

(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
2025年3月20日(20.03.2025)



(10) 国際公開番号

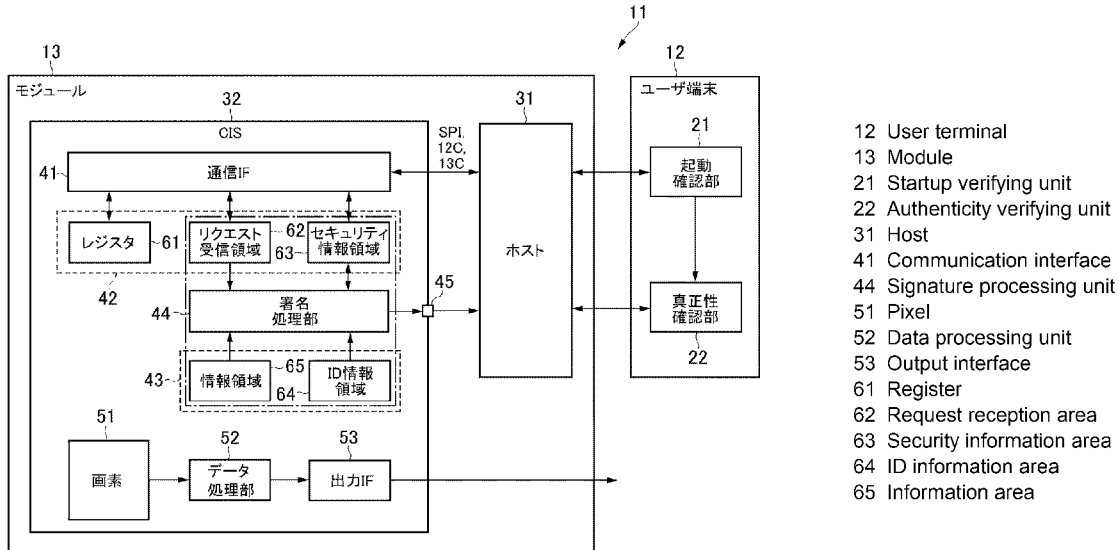
WO 2025/057714 A1

- (51) 国際特許分類:
G06F 21/73 (2013.01) H04L 9/10 (2006.01) 神奈川県厚木市旭町四丁目14番1号 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2024/030366 (72) 発明者: 馬原 久美子 (MAHARA Kumiko);
〒2430014 神奈川県厚木市旭町四丁目14番1号 ソニーセミコンダクタソリューションズ株式会社内 Kanagawa (JP).
- (22) 国際出願日: 2024年8月27日(27.08.2024)
- (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 2023-149028 2023年9月14日(14.09.2023) JP
- (74) 代理人: 西川 孝, 外 (NISHIKAWA Takashi et al.); 〒1700013 東京都豊島区東池袋3丁目9番10号 池袋F Nビル4階 Tokyo (JP).
- (71) 出願人: ソニーセミコンダクタソリューションズ株式会社 (SONY SEMICONDUCTOR SOLUTIONS CORPORATION) [JP/JP]; 〒2430014
- (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) Title: SEMICONDUCTOR CHIP, COMMUNICATION METHOD, AND COMMUNICATION SYSTEM

(54) 発明の名称: 半導体チップ、通信方法、および通信システム

[図1]



(57) Abstract: The present disclosure relates to a semiconductor chip, a communication method, and a communication system that enable reliable management of the authenticity of semiconductor chips. A communication interface communicates with a host in accordance with a predetermined communication standard, and a non-rewritable storage unit stores ID information in a non-rewritable state at the time of shipment. Then, in response to a request from an external terminal via the host, the ID information stored in the non-rewritable storage unit is output from the communication interface. The present technology can be applied, for example, to communication systems that verify the authenticity of CMOS image

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

sensors.

(57) 要約: 本開示は、半導体チップの真正性の管理を確実に行うことができるようにする半導体チップ、通信方法、および通信システムに関する。通信インタフェースは、ホストとの間で、所定の通信規格に従って通信を行い、書き換え不可記憶部は、出荷時には書き換えることが不可となる状態でID情報を記憶する。そして、ホストを介した外部の端末からのリクエストに応じて、書き換え不可記憶部に記憶されているID情報が通信インタフェースから出力される。本技術は、例えば、CMOSイメージセンサの真正性を確認する通信システムに適用できる。

明 細 書

発明の名称：半導体チップ、通信方法、および通信システム

技術分野

[0001] 本開示は、半導体チップ、通信方法、および通信システムに関し、特に、半導体チップの真正性の管理を確実に行うことができるようにした半導体チップ、通信方法、および通信システムに関する。

背景技術

[0002] 近年、CMOS (Complementary Metal-Oxide-Semiconductor) イメージセンサなどの半導体チップを含む様々な部品のトレーサビリティの必要性が強く求められている。例えば、CMOSイメージセンサでは、CMOSイメージセンサ自体やCMOSイメージセンサの製造に関わる製造環境および材料など、市場が求める情報が紐づけられるような機能が必要とされている。

[0003] 従来、特許文献1で開示されているように、イメージセンサおよびホスト（アプリケーションプロセッサ）の間で安全性の高い通信を行う技術が提案されている。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第2022/050057号

発明の概要

発明が解決しようとする課題

[0005] ところで、従来の技術では、イメージセンサと、イメージセンサに直接的に接続されるホストとの間でセキュリティを前提とした通信を行うことができるのに対し、イメージセンサと、外部のユーザ端末との間でセキュリティを前提とした通信を行うことはできなかった。そのため、イメージセンサが保持している情報が正しいことをホストが確認することはできても、イメージセンサが保持している情報が正しいことを外部のユーザ端末は確認することができず、例えば、外部のユーザ端末でイメージセンサの真正性を管理す

ることは困難であった。

[0006] 本開示は、このような状況に鑑みてなされたものであり、半導体チップの真正性の管理を確実に行うことができるようにするものである。

課題を解決するための手段

[0007] 本開示の一側面の半導体チップは、ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、出荷時には書き換えることが不可となる状態でＩＤ情報を記憶する書き換え不可記憶部とを備え、前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ＩＤ情報を前記通信インタフェースから出力する。

[0008] 本開示の一側面の通信方法は、半導体チップが、ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、出荷時には書き換えることが不可となる状態でＩＤ情報を記憶する書き換え不可記憶部とを備え、前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ＩＤ情報を前記通信インタフェースから出力することを含む。

[0009] 本開示の一側面の通信システムは、ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、出荷時には書き換えることが不可となる状態でＩＤ情報を記憶する書き換え不可記憶部とを有する半導体チップと、前記ホストを介してリクエストを送信する外部の端末とを備える通信システムであって、前記リクエストに応じて、前記書き換え不可記憶部に記憶されている前記ＩＤ情報を前記通信インタフェースから出力する。

[0010] 本開示の一側面においては、ホストとの間で、所定の通信規格に従って通信が通信インタフェースによって行われ、出荷時には書き換えることが不可となる状態でＩＤ情報が書き換え不可記憶部に記憶される。そして、ホストを介した外部の端末からのリクエストに応じて、書き換え不可記憶部に記憶されているＩＤ情報が通信インタフェースから出力される。

図面の簡単な説明

[0011] [図1]本技術を適用した通信システムの第１の実施の形態の構成例を示すブロ

ック図である。

[図2]製品IDおよび分類IDの一例を示す図である。

[図3]IF機能について説明する図である。

[図4]本技術を適用した通信システムの第2の実施の形態の構成例を示すブロック図である。

[図5]ID情報を選択する第1の選択方法の一例について説明する図である。

[図6]ID情報を選択する第2の選択方法の一例について説明する図である。

[図7]通信処理の一例について説明するシーケンス図である。

[図8]本技術を適用した通信システムの第3の実施の形態の構成例を示すブロック図である。

[図9]署名データが挿入される画像データのフォーマットの一例を示す図である。

[図10]ID情報の利用例について説明する図である。

[図11]本技術を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

発明を実施するための形態

[0012] 以下、本技術を適用した具体的な実施の形態について、図面を参照しながら詳細に説明する。

[0013] <通信システムの第1の構成例>

図1は、本技術を適用した通信システムの第1の実施の形態の構成例を示すブロック図である。

[0014] 図1に示す通信システム11は、ユーザ端末12がモジュール13と通信を行うことによって、モジュール13に搭載されたCMOSイメージセンサ32の真正性の管理を行うことができる。

[0015] ユーザ端末12は、起動確認部21および真正性確認部22を備えて構成され、例えば、モジュール13が搭載された電子機器などの最終製品を使用するユーザが、モジュール13が備えるCMOSイメージセンサ32の真正性を確認する際に用いられる。また、ユーザ端末12は、モジュール13内に設

けられるホスト 3 1 を介して、CMOSイメージセンサ 3 2 との間で、共通鍵、公開鍵、秘密鍵、またはセッション鍵を用いて暗号化されたデータの送受信を行うことができる。

[0016] 起動確認部 2 1 は、モジュール 1 3 のホスト 3 1 と通信を行って、CMOSイメージセンサ 3 2 が起動していることの確認を要求する起動確認リクエストを送信し、CMOSイメージセンサ 3 2 が起動していることを通知する起動通知レスポンスを受信する。そして、起動確認部 2 1 は、CMOSイメージセンサ 3 2 が起動していることを確認すると、そのことを真正性確認部 2 2 に通知する。

[0017] 真正性確認部 2 2 は、CMOSイメージセンサ 3 2 が起動していることが起動確認部 2 1 によって確認されると、CMOSイメージセンサ 3 2 の真正性の証明を要求するセンサ真正性証明リクエストをモジュール 1 3 のホスト 3 1 に送信する。そして、真正性確認部 2 2 は、CMOSイメージセンサ 3 2 においてセンサ真正性証明処理が行われた結果としてホスト 3 1 から送信されてくるセンサ真正性証明レスポンスを受信する。

[0018] モジュール 1 3 は、ホスト 3 1 およびCMOSイメージセンサ 3 2 を備えて構成される。

[0019] ホスト 3 1 は、ユーザ端末 1 2 およびCMOSイメージセンサ 3 2 との間で、それぞれ通信を行うことができる。例えば、ホスト 3 1 は、CMOSイメージセンサ 3 2 の通信 I F 4 1 との間では、SPI (Serial Peripheral Interface) や、I2C (Inter-Integrated Circuit) 、I3C (Improved Inter Integrated Circuit) などの通信規格に従って通信を行う。ホスト 3 1 は、CMOSイメージセンサ 3 2 の起動を確認する機能（例えば、WDT (Watch Dog Timer) の開始タイミングを知るための機能）や、CMOSイメージセンサ 3 2 の真正性の証明を受け付けるための機能（例えば、センサ真正性証明リクエストや、真正性の証明のために必要なランダムデータなどを受け取る機能）などを備えている。

