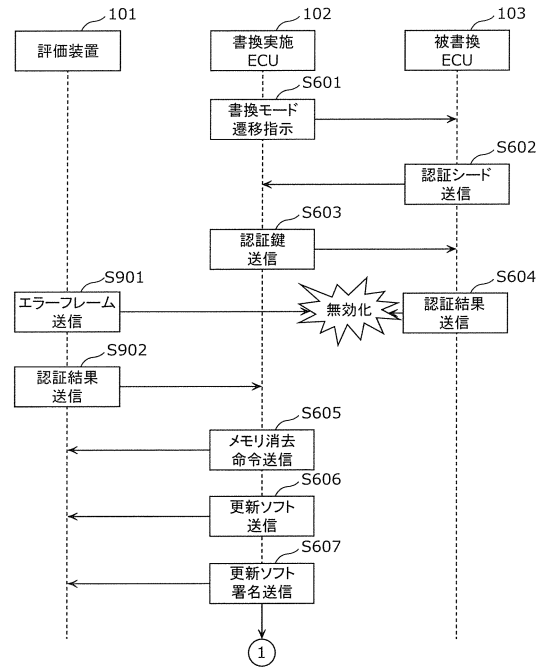
【図 9】



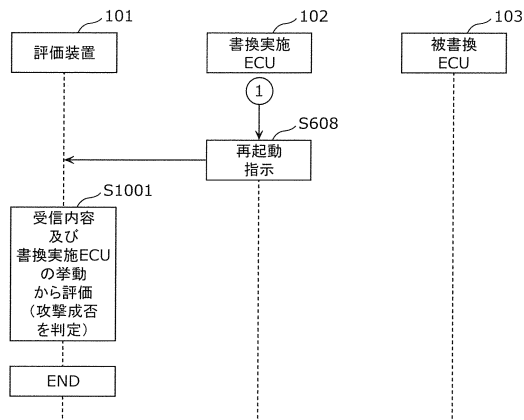
【図 10】



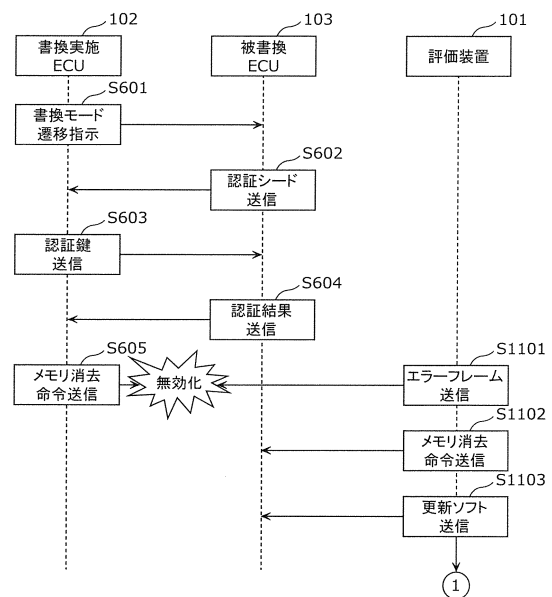
【図 11】



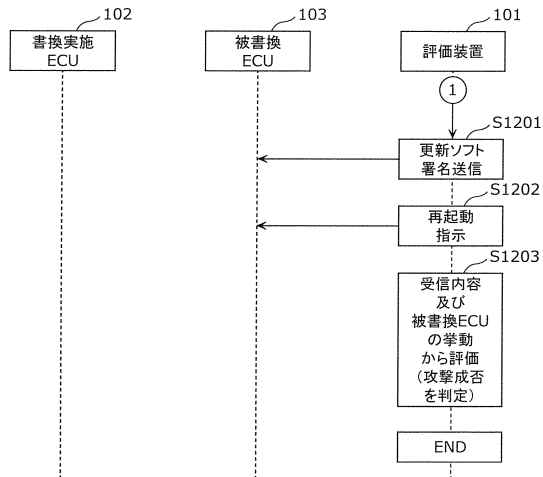
【図 12】



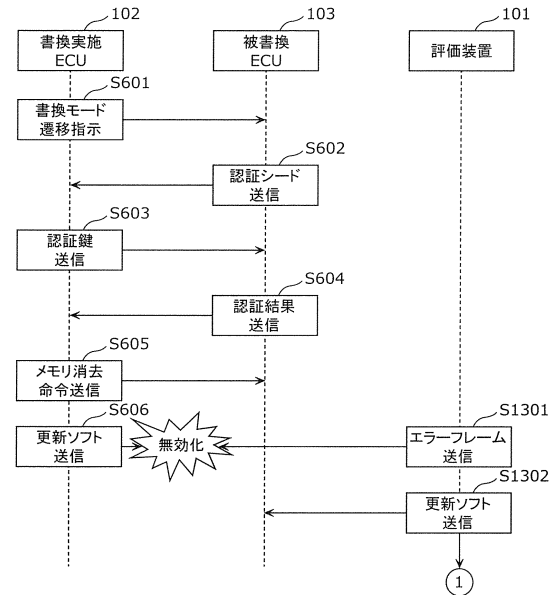
【図 13】



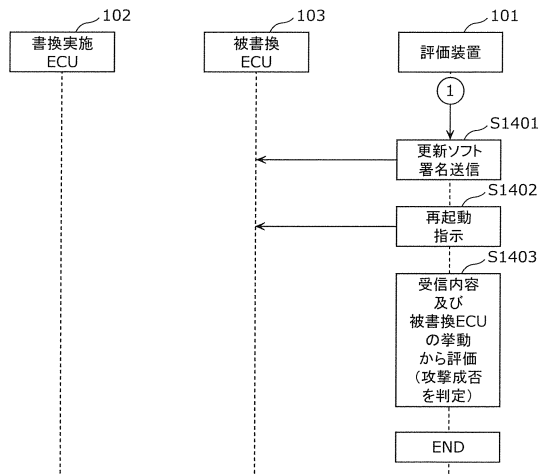
【図 14】



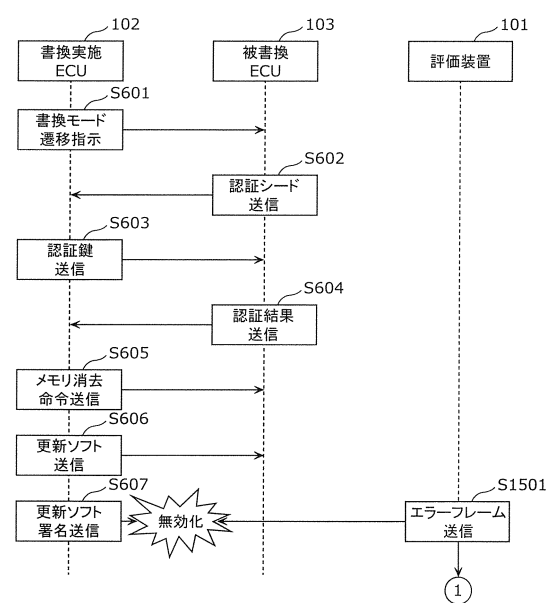
【図 15】



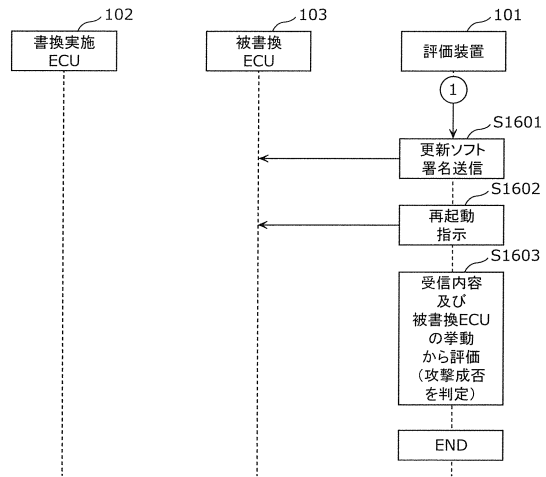
【図 16】



【図 17】



【図 18】



フロントページの続き

- (74)代理人 100131417
弁理士 道坂 伸一
- (72)発明者 天野 博史
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 中野 稔久
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 南 公男
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 広瀬 宜子
大阪府大阪市中央区城見2丁目1番61号 パナソニックIPマネジメント株式会社内

審査官 安藤 一道

- (56)参考文献 特開2015-114833 (JP, A)
倉地 亮 他, CANにおけるエラーフレーム監視機構の提案, CSS2015 コンピュータセキュリティシンポジウム2015 論文集 合同開催 マルウェア対策研究人, 日本, 一般社団法人情報処理学会 コンピュータセキュリティ, 2015年10月14日, 第2015巻, 第3号, p.110~115
大塚 敏史 他, 既存ECUを変更不要な車載LAN向け侵入検知手法, 情報処理学会研究報告 2012 (平成24) 年度▲6▼ [DVD-ROM] 情報処理学会研究報告 研究, 日本, 一般社団法人情報処理学会, 2013年 4月15日, p.1~5

- (58)調査した分野(Int.Cl., DB名)
H04L 12/28