(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
2021年1月14日(14.01.2021)

WIPO | PCT

(10) 国際公開番号
WO 2021/005978 A1

(51) 国際特許分類:
G06F 21/60 (2013.01)

(21) 国際出願番号： PCT/JP2020/023640

(22) 国際出願日： 2020年6月16日(16.06.2020)

(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 2019-127855 2019年7月9日(09.07.2019) JP

(71) 出願人: 株式会社デンソー (**DENSO CORPORATION**) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP).

(72) 発明者: 濱口 賢一 (**HAMAGUCHI Kenichi**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP). 谷端 伸彦 (**TANIBATA Nobuhiko**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP).

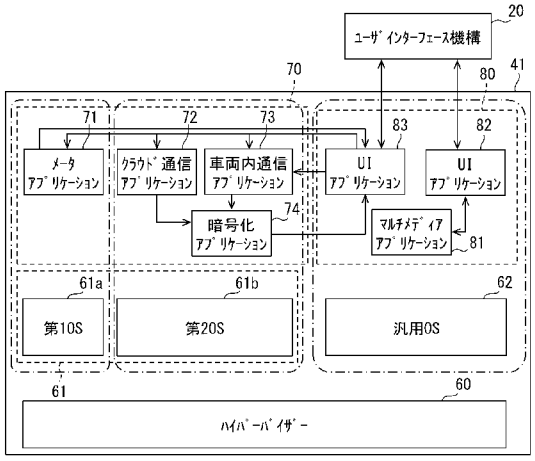
(74) 代理人: 矢作 和行, 外 (**YAHAGI Kazuyuki** et al.); 〒4600003 愛知県名古屋市中区錦２丁目１３番１９号 瀧定ビル６階 Aichi (JP).

(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, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** ARITHMETIC DEVICE AND DATA TRANSMISSION METHOD

(54) 発明の名称： 演算装置およびデータ送信方法

図2



20	User interface mechanism
60	Hypervisor
61a	First OS
61b	Second OS
62	General-purpose OS
71	Meter application
72	Cloud communication application
73	In-vehicle communication application
74	Encryption application
81	Multimedia application
82, 83	UI application

(57) **Abstract:** This arithmetic device is provided with: a general-purpose operating system (62); a high OS-side application (70) which is application software that can be executed by a high operating system (61) having a security level higher than the security level of the general-purpose operating system (62) and that is operated on the high operating system (61); a UI application (83) which is application software operated on the general-purpose operating system (62) and which communicates with the high OS-side application (70), wherein data is communicated between the high OS-side application (70) and the UI application (83) through intra-chip application communication or wired communication, and data transmitted from at least one high OS-side application (70) to the UI application (83) is encrypted.

WO 2021/005978 A1

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(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:

一 国際調査報告(条約第21条(3))

(57) 要約:汎用オペレーティングシステム(６２)と、汎用オペレーティングシステム(６２)よりもセキュリティレベルが高い高オペレーティングシステム(６１)が実行可能であり、かつ、高オペレーティングシステム(６１)上で動作するアプリケーションソフトウェアである高ＯＳ側アプリケーション(７０)と、汎用オペレーティングシステム(６２)上で動作するアプリケーションソフトウェアであって、高ＯＳ側アプリケーション(７０)と通信するＵＩアプリケーション(８３)とを備え、高ＯＳ側アプリケーション(７０)とＵＩアプリケーション(８３)との間は、チップ内アプリケーション通信または有線通信によりデータ通信が行われ、少なくとも１つの高ＯＳ側アプリケーション(７０)からＵＩアプリケーション(８３)へ送信されるデータは暗号化されている。

明　細　書

発明の名称 ： 演算装置およびデータ送信方法

関連出願の相互参照

[0001] 本出願は、２０１９年７月９日に日本に出願された特許出願第２０１９－１２７８５５号を基礎としており、基礎の出願の内容を、全体的に、参照により援用している。

技術分野

[0002] 演算装置、および、その演算装置が実行するデータ送信方法に関する。

背景技術

[0003] 特許文献１には、２つのプラットフォームを備えた車載装置が開示されている。ソフトウェアであるプラットフォームはオペレーティングシステムと呼ばれることも多い。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１４－１３９７７２号公報

発明の概要

[0005] 複数のオペレーティングシステムを備える場合、車両情報などの重要な情報は、相対的にセキュリティレベルの高いオペレーティングシステム上で動作するアプリケーションソフトウェアが扱うようにすることが考えられる。相対的にセキュリティレベルが高いオペレーティングシステムを、説明の便宜上、高オペレーティングシステムとし、相対的にセキュリティレベルが低いオペレーティングシステムを、以下、便宜上、低オペレーティングシステムとする。

[0006] 高オペレーティングシステムとしては、たとえば、ＡＧＬ、ＱＮＸ（登録商標）などを例示できる。低オペレーティングシステムとしては、ＡＮＤＲＯＩＤ（登録商標）などの汎用オペレーティングシステムを例示できる。

[0007] 汎用オペレーティングシステム上で種々のアプリケーションソフトウェア

が動作する。汎用オペレーティングシステム上で動作するアプリケーションソフトウェアとして、ディスプレイや入力装置など、ユーザインターフェースのうちのハードウェア部分（以下、ユーザインターフェース機構）を利用するものがある。

[0008] 高オペレーティングシステム上で動作するアプリケーションソフトウェア（以下、高ＯＳ側アプリケーション）も、ユーザインターフェース機構を利用することがある。高ＯＳ側アプリケーションもユーザインターフェース機構を利用する場合、調停や表示態様の統一性を出すために、高ＯＳ側アプリケーションは直接的にはユーザインターフェース機構を制御せず、ユーザインターフェース機構へ送信するデータを、低オペレーティングシステム側に送信することが考えられる。そして、低オペレーティングシステム上で動作し、ユーザインターフェース機構を制御するユーザインターフェースアプリケーションを設ける。

