(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017 年 7 月 27 日(27.07.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/125978 A1

(51) 国際特許分類:
H04L 12/40 (2006.01) *G06F 21/57* (2013.01)
B60R 16/023 (2006.01)

(21) 国際出願番号: PCT/JP2016/005040

(22) 国際出願日: 2016 年 12 月 1 日(01.12.2016)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2016-007481 2016 年 1 月 18 日(18.01.2016) JP
特願 2016-218329 2016 年 11 月 8 日(08.11.2016) JP

(71) 出願人: パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) [US/US]; 90503 カリフォルニア州トーランス, スイート ２００, マリナー アベニュー ２０００００ California (US).

(72) 発明者: 天野 博史(AMANO, Hiroshi); 〒5718501 大阪府門真市大字門真１００６番地パナソニック株式会社内 Osaka (JP). 中野 稔久(NAKANO, Toshihisa). 南 公男(MINAMI, Kimio). 広瀬 宜子(HIROSE, Takako).

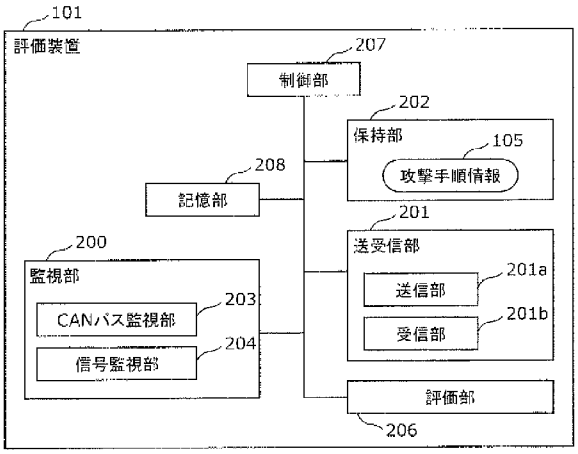
(74) 代理人: 徳田 佳昭, 外(TOKUDA, Yoshiaki et al.); 〒5718501 大阪府門真市大字門真１００６番地 パナソニック株式会社内 Osaka (JP).

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

[続葉有]

(54) **Title**: EVALUATION DEVICE, EVALUATION SYSTEM, AND EVALUATION METHOD

(54) 発明の名称 : 評価装置、評価システム及び評価方法



101 Evaluation device
105 Attack procedure information
200 Monitoring unit
201 Transceiver unit
201a Transmission unit
201b Receiving unit
202 Holding unit
203 CAN bus monitoring unit
204 Signal monitoring unit
206 Evaluation unit
207 Control unit
208 Storage unit

(57) **Abstract**: An evaluation device (101) is connected to a bus used by a plurality of ECUs for communication and is used to conduct evaluations relating to the security of an electronic control system, the evaluation device being equipped with: a transmission unit (201a) that transmits to the bus one or more attack frames including an invalidation frame for invalidating a frame on the bus; a monitoring unit (200) for monitoring one or more ECUs among the plurality of ECUs; and an evaluation unit (206) for carrying out an evaluation on the basis of monitoring results by the monitoring unit (200) during transmission of an attack frame to the bus by the transmission unit (201a).

(57) 要約: 複数のＥＣＵが通信に用いるバスに接続され、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（１０１）は、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、バスに送信する送信部（２０１ａ）と、複数のＥＣＵのうち１つ以上のＥＣＵについて監視する監視部（２００）と、送信部（２０１ａ）により攻撃用のフレームがバスに送信される際における監視部（２００）の監視結果に基づいて評価を行う評価部（２０６）とを備える。

WO 2017/125978 A1

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

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： 評価装置、評価システム及び評価方法

技術分野

[0001] 本開示は、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（ＥＣＵ：Electronic Control Unit）が配置され、ＥＣＵをつなぐ車載ネットワークには、例えばＩＳＯ１１８９８－１で規定されているＣＡＮ（Controller Area Network）規格等が用いられる。

[0003] ＣＡＮ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ＥＣＵ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６ｂｉｔ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ＣＡＮメッセージを送信し、車載ＥＣＵ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ＥＣＵ自体がＶ２Ｘ（

車車間通信（Ｖ２Ｖ：Vehicle to Vehicle）及び路車間通信（Ｖ２Ｉ：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、Ｖ２Ｘに対応するＥＣＵ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ＥＣＵ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ＥＣＵに対するＣＡＮ経由のファジング手法」、ＳＣＩＳ２０１５、２０１５年１月２０日

発明の概要

[0007] 本開示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。

[0008] また、本開示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。

[0009] また、本開示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。

[0010] 本開示によれば、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

[0011] [図1]図１は、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]図２は、評価システムにおける評価装置の構成図である。

[図3]図３は、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]図４は、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。

[図5]図５は、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]図６は、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]図７は、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]図８は、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]図９は、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]図１０は、評価システムの動作例１を示すシーケンス図である。

[図11]図１１は、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]図１２は、評価システムの動作例２を示すシーケンス図である。

[図13]図１３は、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]図１４は、評価システムの動作例３を示すシーケンス図である。

[図15]図１５は、評価システムの動作例４を示すシーケンス図である。

[図16]図１６は、評価システムの動作例４を示すシーケンス図である。

[図17]図１７は、評価システムの動作例５を示すシーケンス図である。

[図18]図１８は、評価システムの動作例５を示すシーケンス図である。

発明を実施するための形態

[0012] （本発明の基礎となった知見）

非特許文献１の手法は、単体の車載ＥＣＵ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ＥＣＵ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。

[0013] そこで、本開示は、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、本開示は、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。

[0014] 本開示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。

[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。

[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。

[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。

[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、本開示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。

[0025] また、本開示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。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。

[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、いずれも本開示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、一例であって本開示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）

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）について評価を行う。

[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。

[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。

[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 Diagnostics２）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。

[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。

[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。

[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。

[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。

[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。

[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２

０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。

[0043] （４）信号監視部２０４

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。

[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。

[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。

[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、確認等のために必要な演算処理を行い得る。

[0047] ［１．３　書換実施ＥＣＵ１０２の構成］

図３は、書換実施ＥＣＵ１０２の構成図である。

[0048] 書換実施ＥＣＵ１０２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ＥＣＵ１０２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ＥＣＵ１０２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ＥＣＵ１０２が被書換ＥＣＵ１０３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ＥＣＵ１０２と被書換ＥＣＵ１０３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ＥＣＵ１０３が送信した認証シードに基づいて、書換実施ＥＣＵ１０２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ＥＣＵ１０２が、被書換ＥＣＵ１０３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ＥＣＵ１０３へ送信し、被書換ＥＣＵ１０３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ＥＣＵ１０２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ＥＣＵ１０２から送信され、これに応じて被書換ＥＣＵ１０３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ＥＣＵ１０３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ＥＣＵ１０３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。