[0020] 例えば、ホスト 3 1 は、起動確認部 2 1 から送信されてくる起動確認リク

エストを受信した場合に、CMOSイメージセンサ32が起動していなかったとき、CMOSイメージセンサ32の電源を投入して起動シーケンスを実行させることができる。そして、ホスト31は、CMOSイメージセンサ32を起動させた後、または、CMOSイメージセンサ32が起動していた場合、起動通知レスポンスを起動確認部21に送信する。

[0021] 例えば、ホスト31は、真正性確認部22から送信されてくるセンサ真正性証明リクエストを受信すると、CMOSイメージセンサ32の定めるシーケンスに沿ってレジスタ通信を行うことができる。ここで、ホスト31は、CMOSイメージセンサ32のレジスタに対するライトまたはリードのみを基本的に行うことができればよく、一般的なホストが備える機能を用いてCMOSイメージセンサ32と通信を行うことが可能である。そして、ホスト31とCMOSイメージセンサ32との間の通信自体にセキュリティ機能が必要とされることはない。例えば、通信システム11においてセキュリティ機能が必要なのは、署名を行うCMOSイメージセンサ32と、その署名の検証を行うユーザ端末12であるので、ホスト31とCMOSイメージセンサ32との間でセキュリティ機能を搭載していても、そのセキュリティ機能が準備できていない状態（例えば、起動直後の状態など）でも動作することができる。

[0022] CMOSイメージセンサ32は、通信IF（Interface）41、書き換え可能記憶部42、書き換え不可記憶部43、署名処理部44、および処理ステート出力端子45を備えて構成される。さらに、CMOSイメージセンサ32は、画素値を出力する画素51、画素51から出力される画素値により構成される画像データに対するデータ処理を施すデータ処理部52、および、データ処理部52でデータ処理が施された画像データを所定のフォーマットで外部に出力する出力IF53を備えている。

[0023] 通信IF41は、ホスト31との間で、SPIや、I2C、I3Cなどの通信規格に従って通信を行うことができ、ホスト31から送信されてきたデータを書き換え可能記憶部42に書き込む。

[0024] 書き換え可能記憶部42は、例えば、不揮発メモリなどにより構成され、

通信 I F 4 1 を介して書き込まれるデータを記憶する。例えば、書き換え可能記憶部 4 2 には、CMOSイメージセンサ 3 2 に対する各種の設定を記憶するレジスタ 6 1、ユーザ端末 1 2 から送信されてきたセンサ真正性証明リクエストなどを記憶するリクエスト受信領域 6 2、および、CMOSイメージセンサ 3 2 から出力されるセンサ真正性証明レスポンスなどを記憶するセキュリティ情報領域 6 3 が設けられる。

[0025] 書き換え不可記憶部 4 3 は、例えば、CMOSイメージセンサ 3 2 の出荷時には書き換えることが不可となるヒューズ型PROM (Programmable ROM) により構成され、CMOSイメージセンサ 3 2 が出荷された後、書き換えを禁止すべきデータを記憶する。例えば、書き換え不可記憶部 4 3 には、ID (Identification) 情報を記憶するID情報領域 6 4、および、ID情報以外の情報を記憶する情報領域 6 5 が設けられる。

[0026] 署名処理部 4 4 は、ユーザ端末 1 2 から送信されてきたセンサ真正性証明リクエストに応じて、書き換え不可記憶部 4 3 のID情報領域 6 4 から読み出したID情報を共通鍵または公開鍵を用いて暗号化することによって署名を施す署名処理を行って、ID情報に署名が施された署名データを、セキュリティ情報領域 6 3 に記憶させる。セキュリティ情報領域 6 3 に記憶された署名データは、真正性確認部 2 2 において、署名処理部 4 4 が用いた共通鍵または公開鍵に対応する秘密鍵を用いて復号することができる。一方、ユーザ端末 1 2 から送信されてくるセンサ真正性証明リクエストは共通鍵または公開鍵（第1の鍵）によって暗号化されており、署名処理部 4 4 は、暗号化されているセンサ真正性証明リクエストを、その暗号化に用いられた共通鍵または公開鍵に対応する秘密鍵（第2の鍵）を用いて復号することができる。さらに、署名処理部 4 4 は、センサ真正性証明処理を開始または終了を示す処理ステートを、処理ステート出力端子 4 5 を介してホスト 3 1 に出力する。なお、ID情報に適用される暗号化方式やセンサ真正性証明リクエストに適用される暗号化方式は、上記に限定されず、例えばセッション鍵暗号方式が用いられてもよい。

[0027] ここで、書き換え不可記憶部43は、例えば、CMOSイメージセンサ32の実装時に情報を反映させたり、CMOSイメージセンサ32の製造時に情報を書き込んだりした後、ヒューズを切断することによって情報の書き換えができない状態となるように構成される。従って、CMOSイメージセンサ32の出荷時には、書き換え不可記憶部43に書き込まれた情報を書き換え不可とすることができる。

[0028] 書き換え不可記憶部43の情報領域65に記憶されるデータには、例えば、後述するクラス情報や、ユーザ端末12などからの生成条件紐づけのためのデータ、出荷時におけるCMOSイメージセンサ32の状態を示す出荷ステータス、CMOSイメージセンサ32の販売先を示す出荷先データなどが含まれる。これらのデータは、個体評価結果や購入先などが決定した時点で書き込むことができるため、ヒューズを切断することによって情報の書き換えが不可となる書き換え不可記憶部43に書き込んだ後、CMOSイメージセンサ32が出荷される。

[0029] 書き換え不可記憶部43のID情報領域64に記憶されるID情報として、製品IDおよび分類IDが少なくとも用いられる。

[0030] 製品IDは、CMOSイメージセンサ32としての製品を識別するためのIDである。即ち、製品IDは、CMOSイメージセンサ32の製品共通の情報に対するIDであって、CMOSイメージセンサ32を製造したメーカ（以下、CISメーカと称する）に関する情報が含まれている。

[0031] 分類IDは、CMOSイメージセンサ32の製造環境や材料などに紐づけられるID（または複数のIDからなるID群）である。例えば、複数のチップが積層された積層型のCMOSイメージセンサ32では、それぞれのチップが異なるファウンドリで設計／製造されることがあり、CMOSイメージセンサ32の分類IDとして、それらのファウンドリに紐づけられた複数のIDが用いられる。その他、分類IDには、市場で求められる各種の情報が紐づけられるようにしてもよい。

[0032] なお、ID情報には、CMOSイメージセンサ32を個別に識別するための個

体識別 I D が含まれていてもよい。例えば、I D 情報に個体識別 I D を含めることは必須ではないが、I D 情報に個体識別 I D を含めることによってセキュリティを高めることができる。

[0033] I D 情報に含まれる製品 I D および分類 I D は、それぞれ発行元が異なるケースがあり、例えば、CIS メーカー、第三者機関、または、委託先（ファウンダリや、装置メーカー、材料メーカーなど）により発行される。なお、発行元に従って、製品 I D および分類 I D の出力を切り替えてもよい。

[0034] また、CIS メーカーにより発行される製品 I D および分類 I D を用いる場合、あるいは、CIS メーカーが製造環境などの情報もマージして第三者機関に新たに認証を受ける場合、製品 I D を製造環境や材料メーカーごとに変えることで、製造環境や材料メーカーなどの情報を製品 I D にまとめること、即ち、複数の分類 I D をマージすることができる。例えば、製品 I D に全ての分類 I D をマージしてもよいが、それぞれの分類 I D を分けることによって必要な情報だけを顧客が使用できるようにすることが好適である。

[0035] 図 2 には、I D 情報として用いられる製品 I D および分類 I D の一例が示されている。

[0036] 例えば、製品 I D は、製品共通の情報に対する I D であって、CIS メーカーにより発行されたものである。分類 I D a は、ファウンダリ情報に紐づけられる I D であって、ファウンダリにより発行されたものである。分類 I D b は、材料情報及び／または材料メーカー情報に紐づけられる I D であって、材料メーカーにより発行されたものである。

[0037] 製品 I D' は、製品共通の情報に対する I D であって、第三者機関により発行されたものである。分類 I D a' は、ファウンダリ情報に紐づけられる I D であって、第三者機関により発行されたものである。分類 I D b' は、材料情報及び／または材料メーカー情報に紐づけられる I D であって、第三者機関により発行されたものである。

[0038] 製品 I D'' は、製品共通の情報に対する I D であって、CIS メーカーまたは第三者機関により発行されたものである。分類 I D x は、ファウンダリ情報

や材料情報などの情報群を識別するためのIDであって、CISメーカまたは第三者機関により発行されたものである。つまり、サプライチェーンで必要な情報について分類IDをマージしてもよく、分類ID a' および分類ID b' をマージしたものが分類ID xとなる。さらに、製品IDに、全ての分類IDをマージしてもよいが、マージできない場合もある。

[0039] 例えば、複数のファウンドリでCMOSイメージセンサ32を設計／製造したり、CMOSイメージセンサ32に使用される材料が複数の材料メーカから提供されたりする場合、製品IDと複数の分類IDとを紐づけることで、CISメーカが開示した情報と照合して、ファウンドリや材料メーカなどの情報と紐づけることができる。そして、CISメーカは、紐づけられた複数の情報のうちの必要最低限の情報を、顧客や最終製品のユーザに開示する。このとき、開示内容は、顧客やユーザごとに異なるものとすることができる。

[0040] このように書き換え不可記憶部43のID情報領域64に記憶されている製品IDおよび分類IDが、真正性証明リクエストに応じてCMOSイメージセンサ32から出力されるID情報として用いられる。また、ID情報に付加して、情報領域65に記憶されている出荷ステータスおよび出荷先データを出力してもよい。

[0041] 図3を参照して、CMOSイメージセンサ32が備えるIF機能について説明する。

[0042] CMOSイメージセンサ32は、ID情報などをセキュアに出力するために、ホスト31との通信手段として、図3に示すようなレジスタIF（シーケンスを実現するために必要なIF機能（レジスタや通信可能なRAM領域など））を備えている。

