

(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
2019年8月15日(15.08.2019)



(10) 国際公開番号

WO 2019/155693 A1

(51) 国際特許分類:
G06F 21/73 (2013.01) *G06F 21/75* (2013.01)

ードライブ 1 ソニー エレクトロニクス
インク内 New Jersey (US).

(21) 国際出願番号: PCT/JP2018/039869

(22) 国際出願日: 2018年10月26日(26.10.2018)

(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:
62/627,552 2018年2月7日(07.02.2018) US

(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 神奈川県厚木市旭町四丁目14番1号 Kanagawa (JP).

(72) 発明者: 平野 広之(HIRANO, Hiroyuki); 07656 ニュージャージー州パークリッジ ソニ

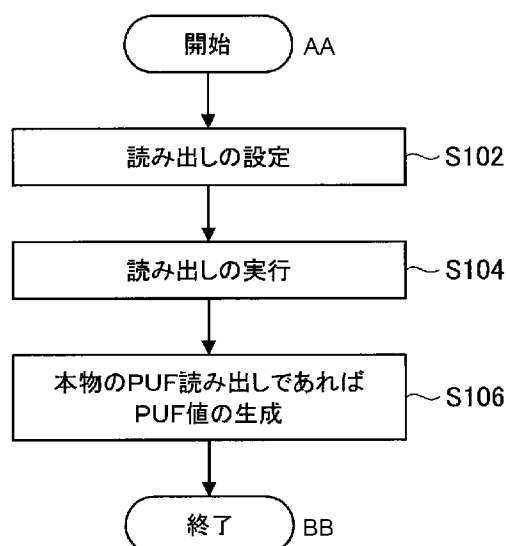
(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング Tokyo (JP).

(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, JP, 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, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: CONTROL DEVICE AND CONTROL METHOD

(54) 発明の名称: 制御装置及び制御方法

【図16】



S102 Set reading
S104 Execute reading
S106 Create PUF value for genuine PUF reading
AA Start
BB End

(57) Abstract: Provided is a control device capable of increasing the difficulty in making an attack by minimizing side-channel leaks that may be caused by a PUF which is realized as a physical parameter until completion of AD conversion. Provided is a control device provided with: a device unit, such as a pixel array, having analog devices regularly arranged; and a reading control unit that executes reading in which genuine PUF reading (first reading) of creating information unique to the device unit, and dummy PUF reading (second reading) of creating no information unique to the device, are combined.

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, 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: 物理パラメータとして実現されているPUFがAD変換完了までに発しうるサイドチャネルリークを最小化し、攻撃を困難化することが可能な、制御装置を提供する。画素アレイのような、規則的に配置されるアナログデバイスを含むデバイス部と、前記デバイス部の固有情報を生成する本物のPUF読み出し(第1の読み出し)と、前記デバイスの固有情報を生成しないダミーPUF読み出し(第2の読み出し)と、を混在させた読み出しを実行する読み出し制御部と、を備える、制御装置が提供される。

明 細 書

発明の名称： 制御装置及び制御方法

技術分野

[0001] 本開示は、制御装置及び制御方法に関する。

背景技術

[0002] 固体撮像装置として、CMOS (Complementary Metal Oxide Semiconductor) 等のMOS型イメージセンサに代表される増幅型固体撮像装置が知られている。また、CCD (Charge Coupled Device) イメージセンサに代表される電荷転送型固体撮像装置が知られている。これら固体撮像装置は、デジタルスチルカメラ、デジタルビデオカメラなどに広く用いられている。近年、カメラ付き携帯電話やPDA (Personal Digital Assistant) などのモバイル機器に搭載される固体撮像装置としては、電源電圧が低く、消費電力の観点などからMOS型イメージセンサが多く用いられている。例えば、特許文献1には、このような固体撮像装置を適用したデジタルカメラの一例が開示されている。

[0003] MOS型の固体撮像装置は、単位画素が光電変換部となるフォトダイオードと複数の画素トランジスタで形成され、この複数の単位画素が2次元アレイ状に配列された画素アレイ（画素領域）と、周辺回路領域を有して構成される。複数の画素トランジスタは、MOSトランジスタで形成され、転送トランジスタ、リセットトランジスタ、増幅トランジスタの3トランジスタ、あるいは選択トランジスタを加えた4トランジスタで構成される。

[0004] 近年では、所謂PUF (Physically Unclonable Function) と呼ばれる、複製困難な物理的特徴を利用してデバイスに固有の値を出力する技術が注目されている。このような、PUFを利用して生成されるデバイスに固有の値は、複製が困難であるという特性から、例えば、個々のデバイスを識別するための識別子 (ID) としての利用や、所謂鍵情報（例えば、暗号化の鍵）としての利用が期待されている。