[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。

[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。

[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。

[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] （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。

[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

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。

[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。

[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。

[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。

[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。

[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] 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。

[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。

[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] 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。

[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。なお、図９に示すシーケンス図は、図１０に示すシーケンス図へ続く。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、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ＥＣＵ１０２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）。

[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する。そして、書換実施ＥＣＵ１０２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。

[0094] 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。

[0095] 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。

[0096] 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。

[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。なお、図１１に示すシーケンス図は、図１２に示すシーケンス図へ続く。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。なお、図１３に示すシーケンス図は、図１４に示すシーケンス図へ続く。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。

[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。

[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。

[0114] ［１．７．５　評価システム１０の動作例４］

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。なお、図１５に示すシーケンス図は、図１６に示すシーケンス図へ続く。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（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] 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] 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。

[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。

[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。なお、図１７に示すシーケンス図は、図１８に示すシーケンス図へ続く。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に即して、動作例５について説明する。

[0123] 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）。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。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。

[0124] 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）。

[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ＥＣＵ１０３の動作、応答等を記憶部２０８に記録する。

[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ＥＣＵ１０３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。

[0129] （変形例）

以上のように、本開示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、本開示に係る技術は、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開示の一実施態様に含まれる。

[0130] （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になりすますことで攻撃する例を示したが、その他のＥＣＵになりす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である場合においては、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。

[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。

[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、ＴＴＣＡＮ（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阻害するために、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。

[0134] （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（バス上にどのＩＤのＣＡＮメッセージが流れた時に送信すべきかに係る条件等）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ＣＡ

Ｎ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の評価部２０６での評価結果は、評価装置１０１によりメモリ等の記憶媒体に記録される他、評価装置１０１の外部に出力（例えば、評価結果の表示、評価結果を示す情報の送信等）され得る。例えば、評価部２０６は、評価結果として評価対象の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。

[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と呼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リ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）本開示の一態様としては、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、本開示の一態様としては、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、本開示の一態様としては、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、本開示の一態様としては、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、本開示の一態様としては、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開示の範囲に含まれる。

産業上の利用可能性

[0146] 本開示は、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

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る

評価装置。

[請求項2] 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記載の評価装置。

[請求項3] 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記載の評価装置。

[請求項4] 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

請求項３記載の評価装置。

[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３又は４記載の評価装置。

[請求項6] 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

請求項２～５のいずれか一項に記載の評価装置。

[請求項7] 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

請求項２～６のいずれか一項に記載の評価装置。

[請求項8] 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

請求項１～７のいずれか一項に記載の評価装置。

[請求項9] 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１～７のいずれか一項に記載の評価装置。

[請求項10] 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１～９のいずれか一項に記載の評価装置。

[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、

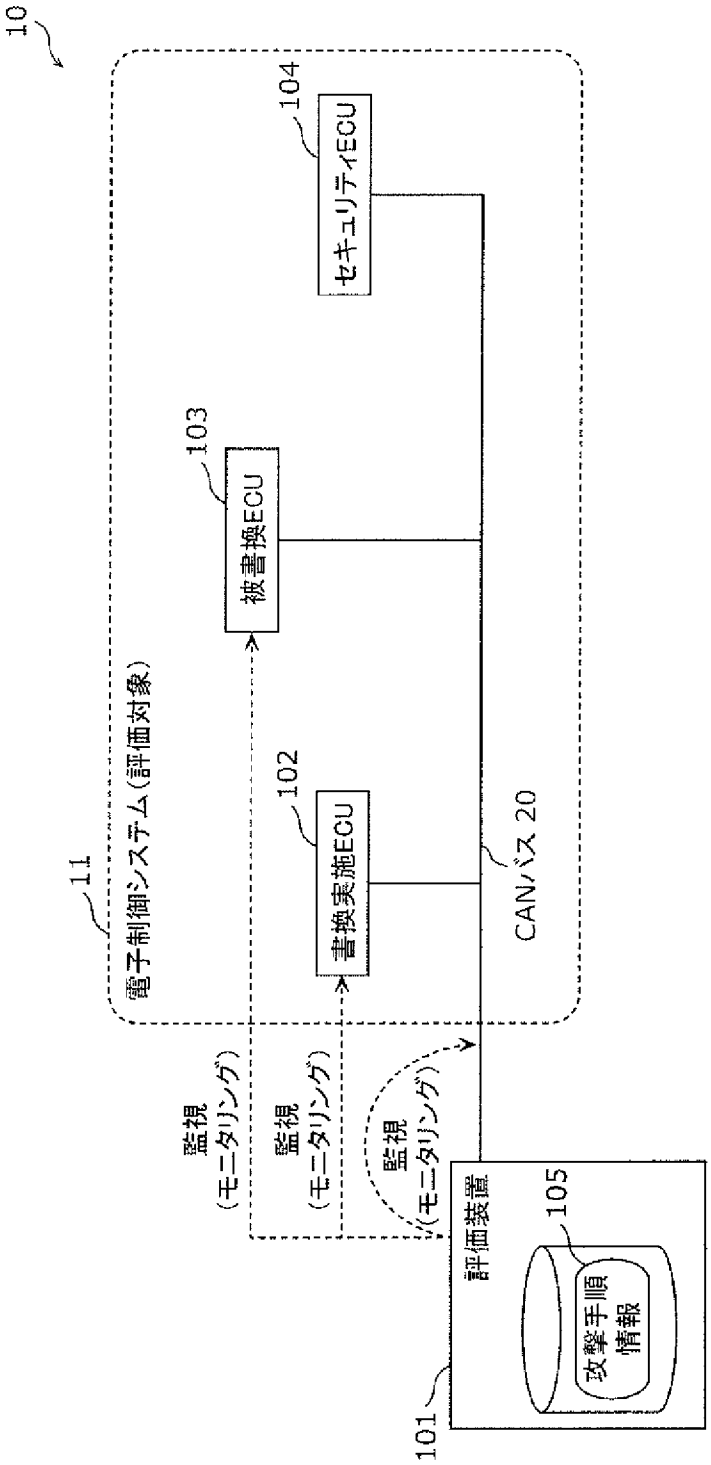
前記バス上のフレームを無効化する無効化フレームを含む、１つ以上の攻撃用のフレームを、前記バスに送信し、