[0043] 図3のAに示すように、CIS_AUT_REQは、ホスト31が真正性証明リクエストを書き込むレジスタIFである。CIS_AUT_REQDATAは、ホスト31がリクエストデータ（RB || Text1）を書き込むレジスタIFである。CIS_AUT_ACKDATAは、ホスト31がレスポンスデータ（TokenAB || CertA）を読み出すレジスタIFである。CIS_AUT_MODEは、センサ真正性証明処理で出力するID情報

を選択（出力モード選択）するためにホスト31が書き込むレジスタIFである。例えば、CIS_AUT_MODEが0の場合には、全てのID情報を出力することが選択され、CIS_AUT_MODEが0以外の場合には、製品や市場に依存したID情報を出力することが選択されるように設定することができる。

[0044] なお、CMOSイメージセンサ32が他のセキュリティのためのIF機能を備える場合、そのIF機能と共有して用いられる構成とすることができる。例えば、他のセキュリティ用のデータ領域をリクエストデータおよびレスポンスデータを書き込む領域として共有化して使用したり、セキュリティコマンドを拡張して真正性証明リクエストレジスタの代わりにコマンド拡張を行ったりしてもよい。

[0045] また、上述したように、処理ステート出力端子45を介して処理ステートをホスト31に出力する他、図3のBに示すように、真正性証明処理の実行中であることを示す1ビットの処理ステートをホスト31が受け取るようにレジスタIFを利用することができる。なお、他の機能とレジスタや信号を共有してもよい。

[0046] 以上のように通信システム11は構成されており、CMOSイメージセンサ32は、ホスト31を介したユーザ端末12からの真正性証明リクエストに応じて、書き換え不可記憶部43に記憶されているID情報をホスト31から出力することができる。そして、通信システム11では、CMOSイメージセンサ32から出力されるID情報に基づいて、ユーザ端末12においてCMOSイメージセンサ32の真正性の管理が行われることになる。

[0047] さらに、通信システム11では、ユーザ端末12と署名処理部44との間で、共通鍵または公開鍵を用いて暗号化したデータ（暗号化されたセンサ真正性証明リクエストや、ID情報に署名が施された署名データなど）の送受信を行うことができる。これにより、通信システム11では、CMOSイメージセンサ32に直接的に接続されていないユーザ端末12との間でセキュアに通信を行うことが可能となり、より確実に、CMOSイメージセンサ32の真正性の管理を行うことができる。

[0048] なお、通信システム 11 では、署名処理に必要となる署名処理部 44 を含むブロックは常に使用されるわけではないので、署名が必要なときにだけ起動するように CMOS イメージセンサ 32 を構成することができる。つまり、図 1 において一点鎖線で囲われた領域に含まれる各ブロック（署名処理部 44、リクエスト受信領域 62、セキュリティ情報領域 63、ID 情報領域 64、および情報領域 65）に対して、通常時には電源またはクロックの供給が停止される。そして、署名処理が行われるときのみ、例えば、ユーザ端末 12 から起動要求があった場合に起動用のレジスタ（CIS_AUT_ACTV）をオンにして、図 1 において一点鎖線で囲われた領域に含まれる各ブロックに対して、電源またはクロックの供給が行われるようにすることができる。

[0049] また、通信システム 11 では、ID 情報などの CMOS イメージセンサ 32 内の情報をセキュアに出力することができる。例えば、CMOS イメージセンサ 32 内の公開鍵ペアとその公開鍵の CA（Certificate Authority）認証書により、ユーザ端末 12 などのようにモジュール 13 外の相手に対して、CMOS イメージセンサ 32 のみが付けることのできる証明書を ID 情報に付加して出力する。

[0050] なお、通信システム 11 では、ユーザ端末 12 は、ホスト 31 と CMOS イメージセンサ 32 の通信 IF 41 とを介して、センサ真正性証明リクエストおよびセンサ真正性証明レスポンスの送受信を行うが、その際の通信を保護する必要はなく、簡易的なシーケンスでよい。つまり、通信システム 11 では、ホスト 31 などの CMOS イメージセンサ 32 と通信する機能を有するブロックを通して、モジュール 13 の外部から、一般的な規格で定められたシーケンスに従った通信が実現できればよい。

[0051] また、顧客の製造環境などで、CMOS イメージセンサ 32 の真正性の確認（真贋判定）を行うときには、簡易的な通信 IF 自身はセキュリティ機能を備える必要はなく、例えば、顧客の製造環境で用いられているパーソナルコンピュータなどを使用することができる。

[0052] <通信システムの第 2 の構成例>

図4は、本技術を適用した通信システムの第2の実施の形態の構成例を示すブロック図である。なお、図4に示す通信システム11Aにおいて、図1の通信システム11と共通するブロックについては、同一の符号を付し、その詳細な説明は省略する。

[0053] 即ち、通信システム11Aでは、ユーザ端末12およびホスト31は、図1の通信システム11と同様に構成されている。一方、通信システム11Aでは、CMOSイメージセンサ32Aが、情報出力選択部46を備えている点で、図1の通信システム11と異なる構成となっている。

[0054] 情報出力選択部46は、図3を参照して上述したCIS_AUT_MODEを参照して、CMOSイメージセンサ32Aから出力されるID情報を選択し、そのID情報をID情報領域64から読み出して署名処理部44に供給する。例えば、情報出力選択部46は、以下で説明するような第1乃至第3の選択方法いずれかを採用して、CMOSイメージセンサ32Aから出力されるID情報を選択することができる。

[0055] 情報出力選択部46がID情報を選択する第1の選択方法は、所定の製品IDおよび分類IDがID情報として登録された複数のテーブルを保持しておき、CIS_AUT_MODEに従って、どのテーブルを出力するのかを選択する方法である。

[0056] 例えば、第1の選択方法では、図5に示すような3つのテーブルが保持される。図5のAには、CISメーカーにより発行された製品ID、ファウンダリにより発行された分類IDa、および、材料メーカーにより発行された分類IDbが、ID情報として登録されたテーブルが示されている。図5のBには、第三者機関により発行された製品ID'、第三者機関により発行された分類IDa'、および、第三者機関により発行された分類IDb'が、ID情報として登録されたテーブルが示されている。図5のCには、CISメーカーまたは第三者機関により発行された製品ID''、および、CISメーカーまたは第三者機関により発行された分類IDxが、ID情報として登録されたテーブルが示されている。

- [0057] そして、情報出力選択部46は、CIS_AUT_MODE=0である場合には、図5のAに示したテーブルを選択し、CIS_AUT_MODE=1である場合には、図5のBに示したテーブルを選択し、CIS_AUT_MODE=2である場合には、図5のCに示したテーブルを選択する。
- [0058] 情報出力選択部46がID情報を選択する第2の選択方法は、CIS_AUT_MODEのビットごとに出力するID情報を割り当てることで、どのID情報を出力するのかを選択する方法である。
- [0059] 例えば、第2の選択方法では、図6に示すように、CIS_AUT_MODEのビットごとに出力するID情報を割り当てることができる。例えば、CIS_AUT_MODEの0ビット目には、CISメーカーにより発行された製品IDを割り当て、CIS_AUT_MODEの1ビット目には、ファウンダリにより発行された分類IDaを割り当て、CIS_AUT_MODEの2ビット目には、材料メーカーにより発行された分類IDbを割り当て、CIS_AUT_MODEの3ビット目には、第三者機関により発行された製品ID'を割り当て、CIS_AUT_MODEの4ビット目には、第三者機関により発行された分類IDa'を割り当て、CIS_AUT_MODEの5ビット目には、第三者機関により発行された分類IDb'を割り当て、CIS_AUT_MODEの6ビット目には、CISメーカーまたは第三者機関により発行された製品ID''を割り当て、CIS_AUT_MODEの7ビット目には、CISメーカーまたは第三者機関により発行された分類IDxを割り当てることができる。
- [0060] そして、情報出力選択部46は、CIS_AUT_MODEの各ビットが1である場合には、そのビットに割り当てられたID情報を出力し、CIS_AUT_MODEの各ビットが0である場合には、そのビットに割り当てられたID情報を出力しない。具体的には、CIS_AUT_MODEの0ビット目が1である場合には製品IDが出力され、CIS_AUT_MODEの3ビット目が0である場合には製品ID'は出力されない。
- [0061] 情報出力選択部46がID情報を選択する第3の選択方法は、第1の選択方法と同様にテーブルを選択した後、そのテーブル内の情報からさらに出力する情報を選択する方法である。例えば、第1の選択方法と同様にテーブル

を選択した後、そのテーブル内のどの情報を入力するかを、別のレジスタまたはヒューズなどで選択することができる。例えば、分類IDは出力せずに、製品IDのみを入力するような選択を行うことができる。

[0062] もちろん、情報出力選択部46は、上述したような第1乃至第3の選択方法以外の選択方法で、CMOSイメージセンサ32Aから出力されるID情報を選択してもよい。

[0063] さらに、CMOSイメージセンサ32Aは、ID情報の出力時に、ID情報以外に開示範囲を指定するクラス情報を、ID情報とともに出力することができる。例えば、クラス情報では、CMOSイメージセンサ32Aから出力されるID情報の開示レベルの設定として、ユーザが第三者機関に問い合わせの際の開示レベルまで含めて署名することで、開示情報を制限することができる。

[0064] そして、ユーザは、証明書などの保証情報を保持する第三者機関に、開示範囲を示すクラス情報をID情報と一緒に出力することができる。このとき、クラス情報にも署名処理部44によって署名を施すことにより、クラス情報を偽造できない形で出力することができ、第三者機関を通じて提出する情報への制約を行うことが可能となる。

[0065] 図7に示すシーケンス図を参照して、通信システム11Aにおいて行われる通信処理の一例について説明する。

[0066] 例えば、CMOSイメージセンサ32Aの起動の確認が行われた後、ステップS11において、ユーザ端末12およびホスト31の間のインタフェースに従った通信が行われ、真正性確認部22は、CMOSイメージセンサ32Aの真正性の証明を要求するセンサ真正性証明リクエストを送信する。センサ真正性証明リクエストには、セキュリティ情報領域63 (CIS_AUT_REQDATA) に書き込まれるリクエストデータ (データ[R_B || Text1]) が含まれている。そして、ホスト31が、センサ真正性証明リクエストの受信を完了すると処理はステップS12に進む。

[0067] ステップS12において、ホスト31は、通信IF41との間で通信を行

って、書き換え可能記憶部42のセキュリティ情報領域63 (CIS_AUT_REQDATA) に、センサ真正性証明リクエストに含まれていたリクエストデータ (データ[R_B || Text1]) を書き込むデータ書き込みを行う。