先行技術文献

特許文献

[0005] 特許文献1：特開2004-173154号公報

発明の概要

発明が解決しようとする課題

[0006] PUFを実際に暗号システムに組み込むには、物理パラメータのアナログ電気信号への変換及びAD変換のプロセスを実行する必要がある。そして、物理パラメータに関する情報が外部からの攻撃により漏れ出すと、悪意のある攻撃者によりデバイスのPUF値が不正に取得され、セキュリティが確保されなくなってしまう。

[0007] そこで、本開示では、物理パラメータとして実現されているPUFがAD変換完了までに発するサイドチャネルリークを最小化し、攻撃を困難化することが可能な、新規かつ改良された制御装置及び制御方法を提案する。

課題を解決するための手段

[0008] 本開示によれば、規則的に配置されるアナログデバイスを有するデバイス部と、前記デバイス部の固有情報を生成する第1の読み出しと、前記デバイスの固有情報を生成しない第2の読み出しと、を混在させた読み出しを実行する読み出し制御部と、を備える、制御装置が提供される。

[0009] また本開示によれば、規則的に配置されるアナログデバイスを有するデバイス部の固有情報を生成する第1の読み出しと、前記デバイスの固有情報を生成しない第2の読み出しと、を混在させた読み出しを実行することを含む、制御方法が提供される。

図面の簡単な説明

[0010] [図1]本開示の一実施形態に係る固体撮像装置の構成の一例を示す概略構成図である。

[図2]本開示に係る技術を適用し得る積層型の固体撮像装置の構成例の概要を示す図である。

[図3]積層型の固体撮像装置23020の第1の構成例を示す断面図である。

[図4]積層型の固体撮像装置23020の第2の構成例を示す断面図である。

[図5]積層型の固体撮像装置23020の第3の構成例を示す断面図である。

[図6]本開示に係る技術を適用し得る積層型の固体撮像装置の他の構成例を示す図である。

[図7]本開示の一実施形態に係る固体撮像装置の一部の機能構成の一例を示すブロック図である。

[図8]本開示の一実施形態に係る単位画素の回路構成の一例を示した図である。

[図9]本実施形態に係る固体撮像装置1を用いたPUFの実施例を示す説明図である。

[図10]PUFが読み出されてからAD変換を終えるまでの間に生じうるサイドチャネルリークの具体例を示す説明図である。

[図11]本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読み出しについて説明する説明図である。

[図12]本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読み出しについて説明する説明図である。

[図13]本開示の実施の形態に係る固体撮像装置1が実装する関数fの具体的な形態を示す説明図である。

[図14]本開示の実施の形態に係る固体撮像装置1が関数fを実行することによる読み出しの設定例を示す説明図である。

[図15]本開示の実施の形態に係る固体撮像装置1の機能構成例を示す説明図である。

[図16]本開示の実施の形態に係る固体撮像装置1の動作例を示す流れ図である。

[図17]本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読み出しの変形例を示す説明図である。

[図18]本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読

み出しの変形例を示す説明図である。

[図19]本開示の実施の形態に係る固体撮像装置 1 が実行するダミー P U F 読み出しの変形例を示す説明図である。

発明を実施するための形態

[0011] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0012] なお、説明は以下の順序で行うものとする。

1. 本開示の実施の形態

1. 1. 経緯

1. 2. 構成例

1. 3. 動作例

1. 4. 変形例

2. まとめ

[0013] <1. 本開示の実施の形態>

[1. 1. 経緯]

まず、本件開示者が本開示の実施の形態に至った経緯について説明する。

[0014] 上述したように、P U F と呼ばれる、複製困難な物理的特徴を利用してデバイスに固有の値を出力する技術が注目されている。P U F の秘密情報は何らかの物理パラメータとして静的にデバイスに保存されている。P U F を実際に暗号システムに組み込むには、物理パラメータのアナログ電気信号への変換及び A D 変換のプロセスを実行する必要がある。以降では、この 2 つのプロセスを総称して「読み出し」と称する。

[0015] 物理パラメータ自体のサイドチャネル漏れ出しのリスクは非常に低く、これが P U F の強みではある。しかし、読み出しや A D 変換中に生じるサイドチャネル漏れ出しに対する脆弱性がないとはいえない。特に P U F の実施態様がイメージセンサのような規則的なアレイパターン及び規則的な A D 変換

器の配置を持つセンサである場合、秘密情報が伝わる信号経路が明らかである場合が多く、電磁界解析といったサイドチャネル攻撃に脆弱である可能性がある。以降、読み出しのときに生じうる電磁波、電流、発光といったあらゆる物理現象をサイドチャネルリークと呼ぶことにする。