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、

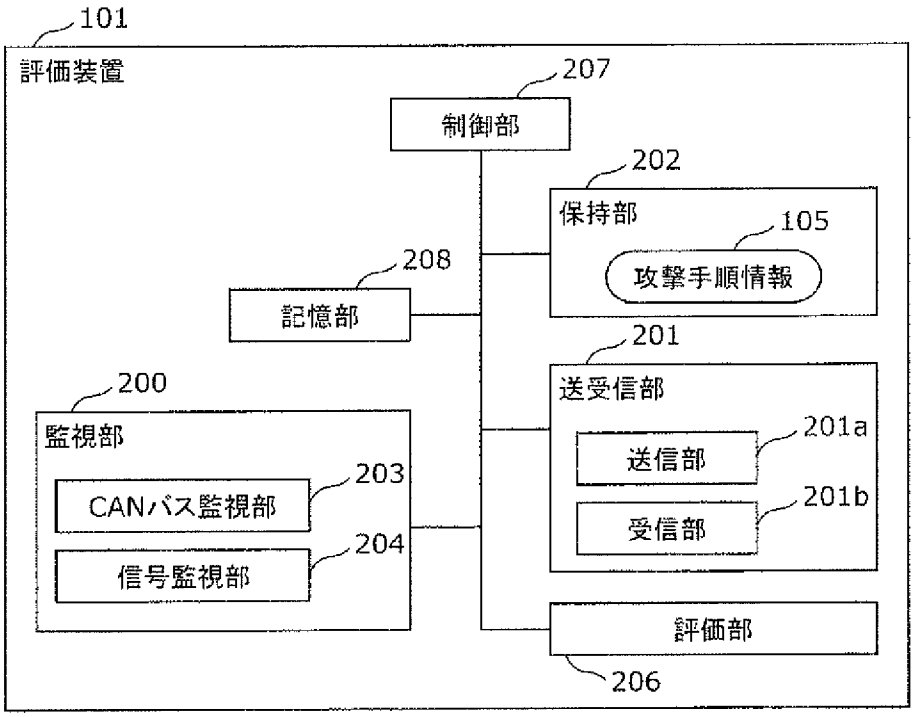
前記監視による監視結果に基づいて前記評価を行う

評価方法。

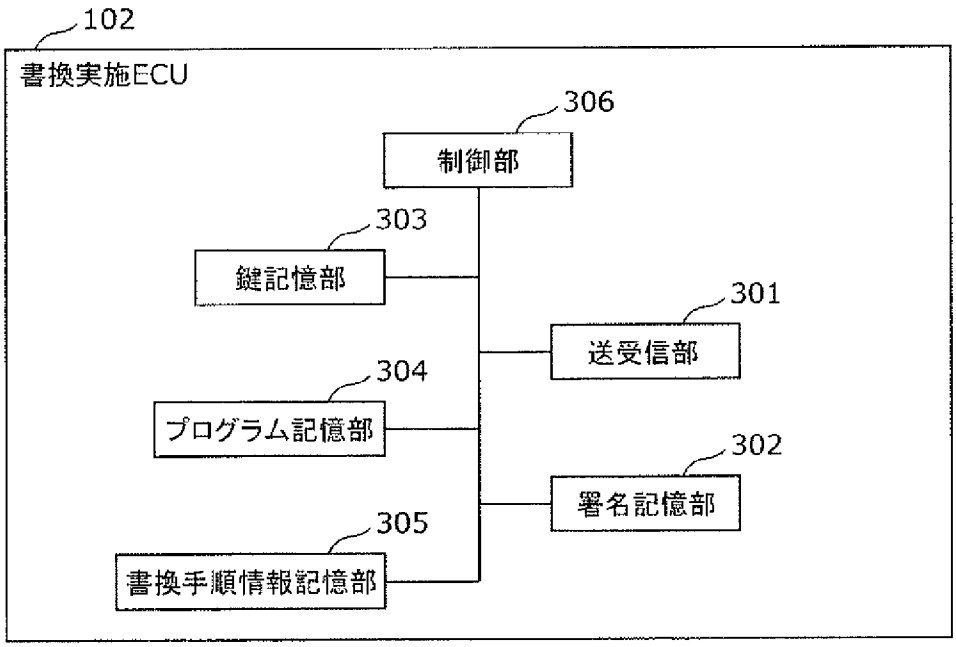
[図1]


10
11
電子制御システム(評価対象)
104
セキュリティECU
103
被書換ECU
102
書換実施ECU
CANバス 20
監視
(モニタリング)
監視
(モニタリング)
監視
(モニタリング)
101
評価装置
105
攻撃手順
情報

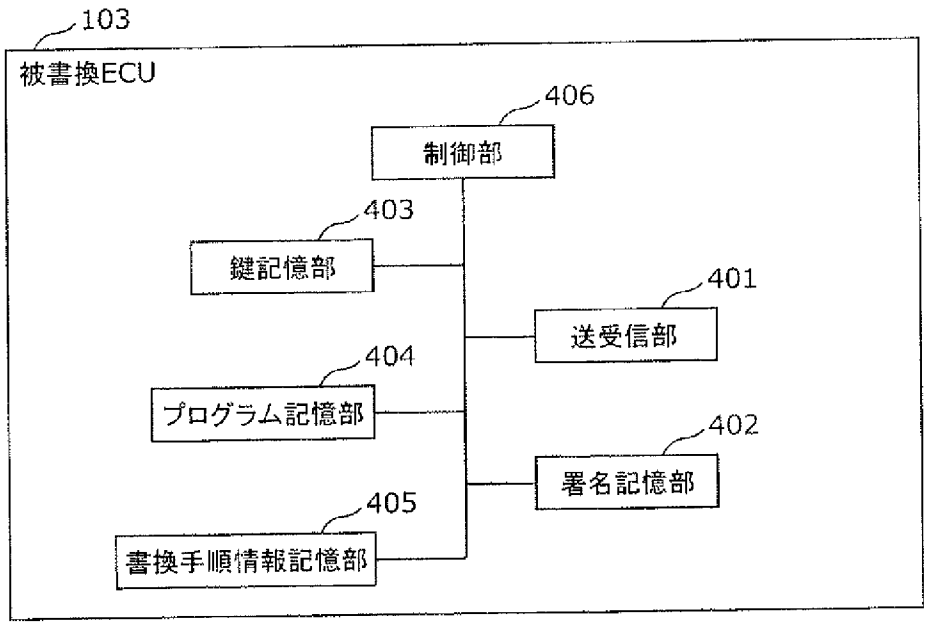
[図2]


101
評価装置
207
制御部
202
保持部
105
攻撃手順情報
208
記憶部
201
送受信部
200
監視部
201a
送信部
203
CANバス監視部
201b
受信部
204
信号監視部
評価部
206

