(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7655680号
(P7655680)

(45)発行日　令和7年4月2日(2025.4.2)

(24)登録日　令和7年3月25日(2025.3.25)

(51)国際特許分類

Ｇ０６Ｆ　21/55　(2013.01)	Ｇ０６Ｆ	21/55		
Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/60	３２０	
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０６Ｆ	21/44		
Ｂ６０Ｒ　16/02　(2006.01)	Ｂ６０Ｒ	16/02	６６０Ｑ	

ＦＩ

請求項の数　16　（全18頁）

(21)出願番号　特願2021-147082(P2021-147082)
(22)出願日　令和3年9月9日(2021.9.9)
(65)公開番号　特開2023-39790(P2023-39790A)
(43)公開日　令和5年3月22日(2023.3.22)
審査請求日　令和6年6月10日(2024.6.10)

(73)特許権者　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(73)特許権者　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人　110001519
弁理士法人太陽国際特許事務所
(72)発明者　宮内　邦裕
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内
(72)発明者　菅島　健司
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
審査官　上島　拓也

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理システム、情報処理方法、及び情報処理プログラム

(57)【特許請求の範囲】

【請求項１】

車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得する取得部と、

セキュリティセンタへ前記取得部が取得した前記セキュリティイベント情報を送信するか否かを判定する第１判定部と、

前記第１判定部によって前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知する通知部と、

前記第１判定部により前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信する送信部と、

前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する検知部と、

を含む情報処理装置。

【請求項２】

自装置及び前記他の情報処理装置は、車両に搭載された電子制御装置である請求項１に記載の情報処理装置。

【請求項３】
前記取得部は、複数の前記他の情報処理装置から複数の前記セキュリティイベント情報を取得し、
前記第１判定部は、複数の前記セキュリティイベント情報に基づいて、前記セキュリティセンタへ前記セキュリティイベント情報を送信するか否かを判定する請求項１に記載の情報処理装置。
【請求項４】
前記第１判定部によって前記セキュリティイベント情報を送信すると判定された場合に、前記セキュリティセンタとの無線通信の可否を確認する確認部を更に含む請求項３又は請求項３に記載の情報処理装置。
【請求項５】
前記セキュリティセンタとの無線通信が不可の場合、前記通知部による通知を行うか否かを判定する第２判定部を更に含む請求項１～４の何れか１項に記載の情報処理装置。
【請求項６】
前記第２判定部は、攻撃回数を用いて判定する請求項５に記載の情報処理装置。
【請求項７】
前記第２判定部は、前記セキュリティセンタとの通信未実施期間を用いて判定する請求項５又は請求項６に記載の情報処理装置。
【請求項８】
前記通知部は、前記セキュリティイベント情報が発生した前記他の情報処理装置以外の前記他の情報処理装置へ前記少なくとも一方を通知する請求項１～７の何れか１項に記載の情報処理装置。
【請求項９】
前記通知部が前記少なくとも一方を通知する際に、前記少なくとも一方に認証符号を付加する認証符号付加部を更に含む請求項１～８の何れか１項に記載の情報処理装置。
【請求項１０】
前記通知部が前記少なくとも一方を通知する際に、前記少なくとも一方を公開鍵暗号方式で暗号化する公開鍵暗号部を更に含む請求項１～８の何れか１項に記載の情報処理装置。
【請求項１１】
前記送信部は、前記通知部が前記少なくとも一方を通知後に、前記セキュリティセンタとの無線通信が可能になった場合に、前記セキュリティセンタへ前記セキュリティイベント情報を送信する請求項１に記載の情報処理装置。
【請求項１２】
前記送信部は、前記通知部が前記少なくとも一方を通知後に、前記セキュリティセンタとの無線通信が可能になった場合に、実施した対応処理を示す情報を更に送信する請求項１１に記載の情報処理装置。
【請求項１３】
前記セキュリティセンタから前記セキュリティイベント情報に対応する対応指示情報を受信し、受信した前記対応指示情報が前記対応指示と異なる場合、前記対応指示をキャンセルして前記対応指示情報を通知するキャンセル通知部を更に含む請求項１１又は請求項１２に記載の情報処理装置。
【請求項１４】
車両に搭載された複数の制御装置を備え、
前記複数の制御装置が協調して、
車両で発生したセキュリティイベント情報を取得し、
セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、
前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、
前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車

両内に通知し、
前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、
前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を行う情報処理システム。
【請求項１５】
コンピュータが、
車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得し、
セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、
前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知し、
前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、
前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を行う情報処理方法。
【請求項１６】
コンピュータに、
車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得し、
セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、
前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知し、
前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、
前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を実行させるための情報処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両の情報を処理する情報処理装置、情報処理システム、情報処理方法、及び情報処理プログラムに関する。
【背景技術】
【０００２】
車両に搭載されたＥＣＵにおいて発生したセキュリティイベントを収集する技術がある。従来の技術では、収集したセキュリティイベントの内容に応じてセキュリティセンタへ無線通信によりセキュリティイベント情報を通知する。そして、セキュリティセンタにおいて、通知されたセキュリティイベント情報に基づき、危険度を判定し、車両が危険状態にあると判断した場合、危険状態を回避するために、車両に対して特定の機能を停止させる命令を発行する。
【０００３】
例えば、特許文献１には、車載ネットワークから送信されるログデータを取得し、取得されたログデータと脅威情報との相関を求めることで異常動作を表すログデータを検知し

、異常動作の検知情報に基づいて異常動作が及ぼす影響の範囲、危険の度合い及び脅威の種別又は原因もしくはその両方をそれぞれ推定し、これらの推定結果に基づいて対応指示の通知対象となる車両を選択して、選択した車両に対し対応指示を送信する車両セキュリティ監視装置が提案されている。

【先行技術文献】

【特許文献】

【０００４】

【文献】特開２０２０－１１９０９０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１では、車載ネットワークから送信されるログデータに基づいてセキュリティ対策を実行することが可能となる。

【０００６】

しかしながら、特許文献１の技術では、車両の無線機能が故障、又は地下などの電波の届かない場所にいる場合、セキュリティイベント情報をセキュリティセンタへ通知できず、適切な命令が発行されず、セキュリティイベントに対応できない虞がある。

【０００７】

本発明は、上記事実を考慮して成されたもので、セキュリティセンタとの無線通信ができない状況であっても、セキュリティイベントに対応することが可能な情報処理装置、情報処理システム、情報処理方法、及び情報処理プログラム提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記目的を達成するために請求項１に記載の情報処理装置は、車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得する取得部と、セキュリティセンタへ前記取得部が取得した前記セキュリティイベント情報を送信するか否かを判定する第１判定部と、前記第１判定部によって前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知する通知部と、前記第１判定部により前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信する送信部と、前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する検知部と、を含む。