[0009] ユーザインターフェースアプリケーションを低オペレーティングシステム側に設けることで、ユーザインターフェース機構を利用する、低オペレーティングシステム側のアプリケーションとの間で調停や表示態様の統一が容易になる。

[0010] しかし、低オペレーティングシステムは、高オペレーティングシステムよりもハッキングに弱い。高オペレーティングシステムから低オペレーティングシステムへデータを送信すると、低オペレーティングシステムがハッキングされることで、高オペレーティングシステム側のデータの流出する恐れが高くなる。

[0011] 本開示は、この事情に基づいて成されたものであり、その目的とするところは、セキュリティレベルが高いオペレーティングシステム上で扱われるデータの流出を抑制することができる演算装置およびデータ送信方法を提供することにある。

[0012] 上記目的は独立請求項に記載の特徴の組み合わせにより達成され、また、下位請求項は更なる有利な具体例を規定する。請求の範囲に記載した括弧内

の符号は、一つの態様として後述する実施形態に記載の具体的態様との対応関係を示すものであって、開示した技術的範囲を限定するものではない。

[0013] 上記目的を達成するための演算装置に係る１つの開示は、

相互にセキュリティレベルが異なる複数のオペレーティングシステムを実行する演算装置であって、

複数のオペレーティングシステムのうちの相対的にセキュリティレベルが低いオペレーティングシステムを低オペレーティングシステムとし、

複数のオペレーティングシステムのうち、低オペレーティングシステムよりもセキュリティレベルが高いオペレーティングシステムを高オペレーティングシステムとしたとき、

高オペレーティングシステム上で動作するアプリケーションソフトウェアである少なくとも１つの高ＯＳ側アプリケーションと、

低オペレーティングシステム上で動作するアプリケーションソフトウェアであって、高ＯＳ側アプリケーションと通信する低ＯＳ側通信アプリケーションとを備え、

高ＯＳ側アプリケーションと低ＯＳ側通信アプリケーションとの間は、チップ内アプリケーション通信または有線通信によりデータ通信が行われ、

少なくとも１つの高ＯＳ側アプリケーションから低ＯＳ側通信アプリケーションへ送信されるデータは暗号化されている。

[0014] この演算装置では、少なくとも１つの高ＯＳ側アプリケーションは、データを暗号化して低ＯＳ側通信アプリケーションに送信する。これにより、低オペレーティングシステムがハッキングされた場合に、高ＯＳ側アプリケーションが扱うデータが流出してしまうことが抑制される。

[0015] 上記目的を達成するためのデータ送信方法に係る１つの開示は、上記演算装置が実行するデータ送信方法である。すなわち、そのデータ送信方法は、

相互にセキュリティレベルが異なる複数のオペレーティングシステムのうちの相対的にセキュリティレベルが低いオペレーティングシステムを低オペレーティングシステムとし、

複数のオペレーティングシステムのうち、低オペレーティングシステムよりもセキュリティレベルが高いオペレーティングシステムを高オペレーティングシステムとしたとき、

高オペレーティングシステム上で動作するアプリケーションソフトウェアである少なくとも１つの高ＯＳ側アプリケーションから、低オペレーティングシステム上で動作するアプリケーションソフトウェアである低ＯＳ側通信アプリケーションへデータを送信するデータ送信方法であって、

高ＯＳ側アプリケーションと低ＯＳ側通信アプリケーションとの間は、チップ内アプリケーション通信または有線通信によりデータ通信が行われ、

少なくとも１つの高ＯＳ側アプリケーションが低ＯＳ側通信アプリケーションへ送信する元データを生成し、

生成した元データを暗号化したデータを低ＯＳ側通信アプリケーションへ送信する。

図面の簡単な説明

[0016] [図1]車載システム１の全体構成を示す図である。

[図2]ＣＰＵ４１が実行するソフトウェアを示す図である。

[図3]ＯＳ間通信に関する処理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

[0017] 以下、実施形態を図面に基づいて説明する。図１に示す車載システム１は、車両Ｃに搭載されている。車載システム１は、ユーザインターフェース機構２０と、無線通信装置３０と、演算装置であるコンピュータ４０とを備えている。

[0018] ユーザインターフェース機構２０は、ユーザとコンピュータ４０との間の情報伝達を行う構成のうちのハードウェア構成を意味する。図１には、ユーザインターフェース機構２０として、ディスプレイ２１と入力装置２２を開示している。

[0019] ディスプレイ２１は、車両Ｃの車室において乗員が視認できる位置に配置されている。ディスプレイ２１は、種々の画像が表示可能である。ディスプ

レイ２１として、液晶ディスプレイや有機ＥＬディスプレイを用いることができる。

[0020] 入力装置２２は、車両Ｃの乗員が種々の入力操作をする部分である。入力装置２２は、たとえば、ディスプレイ２１の表示面に重畳されたタッチパネル、メカニカルスイッチである。また、音声入力を行うためのマイクを入力装置２２として設けることもできる。無線通信装置３０は、車両Ｃの外部との間で無線通信を行う。無線通信装置３０は、たとえば、クラウドサーバと通信を行う。

[0021] コンピュータ４０は、ユーザインターフェース機構２０に接続されているとともに車内ＬＡＮバス５０に接続されている。コンピュータ４０は、車内ＬＡＮバス５０を介して、車両Ｃに搭載された種々の機器との間で信号の送受信が可能である。

[0022] コンピュータ４０が車内ＬＡＮバス５０を介して受信する信号としては、たとえば、ディスプレイ２１に画像として表示される車両計器類において現在の状態を示す信号がある。この信号には、たとえば、車速を示す信号、燃料残量を示す信号などが含まれる。他にも、入力装置２２の入力操作により要求された種々の車載機器の制御情報、無線通信装置３０が受信した車外の情報を、コンピュータ４０が取得できるようにしてもよい。なお、コンピュータ４０は、無線通信装置３０が受信した車外の情報を、車両Ｃに搭載されたＥＣＵを介して取得してもよい。