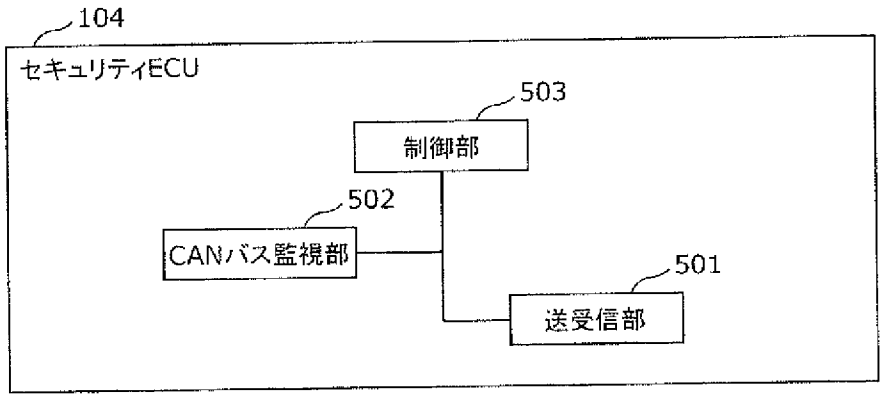
[図3]


102
書換実施ECU
306
制御部
303
鍵記憶部
301
送受信部
304
プログラム記憶部
302
署名記憶部
305
書換手順情報記憶部

[図4]


103
被書換ECU
406
制御部
403
鍵記憶部
401
送受信部
404
プログラム記憶部
402
署名記憶部
405
書換手順情報記憶部

[図5]


104
セキュリティECU
503
制御部
502
CANバス監視部
501
送受信部

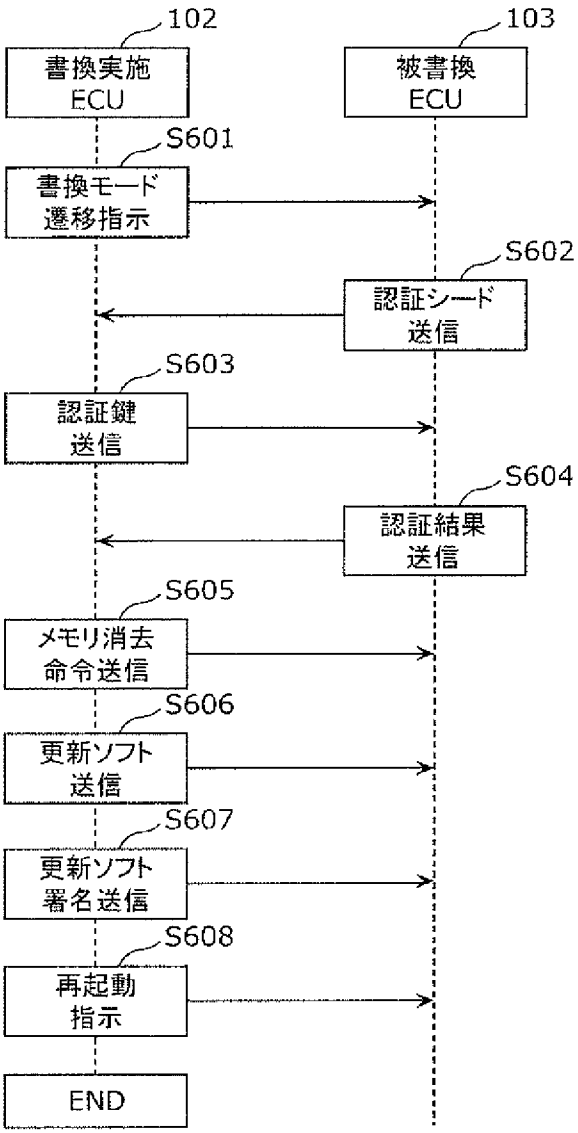
[図6]

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
	認証応答	0x0256	20ms	3
書換実施機能2	エラーフレーム	—	—	1
	認証応答	0x0256	20ms	2

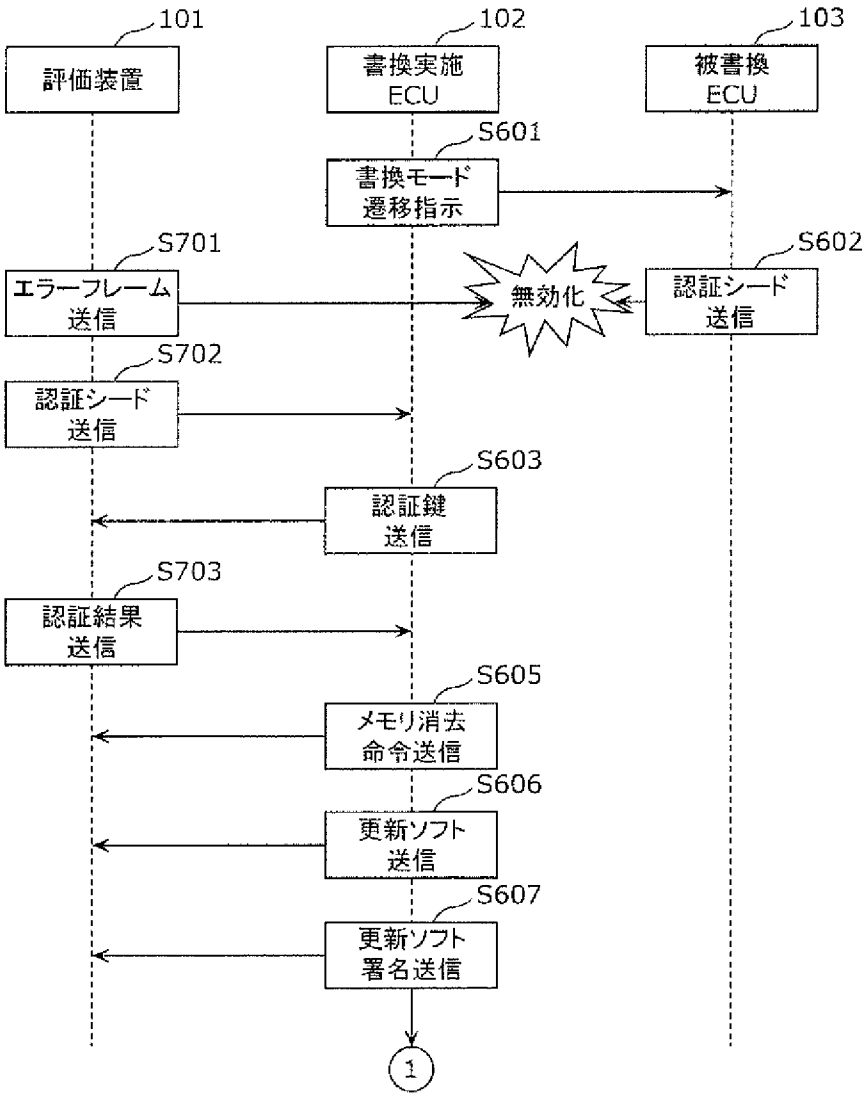
[図7]