【０００９】

請求項１に記載の発明によれば、取得部では、車両に搭載された他の情報処理装置から車両のセキュリティイベント情報が取得される。

【００１０】

そして、通知部では、セキュリティセンタとの無線通信が不可の場合、セキュリティイベント情報に応じて予め定めた対応指示、及びセキュリティイベント情報の少なくとも一方が車両内に通知される。これにより、セキュリティセンタと通信できない場合であっても、セキュリティイベント情報に応じた対応指示、及びセキュリティイベント情報の少なくとも一方を車両内に通知するので、セキュリティに関する危険状態を回避することが可能となる。

【００１１】

なお、自装置及び前記他の情報処理装置は、車両に搭載された電子制御装置を適用してもよい。

【００１３】

また、前記取得部は、複数の前記他の情報処理装置から複数の前記セキュリティイベン

ト情報を取得し、前記第１判定部は、複数の前記セキュリティイベント情報に基づいて、前記セキュリティセンタへ前記セキュリティイベント情報を送信するか否かを判定してもよい。

【００１４】

また、前記第１判定部によって前記セキュリティイベント情報を送信すると判定された場合に、前記セキュリティセンタとの無線通信の可否を確認する確認部を更に含むようにしてもよい。

【００１７】

また、前記セキュリティセンタとの無線通信が不可の場合、前記通知部による通知を行うか否かを判定する第２判定部を更に含むようにしてもよい。

【００１８】

また、前記第２判定部は、攻撃回数を用いて判定してもよい。

【００１９】

また、前記第２判定部は、前記セキュリティセンタとの通信未実施期間を用いて判定してもよい。

【００２０】

また、前記通知部は、前記セキュリティイベント情報が発生した前記他の情報処理装置以外の前記他の情報処理装置へ前記少なくとも一方を通知してもよい。

【００２１】

また、前記通知部が前記少なくとも一方を通知する際に、前記少なくとも一方に認証符号を付加する認証符号付加部を更に含むようにしてもよい。

【００２２】

また、前記通知部が前記少なくとも一方を通知する際に、前記少なくとも一方を公開鍵暗号方式で暗号化する公開鍵暗号部を更に含むようにしてもよい。

【００２３】

また、前記送信部は、前記通知部が前記少なくとも一方を通知後に、前記セキュリティセンタとの無線通信が可能になった場合に、前記セキュリティセンタへ前記セキュリティイベント情報を送信してもよい。

【００２４】

また、前記送信部は、前記通知部が前記少なくとも一方を通知後に、前記セキュリティセンタとの無線通信が可能になった場合に、実施した対応処理を示す情報を更に送信してもよい。

【００２５】

また、前記セキュリティセンタから前記セキュリティイベント情報に対応する対応指示情報を受信し、受信した前記対応指示情報が前記対応指示と異なる場合、前記対応指示をキャンセルして前記対応指示情報を通知するキャンセル通知部を更に含むようにしてもよい。

【００２８】

なお、車両に搭載された複数の制御装置を備え、前記複数の制御装置が協調して、車両で発生したセキュリティイベント情報を取得し、セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知し、前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を行う情報処理システムとしてもよい。

【００２９】

また、コンピュータが、車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得し、セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知し、前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を行う情報処理方法としてもよい。

【００３０】

さらに、コンピュータに、車両に搭載された他の情報処理装置から車両のセキュリティイベント情報を取得し、セキュリティセンタへ取得した前記セキュリティイベント情報を送信するか否かを判定し、前記セキュリティセンタに前記セキュリティイベント情報を送信すると判定された際に、前記セキュリティセンタとの無線通信が不可の場合、前記セキュリティイベント情報に応じて予め定めた対応指示、及び前記セキュリティイベント情報の少なくとも一方を前記車両内に通知し、前記セキュリティイベント情報を送信すると判定された場合に、無線通信機能を有する電子制御装置を介して前記セキュリティセンタへ前記セキュリティイベント情報を送信し、前記セキュリティセンタとの通信が再開され、前記セキュリティセンタとの通信が不可の期間が予め定めた時間以上であった場合に、前記無線通信機能を有する電子制御装置の改ざんを検知する処理を行う情報処理方法としてもよい。

【発明の効果】

【００３１】

以上説明したように本発明によれば、セキュリティセンタとの無線通信ができない状況であっても、セキュリティイベントに対応することが可能な情報処理装置、情報処理システム、情報処理方法、及び情報処理プログラム提供できる。

【図面の簡単な説明】

【００３２】

【図１】本実施形態に係る情報処理システムの概略構成を示す図である。

【図２】本実施形態に係る情報処理システムにおける車両内の構成例を示すブロック図である。

【図３】セキュリティ監視ＥＣＵのＳＯＣのソフトウエア構造を示すブロック図である。

【図４】セキュリティイベント情報に含まれる情報を示す図である。

【図５】セキュリティ監視アプリと、無線通信ＥＣＵの機能を示す機能ブロック図である。

【図６】本実施形態に係る情報処理システムにおいて、セキュリティ監視アプリがセキュリティイベント情報を受信した際に行われる処理の流れの一例を示すフローチャートである。

【図７】セキュリティイベント情報の危険度の判定条件を示す図である。

【図８】本実施形態に係る情報処理システムにおいて、セキュリティ監視アプリがセキュリティセンタから対応指示を受信した際の処理の流れの一例を示すフローチャートである。

【図９】本実施形態に係る情報処理システムにおいて、セキュリティ監視アプリが対応指示を該当アプリ又は該当ＥＣＵに送信後にセキュリティセンタから対応指示の受信時の処理の流れの一例を示すフローチャートである。

【図１０】本実施形態に係る情報処理システムにおいて、セキュリティ監視アプリが、送信済みの対応指示をキャンセルする際に行われる処理の流れの一例を示すフローチャートである。

【発明を実施するための形態】

【００３３】

以下、図面を参照して本発明の実施の形態の一例を詳細に説明する。図１は、本実施形態に係る情報処理システムの概略構成を示す図である。

【００３４】

本実施形態に係る情報処理システム１０は、図１に示すように、車両１４と、セキュリティセンタ１２とが通信ネットワーク１８を介して接続されている。本実施形態に係る情報処理システム１０は、車両１４に搭載された各種ＥＣＵ（Electronic Control Unit）にて発生するセキュリティイベント情報を車両１４内で収集し、セキュリティセンタ１２へ通知する必要がある場合に、セキュリティセンタ１２へセキュリティイベント情報を送信する。セキュリティセンタ１２では、車両１４から送信されたセキュリティイベント情報に基づいて、対応内容を判断し、対応指示を車両１４に返信する。