[0016] 一方で、A/D変換後の信号処理に関するサイドチャネル攻撃対策は既に広く知られている。A/D変換後の信号処理に関するサイドチャネル攻撃対策には、例えばAES (Advanced Encryption Standard) 暗号回路へのDPA (Differential Power Analysis) 攻撃への対策が有名である。しかし、この技術はA/D変換終了後のみに限られ、物理パラメータからアナログ電気信号へ変換し、A/D変換を終えるまでの経路におけるサイドチャネル攻撃対策にはなっていない。

[0017] そこで本件開示者は、上述した点に鑑み、物理パラメータとして実現されているPUFがA/D変換完了までに発しうるサイドチャネルリークを最小化し、攻撃者による攻撃を困難化することが可能な技術について鋭意検討を行った。その結果、本件開示者は、以下で説明するように、物理パラメータとして実現されているPUFがA/D変換完了までに発しうるサイドチャネルリークを最小化し、攻撃者による攻撃を困難化することが可能な技術を考案するに至った。

[0018] 以上、本開示の実施の形態に至った経緯について説明した。続いて、本開示の実施の形態について詳細に説明する。

[0019] [1. 2. 構成例]

図1に、本開示の一実施形態に係る固体撮像装置の構成の一例として、CMOS固体撮像装置の概略構成を示す。このCMOS固体撮像装置は、各実施の形態の固体撮像装置に適用される。本例の固体撮像装置1は、図1に示すように、半導体基板11、例えばシリコン基板に複数の光電変換部を含む画素2が規則的に2次元アレイ状に配列された画素アレイ（いわゆる画素領域）3と、周辺回路部とを有して構成される。画素2は、光電変換部となる例えばフォトダイオードと、複数の画素トランジスタ（いわゆるMOSトラ

ンジスタ)を有して成る。複数の画素トランジスタは、例えば転送トランジスタ、リセットトランジスタ及び増幅トランジスタの3つのトランジスタで構成することができる。その他、選択トランジスタ追加して4つのトランジスタで構成することもできる。なお、単位画素の等価回路の一例については別途後述する。画素2は、1つの単位画素として構成することができる。また、画素2は、共有画素構造とすることもできる。この共有画素構造は、複数のフォトダイオードと、複数の転送トランジスタと、共有する1つのフローティングディフージョンと、共有する1つずつの他の画素トランジスタとから構成される。すなわち、共有画素では、複数の単位画素を構成するフォトダイオード及び転送トランジスタが、他の1つずつの画素トランジスタを共有して構成される。

[0020] 周辺回路部は、垂直駆動回路4と、カラム信号処理回路5と、水平駆動回路6と、出力回路7と、制御回路8などを有して構成される。

[0021] 制御回路8は、入力クロックと、動作モードなどを指令するデータを受け取り、また固体撮像装置の内部情報などのデータを出力する。すなわち、制御回路8では、垂直同期信号、水平同期信号及びマスタクロックに基づいて、垂直駆動回路4、カラム信号処理回路5及び水平駆動回路6などの動作の基準となるクロック信号や制御信号を生成する。そして、これらの信号を垂直駆動回路4、カラム信号処理回路5及び水平駆動回路6等に入力する。

[0022] 垂直駆動回路4は、例えばシフトレジスタによって構成され、画素駆動配線を選択し、選択された画素駆動配線に画素を駆動するためのパルスを供給し、行単位で画素を駆動する。すなわち、垂直駆動回路4は、画素アレイ3の各画素2を行単位で順次垂直方向に選択走査し、垂直信号線9を通して各画素2の光電変換部となる例えばフォトダイオードにおいて受光量に応じて生成した信号電荷に基づく画素信号をカラム信号処理回路5に供給する。

[0023] カラム信号処理回路5は、画素2の例えば列ごとに配置されており、1行分の画素2から出力される信号を画素列ごとにノイズ除去などの信号処理を行う。すなわちカラム信号処理回路5は、画素2固有の固定パターンノイズ

を除去するためのCDSや、信号増幅、AD変換等の信号処理を行う。カラム信号処理回路5の出力段には水平選択スイッチ（図示せず）が水平信号線10との間に接続されて設けられる。

[0024] 水平駆動回路6は、例えばシフトレジスタによって構成され、水平走査パルスを順次出力することによって、カラム信号処理回路5の各々を順番に選択し、カラム信号処理回路5の各々から画素信号を水平信号線10に出力させる。