[0068] ステップS13において、ホスト31は、通信IF41との間で通信を行って、書き換え可能記憶部42のリクエスト受信領域62にCIS_AUT_MODEを書き込み、ユーザ端末12に対して開示すべき開示領域を設定する開示領域設定を行う。

[0069] ステップS14において、ホスト31は、通信IF41との間で通信を行って、書き換え可能記憶部42のリクエスト受信領域62 (CIS_AUT_REQ) に真正性証明リクエストを書き込み、ID情報に署名が施された署名データの生成を要求する署名データ生成要求を行う。

[0070] そして、ステップS12乃至S14の処理が完了すると、処理はステップS15に進む。

[0071] ステップS15において、署名処理部44は、処理ステート出力端子45を介して、センサ真正性証明処理の開始を示す処理ステートをホスト31に出力し、処理はステップS16に進む。

[0072] ステップS16において、CMOSイメージセンサ32Aではセンサ真正性証明処理が実行される。センサ真正性証明処理において、情報出力選択部46は、ステップS13でホスト31によりリクエスト受信領域62に書き込まれたCIS_AUT_MODEを参照して、CMOSイメージセンサ32Aから出力されるID情報を選択し、そのID情報をID情報領域64から読み出して署名処理部44に供給する。署名処理部44は、情報出力選択部46から供給されたID情報に対して署名を施し、ID情報に署名が施された署名データを、書き換え可能記憶部42のセキュリティ情報領域63に書き込む。これにより、センサ真正性証明処理が完了すると、処理はステップS17に進む。

[0073] ステップS17において、署名処理部44は、処理ステート出力端子45を介して、センサ真正性証明処理の終了を示す処理ステートをホスト31に出力し、処理はステップS18に進む。

- [0074] ステップS 1 8において、ホスト3 1は、通信 I F 4 1との間で通信を行って、書き換え可能記憶部4 2のセキュリティ情報領域6 3 (CIS_AUT_ACKDATA) に書き込まれている署名データ (データ[TokenAB || CertA]) を読み出すデータ読み出しを行う。
- [0075] ステップS 1 9において、ユーザ端末1 2およびホスト3 1の間のインタフェースに従った通信が行われ、ホスト3 1は、書き換え可能記憶部4 2のセキュリティ情報領域6 3 (CIS_AUT_ACKDATA) から読み出した署名データ (データ[TokenAB || CertA]) を、センサ真正性証明レスポンスとして送信する。そして、ユーザ端末1 2の真正性確認部2 2がセンサ真正性証明レスポンスを受信すると処理は終了される。
- [0076] 以上のように、通信システム1 1 Aでは、ユーザ端末1 2から送信されてくるデータを書き込み可能な通信領域を持つことで、ホスト3 1が、従来のレジスタ通信機能を通じてデータを送受信するだけで、ユーザ端末1 2およびCMOSイメージセンサ3 2 Aの間で、 I D情報に署名が施された署名データをやり取りすることができる。
- [0077] また、通信システム1 1 Aでは、ホスト3 1が、CMOSイメージセンサ3 2 Aから開示される I D情報を制限するレジスタまたはヒューズを持つことで、CMOSイメージセンサ3 2 A内の I D情報のうち、ホスト3 1が開示してよい I D情報のみを出力させることができる。例えば、レジスタの場合、ステップS 1 4で署名データ生成要求を行う前に、ステップS 1 3で開示領域設定が行われる。なお、ヒューズの場合、カメラなどの電子機器へのモジュール1 3の組み込み時に開示領域設定が行われるため、開示領域設定を行うステップS 1 3の処理はスキップすることができる。
- [0078] <通信システムの第3の構成例>

図8は、本技術を適用した通信システムの第3の実施の形態の構成例を示すブロック図である。なお、図8に示す通信システム1 1 Bにおいて、図1の通信システム1 1と共通するブロックについては、同一の符号を付し、その詳細な説明は省略する。

[0079] 即ち、通信システム 11 B では、ユーザ端末 12 およびホスト 31 は、図 1 の通信システム 11 と同様に構成されている。一方、通信システム 11 B では、CMOS イメージセンサ 32 B が、署名処理部 44 B および出力 I/F 53 B を備えている点で、図 1 の通信システム 11 と異なる構成となっている。

[0080] 署名処理部 44 B は、書き換え不可記憶部 43 の ID 情報領域 64 から読み出した ID 情報に対して署名を施す署名処理を行って、ID 情報に署名が施された署名データを出力 I/F 53 B に供給する。

[0081] 出力 I/F 53 B は、署名処理部 44 B から供給される署名データを、CMOS イメージセンサ 32 B から画像データを出力する際のフォーマットの所定個所に挿入して、画像データと署名データとを一緒に出力する。

[0082] 例えば、図 9 の A に示すように、SLVS-EC (Scalable Low Voltage Signaling with Embedded Clock) や MIPI (Mobile Industry Processor Interface) などでは、CMOS イメージセンサ 32 B の情報を画像データ (RAW データ) に付加するためのエンベデットデータ (EBD: Embedded Data) が設けられたフォーマットが採用される。出力 I/F 53 B は、このエンベデットデータの領域に署名データを挿入することができる。

[0083] または、CMOS イメージセンサ 32 B が、ホスト 31 との間の SLVS-EC のセキュリティフォーマットに対応している場合、図 9 の B に示すように、出力 I/F 53 B は、SLVS-EC のセキュリティ関連情報を出力する領域に署名データを挿入することができる。

[0084] 例えば、CMOS イメージセンサ 32 B が画像データの出力を停止しているときにもセンサ真正性証明処理を実行するために、通信 I/F 41 を介して署名データを出力するような構成とする必要がある。これに対し、CMOS イメージセンサ 32 B が画像データを出力している場合には、出力 I/F 53 B を介して、署名データを画像データに付加して出力することができる。そして、画像データに付加された署名データは、ホスト 31 を介してユーザ端末 12 へ出力することができる。

[0085] < ID 情報の利用例 >

図10を参照して、ID情報の利用例について説明する。

- [0086] 例えば、CISメーカーは、ファウンドリにより発行された分類IDa、材料メーカーにより発行された分類IDb、および、装置メーカーにより発行された分類IDcをID情報領域64に書き込んだCMOSイメージセンサ32を製造し、最終製品を製造する製造工場に出荷する。このとき、CISメーカーは、ファウンドリ、材料メーカー、および装置メーカーそれぞれからの情報や、それらのデータベースなどに基づいて要求を満たしていることを事前に確認し、設計、材料、および装置の調達を行う。
- [0087] また、ファウンドリ、材料メーカー、および装置メーカーは、第三者機関に対して、それぞれ分類IDa、分類IDb、および分類IDcの発行を依頼する。第三者機関は、分類IDa、分類IDb、および分類IDcに紐づける形で証明書を管理する。
- [0088] CMOSイメージセンサ32が搭載された電子機器などの最終製品が製造工場において製造され、ユーザは、最終製品を入手することができる。そして、ユーザは、ユーザ端末12を用いて、図7を参照して説明した通信処理を行って、CMOSイメージセンサ32からID情報（分類IDa、分類IDb、および分類IDc）を読み出して、第三者機関から必要な証明書を取得することができる。つまり、ユーザは、CMOSイメージセンサ32から読み出したID情報に基づいて、CMOSイメージセンサ32の製品関連情報を整合することができる。
- [0089] このとき、第三者機関を利用することで、ユーザや顧客に対して委託会社を秘匿したまま、証明書の取得を行わせることができる。ユーザは、CMOSイメージセンサ32から読み出したID情報（分類IDa、分類IDb、および分類IDc）に基づいて、設計、材料、および装置などの証明書と実際の最終製品が紐づいていることを確認することができる。これにより、ユーザは、例えば、ポリシーに沿った部品を使用しているか否かを確認することができる。
- [0090] なお、第三者機関の代わりに、ファウンドリ、材料メーカー、および装置メ

一カそれぞれのデータベースにおいて、証明書を管理してもよい。

- [0091] ところで、通信システム 11 では、書き換え不可記憶部 43 に、以下で説明する出荷状況ステータスおよび販売先情報を書き込み、ID 情報とともに出力することができる。例えば、以下で説明する出荷状況ステータスおよび販売先情報も、オプション用のモードレジスタ (CIS_OPT_MODE) などを用いて出力のオン／オフを切り替えることができる。
- [0092] 出荷状況ステータスとして、サンプル品や、廃棄品（例えば、品質に満たないもの）、販売品などが分かるステータスを用いることができる。例えば、出荷状況ステータスによって、正規販売品や、サンプル品、廃棄品（信頼性などの条件を満たさず廃棄対象の製品）などを管理することができる。
- [0093] 販売先情報として、社内で識別するための販売先を管理する情報を用いることができる。例えば、販売先情報によって、契約以外の市場に CMOS イメージセンサ 32 が使われていた場合の流通経路を管理することができる。
- [0094] なお、通信システム 11 では、顧客が更新できる領域が書き換え不可記憶部 43 に設けられていてもよい。
- [0095] 例えば、書き換え不可記憶部 43 に顧客がアクセスできる領域を設けておくことで、顧客が CMOS イメージセンサ 32 を廃棄するときに書き換え不可記憶部 43 のヒューズを切断することによって、廃棄ステータスを更新することができる。このように、書き換え不可記憶部 43 において廃棄ステータスを更新した後は、その後の情報の更新を行うことはできなくなる。これにより、例えば、廃棄業者の不正管理を行うことが可能になる。
- [0096] さらに、通信システム 11 では、通信 IF 41 を介して入力されたユーザなどからの生成条件紐づけのためのデータなどの情報を、ID 情報と一緒に署名を施して出力することができる。例えば、ユーザ ID やタイムスタンプなどのように、データ受取先を識別するための情報を外部からレジスタで受け取って、それらの情報を含めて署名を施すことができる。例えば、第三者機関への問い合わせ時にタイムスタンプが確認される。
- [0097] この場合、ユーザ端末 12 は、これらの情報をレジスタ IF から入力する

乱数 (R_B) の一部にするか、あるいは、Text1の情報に入れるなどしてCMOSイメージセンサ32へ送信する。そして、CMOSイメージセンサ32は、ユーザ端末12から送信されてきた情報とIDなどの情報とをマージして、データ全体に署名を施して出力する。

[0098] なお、本実施の形態では、署名処理部44においてID情報に対して署名が施された署名データがCMOSイメージセンサ32から出力される構成例について説明したが、例えば、署名が施されていないID情報がCMOSイメージセンサ32から出力される構成であってもよい。