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

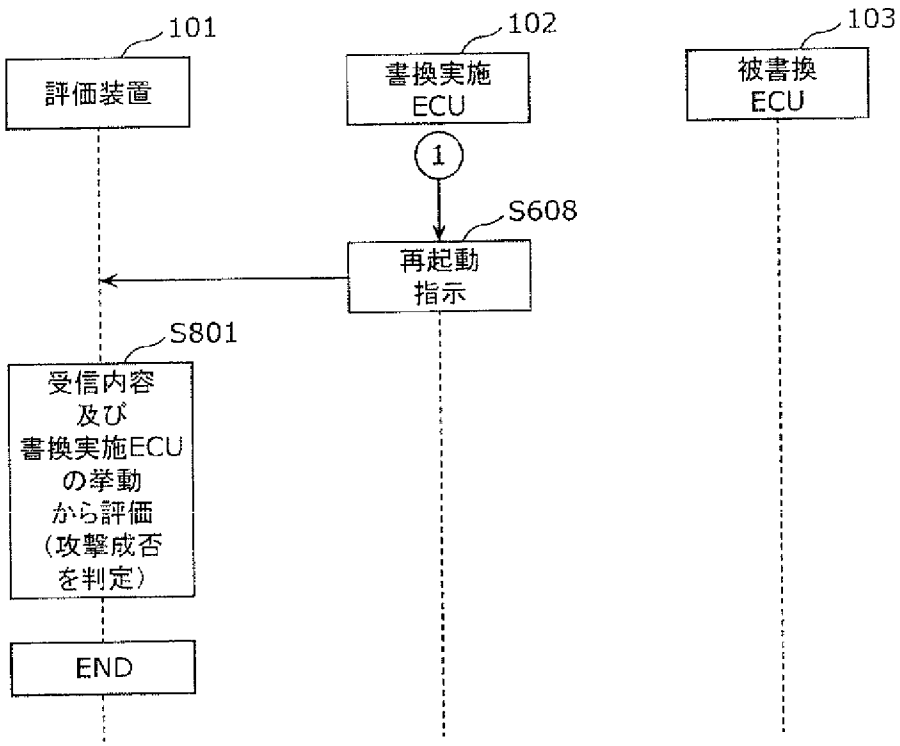
[図8]


102
書換実施
ECU
103
被書換
ECU
S601
書換モード
遷移指示
S602
認証シード
送信
S603
認証鍵
送信
S604
認証結果
送信
S605
メモリ消去
命令送信
S606
更新ソフト
送信
S607
更新ソフト
署名送信
S608
再起動
指示
END

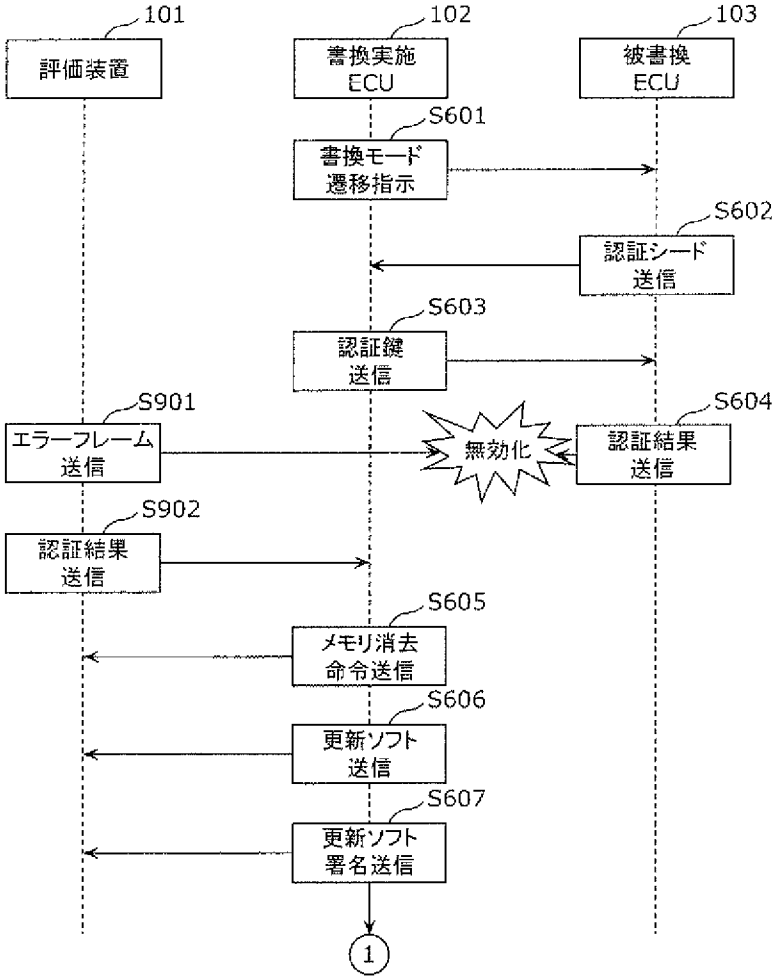
[図9]


101
評価装置
102
書換実施
ECU
103
被書換
ECU
S601
書換モード
遷移指示
S701
エラーフレーム
送信
無効化
S602
認証シード
送信
S702
認証シード
送信
S603
認証鍵
送信
S703
認証結果
送信
S605
メモリ消去
命令送信
S606
更新ソフト
送信
S607
更新ソフト
署名送信
1

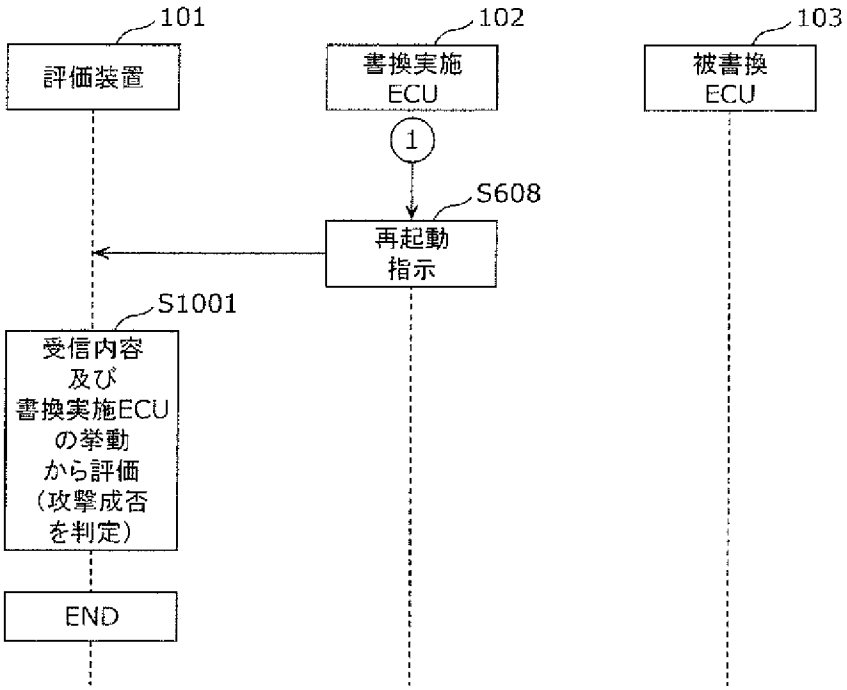
[図10]