[0025] 出力回路7は、カラム信号処理回路5の各々から水平信号線10を通して順次に供給される信号に対し、信号処理を行って出力する。例えば、バッファリングだけする場合もあるし、黒レベル調整、列ばらつき補正、各種デジタル信号処理などが行われる場合もある。入出力端子12は、外部と信号のやりとりをする。

[0026] また、図2は、本開示に係る技術を適用し得る積層型の固体撮像装置の構成例の概要を示す図である。

[0027] 図2のAは、非積層型の固体撮像装置の概略構成例を示している。固体撮像装置23010は、図2のAに示すように、1枚のダイ（半導体基板）23011を有する。このダイ23011には、画素がアレイ状に配置された画素領域23012と、画素の駆動その他の各種の制御を行う制御回路23013と、信号処理するためのロジック回路23014とが搭載されている。

[0028] 図2のB及びCは、積層型の固体撮像装置の概略構成例を示している。固体撮像装置23020は、図2のB及びCに示すように、センサダイ23021とロジックダイ23024との2枚のダイが積層され、電氣的に接続されて、1つの半導体チップとして構成されている。

[0029] 図2のBでは、センサダイ23021には、画素領域23012と制御回路23013が搭載され、ロジックダイ23024には、信号処理を行う信号処理回路を含むロジック回路23014が搭載されている。

[0030] 図2のCでは、センサダイ23021には、画素領域23012が搭載され、ロジックダイ23024には、制御回路23013及びロジック回路23014が搭載されている。

- [0031] 図3は、積層型の固体撮像装置23020の第1の構成例を示す断面図である。
- [0032] センサダイ23021には、画素領域23012となる画素を構成するPD（フォトダイオード）や、FD（フローティングディフュージョン）、Tr（MOS FET）、及び、制御回路23013となるTr等が形成される。さらに、センサダイ23021には、複数層、本例では3層の配線23110を有する配線層23101が形成される。なお、制御回路23013（となるTr）は、センサダイ23021ではなく、ロジックダイ23024に構成することができる。
- [0033] ロジックダイ23024には、ロジック回路23014を構成するTrが形成される。さらに、ロジックダイ23024には、複数層、本例では3層の配線23170を有する配線層23161が形成される。また、ロジックダイ23024には、内壁面に絶縁膜23172が形成された接続孔23171が形成され、接続孔23171内には、配線23170等と接続される接続導体23173が埋め込まれる。
- [0034] センサダイ23021とロジックダイ23024とは、互いの配線層23101及び23161が向き合うように貼り合わされ、これにより、センサダイ23021とロジックダイ23024とが積層された積層型の固体撮像装置23020が構成されている。センサダイ23021とロジックダイ23024とが貼り合わされる面には、保護膜等の膜23191が形成されている。
- [0035] センサダイ23021には、センサダイ23021の裏面側（PDに光が入射する側）（上側）からセンサダイ23021を貫通してロジックダイ23024の最上層の配線23170に達する接続孔23111が形成される。さらに、センサダイ23021には、接続孔23111に近接して、センサダイ23021の裏面側から1層目の配線23110に達する接続孔23121が形成される。接続孔23111の内壁面には、絶縁膜23112が形成され、接続孔23121の内壁面には、絶縁膜23122が形成される。そして、接続孔23111及び23121内には、接続導体23113及び23123がそれぞれ埋め込まれる。接続導体23113と接続導体23123とは、センサダイ23021の裏面側で電氣的に接続され、これにより、センサダイ23021とロジックダイ23024とが、配線層23101、接続孔23121、接続孔23111、及び、配線層23161を介して、電氣的に接続される。

[0036] 図4は、積層型の固体撮像装置23020の第2の構成例を示す断面図である。

[0037] 固体撮像装置23020の第2の構成例では、センサダイ23021に形成する1つの接続孔23211によって、センサダイ23021（の配線層23101（の配線23110））と、ロジックダイ23024（の配線層23161（の配線23170））とが電氣的に接続される。

[0038] すなわち、図4では、接続孔23211が、センサダイ23021の裏面側からセンサダイ23021を貫通してロジックダイ23024の最上層の配線23170に達し、且つ、センサダイ23021の最上層の配線23110に達するように形成される。接続孔23211の内壁面には、絶縁膜23212が形成され、接続孔23211内には、接続導体23213が埋め込まれる。上述の図3では、2つの接続孔23111及び23121によって、センサダイ23021とロジックダイ23024とが電氣的に接続されるが、図4では、1つの接続孔23211によって、センサダイ23021とロジックダイ23024とが電氣的に接続される。