【００３５】

図２は、本実施形態に係る情報処理システム１０における車両１４内の構成例を示すブロック図である。

【００３６】

車両１４には、図２に示すように、情報処理装置の一例としてのセキュリティ監視ＥＣＵ２０を含む複数のＥＣＵ２４が電子制御装置の一例として設けられている。

【００３７】

セキュリティ監視ＥＣＵ２０は、ＳＯＣ（System On Chip）２２及びＥｔｈｅｒ　ＳＷ２６を含んで構成されている。ＳＯＣ２２は、ＣＰＵ（Central Processing Unit）機能、メモリ機能、及び通信インタフェース機能を有し、ＳＯＣ２２には複数のＥＣＵ２４が接続されている。複数のＥＣＵ２４のうちの一部は、Ｅｔｈｅｒ　ＳＷ２６を介して接続されている。

【００３８】

ＳＯＣ２２に接続されるＥＣＵ２４の一例としては、車両１４の駆動を制御するＥＣＵ、制動を制御するＥＣＵ、操舵を制御するＥＣＵ、空調を制御するＥＣＵ、安全装備を制御するＥＣＵ等がある。

【００３９】

一方、Ｅｔｈｅｒ　ＳＷ２６を介してＳＯＣ２２に接続されるＥＣＵ２４の一例としては、文字、音声、静止画、動画などの複数のメディアを制御するマルチメディアＥＣＵ、人と道路と車両１４との間で情報の受発信を行って交通安全、渋滞対策、環境対策等を制御するためのＩＴＳ　ＥＣＵ（Intelligent Transport Systems）、アンテナ２８を介して車外と無線通信する無線通信ＥＣＵ２４Ａ等がある。

【００４０】

なお、セキュリティ監視ＥＣＵ２０と複数のＥＣＵ２４との接続は、物理的な配線は１つで、複数のＥＣＵ２４のうち何れかを介して１以上のＥＣＵ２４と通信可能としてもよい。

【００４１】

セキュリティ監視ＥＣＵ２０は、車両１４内のＥＣＵ２４において発生したセキュリティイベント情報を収集し、内容に応じて危険度を判定する。危険度に応じてセキュリティセンタ１２へ無線通信によりセキュリティイベント情報を通知する。セキュリティセンタ１２は、この通知結果に基づいて、危険度を判定して、車両１４が危険状態であると判断した場合に、危険状態を回避するために車両１４に対して特定の機能を停止させる等の命令を発効する。

【００４２】

図３は、セキュリティ監視ＥＣＵ２０のＳＯＣ２２のソフトウエア構造を示すブロック図である。

【００４３】

ＳＯＣ２２内には、複数のＣＰＵ　ＣＯＲＥ（図３の例では、ＣＰＵ　ＣＯＲＥ１～ＣＰＵ　ＣＯＲＥ４の４つ）３０が存在し、Ｈｙｐｅｒｖｉｓｏｒ３２により、物理ＣＰＵ　ＣＯＲＥ３０が仮想化され、ＶＭ（Virtual Machine）３４が配置される。図３では、ＶＭ

１及びＶＭ２の２つのＶＭ３４を示す。各ＶＭ３４上にＯＳ（Operating System）３６が配置され、ＯＳ３６上でアプリケーション（図３では、セキュリティ監視アプリ３８、Ａｐｐ２～Ａｐｐ４の４つのアプリケーション）が動作する。セキュリティ監視アプリ３８は、セキュリティ監視ＥＣＵ２０に接続される複数のＥＣＵ２４からのセキュリティイベント情報を受信する。なお、以下では、アプリケーションはアプリと簡略化して記載する。

【００４４】

ここで、セキュリティイベント情報について説明する。図４は、セキュリティイベント情報に含まれる情報を示す図である。

【００４５】

セキュリティイベント情報は、Protocol Version、Protocol Header、Instance ID、Sensor Instance ID、Event Definition ID、Count、Timestamp、Context Data、Signatureの９項目を含む。

【００４６】

Protocol Versionはセキュリティイベント情報送信プロトコルのバージョンである。Protocol Headerはセキュリティイベント情報の特定項目の有無を指定するものである。Instance IDはセキュリティイベント識別用ＩＤである。Sensor Instance IDはセキュリティイベント送信元ＩＤである。Event Definition IDはセキュリティイベント種類ＩＤである。Countは短期間で複数イベントが発生し、集約して送信する際の集約数である。Timestampはセキュリティイベントの発生時刻情報である。Context Dataはセキュリティイベントの詳細情報である。Signatureは署名又は認証符号である。ポートスキャンに関する情報として、ボート番号や攻撃元のＩＰアドレスといった情報がContextに含まれる。

【００４７】

セキュリティ監視アプリ３８と、セキュリティイベント送信元である攻撃検知機能を有するＥＣＵ２４にて共通の鍵を所有する。Signatureに認証符号を付加して受信側で共通鍵を用いてセキュリティイベント情報の完全性を担保する。なお、共通鍵によるメッセージ認証方式ではなく、公開鍵暗号方式を用いて情報の完全性を担保してもよい。

【００４８】

ここで、セキュリティ監視アプリ３８の機能と、無線通信ＥＣＵ２４Ａの機能について説明する。図５は、セキュリティ監視アプリ３８と、無線通信ＥＣＵ２４Ａの機能を示す機能ブロック図である。

【００４９】

セキュリティ監視アプリ３８は、セキュリティイベント情報受信機能４０、センタ送信要否判定機能４２、センタ間通信可否判定機能４４、対応指示送信機能４６、公開鍵暗号機能４８、攻撃回数カウント機能５０、センタ通信未実施期間計測機能５２、及び対応指示キャンセル機能５４を有する。なお、セキュリティイベント情報受信機能４０は取得部の一例に対応し、対応指示送信機能４６は通知部及び送信部の一例に対応し、センタ送信要否判定機能４２は第１判定部及び第２判定部の一例に対応する。また、センタ間通信可否判定機能４４は確認部の一例に対応し、公開鍵暗号機能４８は認証符号付加部及び公開鍵暗号部の一例に対応する。また、対応指示キャンセル機能５４はキャンセル通知部の一例に対応する。また、ソフトウエア改ざん検知機能６２は検知部の一例に対応する。

【００５０】

セキュリティイベント情報受信機能４０では、車両１４に設けられた複数のＥＣＵ２４からセキュリティイベント情報を受信する。

【００５１】

センタ送信要否判定機能４２では、受信したセキュリティイベント情報の内容に基づいてセキュリティセンタ１２に通知する必要があるか否かを判定する。

【００５２】

センタ間通信可否判定機能４４では、車両１４とセキュリティセンタ１２間の通信が可

能か否かを判定する。

【００５３】

対応指示送信機能４６は、センタ送信要否判定機能４２によりセキュリティイベント情報をセキュリティセンタ１２に通知する必要があると判定された場合に、セキュリティイベント情報をセキュリティセンタ１２へ送信する。また、対応指示送信機能４６は、センタ間通信可否判定機能４４によってセキュリティセンタ１２との通信が不可能な場合に、セキュリティイベント情報、及びセキュリティイベント情報に対応する対応指示の少なくとも一方を、車両内の一例としての該当するＥＣＵ２４又はアプリに送信する。また、対応指示送信機能４６は、セキュリティイベント情報のセキュリティセンタ１２への送信後に、セキュリティセンタ１２との無線通信が可能になった場合に、実施した対応処理を示す情報をセキュリティセンタ１２に送信する。