[0099] <コンピュータの構成例>

次に、上述した一連の処理（通信方法）は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータ等にインストールされる。

[0100] 図11は、上述した一連の処理をプログラムにより実行するコンピュータのハードウェアの構成例を示すブロック図である。

[0101] コンピュータにおいて、CPU (Central Processing Unit) 101、ROM (Read Only Memory) 102、RAM (Random Access Memory) 103、およびEEPROM (Electrically Erasable and Programmable Read Only Memory) 104は、バス105により相互に接続されている。バス105には、さらに、入出力インタフェース106が接続されており、入出力インタフェース106が外部に接続される。

[0102] 以上のように構成されるコンピュータでは、CPU101が、例えば、ROM102およびEEPROM104に記憶されているプログラムを、バス105を介してRAM103にロードして実行することにより、上述した一連の処理が行われる。また、コンピュータ（CPU101）が実行するプログラムは、ROM102に予め書き込んでおく他、入出力インタフェース106を介して外部からEEPROM104にインストールしたり、更新したりすることができる。

[0103] ここで、本明細書において、コンピュータがプログラムに従って行う処理

は、必ずしもフローチャートとして記載された順序に沿って時系列に行われる必要はない。すなわち、コンピュータがプログラムに従って行う処理は、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含む。

[0104] また、プログラムは、1のコンピュータ（プロセッサ）により処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

[0105] さらに、本明細書において、システムとは、複数の構成要素（装置、モジュール（部品）等）の集合を意味し、すべての構成要素が同一筐体中にあるか否かは問わない。したがって、別個の筐体に収納され、ネットワークを介して接続されている複数の装置、及び、1つの筐体の中に複数のモジュールが収納されている1つの装置は、いずれも、システムである。

[0106] また、例えば、1つの装置（または処理部）として説明した構成を分割し、複数の装置（または処理部）として構成するようにしてもよい。逆に、以上において複数の装置（または処理部）として説明した構成をまとめて1つの装置（または処理部）として構成されるようにしてもよい。また、各装置（または各処理部）の構成に上述した以外の構成を付加するようにしてももちろんよい。さらに、システム全体としての構成や動作が実質的に同じであれば、ある装置（または処理部）の構成の一部を他の装置（または他の処理部）の構成に含めるようにしてもよい。

[0107] また、例えば、本技術は、1つの機能を、ネットワークを介して複数の装置で分担、共同して処理するクラウドコンピューティングの構成をとることができる。

[0108] また、例えば、上述したプログラムは、任意の装置において実行することができる。その場合、その装置が、必要な機能（機能ブロック等）を有し、必要な情報を得ることができるようにすればよい。

[0109] また、例えば、上述のフローチャートで説明した各ステップは、1つの装

置で実行する他、複数の装置で分担して実行することができる。さらに、1つのステップに複数の処理が含まれる場合には、その1つのステップに含まれる複数の処理は、1つの装置で実行する他、複数の装置で分担して実行することができる。換言するに、1つのステップに含まれる複数の処理を、複数のステップの処理として実行することもできる。逆に、複数のステップとして説明した処理を1つのステップとしてまとめて実行することもできる。

[0110] なお、コンピュータが実行するプログラムは、プログラムを記述するステップの処理が、本明細書で説明する順序に沿って時系列に実行されるようにしても良いし、並列に、あるいは呼び出しが行われたとき等の必要なタイミングで個別に実行されるようにしても良い。つまり、矛盾が生じない限り、各ステップの処理が上述した順序と異なる順序で実行されるようにしてもよい。さらに、このプログラムを記述するステップの処理が、他のプログラムの処理と並列に実行されるようにしても良いし、他のプログラムの処理と組み合わせられて実行されるようにしても良い。

[0111] なお、本明細書において複数説明した本技術は、矛盾が生じない限り、それぞれ独立に単体で実施することができる。もちろん、任意の複数の本技術を併用して実施することもできる。例えば、いずれかの実施の形態において説明した本技術の一部または全部を、他の実施の形態において説明した本技術の一部または全部と組み合わせられて実施することもできる。また、上述した任意の本技術の一部または全部を、上述していない他の技術と併用して実施することもできる。

[0112] <構成の組み合わせ例>

なお、本技術は以下のような構成も取ることができる。

(1)

ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、

出荷時には書き換えることが不可となる状態でID (Identification) 情報を記憶する書き換え不可記憶部と

を備え、

前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ＩＤ情報を前記通信インタフェースから出力する

半導体チップ。

(2)

前記ＩＤ情報として、前記半導体チップとしての製品を識別するための製品ＩＤ、および、前記半導体チップの製造環境および材料に関する情報に紐づけられる分類ＩＤが少なくとも用いられる

上記(1)に記載の半導体チップ。

(3)

前記ＩＤ情報に付加して、前記半導体チップの出荷ステータスおよび出荷先データを出力する

上記(1)または(2)に記載の半導体チップ。

(4)

前記書き換え不可記憶部に記憶されている複数の前記ＩＤ情報のうちの、前記通信インタフェースから出力する前記ＩＤ情報を選択する情報出力選択部

をさらに備える上記(1)から(3)までのいずれかに記載の半導体チップ。

(5)

前記ＩＤ情報に対して鍵を用いて暗号化することによって署名を施す署名処理を行って、前記ＩＤ情報に署名が施された署名データを前記通信インタフェースから出力させる署名処理部

をさらに備える上記(1)から(4)までのいずれかに記載の半導体チップ。

(6)

前記外部の端末から送信されてくる前記リクエストは第1の鍵によって暗

号化されており、

前記署名処理部は、前記第 1 の鍵に対応する第 2 の鍵を用いて前記リクエストを復号する

上記（５）に記載の半導体チップ。

（７）

前記署名処理部は、画像データを出力する際のフォーマットの所定個所に前記署名データを挿入し、前記署名データを前記画像データに付加して出力させる

上記（５）または（６）に記載の半導体チップ。

（８）

前記署名処理が行われるときのみ、前記署名処理に必要となる前記署名処理部を含むブロックに対して電源またはクロックの供給が行われる

上記（５）から（７）までのいずれかに記載の半導体チップ。

（９）

半導体チップが、

ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、

出荷時には書き換えることが不可となる状態でＩＤ（Identification）情報を記憶する書き換え不可記憶部と

を備え、

前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ＩＤ情報を前記通信インタフェースから出力すること

を含む通信方法。

（１０）

ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、

出荷時には書き換えることが不可となる状態でＩＤ（Identification）

情報を記憶する書き換え不可記憶部と

を有する半導体チップと、

前記ホストを介してリクエストを送信する外部の端末と

を備える通信システムであって、

前記リクエストに応じて、前記書き換え不可記憶部に記憶されている前記

ID情報を前記通信インタフェースから出力する

通信システム。

[0113] なお、本実施の形態は、上述した実施の形態に限定されるものではなく、本開示の要旨を逸脱しない範囲において種々の変更が可能である。また、本明細書に記載された効果はあくまで例示であって限定されるものではなく、他の効果があってもよい。

符号の説明

[0114] 11 通信システム, 12 ユーザ端末, 13 モジュール, 21 起動確認部, 22 真正性確認部, 31 ホスト, 32 CMOSイメージセンサ, 41 通信IF, 42 書き換え可能記憶部, 43 書き換え不可記憶部, 44 署名処理部, 45 処理ステート出力端子, 46 情報出力選択部, 51 画素, 52 データ処理部, 53 出力IF, 61 レジスタ, 62 リクエスト受信領域, 63 セキュリティ情報領域, 64 ID情報領域, 65 情報領域

請求の範囲

- [請求項1] ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、
- 出荷時には書き換えることが不可となる状態でID (Identification) 情報を記憶する書き換え不可記憶部と
- を備え、
- 前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ID情報を前記通信インタフェースから出力する
- 半導体チップ。
- [請求項2] 前記ID情報として、前記半導体チップとしての製品を識別するための製品ID、および、前記半導体チップの製造環境および材料に関する情報に紐づけられる分類IDが少なくとも用いられる
- 請求項1に記載の半導体チップ。
- [請求項3] 前記ID情報に付加して、前記半導体チップの出荷ステータスおよび出荷先データを出力する
- 請求項1に記載の半導体チップ。
- [請求項4] 前記書き換え不可記憶部に記憶されている複数の前記ID情報のうちの、前記通信インタフェースから出力する前記ID情報を選択する
- 情報出力選択部
- をさらに備える請求項1に記載の半導体チップ。
- [請求項5] 前記ID情報に対して鍵を用いて暗号化することによって署名を施す署名処理を行って、前記ID情報に署名が施された署名データを前記通信インタフェースから出力させる署名処理部
- をさらに備える請求項1に記載の半導体チップ。
- [請求項6] 前記外部の端末から送信されてくる前記リクエストは第1の鍵によって暗号化されており、
- 前記署名処理部は、前記第1の鍵に対応する第2の鍵を用いて前記