101
評価装置
102
書換実施
ECU
103
被書換
ECU
1
S608
再起動
指示
S801
受信内容
及び
書換実施ECU
の挙動
から評価
(攻撃成否
を判定)
END

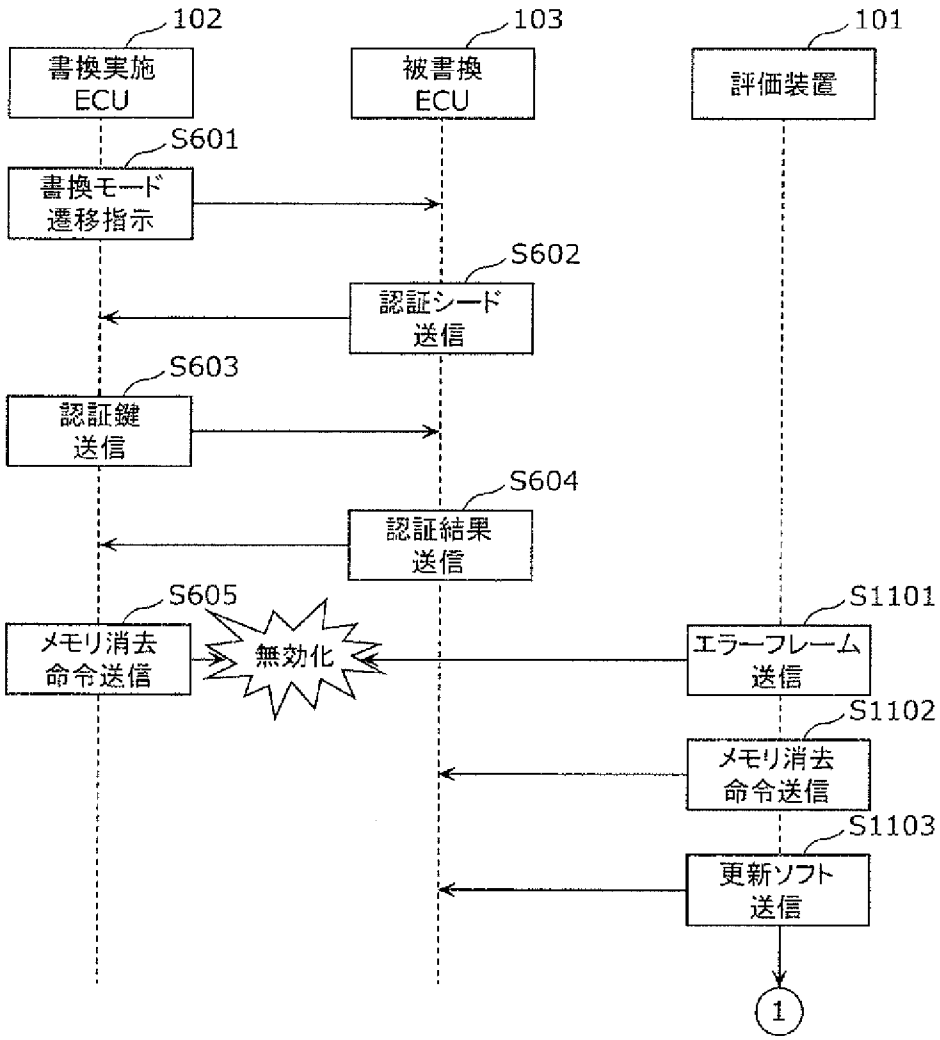
[図11]


101
102
103
評価装置
書換実施ECU
被書換ECU
S601
書換モード遷移指示
S602
認証シード送信
S603
認証鍵送信
S901
エラーフレーム送信
無効化
S604
認証結果送信
S902
認証結果送信
S605
メモリ消去命令送信
S606
更新ソフト送信
S607
更新ソフト署名送信
1

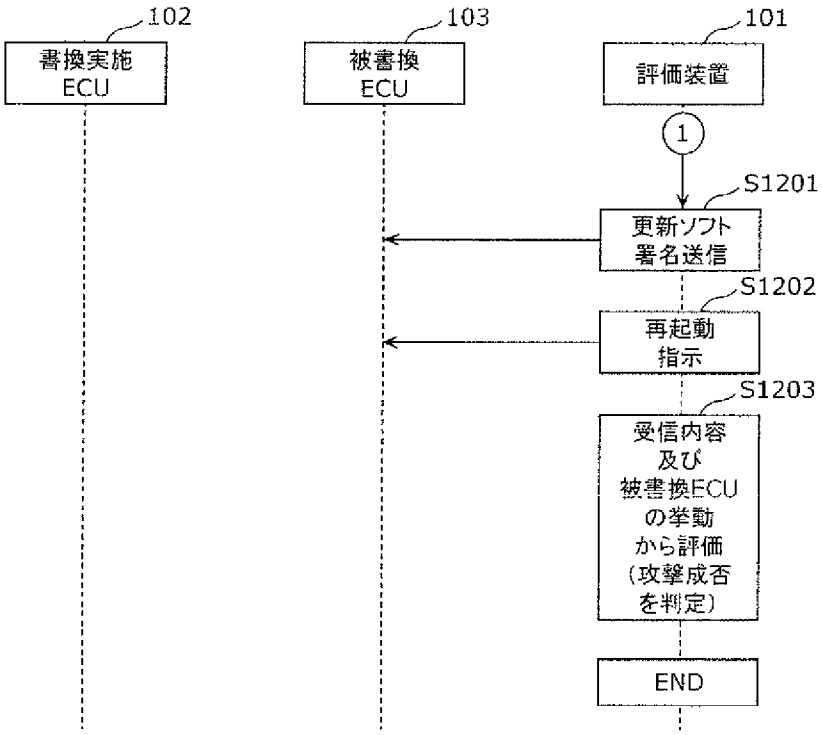
[図12]


101
102
103
評価装置
書換実施
ECU
被書換
ECU
1
S608
再起動
指示
S1001
受信内容
及び
書換実施ECU
の挙動
から評価
(攻撃成否
を判定)
END