[0023] ［コンピュータ４０の構成］

コンピュータ４０は、図１に示すように、プロセッサモジュール４１、ＲＡＭ４２、フラッシュメモリ４３、バスライン４４などを備えている。プロセッサモジュール４１は、複数のプロセッサコアを備える。

[0024] ＲＡＭ４２は、フラッシュメモリ４３から読み出された情報などを一時的に記憶する。フラッシュメモリ４３は不揮発性のメモリであり、プロセッサモジュール４１が実行する種々のソフトウェアを記憶している。

[0025] プロセッサモジュール４１は、図２に示すソフトウェアを実行する。した

がって、フラッシュメモリ４３には図２に示す各ソフトウェアが記憶されている。なお、図２に示す種々のソフトウェアは、コンピュータ４０が他の不揮発性有形記憶媒体を備えている場合には、図２に示す種々のソフトウェアは、フラッシュメモリ４３以外の不揮発性有形記憶媒体に記憶されていてもよい。

[0026] 図２は、コンピュータ４０が各ソフトウェアを実行する際のソフトウェア間の階層構造も概略的に示している。図２に示すように、プロセッサモジュール４１は、ハイパーバイザー６０、高オペレーティングシステム６１、汎用オペレーティングシステム６２、高ＯＳ側アプリケーション７０、低ＯＳ側アプリケーション８０を備えている。なお、アプリケーションは、アプリケーションソフトウェアともいう。

[0027] ハイパーバイザー６０は、コンピュータ４０に仮想化環境を作り出すソフトウェアである。ハイパーバイザー６０は具体的には、１つのコンピュータ４０にて、高オペレーティングシステム６１と汎用オペレーティングシステム６２が並列に動作可能な環境を作り出すソフトウェアである。高オペレーティングシステム６１は、汎用オペレーティングシステム６２に比べてセキュリティレベルが高いオペレーティングシステムである。

[0028] 本実施形態では、プロセッサモジュール４１は、高オペレーティングシステム６１として、第１オペレーティングシステム６１ａと第２オペレーティングシステム６１ｂの２種類のオペレーティングシステムを実行する。第１オペレーティングシステム６１ａを実行するプロセッサコアと、第２オペレーティングシステム６１ｂを実行するプロセッサコアと、汎用オペレーティングシステム６２を実行するプロセッサコアは、互いに異なるプロセッサコアとすることができる。ただし、プロセッサモジュール４１が備える一部または全部のプロセッサコアを、複数のオペレーティングシステムを実行するプロセッサコアとして共用してもよい。なお、プロセッサモジュール４１が実行する高オペレーティングシステム６１は１種類のみでもよい。

[0029] 第１オペレーティングシステム６１ａは、たとえば、リアルタイムオペレ

ーティングシステムとすることができる。リアルタイムオペレーティングシステムは、リアルタイム処理を行うオペレーティングシステムである。リアルタイムオペレーティングシステムは、安定性に優れているという特徴を持つ。リアルタイムオペレーティングシステムは、たとえば、ＱＮＸである。

[0030] 第２オペレーティングシステム６１ｂは、たとえば、ＡＧＬとすることができる。なお、第１オペレーティングシステム６１ａと第２オペレーティングシステム６１ｂとの間のセキュリティレベルはどちらが高くてもよい。

[0031] 汎用オペレーティングシステム６２は、高オペレーティングシステム６１よりもセキュリティレベルが低いオペレーティングシステムである。汎用オペレーティングシステム６２は低オペレーティングシステムの一例である。汎用オペレーティングシステム６２は、たとえばＡＮＤＲＯＩＤである。

[0032] 高ＯＳ側アプリケーション７０として、図２には、メータアプリケーション７１、クラウド通信アプリケーション７２、車両内通信アプリケーション７３、暗号化アプリケーション７４が示されている。

[0033] これらのうち、メータアプリケーション７１は、第１オペレーティングシステム６１ａ上で動作する。一方、クラウド通信アプリケーション７２、車両内通信アプリケーション７３、暗号化アプリケーション７４は、第２オペレーティングシステム６１ｂ上で動作する。

[0034] メータアプリケーション７１は、ディスプレイ２１に表示される車両計器類の画像を決定するための情報である車速等を決定する。メータアプリケーション７１は、決定した車速等を示すデータを、ユーザインターフェースアプリケーション（以下、ＵＩアプリケーション）８３に送信する。

[0035] クラウド通信アプリケーション７２は、無線通信装置３０を制御して、クラウドサーバとの間でデータの送受信を行う。クラウド通信アプリケーション７２がクラウドサーバから取得することができるデータには、車両Ｃに関する種々の情報または車両Ｃの乗員に関する種々の情報の少なくとも一方が含まれることがある。クラウド通信アプリケーション７２は、クラウドサーバから取得した情報を、ＵＩアプリケーション８３に提供できる情報に変換

する。そして、変換後の情報を、暗号化アプリケーション７４を介してＵＩアプリケーション８３に送る。

[0036] 車両内通信アプリケーション７３は、ＵＩアプリケーション８３からの指示に従い、車両Ｃに搭載された種々のＥＣＵ等と通信を行って種々の車両内情報を取得する。そして、車両内通信アプリケーション７３は、取得した車両内情報をＵＩアプリケーション８３が理解可能な形式に変更する。ＵＩアプリケーション８３は、形式を変更した後のデータを、暗号化アプリケーション７４を介してＵＩアプリケーション８３に送る。

[0037] 暗号化アプリケーション７４は、クラウド通信アプリケーション７２、車両内通信アプリケーション７３から供給されたデータを暗号化して、ＵＩアプリケーション８３に送信する。暗号化アプリケーション７４から見た場合、クラウド通信アプリケーション７２、車両内通信アプリケーション７３は、ＵＩアプリケーション８３に送信する元データを作成する元データ作成アプリケーションである。