リクエストを復号する

請求項5に記載の半導体チップ。

[請求項7] 前記署名処理部は、画像データを出力する際のフォーマットの所定個所に前記署名データを挿入し、前記署名データを前記画像データに付加して出力させる

請求項5に記載の半導体チップ。

[請求項8] 前記署名処理が行われるときのみ、前記署名処理に必要なとなる前記署名処理部を含むブロックに対して電源またはクロックの供給が行われる

請求項5に記載の半導体チップ。

[請求項9] 半導体チップが、
ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、

出荷時には書き換えることが不可となる状態でID (Identification) 情報を記憶する書き換え不可記憶部と

を備え、

前記ホストを介した外部の端末からのリクエストに応じて、前記書き換え不可記憶部に記憶されている前記ID情報を前記通信インタフェースから出力すること

を含む通信方法。

[請求項10] ホストとの間で、所定の通信規格に従って通信を行う通信インタフェースと、

出荷時には書き換えることが不可となる状態でID (Identification) 情報を記憶する書き換え不可記憶部と

を有する半導体チップと、

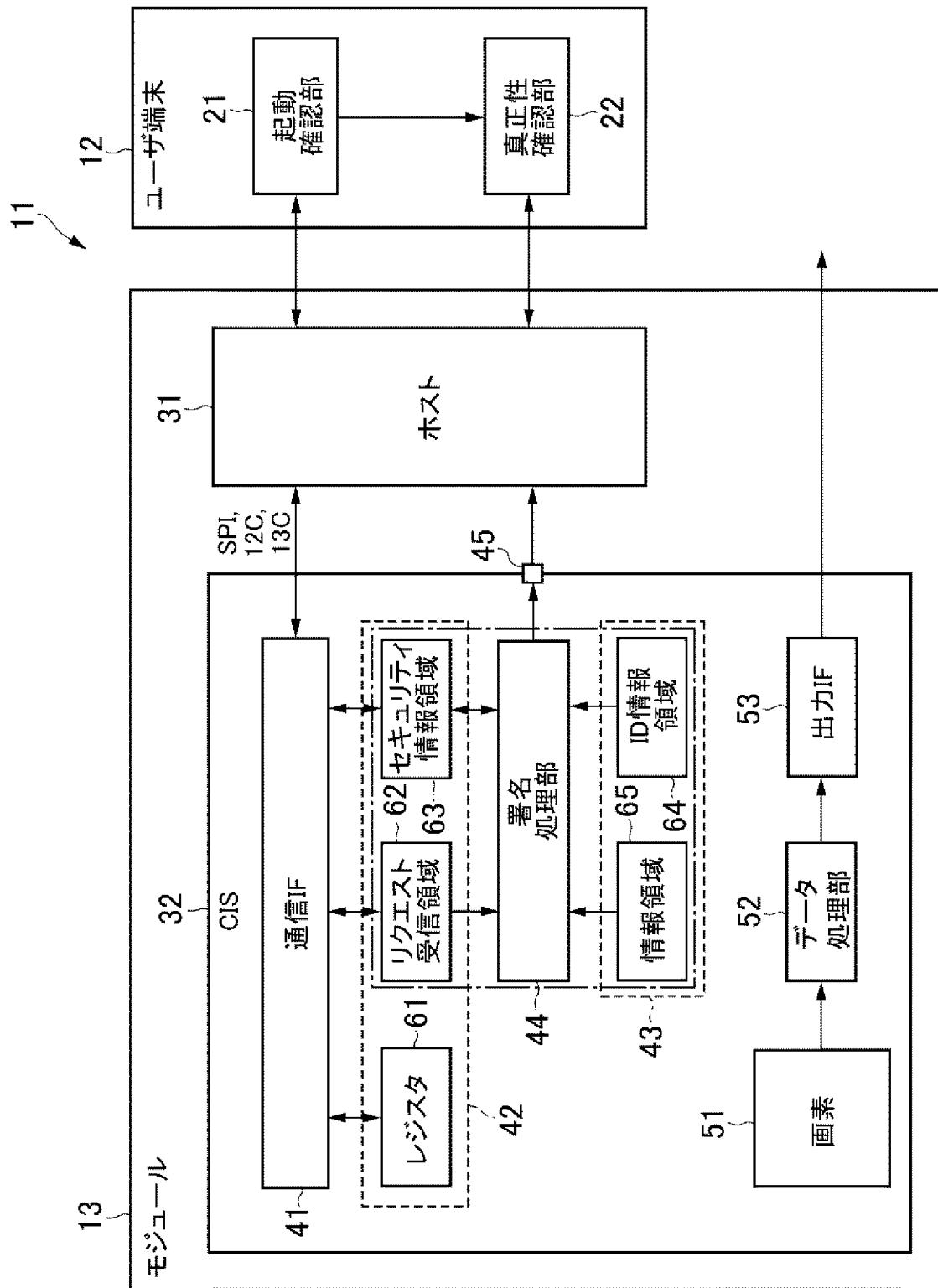
前記ホストを介してリクエストを送信する外部の端末と

を備える通信システムであって、

前記リクエストに応じて、前記書き換え不可記憶部に記憶されてい

る前記 I D 情報を前記通信インタフェースから出力する
通信システム。

[図1]
FIG.1



[図2]

FIG.2

製品ID	製品共通の情報に対するID (CISメーカー発行)
分類IDa	ファウンダリ情報紐づけID (ファウンダリ発行)
分類IDb	材料情報及び/または材料メーカー情報紐づけID (材料メーカー発行)
製品ID'	製品共通の情報に対するID (第三者機関発行)
分類IDa'	ファウンダリ情報紐づけID (第三者機関発行)
分類IDb'	材料情報及び/または材料メーカー情報紐づけID (第三者機関発行)
製品ID''	製品共通の情報に対するID (CISメーカーまたは第三者機関発行)
分類IDx	ファウンダリや材料情報などの情報群を 識別するためのID (CISメーカーまたは第三者機関発行)

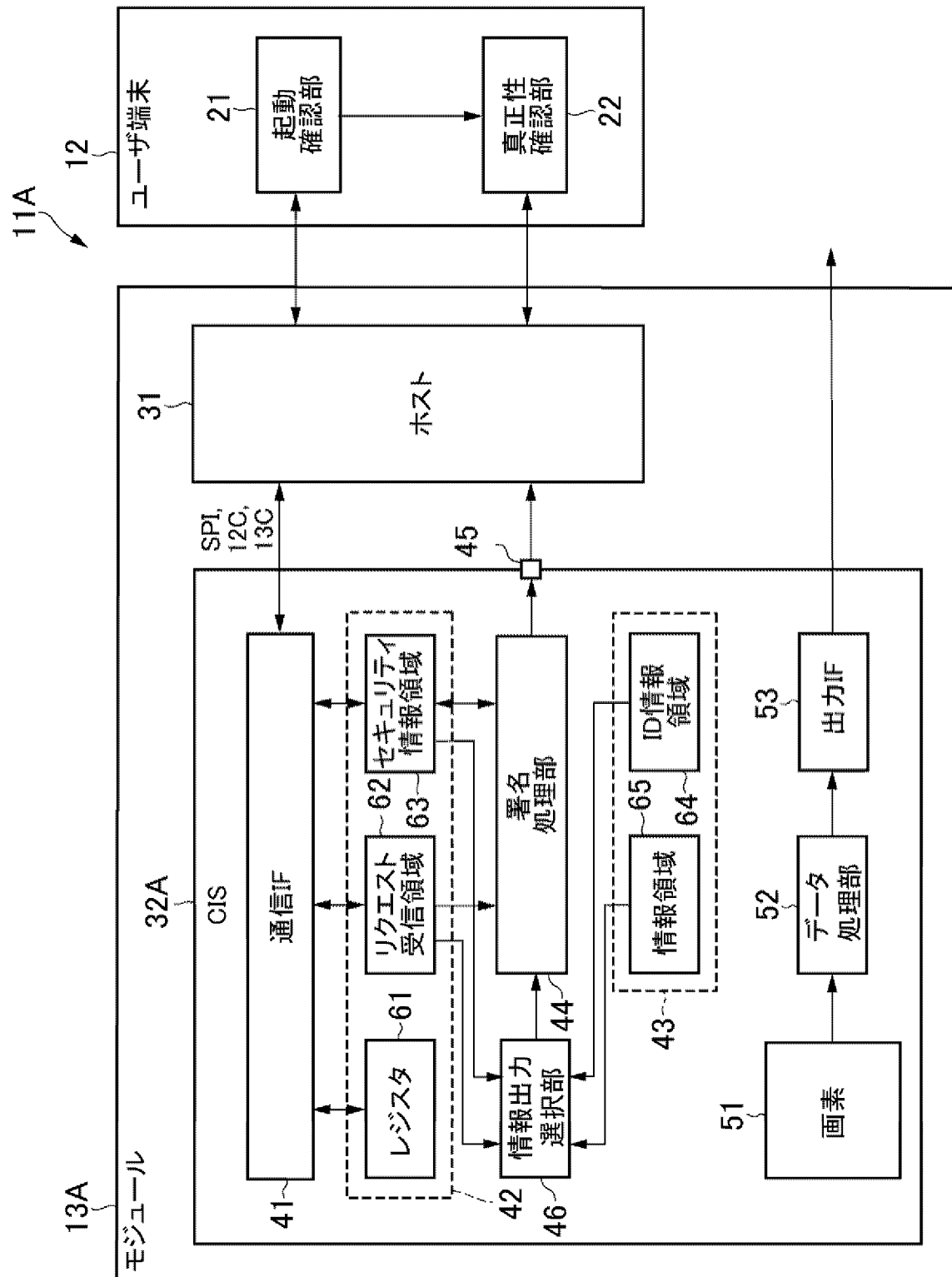
[図3]

FIG.3

A			
レジスタ	レジスタ属性	コメント	
CIS_AUT_REQ	Write	真正性証明リクエスト	
CIS_AUT_REQDATA	Write	リクエストデータ	
CIS_AUT_ACKDATE	Read	レスポンスデータ	
CIS_AUT_MODE	Write	認証で出力するID情報選択(出力モード選択) 0:全ての情報, 0以外:製品や市場依存	
B			
レジスタ	レジスタ属性	Bit	コメント
処理ステータ	Read	1	真正性証明処理実行中

[図4]

FIG.4



[図5]

FIG.5

A	CIS_AUT_MODE=0	
	番号	
	製品ID	製品共通の情報に対するID (CISメーカー発行)
	分類IDa	ファウンダリ情報紐づけID (ファウンダリ発行)
B	CIS_AUT_MODE=1	
	番号	
	製品ID'	製品共通の情報に対するID (第三者機関発行)
	分類IDa'	ファウンダリ情報紐づけID (第三者機関発行)
C	CIS_AUT_MODE=2	
	番号	
	製品ID''	製品共通の情報に対するID (CISメーカーまたは第三者機関発行)
	分類IDx	ファウンダリや材料情報などの情報群を 識別するためのID (CISメーカーまたは第三者機関発行)