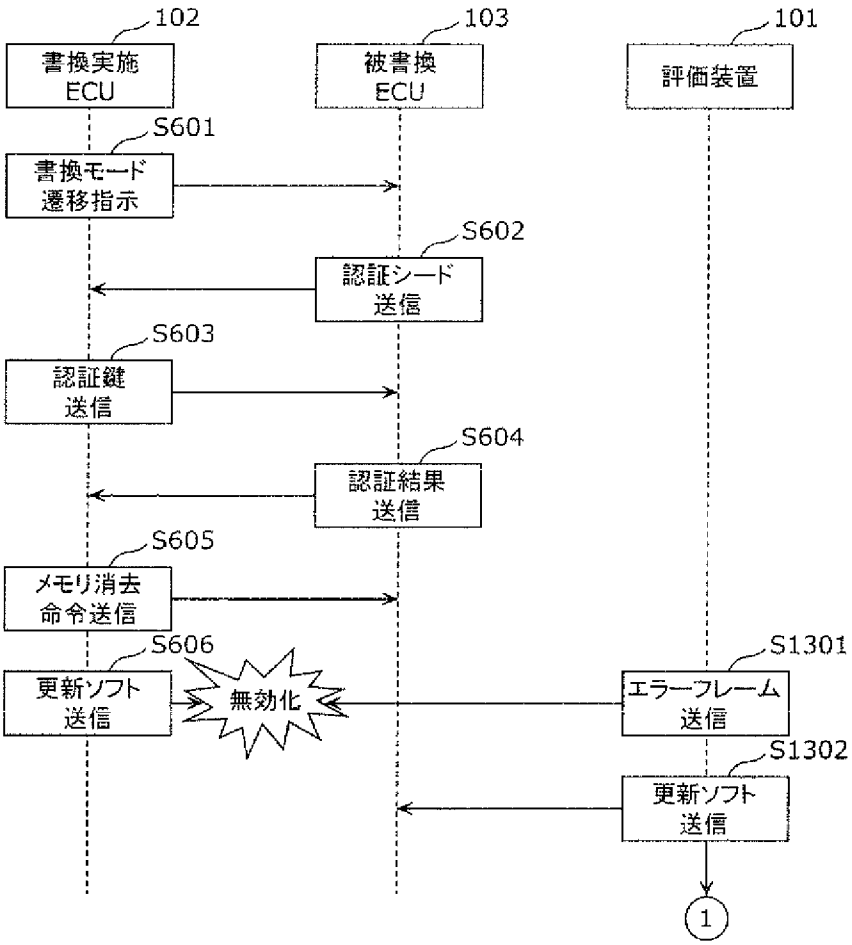
[図13]


102
書換実施
ECU
103
被書換
ECU
101
評価装置
S601
書換モード
遷移指示
S602
認証シード
送信
S603
認証鍵
送信
S604
認証結果
送信
S605
メモリ消去
命令送信
無効化
S1101
エラーフレーム
送信
S1102
メモリ消去
命令送信
S1103
更新ソフト
送信
1

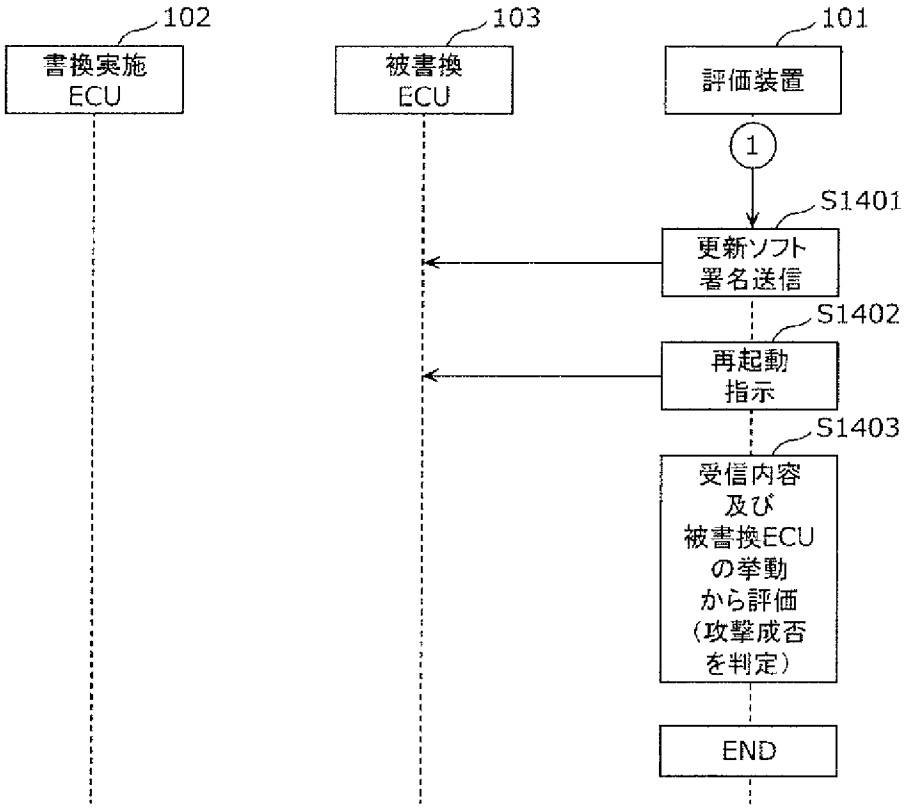
[図14]


102
書換実施
ECU
103
被書換
ECU
101
評価装置
1
S1201
更新ソフト
署名送信
S1202
再起動
指示
S1203
受信内容
及び
被書換ECU
の挙動
から評価
(攻撃成否
を判定)
END

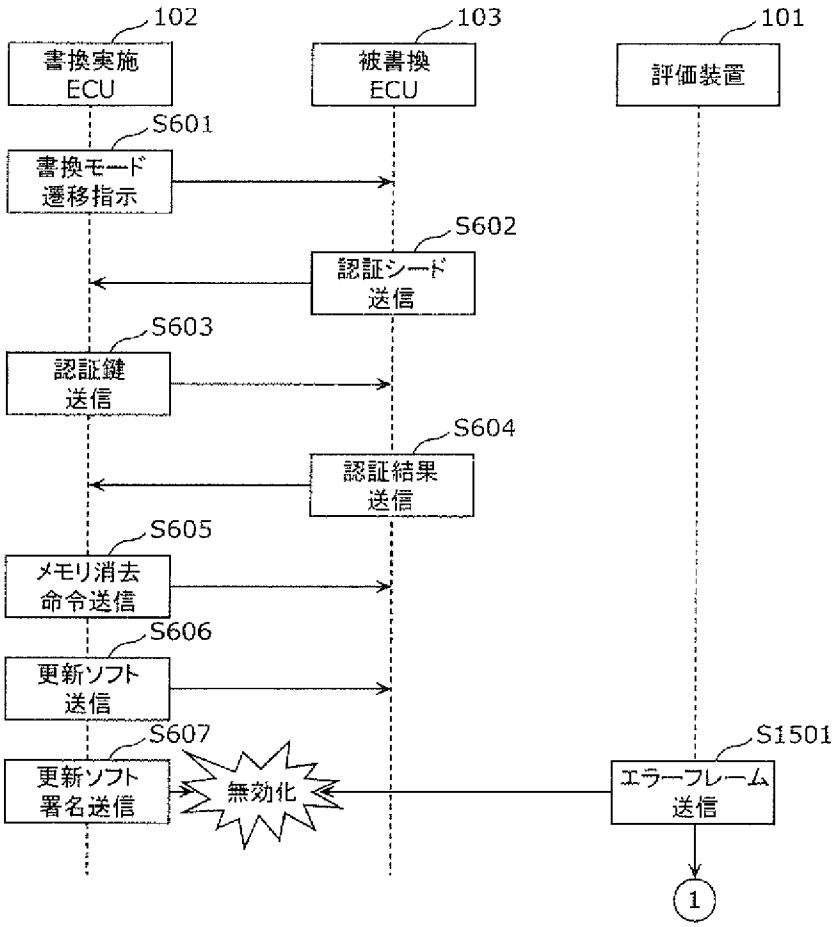
[図15]