[0038] 暗号化アプリケーション７４とＵＩアプリケーション８３との間の通信方式に特に制限はない。共有メモリ方式、ソケット通信など、種々の通信方式を用いて暗号化アプリケーション７４とＵＩアプリケーション８３は通信することができる。

[0039] 暗号化アプリケーション７４とＵＩアプリケーション８３は、ともに、同じプロセッサモジュール４１が実行する。したがって、通信方式によらず、暗号化アプリケーション７４とＵＩアプリケーション８３との間の通信はチップ内アプリケーション通信である。チップ内アプリケーション通信は、１つのチップが備える１つまたは複数のプロセッサが実行するアプリケーション間の通信を意味する。また、暗号化の方式は特に制限はない。たとえば、ＳＳＨにより、暗号化アプリケーション７４とＵＩアプリケーション８３は通信することができる。

[0040] 低ＯＳ側アプリケーション８０は、マルチメディアアプリケーション８１、ＵＩアプリケーション８２、８３を備える。図２には、１つのマルチメデ

ィアアプリケーション８１を示しているが、マルチメディアアプリケーション８１の数は複数でもよい。マルチメディアアプリケーション８１は、具体的には、ナビゲーションアプリケーション、オーディオアプリケーションなどである。

[0041] マルチメディアアプリケーション８１は、ＵＩアプリケーション８２に種々のデータを送信する。また、ＵＩアプリケーション８２からの指示に応じた処理を実行する。たとえば、マルチメディアアプリケーション８１がナビゲーションアプリケーションである場合には、ＵＩアプリケーション８２から、経路探索の指示などが入力される。ＵＩアプリケーション８２は、経路探索の指示などを入力装置２２から取得する。経路探索の指示が入力された場合には、ナビゲーションアプリケーションは、経路探索処理を実行する。経路探索処理を実行したことにより探索された経路を示すデータは、ＵＩアプリケーション８２に送信される。なお、マルチメディアアプリケーション８１とＵＩアプリケーション８２との間の通信は暗号化されていない。

[0042] ＵＩアプリケーション８２は、マルチメディアアプリケーション８１とユーザとの間のインターフェースのうちのソフトウェア部分である。マルチメディアアプリケーション８１とユーザとの間のインターフェースのうちのハードウェア部分はユーザインターフェース機構２０である。

[0043] ＵＩアプリケーション８２は、入力装置２２から入力された信号に基づいて定まる指示を、マルチメディアアプリケーション８１に出力する。また、ＵＩアプリケーション８２は、マルチメディアアプリケーション８１から入力されたデータに基づいてディスプレイ２１に表示する表示内容を決定し、その表示内容をディスプレイ２１に表示する。

[0044] ＵＩアプリケーション８３は、低ＯＳ側通信アプリケーションに相当しており、高ＯＳ側アプリケーション７０とユーザとの間のインターフェースのうちのソフトウェア部分である。ＵＩアプリケーション８３は、入力装置２２から入力された信号が高ＯＳ側アプリケーション７０に対する指示である場合には、その指示を、指示内容に基づいて定まる高ＯＳ側アプリケーショ

ン７０に送信する。

[0045] また、ＵＩアプリケーション８３は、暗号化アプリケーション７４からデータが送信されてきた場合には、そのデータを復号し、復号したデータに基づいて定まる処理を実行する。たとえば、復号したデータが車速を示す場合には、ディスプレイ２１に表示している車速を、新たに取得した車速を表すように変更する。

[0046] また、ＵＩアプリケーション８３は、入力装置２２から、クラウドサーバに保存されているデータ取得要求があった場合には、クラウドサーバからデータを取得する指示を、クラウド通信アプリケーション７２に送信する。クラウド通信アプリケーション７２はこの指示を受けると、指示に基づいて定まるデータを、クラウドサーバから取得する。そして、そのデータを、暗号化アプリケーション７４を介してＵＩアプリケーション８３に送信する。ＵＩアプリケーション８３は、このデータを復号して、ユーザインターフェース機構２０に出力する。

[0047] ［ＯＳ間通信に関する処理］

図３に、ＯＳ間でデータを通信する際の処理の一例をフローチャートにして示す。図３によりデータ送信方法が説明されている。ステップ（以下、ステップを省略）Ｓ１～Ｓ３は、クラウド通信アプリケーション７２、車両内通信アプリケーション７３のいずれかが実行する。Ｓ４、Ｓ５は、暗号化アプリケーション７４が実行する。Ｓ６～Ｓ８はＵＩアプリケーション８３が実行する。

[0048] Ｓ１ではトリガ信号を取得する。トリガ信号は、クラウド通信アプリケーション７２であれば、たとえば、クラウドサーバに記憶された情報を取得する指示信号である。車両内通信アプリケーション７３であれば、トリガ信号は、たとえば車載機器の設定状態を示す信号である。

[0049] Ｓ２では、Ｓ１で取得したトリガ信号により定まる元データを生成する。元データは、ＵＩアプリケーション８３へ送信するデータであって、暗号化前のデータである。Ｓ３では、Ｓ２で生成した元データを暗号化アプリケー

ション７４へ送る。Ｓ４において、暗号化アプリケーション７４は元データを暗号化する。そして、Ｓ５において、暗号したデータをＵＩアプリケーション８３に送信する。

[0050] Ｓ６において、ＵＩアプリケーション８３は、暗号化アプリケーション７４が送信したデータを受信する。Ｓ７において、ＵＩアプリケーション８３は、受信したデータを復号する。Ｓ８では、Ｓ７で復号したデータにより定まる処理を実行する。