【００５４】

公開鍵暗号機能４８は、公開鍵暗号方式を用いる場合に、公開鍵を用いてセキュリティイベント情報を含むセキュリティイベントに関する関連情報を暗号化する。共通鍵によるメッセージ認証方式の場合は、共通鍵を用いてセキュリティイベント情報を含むセキュリティイベントに関する関連情報を暗号化する。関連情報としては、セキュリティイベント情報に対応する対応指示などの情報を含む。

【００５５】

攻撃回数カウント機能５０は、セキュリティイベントが発生する攻撃を受けた回数をカウントする。

【００５６】

センタ通信未実施期間計測機能５２は、セキュリティセンタ１２との通信の未実施期間を計測する。

【００５７】

対応指示キャンセル機能５４は、セキュリティセンタ１２との通信が回復した場合に、対応指示送信機能４６により送信されたセキュリティイベント情報に対応する対応指示をキャンセルする。

【００５８】

一方、無線通信ＥＣＵ２４Ａは、センタ間無線通信機能５６、センタ間暗号通信機能５８、ＥＣＵ間送受信機能６０、ソフトウエア改ざん検知機能６２、及びメッセージ認証機能６４を有する。

【００５９】

センタ間無線通信機能５６は、車両１４とセキュリティセンタ１２との間の情報の授受を無線通信によって行う。

【００６０】

センタ間暗号通信機能５８は、車両１４とセキュリティセンタ１２との間の通信を行う際に、暗号化して通信を行う。

【００６１】

ＥＣＵ間送受信機能６０は、車両１４内に設けられた複数のＥＣＵ２４間で情報の送受信を行う。

【００６２】

ソフトウエア改ざん検知機能６２は、ソフトウエアが上書きされて改ざんされているか否かを検知する。

【００６３】

メッセージ認証機能６４は、伝送された情報が途中で改ざんされていないかを確認するために、通信データに共通鍵や公開鍵等のメッセージ認証情報を付与することで通信データの認証を可能とし、データの完全性の確認を行う。

【００６４】

続いて、上述のように構成された情報処理システム１０の作用として、セキュリティ監視アプリ３８がセキュリティイベント情報を受信した際に行われる具体的な処理について

説明する。図６は、本実施形態に係る情報処理システム１０において、セキュリティ監視アプリ３８がセキュリティイベント情報を受信した際に行われる処理の流れの一例を示すフローチャートである。

【００６５】

ステップ１００では、セキュリティ監視アプリ３８が、セキュリティイベント情報を受信したか否かを判定する。該判定は、セキュリティイベント情報受信機能４０によりセキュリティイベント情報を受信したか否かを判定する。該判定が肯定された場合にはステップ１０２へ移行し、否定された場合にはステップ１０４へ移行する。

【００６６】

ステップ１０２では、セキュリティ監視アプリ３８が、セキュリティイベント情報を受信したことを表す受信フラグをオンしてタイマカウントを予め定めた値（Ｎ秒）にセットしてステップ１００に戻って上述の処理を繰り返す。本実施形態では、一定期間セキュリティイベント情報の受信がなくなるまで、すなわち、一定期間以上攻撃が収まるまで、セキュリティセンタへの情報送信をしないようにしている。

【００６７】

ステップ１０４では、セキュリティ監視アプリ３８が、受信フラグがオンであるか否かを判定する。該判定が否定された場合にはステップ１００に戻って上述の処理を繰り返し、判定が肯定された場合にはステップ１０６へ移行する。

【００６８】

ステップ１０６では、セキュリティ監視アプリ３８が、セットしたタイマカウントのカウント値のＮ秒を経過したか否かを判定する。該判定が否定された場合にはステップ１００に戻って上述の処理を繰り返し、判定が肯定された場合にはステップ１０８へ移行する。

【００６９】

ステップ１０８では、セキュリティ監視アプリ３８が、受信したセキュリティイベント情報を不揮発性メモリに保存してステップ１１０へ移行する。

【００７０】

ステップ１１０では、セキュリティ監視アプリ３８が、セキュリティイベント情報をセキュリティセンタ１２へ送信する必要があるか否かを判定する。該判定は、センタ送信要否判定機能４２によりセキュリティイベント情報の送信の要否を判定する。該判定が否定された場合にはステップ１００に戻って上述の処理を繰り返し、判定が肯定された場合にはステップ１１２へ移行する。具体的には、受信した一連のセキュリティイベント情報群から、危険度を判定し、セキュリティセンタ１２へ送信するか否かを判定する。例えば、図７に示すセキュリティセンタ判定条件を用いてセキュリティイベント情報の危険度を判定する。図７は、セキュリティイベント情報の危険度の判定条件を示す図である。すなわち、セキュリティ監視アプリ３８が、受信した一連のセキュリティイベント情報群が、Ｎｏ１．からＮｏＮまでに該当するものが含まれるかを確認する。Ｎｏ．１では、Sensor Instance IDが１で、Event Definition IDが２、かつContext DataがＡＢＣＤという値のセキュリティイベントが含まれる場合を危険度５と判定する。また、ＮＯ．２では、Sensor Instance IDが１で、Event Definition IDが２のセキュリティイベントと、Sensor Instance IDが２で、Event Definition IDが２のセキュリティイベントと、Sensor Instance IDが３で、Event Definition IDが２のセキュリティイベント情報が含まれていた場合に危険度２と判定する、というように１又は複数のセキュリティイベントから危険度を判定する。なお、Timestamp情報により、セキュリティイベントの発生した順番を条件としたり、Count情報によって攻撃回数を条件としたりしてもよい。これら判定により導いた危険度を、別途保有する、予め定めた危険度閾値と比較し、値が閾値を超えた場合にセキュリティセンタ１２に送信する。ここで、危険度の比較を条件としたが、これに限るものではなく、判定条件に合致するものがあれば送信してもよい。また、複数合致する場合は危険度を合算してもよい。また、ステップ１１０の判定を省略して、セキュリティイベント情報の送信要否の判定を行うことなく、全てのセキュリティイベント情報をセキュリティセンタ１２に送信する形態としてもよい。