102
書換実施ECU
103
被書換ECU
101
評価装置
S601
書換モード遷移指示
S602
認証シード送信
S603
認証鍵送信
S604
認証結果送信
S605
メモリ消去命令送信
S606
更新ソフト送信
無効化
S1301
エラーフレーム送信
S1302
更新ソフト送信
1

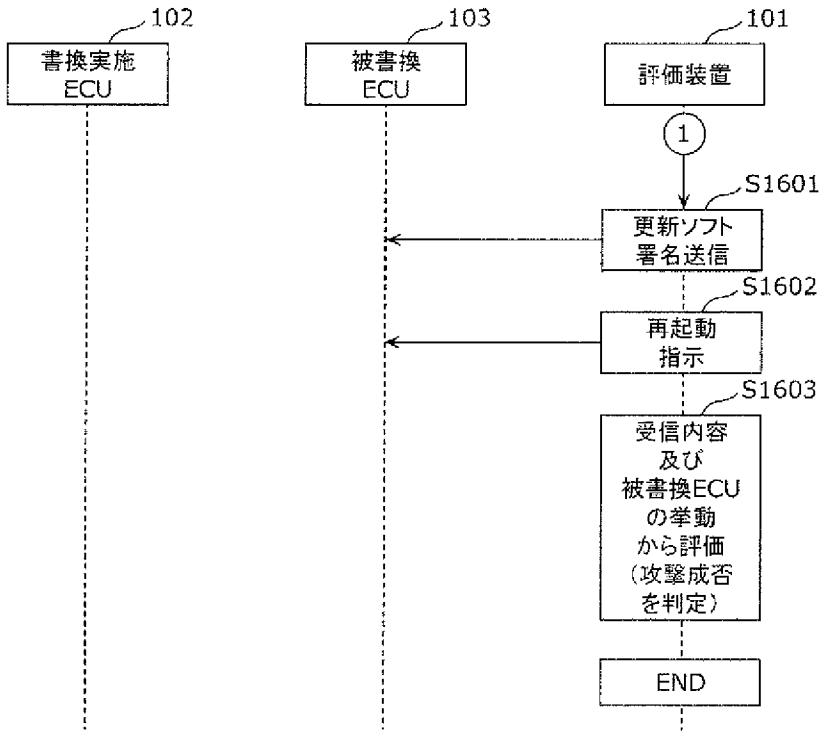
[図16]


102
書換実施
ECU
103
被書換
ECU
101
評価装置
1
S1401
更新ソフト
署名送信
S1402
再起動
指示
S1403
受信内容
及び
被書換ECU
の挙動
から評価
(攻撃成否
を判定)
END

[図17]


102
103
101
書換実施 ECU
被書換 ECU
評価装置
S601
書換モード 遷移指示
S602
認証シード 送信
S603
認証鍵 送信
S604
認証結果 送信
S605
メモリ消去 命令送信
S606
更新ソフト 送信
S607
更新ソフト 署名送信
無効化
S1501
エラーフレーム 送信
1

[図18]


102
書換実施
ECU
103
被書換
ECU
101
評価装置
1
S1601
更新ソフト
署名送信
S1602
再起動
指示
S1603
受信内容
及び
被書換ECU
の挙動
から評価
(攻撃成否
を判定)
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/005040

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/40(2006.01)i, *B60R16/023*(2006.01)i, *G06F21/57*(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/40, B60R16/023, G06F21/57

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2015-114833 A (Mitsubishi Electric Corp.), 22 June 2015 (22.06.2015), paragraphs [0003], [0013] to [0026], [0044] (Family: none)	1-3,5,8-12 4,6,7
Y A	Ryo KURACHI et al., "Proposal of the Error Frame Monitoring System with Improved Controller Area Network (CAN) Controller", CSS2015 Computer Security Symposium 2015 Ronbunshu Godo Kaisai Anti Malware Engineering Workshop 2015 Privacy Workshop 2015 IPSJ Symposium Series, vol.2015, no.3, [CD-ROM] Computer Security Symposium 2015 Ronbunshu IPSJ Symposium Series, vol.2015, no.3, 14 October 2015 (14.10.2015), vol.2015, no.3, pages 110 to 115	1-3,5,8-12 4,6,7

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 February 2017 (07.02.17)	14 February 2017 (14.02.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/005040

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Satoshi OTSUKA et al., "Intrusion Detection for In-vehicle Networks without Modifying Legacy ECUs", IPSJ SIG Notes 2012 (Heisei 24) Nendo ▲6▼ [DVD-ROM] IPSJ SIG Notes Embedded Systems (EMB) no.28, 15 April 2013 (15.04.2013), pages 1 to 5	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／００５０４０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/40(2006.01)i, B60R16/023(2006.01)i, G06F21/57(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/40, B60R16/023, G06F21/57

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2015-114833 A（三菱電機株式会社）2015.06.22, 段落［０００３］, ［００１３］～［００２６］, ［００４４］（ファミリーなし）	1-3,5,8-12 4,6,7

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０７．０２．２０１７	国際調査報告の発送日 １４．０２．２０１７
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　９１９９ 衣鳩　文彦 電話番号　０３－３５８１－１１０１　内線　３５９６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	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材育成ワークショップ２０１５　プライバシーワークショップ２０１５　情報処理学会シンポジウムシリーズ　Ｖｏｌ．２０１５　Ｎｏ．３　［ＣＤ－ＲＯＭ］　コンピュータセキュリティシンポジウム２０１５　論文集　情報処理学会シンポジウムシリーズ　Ｖｏｌ．２０１５　Ｎｏ．３，2015.10.14，第2015巻，第3号，p.110～115	1-3, 5, 8-12 4, 6, 7
A	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　研究報告　組込みシステム（ＥＭＢ）　Ｎｏ．２８，2013.04.15，p.1～5	1-12