[0051] ［実施形態のまとめ］

以上、説明した本実施形態の車載システム１では、高オペレーティングシステム６１と汎用オペレーティングシステム６２は、同じプロセッサモジュール４１で動作する。同じプロセッサモジュール４１上で動作する複数のオペレーティングシステム間でデータを送受信する場合、通常、データは暗号化されずに送受信される。しかし、高オペレーティングシステム６１のセキュリティレベルが高くても、汎用オペレーティングシステム６２がハッキングされることで、高オペレーティングシステム６１側で動作するアプリケーションが扱うデータが流出する恐れや改ざんされる恐れがある。

[0052] そこで、本実施形態の車載システム１では、高ＯＳ側アプリケーション７０は、データを暗号化して汎用オペレーティングシステム６２側に送信する。これにより、汎用オペレーティングシステム６２がハッキングされた場合に、高ＯＳ側アプリケーション７０が扱うデータが流出したり改ざんされたりしてしまうことが抑制される。

[0053] また、本実施形態では、高ＯＳ側アプリケーション７０と通信し、ユーザインターフェース機構２０を制御するＵＩアプリケーション８３を、汎用オペレーティングシステム６２上で動作するアプリケーションとしている。これにより、高ＯＳ側アプリケーション７０と低ＯＳ側アプリケーション８０との間で調停や表示態様の統一性を維持することができる。しかも、クラウド通信アプリケーション７２と車両内通信アプリケーション７３からＵＩアプリケーション８３へ送信するデータは暗号化されている。よって、クラウ

ド通信アプリケーション７２と車両内通信アプリケーション７３からＵＩアプリケーション８３へデータを送信することにより、そのデータが流出したり、改ざんされたりしてしまうことも抑制される。

[0054] また、本実施形態では、高ＯＳ側アプリケーション７０としてクラウド通信アプリケーション７２を備えている。クラウド通信アプリケーション７２は、クラウドサーバから車両Ｃに関する種々の情報または車両Ｃの乗員に関する種々の情報の少なくとも一方を取得し、取得した情報をＵＩアプリケーション８３に提供することができる。車両Ｃに関する種々の情報または車両Ｃの乗員に関する種々の情報が流出したり改ざんされたりしてしまうと、車両の走行に支障をきたす以上の問題が生じる恐れもある。しかし、本実施形態では、クラウド通信アプリケーション７２がＵＩアプリケーション８３に送信するデータも暗号化される。よって、車両Ｃに関する種々の情報または車両Ｃの乗員に関する種々の情報が流出したり改ざんされたりしてしまうことが抑制される。

[0055] また、本実施形態では、暗号化アプリケーション７４が、クラウド通信アプリケーション７２、車両内通信アプリケーション７３からデータを取得して、取得したデータを暗号化する。そして、暗号化したデータをＵＩアプリケーション８３へ送信する。このようにすることで、複数の高ＯＳ側アプリケーション７０が個別にデータを暗号化するよりも、高ＯＳ側アプリケーション７０全体のプログラムを小さくできる。

[0056] 以上、実施形態を説明したが、開示した技術は上述の実施形態に限定されるものではなく、次の変形例も開示した範囲に含まれ、さらに、下記以外にも要旨を逸脱しない範囲内で種々変更して実施できる。なお、以下の説明において、それまでに使用した符号と同一番号の符号を有する要素は、特に言及する場合を除き、それ以前の実施形態における同一符号の要素と同一である。また、構成の一部のみを説明している場合、構成の他の部分については先に説明した実施形態を適用できる。

[0057] ＜変形例１＞

たとえば、実施形態では、１つのコンピュータ４０が備える１つのプロセッサモジュール４１が、高オペレーティングシステム６１と汎用オペレーティングシステム６２を並列に実行していた。しかし、これに限られず、１つのコンピュータが複数のプロセッサモジュールを備え、高オペレーティングシステム６１を実行するプロセッサモジュールと汎用オペレーティングシステム６２を実行するプロセッサモジュールが異なっていてもよい。

[0058] また、複数のコンピュータを備え、各コンピュータが有線接続されており、高オペレーティングシステム６１を実行するコンピュータと、汎用オペレーティングシステム６２を実行するコンピュータが別のコンピュータになっていてもよい。この場合、高ＯＳ側アプリケーション７０と低ＯＳ側通信アプリケーションであるＵＩアプリケーション８３との間は、有線通信によりデータ通信が行われる。

[0059] ＜変形例２＞

実施形態では、クラウド通信アプリケーション７２、車両内通信アプリケーション７３が作成したデータを暗号化する暗号化アプリケーション７４を備えていた。しかし、クラウド通信アプリケーション７２、車両内通信アプリケーション７３がそれぞれ、データを暗号化してＵＩアプリケーション８３に送信してもよい。

[0060] ＜変形例３＞

実施形態では、低ＯＳ側通信アプリケーションとして、ユーザインターフェース機構２０を制御するＵＩアプリケーション８３を備えていた。しかし、低ＯＳ側通信アプリケーションは、高ＯＳ側アプリケーション７０と通信する機能を備えていればよく、ユーザインターフェース機構２０を制御する機能以外の機能を備えたアプリケーションでもよい。

[0061] ＜変形例４＞

実施形態では、高ＯＳ側アプリケーション７０からＵＩアプリケーション８３へ送信するデータが暗号化されていた。これに加えて、ＵＩアプリケーション８３から高ＯＳ側アプリケーション７０へ送信するデータが暗号化さ

れていてもよい。

[0062] ＜変形例５＞

実施形態では、メータアプリケーション７１は、データを暗号化せずに、ＵＩアプリケーション８３に送信していた。しかし、メータアプリケーション７１もデータを暗号化してＵＩアプリケーション８３に送信してもよい。この場合、メータアプリケーション７１がデータを暗号化すればよい。あるいは、第１オペレーティングシステム６１ａ上で動作する暗号化アプリケーションを設けてもよい。

請求の範囲

[請求項1] 相互にセキュリティレベルが異なる複数のオペレーティングシステムを実行する演算装置であって、

複数の前記オペレーティングシステムのうちの相対的にセキュリティレベルが低いオペレーティングシステムを低オペレーティングシステム（６２）とし、

複数の前記オペレーティングシステムのうち、前記低オペレーティングシステムよりもセキュリティレベルが高いオペレーティングシステムを高オペレーティングシステム（６１）としたとき、