【００７１】
ステップ１１２では、セキュリティ監視アプリ３８が、セキュリティセンタ１２へのセキュリティイベント情報の送信が必要と判断された場合に、セキュリティセンタ１２との通信が可能であるか否かを判定する。該判定は、センタ間通信可否判定機能４４によりセキュリティセンタ１２との通信の可否を判定する。該判定が肯定された場合にはステップ１１４へ移行し、否定された場合にはステップ１１８へ移行する。
【００７２】
ステップ１１４では、セキュリティ監視アプリ３８が、セキュリティセンタ１２への送信が可能であった場合に、セキュリティセンタ１２へセキュリティイベント情報を送信してステップ１１６へ移行する。なお、ステップ１１２において通信の可否を判定する代わりに、送信を試みて、正常に送信できなかったことを持って送信不可と判断してもよい。
【００７３】
ステップ１１６では、セキュリティ監視アプリ３８が、送信フラグをオフして、タイマカウントをオフしてステップ１００に戻って上述の処理を繰り返す。
【００７４】
一方、ステップ１１８では、セキュリティ監視アプリ３８が、該当アプリへ対応指示を送信する必要があるか否かを判定する。該判定は、センタ送信要否判定機能４２により対応指示を通知する必要があるか否かを判定する。例えば、セキュリティセンタ送信判定条件の危険度が、予め定めた対応指示判定閾値を超えているか否かを判定する。該判定が否定された場合にはステップ１００に戻って上述の処理を繰り返し、判定が肯定された場合にはステップ１２０へ移行する。このように、末端のＥＣＵ２４で判定する機能をセキュリティ監視アプリ３８に集約することにより、開発コストの低減が可能となる。なお、ステップ１１８の判定は、セキュリティセンタ送信判定条件とは別に、同様の対応指示送信判定条件を予め用意して判定してもよい。また、送信判定条件に受信した攻撃回数、及びセキュリティセンタ１２との通信未実施期間の少なくとも一方を送信判定条件に含めるようにしてもよい。例えば、攻撃回数は、セキュリティ監視アプリ３８が保有する攻撃回数の閾値を超えた場合に対応指示を送信する。閾値以下で対応指示を送信しない場合は、定期的にセキュリティセンタ１２との通信未実施期間を確認し、通信未実施期間が予め定めた閾値以上になった場合に対応指示を送信する。攻撃回数を送信判定条件に含めることでセキュリティセンタ１２との無線機能が故障した場合に、攻撃の頻度により危険度を判断して深刻な事態を回避することが可能となる。また、セキュリティセンタ１２との通信未実施期間を送信判定条件に含めることで、セキュリティセンタ１２との無線通信が、意図的に故障や通信切断状態になるような不自然な状態を確度高く判定することが可能となる。
【００７５】
ステップ１２０では、セキュリティ監視アプリ３８が、対応指示を該当アプリへ送信してステップ１００に戻って上述の処理を繰り返す。すなわち、対応指示送信機能４６により、対応指示が該当アプリに送信される。なお、対応指示を送信する代わりに、セキュリティイベント情報の１つ又は複数を該当ＥＣＵ２４又はアプリへ送信してもよい。また、該当アプリや該当ＥＣＵ２４は、例えば、図７に示すように、セキュリティセンタ判定条件の判定条件毎に予め定義される。なお、該当アプリ又は該当ＥＣＵ２４に対して対応指示を送信する代わりに、バス単位や、ブロードキャストで対応指示を送信してもよい。また、対応指示やセキュリティイベント情報の該当アプリへの送信は、セキュリティイベントが発生したＥＣＵ２４に送信する他に、セキュリティイベントが発生したＥＣＵ２４以外の他のＥＣＵ２４に送信してもよい。例えば、上流側のＥＣＵ２４でセキュリティイベントが発生して、下流側のＥＣＵ２４に対応指示やセキュリティイベント情報を送信してもよい。
【００７６】
このように、本実施形態では、セキュリティセンタ１２と通信できない場合であっても、セキュリティ監視アプリ３８が、セキュリティイベント情報に応じた対応指示、及びセキュリティイベント情報の少なくとも一方を通知するので、セキュリティに関する危険状

態を回避することが可能となる。

【００７７】

なお、セキュリティ監視アプリ３８は、対応指示及びセキュリティイベント情報の少なくとも一方を送信する際には、所有する共通鍵により認証符号を付加して送信してもよい。受信側の該当アプリ又は該当ＥＣＵ２４は、所有する共通鍵を用いて、受信した対応指示の内容をメッセージ認証して完全性の確認を行う。なお、共通鍵によるメッセージ認証方式の代わりに、公開鍵暗号方式を用いて情報を暗号化してもよい。このように認証符号を付加したり、公開暗号方式を用いた暗号化したりすることで、対応指示の送信者がセキュリティ監視アプリ３８からであり、かつ送信情報が改ざんされていないことを担保することが可能となる。

【００７８】

続いて、セキュリティセンタ１２からセキュリティ監視アプリ３８が、対応指示を受信した際の処理について説明する。図８は、本実施形態に係る情報処理システム１０において、セキュリティ監視アプリ３８がセキュリティセンタ１２から対応指示を受信した際の処理の流れの一例を示すフローチャートである。

【００７９】

ステップ１５０では、セキュリティ監視アプリ３８が、セキュリティセンタ１２からの対応指示を無線通信により受信してステップ１５２へ移行する。ここで、対応指示の受信条件として、既にセキュリティセンタ１２へ送信したセキュリティイベント情報と関連する対応指示であるかを判定して、関連するものでない場合は破棄してもよい。

【００８０】

ステップ１５２では、セキュリティ監視アプリ３８が、受信した対応指示を該当アプリ又は該当ＥＣＵ２４へ送信して一連の処理を終了する。

【００８１】

次に、セキュリティ監視アプリ３８が対応指示を該当アプリ又は該当ＥＣＵ２４に送信後にセキュリティセンタ１２から対応指示の受信時の処理について説明する。図９は、本実施形態に係る情報処理システム１０において、セキュリティ監視アプリ３８が対応指示を該当アプリ又は該当ＥＣＵ２４に送信後にセキュリティセンタ１２から対応指示の受信時の処理の流れの一例を示すフローチャートである。

【００８２】

ステップ２００では、セキュリティ監視アプリ３８が、セキュリティセンタ１２と通信可能か否かを判定する。該判定は、セキュリティ監視アプリ３８が対応指示を該当アプリ又は該当ＥＣＵ２４に送信後、セキュリティセンタ１２との通信が可能か否かを定期的に確認する。該判定が肯定される待機してステップ２０２へ移行する。

【００８３】

ステップ２０２では、セキュリティ監視アプリ３８が、セキュリティイベント情報と、セキュリティ監視アプリ３８が送信した対応指示コマンドをセキュリティセンタ１２に送信してステップ２０４へ移行する。すなわち、対応指示送信機能４６により、セキュリティイベント情報のセキュリティセンタ１２への送信後に、セキュリティセンタ１２との無線通信が可能になった場合に、実施した対応処理を示す情報として対応指示コマンドがセキュリティセンタ１２に送信される。セキュリティセンタ１２が送信する対応指示コマンドには、対応指示先のアプリ又はＥＣＵ２４を特定する情報や、指示実施時刻情報、指示受信のＥＣＵ２４の応答結果等が含まれる。これにより、車両１４において実施した対応指示によるセキュリティイベントに対する対応処理の妥当性をセキュリティセンタ１２側で判断可能となる。ここで、妥当であると判断できる場合、セキュリティセンタ１２から車両１４へ対応指示の送信が不要となる。