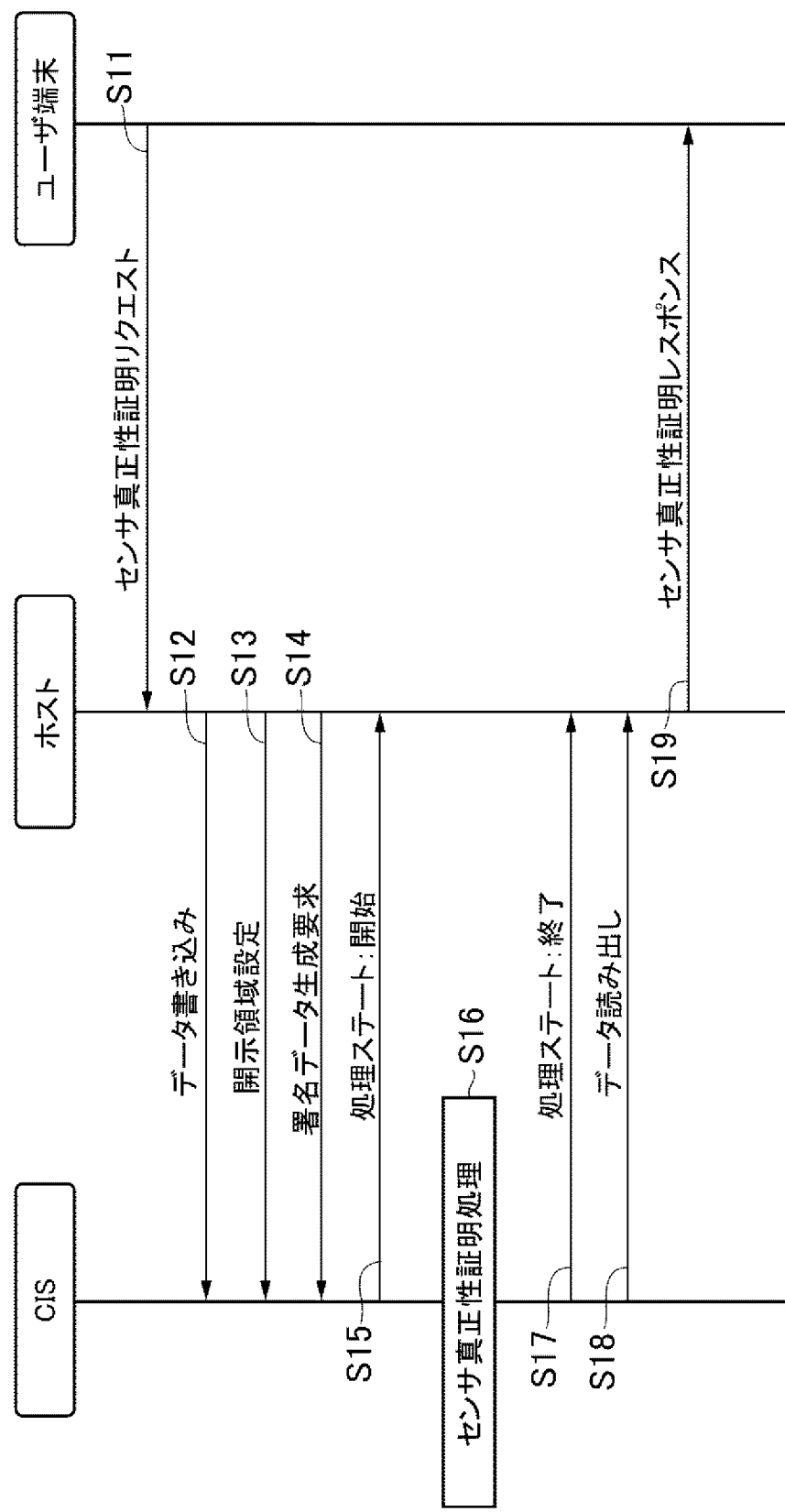
[図6]

FIG.6

CIS_AUT_MODE [bit]	番号	
[0]	製品ID	製品共通の情報に対するID (CISメーカー発行)
[1]	分類IDa	ファウンダリ情報紐づけID (ファウンダリ発行)
[2]	分類IDb	材料情報及び/または材料メーカー情報紐づけID (材料メーカー発行)
[3]	製品ID'	製品共通の情報に対するID (第三者機関発行)
[4]	分類IDa'	ファウンダリ情報紐づけID (第三者機関発行)
[5]	分類IDb'	材料情報及び/または材料メーカー情報紐づけID (第三者機関発行)
[6]	製品ID''	製品共通の情報に対するID (CISメーカーまたは第三者機関発行)
[7]	分類IDx	ファウンダリや材料情報などの情報群を 識別するためのID (CISメーカーまたは第三者機関発行)

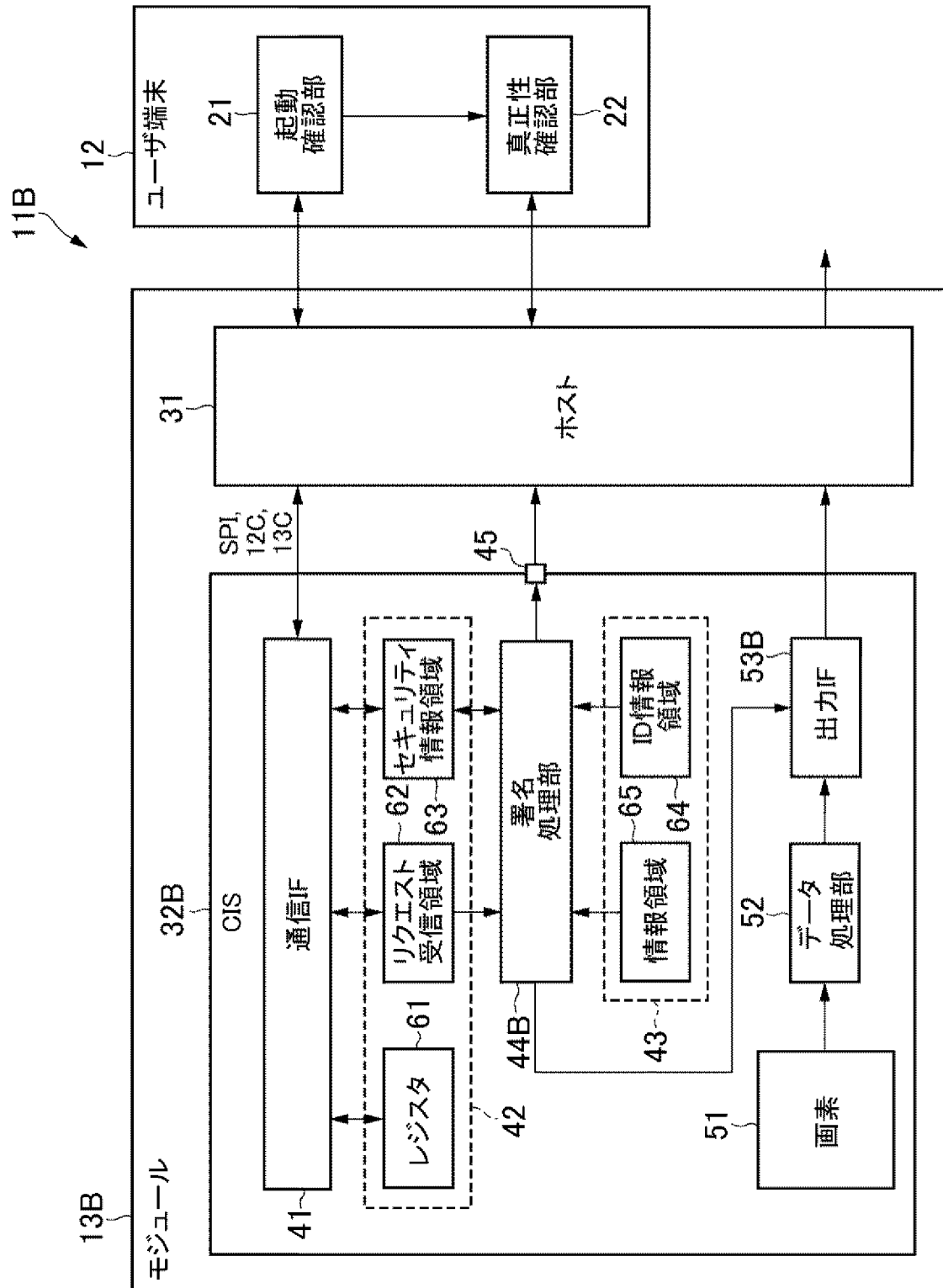
[図7]

FIG.7



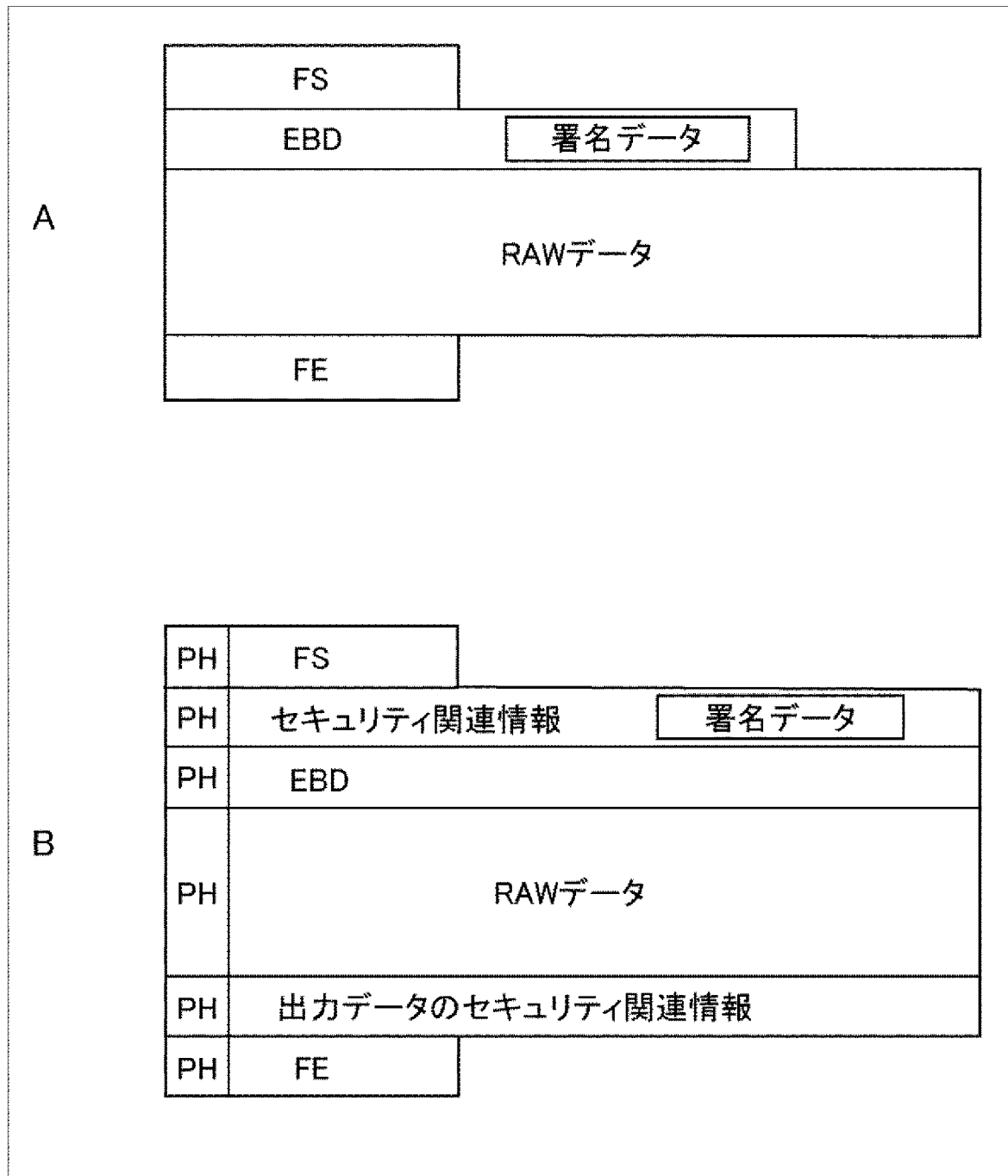
[図8]