前記高オペレーティングシステム上で動作するアプリケーションソフトウェアである少なくとも１つの高ＯＳ側アプリケーション（７０）と、

前記低オペレーティングシステム上で動作するアプリケーションソフトウェアであって、前記高ＯＳ側アプリケーションと通信する低ＯＳ側通信アプリケーション（８３）とを備え、

前記高ＯＳ側アプリケーションと前記低ＯＳ側通信アプリケーションとの間は、チップ内アプリケーション通信または有線通信によりデータ通信が行われ、

少なくとも１つの前記高ＯＳ側アプリケーションから前記低ＯＳ側通信アプリケーションへ送信されるデータは暗号化されている、演算装置。

[請求項2] コンピュータ（４０）を備え、

前記高オペレーティングシステムおよび前記低オペレーティングシステムは、前記コンピュータが並列に実行する、請求項１に記載の演算装置。

[請求項3] 前記コンピュータは少なくとも１つのプロセッサ（４１）を備え、

前記高オペレーティングシステムおよび前記低オペレーティングシステムは、同じ前記プロセッサが実行する、請求項２に記載の演算装

置。

[請求項4] 前記低ＯＳ側通信アプリケーションは、ユーザインターフェース機構（２０）を制御するアプリケーションである、請求項１～３のいずれか１項に記載の演算装置。

[請求項5] 前記演算装置は車両（Ｃ）で使用され、

前記高ＯＳ側アプリケーションは、前記車両に関する情報または前記車両の乗員に関する情報の少なくとも一方を示すデータを、前記低ＯＳ側通信アプリケーションを介して前記ユーザインターフェース機構へ送信する、請求項４に記載の演算装置。

[請求項6] 前記高ＯＳ側アプリケーションとして、

前記低ＯＳ側通信アプリケーションへ送信する元データを作成する複数の元データ作成アプリケーション（７２、７３）と、

複数の前記元データ作成アプリケーションから前記元データを取得して、取得した元データを暗号化したデータを、前記低ＯＳ側通信アプリケーションへ送信する暗号化アプリケーション（７４）とを備える、請求項１～５のいずれか１項に記載の演算装置。

[請求項7] 相互にセキュリティレベルが異なる複数のオペレーティングシステムのうちの相対的にセキュリティレベルが低いオペレーティングシステムを低オペレーティングシステム（６２）とし、

複数の前記オペレーティングシステムのうち、前記低オペレーティングシステムよりもセキュリティレベルが高いオペレーティングシステムを高オペレーティングシステム（６１）としたとき、

前記高オペレーティングシステム上で動作するアプリケーションソフトウェアである少なくとも１つの高ＯＳ側アプリケーション（７０）から、前記低オペレーティングシステム上で動作するアプリケーションソフトウェアである低ＯＳ側通信アプリケーション（８３）へデータを送信するデータ送信方法であって、

前記高ＯＳ側アプリケーションと前記低ＯＳ側通信アプリケーショ

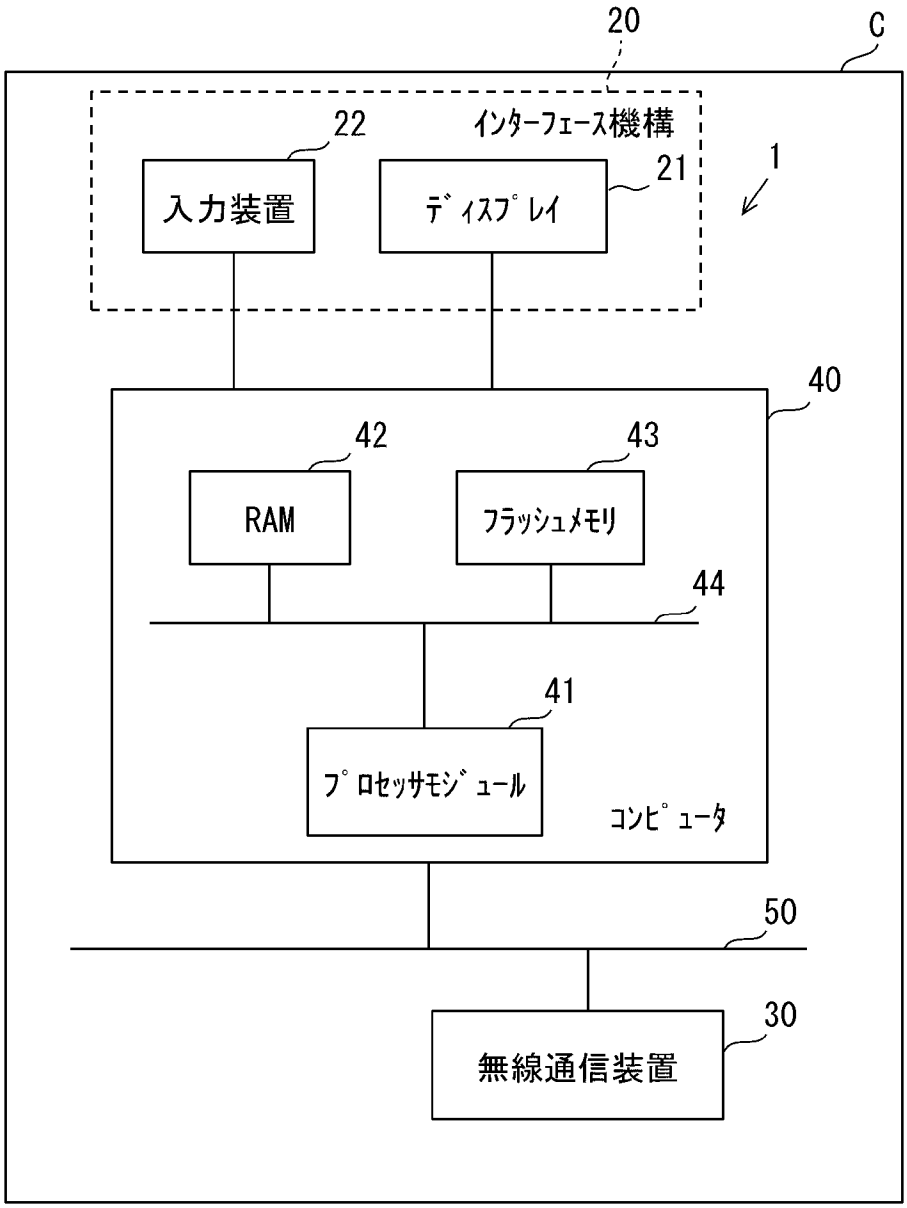
ンとの間は、チップ内アプリケーション通信または有線通信によりデータ通信が行われ、