【００８４】

ステップ２０４では、セキュリティ監視アプリ３８が、送信した対応指示コマンドを不揮発性メモリ等に保持して一連の処理を終了する。

【００８５】

続いて、セキュリティセンタ１２とセキュリティ監視アプリ３８との間の通信が回復後に、送信済みの対応指示をキャンセルする際の処理について説明する。図１０は、本実施形態に係る情報処理システム１０において、セキュリティ監視アプリ３８が、送信済みの対応指示をキャンセルする際に行われる処理の流れの一例を示すフローチャートである。

【００８６】

ステップ２５０では、セキュリティ監視アプリ３８が、セキュリティセンタ１２から対応指示を受信してステップ２５２へ移行する。すなわち、対応指示コマンドのセキュリティセンタ１２への送信後に、セキュリティセンタ１２から対応指示情報として対応指示コマンドを受信する。

【００８７】

ステップ２５２では、セキュリティ監視アプリ３８が、対応済みセキュリティイベントに関する指示であるか否かを判定する。該判定は、セキュリティセンタ１２から受信した対応指示の内容が、セキュリティ監視アプリ３８が保持する対応指示コマンドと同様か否かを判定する。該判定が肯定された場合にはステップ２５４へ移行し、肯定された場合にはステップ２５６へ移行する。

【００８８】

ステップ２５４では、セキュリティ監視アプリ３８が、実施済み対応指示のキャンセルを行ってステップ２５６へ移行する。すなわち、対応指示キャンセル機能５４により、対応指示送信機能４６により送信されたセキュリティイベント情報に対応する対応指示がキャンセルされる。ここで、キャンセルを意味するコマンドを送信する代わりに、セキュリティセンタ１２から受信した対応指示を、該当アプリ又は該当ＥＣＵ２４に送信することでセキュリティ監視アプリ３８が既に送信した対応指示を上書きする形態としてもよい。

【００８９】

ステップ２５６では、セキュリティ監視アプリ３８が、受信した対応指示を該当アプリ又は該当ＥＣＵ２４へ送信してステップ２５８へ移行する。

【００９０】

ステップ２５８では、セキュリティ監視アプリ３８が、セキュリティセンタ１２への対応完了応答を送信して一連の処理を終了する。

【００９１】

ここで、上述の図１０の送信済みの対応指示をキャンセルする際の処理について具体例を挙げて説明する。

【００９２】

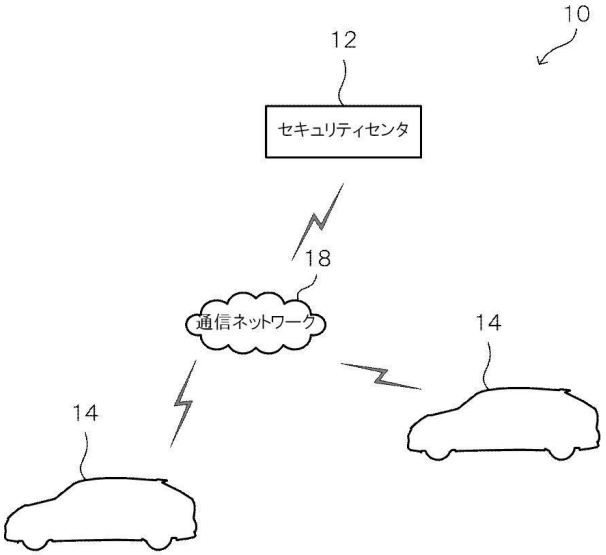
例えば、Ｅｔｈｅｒ　ＳＷ２６にマルチメディアＥＣＵとＩＴＳ　ＥＣＵが接続されているものとする。セキュリティ監視アプリ３８がマルチメディアＥＣＵ、Ｅｔｈｅｒ　ＳＷ２６の各々からセキュリティイベント情報を受信する。マルチメディアＥＣＵが持つワイヤレスＬＡＮ（Local Area Network）のアクセスポイント機能において、大量の認証エラーを検知したため、危険度が高いと判定し、セキュリティセンタ１２へのセキュリティイベント情報の送信を試みるが、セキュリティセンタ１２と通信できず送信が成功しない。セキュリティ監視アプリ３８は、危険度から当指示が必要と判定し、マルチメディアＥＣＵへワイヤレスＬＡＮのアクセスポイント機能を無効かする対応指示を送信する。その後、無線通信状況が良好となり、セキュリティセンタ１２との通信が復帰し、セキュリティ監視アプリ３８が対応指示送信後の定期的なセキュリティセンタ１２との通信状態確認により、通信可能であることを検出する。セキュリティセンタ１２へセキュリティイベント情報を送信する。セキュリティセンタ１２側にてマルチメディアＥＣＵは危殆化していないと判断し、Ｅｔｈｅｒ　ＳＷ２６のセキュリティイベント情報、及びセキュリティセンタ１２側が持つ公知の脆弱性情報などから、接続されるＩＴＳ　ＥＣＵが危殆化していると判断する。セキュリティセンタ１２よりマルチメディアＥＣＵに既に送信している対応指示のキャンセル指示と、Ｅｔｈｅｒ　ＳＷ２６のＩＴＳ　ＥＣＵが接続されるポートを無効にする対応指示を受信する。なお、キャンセル指示は、対応指示のキャンセル指示の代わりに、アクセスポイント機能を有効にする新たな対応指示としてもよい。