FIG.8



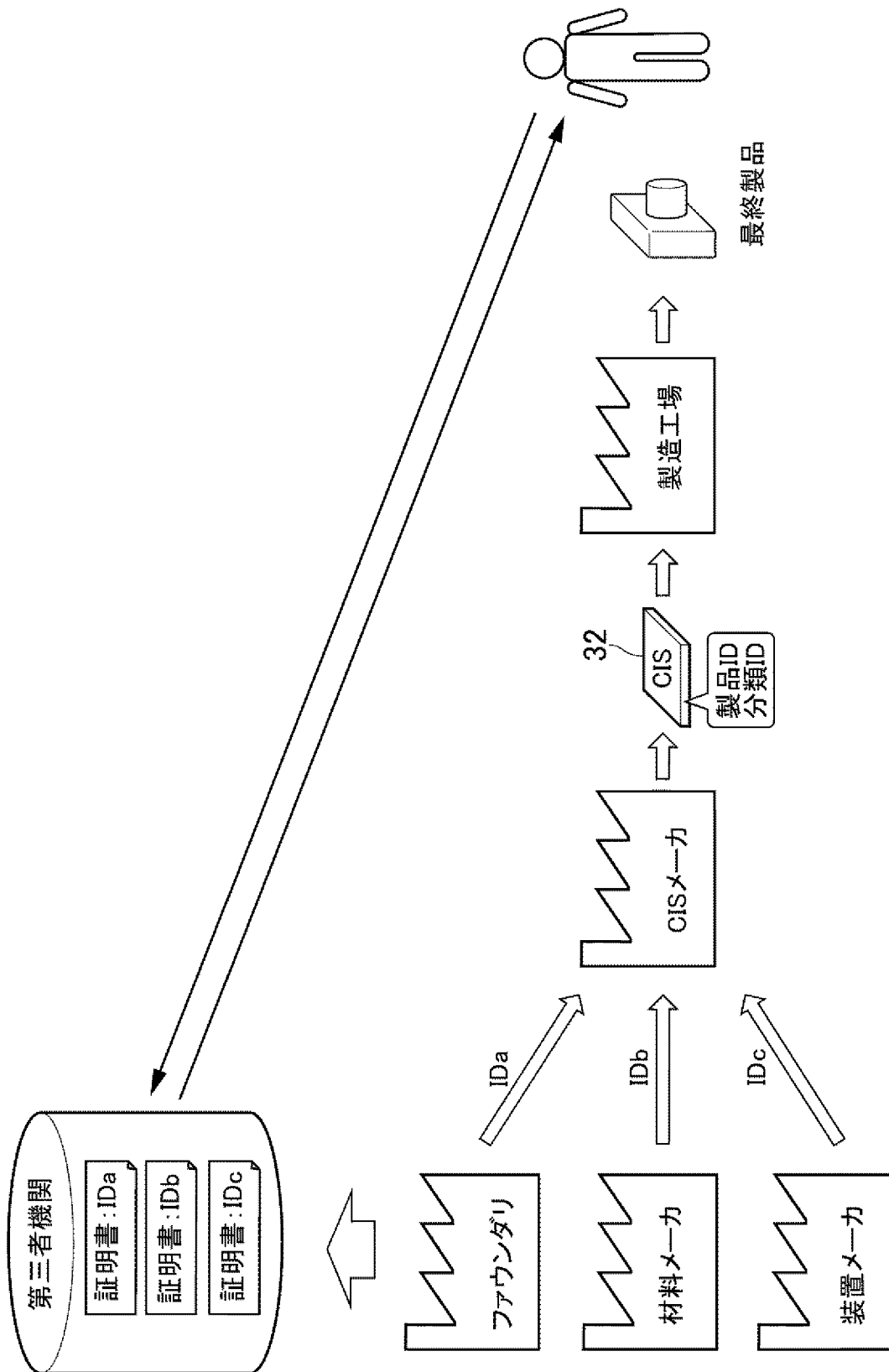
[図9]

FIG.9



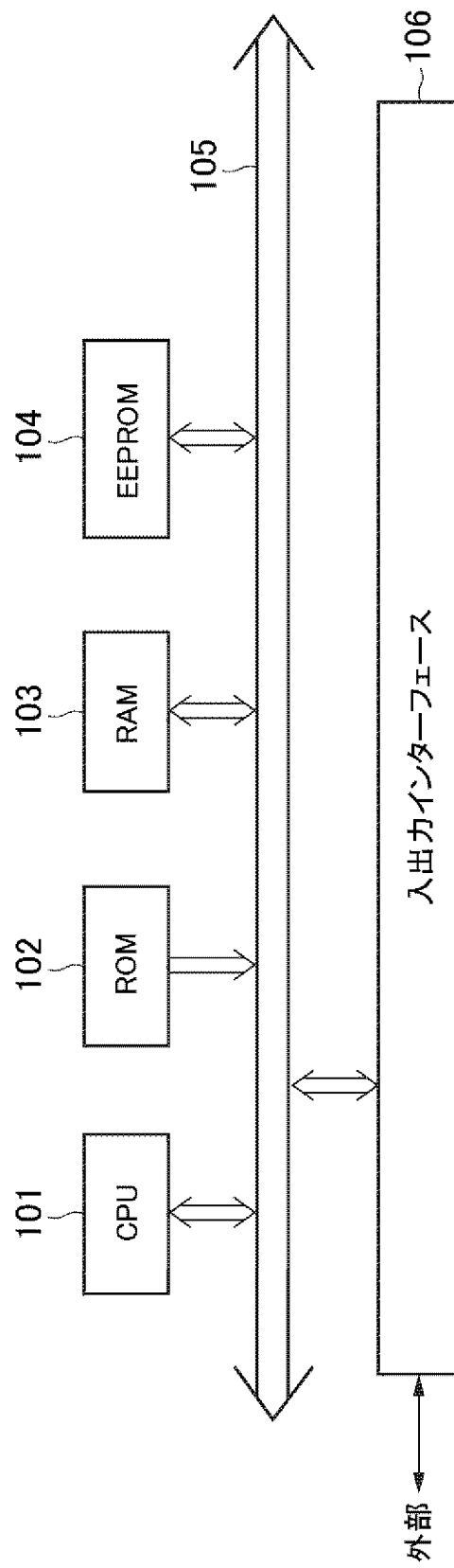
[図10]

FIG.10



[図11]

FIG.11



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/030366

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/73 (2013.01)i; H04L 9/10 (2006.01)i FI: G06F21/73; H04L9/10 Z 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) G06F21/73; H04L9/10 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 1971-2024 Registered utility model specifications of Japan 1996-2024 Published registered utility model applications of Japan 1994-2024 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	WO 01/93275 A1 (HITACHI, LTD.) 06 December 2001 (2001-12-06) specification, p. 13, line 2 to p. 18, line 19, fig. 1-6	1-2, 9-10
Y		3-6
A		7-8
Y	JP 2004-96666 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 25 March 2004 (2004-03-25) paragraphs [0028]-[0041], fig. 1-2	3-4
A		1-2, 5-10
Y	JP 2022-523294 A (MICRON TECHNOLOGY INC.) 22 April 2022 (2022-04-22) paragraph [0079]	5-6
A		1-4, 7-10
☐ 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 “D” document cited by the applicant in the international application “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 18 September 2024		Date of mailing of the international search report 01 October 2024
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/030366

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO	01/93275	A1	06 December 2001	(Family: none)	
JP	2004-96666	A	25 March 2004	US 2004/0059928	A1
				paragraphs [0038]-[0051], fig. 1-2	
				EP 1396778	A2
				CN 1495620	A
JP	2022-523294	A	22 April 2022	US 2020/0233967	A1
				paragraph [0085]	
				WO 2020/154006	A1
				EP 3915035	A1
				CN 113348456	A
				KR 10-2021-0107148	A

A. 発明の属する分野の分類（国際特許分類（IPC））

G06F 21/73(2013.01)i; H04L 9/10(2006.01)i

FI: G06F21/73; H04L9/10 Z

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））

G06F21/73; H04L9/10

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 - 2024年

日本国実用新案登録公報

1996 - 2024年

日本国登録実用新案公報

1994 - 2024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 01/93275 A1（株式会社 日立製作所） 06.12.2001（2001 - 12 - 06） 明細書第13頁第2行-第18頁第19行，図1-6	1-2, 9-10
Y		3-6
A		7-8
Y	JP 2004-96666 A（松下電器産業株式会社） 25.03.2004（2004 - 03 - 25） 段落0028-0041，図1-2	3-4
A		1-2, 5-10
Y	JP 2022-523294 A（マイクロン テクノロジー，インク．） 22.04.2022（2022 - 04 - 22） 段落0079	5-6
A		1-4, 7-10

☐ 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、一般的技术水準を示すもの

“D” 国際出願で出願人が先行技術文献として記載した文献

“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

18.09.2024

国際調査報告の発送日

01.10.2024

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）

三森 雄介 5S 4061

電話番号 03-3581-1101 内線 3529

様式 PCT/ISA/210（第2ページ）（2022年7月）

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/JP2024/030366

引用文献			公表日	パテントファミリー文献	公表日
WO	01/93275	A1	06.12.2001	(ファミリーなし)	
JP	2004-96666	A	25.03.2004	US 2004/0059928	A1
				段落0038-0051, 図1-2	
				EP 1396778	A2
				CN 1495620	A
JP	2022-523294	A	22.04.2022	US 2020/0233967	A1
				段落0085	
				WO 2020/154006	A1
				EP 3915035	A1
				CN 113348456	A
				KR 10-2021-0107148	A