少なくとも１つの前記高ＯＳ側アプリケーションが前記低ＯＳ側通信アプリケーションへ送信する元データを生成し（Ｓ２）、

生成した元データを暗号化したデータを前記低ＯＳ側通信アプリケーションへ送信する（Ｓ４）、データ送信方法。

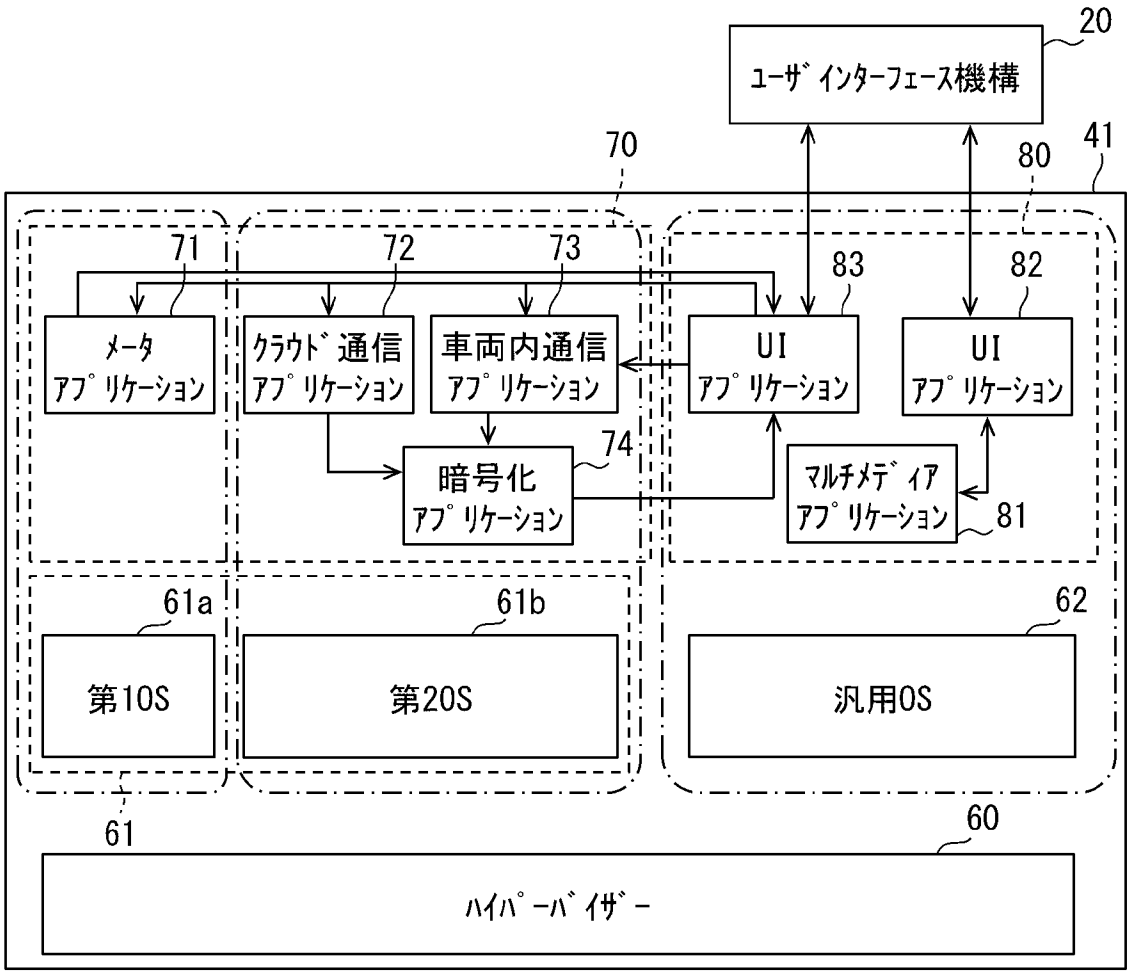
[図1]