【００９３】
　また、本実施形態では、セキュリティセンタ１２との通信が可能となったことを検出した際、セキュリティセンタ１２へセキュリティイベント情報と対応指示コマンドを送信する前に、正しくセキュリティセンタ１２と通信できるかを検証してもよい。これにより、無線通信ＥＣＵ２４Ａが改ざんされてセキュリティセンタ１２のように振る舞うダミープログラムがインストールされて、既に実施した車両内の対応指示が解除されてしまうことを回避することが可能となる。例えば、無線通信ＥＣＵ２４Ａのソフトが上書きされていないかを確認するために、セキュリティ監視アプリ３８は、無線通信ＥＣＵ２４Ａが正常かを確認するコマンドを送信する。コマンドへは乱数を含ませ、公開鍵暗号機能４８により保有する共通鍵で符号化し、受信した符号と一致するかを検証する。ここで、無線通信ＥＣＵ２４Ａにセキュアブート機能を持たせ、無線通信ＥＣＵ２４Ａが起動する際に、ソフトウエア改ざん検知機能６２によりソフトウエアの正当性を検証し、異常なソフトウエアであった場合は起動しない、などとしてもよい。ここで、無線通信ＥＣＵ２４Ａは、起動時にセキュリティセンタ１２との通信が行われていない期間を確認し、予め定めた時間以上であった場合のみ、ソフトの上書きがされていないかを確認するようにしてもよい。これにより、無線通信ＥＣＵ２４Ａの処理負荷を抑えたい場合など、改ざんが可能となるような一定時間以上無通信状態が続いた場合などの特定条件に該当する場合のみ、改ざん確認を行うことが可能となる。
【００９４】
　また、本実施形態におけるセキュリティ監視アプリ３８等のアプリケーションプログラムは、ＯＴＡ（Over The Air）によってセキュリティ監視ＥＣＵ２０や他のＥＣＵ２４にインストールしてもよい。また、セキュリティイベントに応じた対応指示についてもＯＴＡによりセキュリティ監視ＥＣＵ２０や他のＥＣＵ２４に送受信してもよい。
【００９５】
　なお、上記の実施形態では、セキュリティ監視アプリ３８が単一のセキュリティ監視ＥＣＵ２０上で動作する例を説明したが、これに限るものではない。例えば、複数のＥＣＵ２４が協同してセキュリティ監視アプリ３８が行う処理（図６及び図８～１０の処理）を実行する形態としてもよい。
【００９６】
　また、上記の各実施形態におけるセキュリティ監視ＥＣＵ２０のＳＯＣ２２で行われる処理は、プログラムを実行することにより行われるソフトウエア処理として説明したが、これに限るものではない。例えば、ＧＰＵ（Graphics Processing Unit）、ＡＳＩＣ（Application Specific Integrated Circuit）、及びＦＰＧＡ（Field-Programmable Gate Array）等のハードウエアで行う処理としてもよい。或いは、ソフトウエア及びハードウエアの双方を組み合わせた処理としてもよい。また、ソフトウエアの処理とした場合には、プログラムを各種記憶媒体に記憶して流通させるようにしてもよい。
【００９７】
　さらに、本発明は、上記に限定されるものでなく、上記以外にも、その主旨を逸脱しない範囲内において種々変形して実施可能であることは勿論である。
【符号の説明】
【００９８】
１０　情報処理システム
１２　セキュリティセンタ
１４　車両
２０　セキュリティ監視ＥＣＵ（情報処理装置）
２２　ＳＯＣ
２４　ＥＣＵ
２４Ａ　無線通信ＥＣＵ
３８　セキュリティ監視アプリ
４０　セキュリティイベント情報受信機能（取得部）

４２　センタ送信要否判定機能（第１判定部及び第２判定部）
４４　センタ間通信可否判定機能（確認部）
４６　対応指示送信機能（通知部及び送信部）
４８　公開鍵暗号機能（認証符号付加部及び公開鍵暗号部）
５４　対応指示キャンセル機能（キャンセル通知部）
６２　ソフトウエア改ざん検知機能（検知部）