図1


20
C
22
インターフェース機構
入力装置
21
ディスプレイ
1
40
42
43
RAM
フラッシュメモリ
44
41
プロセッサモジュール
コンピュータ
50
30
無線通信装置

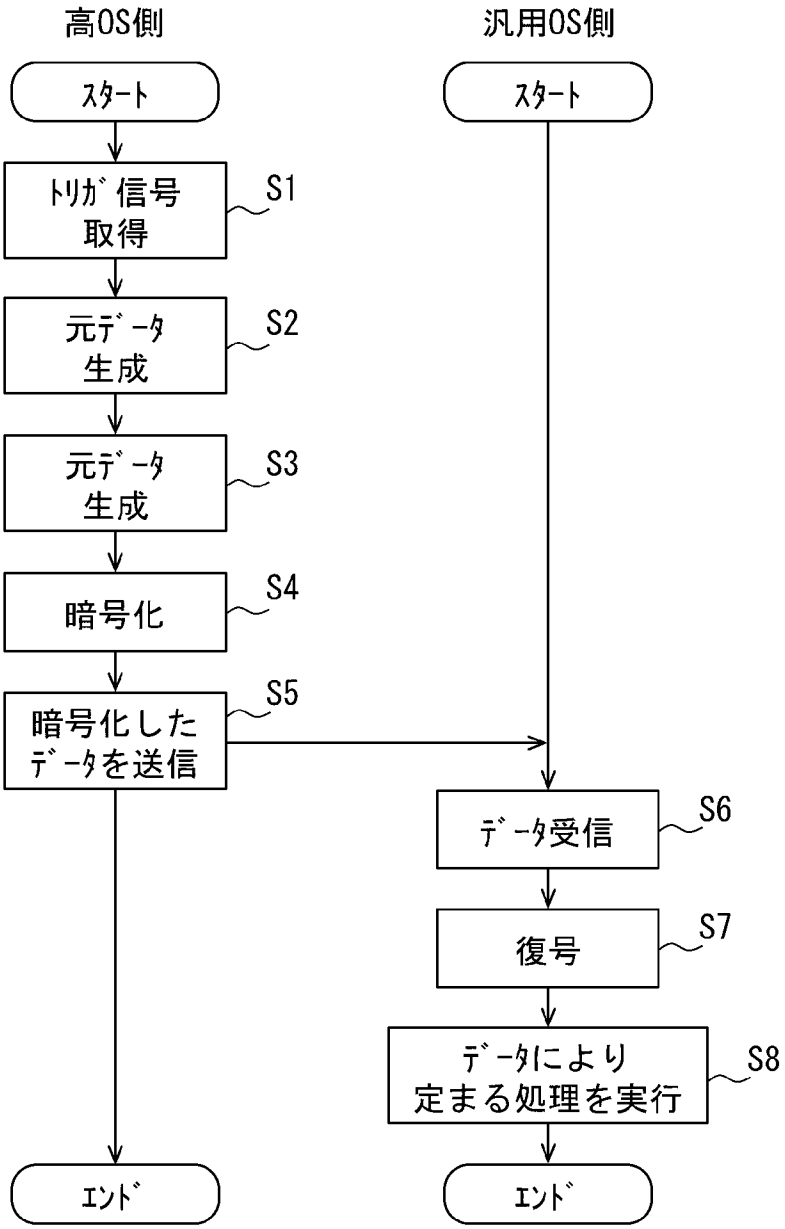
[図2]

図2


20
ユーザ インターフェース機構
70
80
41
71
72
73
83
82
メータ アプリケーション
クラウド 通信 アプリケーション
車両内通信 アプリケーション
UI アプリケーション
UI アプリケーション
74
暗号化 アプリケーション
マルチメディア アプリケーション
81
61a
61b
62
第1OS
第2OS
汎用OS
61
60
ハイパーバイザー

[図3]

図3


高OS側
汎用OS側
ｽﾀｰﾄ
ﾄﾘｶﾞ信号
取得
S1
元ﾃﾞｰﾀ
生成
S2
元ﾃﾞｰﾀ
生成
S3
暗号化
S4
暗号化した
ﾃﾞｰﾀを送信
S5
ｽﾀｰﾄ
ﾃﾞｰﾀ受信
S6
復号
S7
ﾃﾞｰﾀにより
定まる処理を実行
S8
ｴﾝﾄﾞ
ｴﾝﾄﾞ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/023640

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/60(2013.01)i
FI: G06F21/60360, G06F21/60320

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)
Int.Cl. G06F21/60

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
X Y	WO 2018/008605 A1 (SELTECH CORPORATION) 11.01.2018 (2018-01-11), paragraphs [0018]-[0034], fig. 1, 2	1, 4-7 2-3
Y	JP 2019-66995 A (SELTECH CORPORATION) 25.04.2019 (2019-04-25), paragraphs [0015], [0024], fig. 1	2-3
A	WO 2019/012956 A1 (SELTECH CORPORATION) 17.01.2019 (2019-01-17)	1-7
A	WO 2011/074168 A1 (PANASONIC CORPORATION) 23.06.2011 (2011-06-23)	1-7

☐ 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
09.09.2020	24.09.2020

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/023640

WO 2018/008605 A1	11.01.2018	JP 2018-85135 A JP 2018-85136 A
JP 2019-66995 A	25.04.2019	(Family: none)
WO 2019/012956 A1	17.01.2019	(Family: none)
WO 2011/074168 A1	23.06.2011	US 2011/0289294 A1 EP 2515239 A1

国際調査報告

国際出願番号
PCT/JP2020/023640

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/60(2013.01)i
FI: G06F21/60 360; G06F21/60 320

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））

G06F21/60

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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
X	WO 2018/008605 A1 (株式会社ＳＥＬＴＥＣＨ) 11.01.2018 (2018-01-11) [0018]-[0034], 図1-2	1,4-7
Y	[0018]-[0034], 図1-2	2-3
Y	JP 2019-66995 A (株式会社ＳＥＬＴＥＣＨ) 25.04.2019 (2019-04-25) [0015], [0024], 図1	2-3
A	WO 2019/012956 A1 (株式会社ＳＥＬＴＥＣＨ) 17.01.2019 (2019-01-17)	1-7
A	WO 2011/074168 A1 (パナソニック株式会社) 23.06.2011 (2011-06-23)	1-7

☐ 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抵触するものではなく、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	国際調査報告の発送日
09.09.2020	24.09.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
岸野　徹 5S 3983
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/023640

引用文献	公表日	パテントファミリー文献	公表日
WO 2018/008605 A1	11.01.2018	JP 2018-85135 A	
		JP 2018-85136 A	
JP 2019-66995 A	25.04.2019	（ファミリーなし）	
WO 2019/012956 A1	17.01.2019	（ファミリーなし）	
WO 2011/074168 A1	23.06.2011	US 2011/0289294 A1	
		EP 2515239 A1	