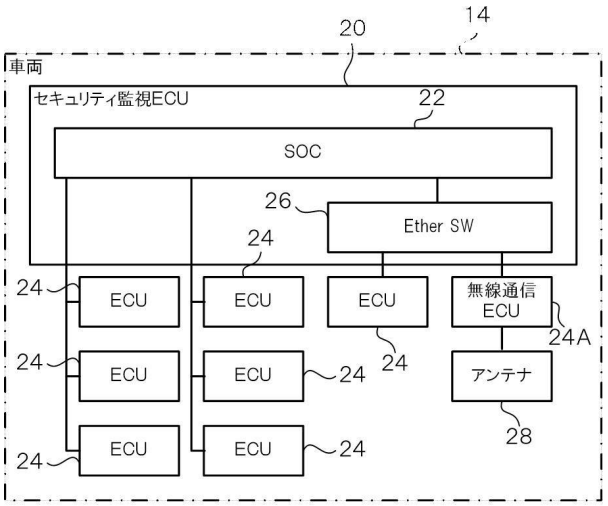
【図面】

【図１】



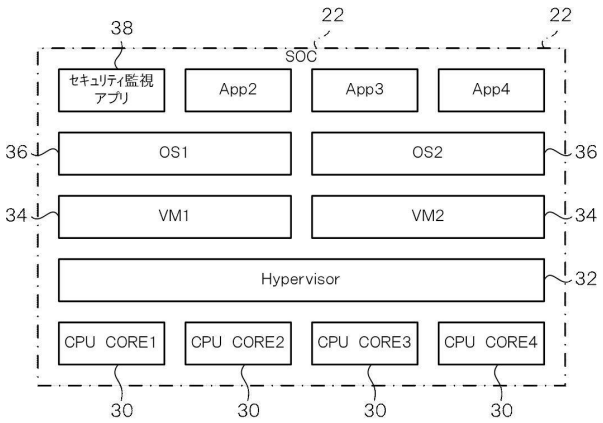
10　情報処理システム
12　セキュリティセンタ
14　車両

【図２】



20　セキュリティ監視ECU(情報処理装置)
22　SOC
24　ECU
24A　無線通信ECU

【図３】

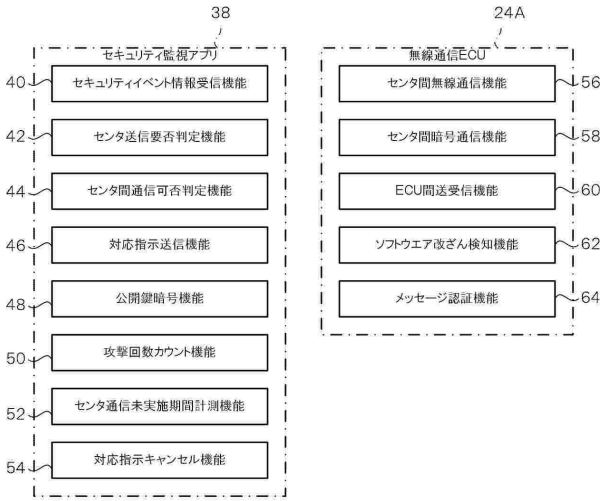


38　セキュリティ監視アプリ

【図４】

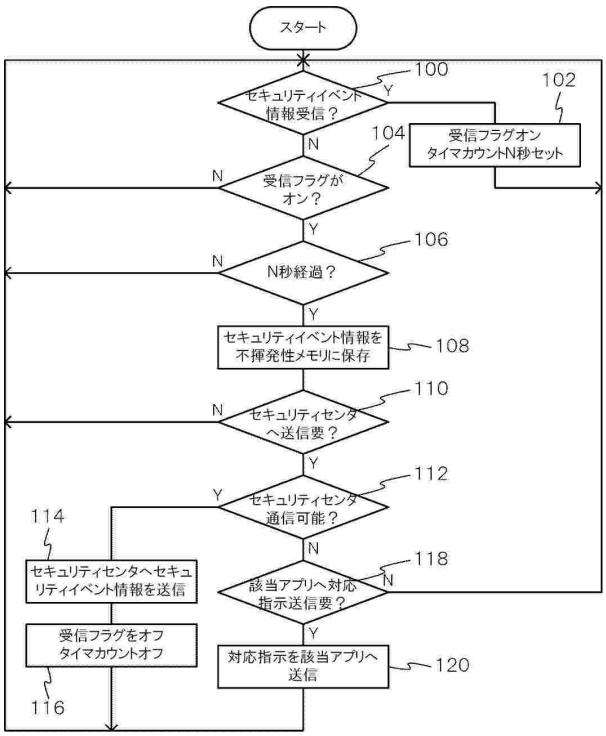
項目名	役割
Protocol Version	セキュリティイベント情報送信プロトコルのバージョン
Protocol Header	セキュリティイベント情報の特定項目の有無を指定
Instancce ID	セキュリティイベント識別用ID
Sensor Instance ID	セキュリティイベント送信元ID
Event Definision ID	セキュリティイベント種類ID
Count	短期間で複数イベントが発生し、集約して送信する際の集約数
Timestamp	セキュリティイベント発生時刻情報
Context Data	セキュリティイベントの詳細情報
Signature	署名、または認証符号

【図５】



40 セキュリティイベント情報受信機能（取得部）
42 センタ送信要否判定機能（第１判定部及び第２判定部）
44 センタ間通信可否判定機能（確認部）
46 対応指示送信機能（通知部及び送信部）
48 公開鍵暗号機能（認証符号付加部及び公開鍵暗号部）
54 対応指示キャンセル機能（キャンセル通知部）
62 ソフトウエア改ざん検知機能（検知部）

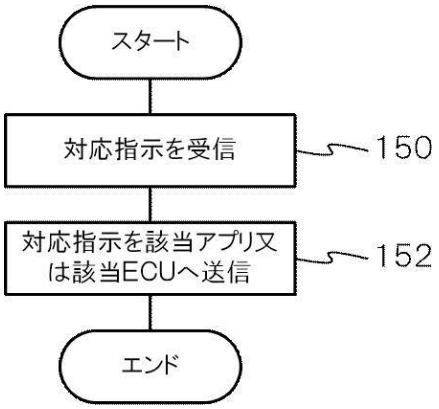
【図６】



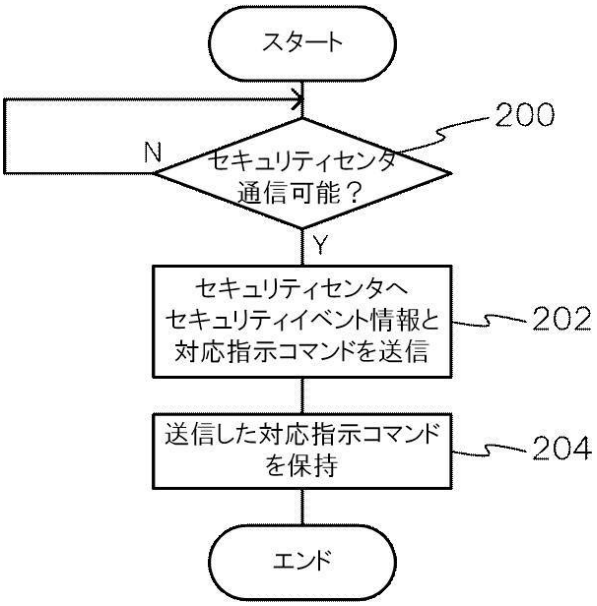
【図７】

NO.	セキュリティイベント1	セキュリティイベント2	セキュリティイベント3	…	セキュリティイベントN	危険度	送信先アプリ
1	Sensor Instance ID:1 Event Definition ID:2 Context Data:ABCD	–	–	…	–	5	アプリA
2	Sensor Instance ID:1 Event Definition ID:2	Sensor Instance ID:2 Event Definition ID:2	Sensor Instance ID:3 Event Definition ID:2	…	–	2	アプリA ＋ アプリB
3	Sensor Instance ID:1 Event Definition ID:2	Sensor Instance ID:2 Event Definition ID:3	–	…	–	1	なし
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	…	・ ・ ・	・ ・ ・	・ ・ ・
N	・ ・ ・	・ ・ ・	・ ・ ・	…	・ ・ ・	・ ・ ・	・ ・ ・

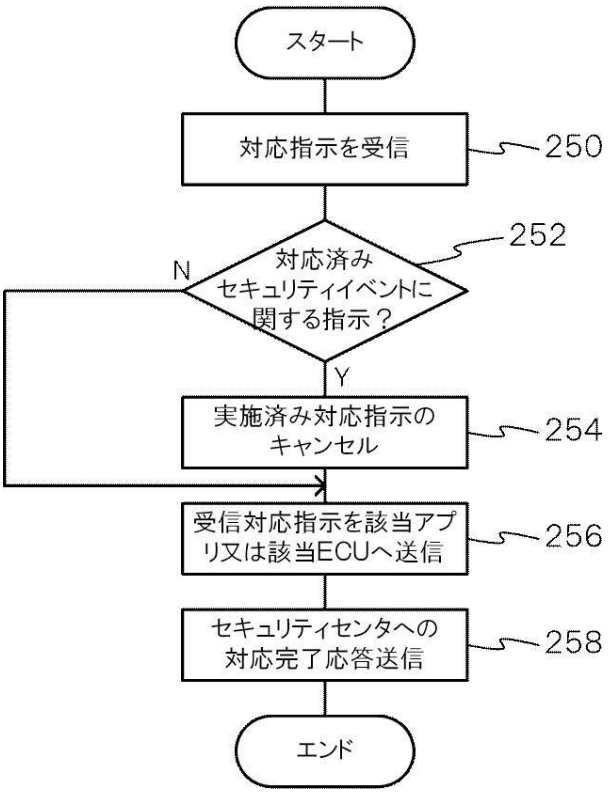
【図８】



【図９】


スタート
200
N
セキュリティセンタ
通信可能？
Y
セキュリティセンタへ
セキュリティイベント情報と
対応指示コマンドを送信
202
送信した対応指示コマンド
を保持
204
エンド

【図１０】


スタート
対応指示を受信
250
252
N
対応済み
セキュリティイベントに
関する指示？
Y
実施済み対応指示の
キャンセル
254
受信対応指示を該当アプ
リ又は該当ECUへ送信
256
セキュリティセンタへの
対応完了応答送信
258
エンド

フロントページの続き

(56)参考文献　特開２０１９－１２５３４４（ＪＰ，Ａ）
特開２０１４－２３４１００（ＪＰ，Ａ）
国際公開第２０１８／０３７４９３（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｇ０６Ｆ　２１／６０
Ｇ０６Ｆ　２１／４４
Ｂ６０Ｒ　１６／０２