[0039] 図5は、積層型の固体撮像装置23020の第3の構成例を示す断面図である。

[0040] 図5の固体撮像装置23020は、センサダイ23021とロジックダイ23024とが貼り合わされる面に、保護膜等の膜23191が形成されていない点で、センサダイ23021とロジックダイ23024とが貼り合わされる面に、保護膜等の膜23191が形成されている図3の場合と異なる。

[0041] 図5の固体撮像装置23020は、配線23110及び23170が直接接触するように、センサダイ23021とロジックダイ23024とを重ね合わせ、所要の加重をかけながら加熱し、配線23110及び23170を直接接合することで構成される。

[0042] 図6は、本開示に係る技術を適用し得る積層型の固体撮像装置の他の構成例を示す断面図である。

[0043] 図6では、固体撮像装置23401は、センサダイ23411と、ロジックダイ23412と、メモリダイ23413との3枚のダイが積層された3層の積層構造になっている。

[0044] メモリダイ23413は、例えば、ロジックダイ23412で行われる信号処理において一時的に必要となるデータの記憶を行うメモリ回路を有する。

- [0045] 図6では、センサダイ23411の下に、ロジックダイ23412及びメモリダイ23413が、その順番で積層されているが、ロジックダイ23412及びメモリダイ23413は、逆順、すなわち、メモリダイ23413及びロジックダイ23412の順番で、センサダイ23411の下に積層することができる。
- [0046] なお、図6では、センサダイ23411には、画素の光電変換部となるPDや、画素Trのソース／ドレイン領域が形成されている。
- [0047] PDの周囲にはゲート絶縁膜を介してゲート電極が形成され、ゲート電極と対のソース／ドレイン領域により画素Tr23421、画素Tr23422が形成されている。
- [0048] PDに隣接する画素Tr23421が転送Trであり、その画素Tr23421を構成する対のソース／ドレイン領域の一方がFDになっている。
- [0049] また、センサダイ23411には、層間絶縁膜が形成され、層間絶縁膜には、接続孔が形成される。接続孔には、画素Tr23421、及び、画素Tr23422に接続する接続導体23431が形成されている。
- [0050] さらに、センサダイ23411には、各接続導体23431に接続する複数層の配線23432を有する配線層23433が形成されている。
- [0051] また、センサダイ23411の配線層23433の最下層には、外部接続用の電極となるアルミパッド23434が形成されている。すなわち、センサダイ23411では、配線23432よりもロジックダイ23412との接着面23440に近い位置にアルミパッド23434が形成されている。アルミパッド23434は、外部との信号の入出力に係る配線の一端として用いられる。
- [0052] さらに、センサダイ23411には、ロジックダイ23412との電氣的接続に用いられるコンタクト23441が形成されている。コンタクト23441は、ロジックダイ23412のコンタクト23451に接続されるとともに、センサダイ23411のアルミパッド23442にも接続されている。
- [0053] そして、センサダイ23411には、センサダイ23411の裏面側（上側）からアルミパッド23442に達するようにパッド孔23443が形成されている。
- [0054] 本開示に係る技術は、以上のような固体撮像装置に適用することができる

。

[0055] なお、図3～図6を参照して説明した例において、各種配線には、例えば、銅（Cu）配線が用いられる。また、以降では、図5に示すように、互いに積層されるセンサダイ間において配線間（例えば、図5に示す配線23110及び23170間）を直接接合する構成を「Cu－Cu接合」とも称する。

[0056] <1. 2. 機能構成>

続いて、図7を参照して、本開示の一実施形態に係る固体撮像装置の機能構成の一例について説明する。図7は、本開示の一実施形態に係る固体撮像装置の一部の機能構成の一例を示すブロック図である。図7に示される固体撮像装置1は、例えば、CMOS（Complementary Metal Oxide Semiconductor）イメージセンサやCCD（Charge Coupled Device）イメージセンサ等の、被写体を撮像し、撮像画像のデジタルデータを得る撮像素子である。

。

[0057] 図7に示されるように、固体撮像装置1は、制御部101、画素アレイ部111、選択部112、A/D変換部（ADC（Analog Digital Converter））113、及び定電流回路部114を有する。

[0058] 制御部101は、固体撮像装置1の各部を制御し、画像データ（画素信号）の読み出し等に関する処理を実行させる。

[0059] 画素アレイ部111は、フォトダイオード等の光電変換素子を有する画素構成が行列（アレイ）状に配置される画素領域である。画素アレイ部111は、制御部101に制御されて、各画素で被写体の光を受光し、その入射光を光電変換して電荷を蓄積し、所定のタイミングにおいて、各画素に蓄積された電荷を画素信号として出力する。

[0060] 画素121および画素122は、その画素アレイ部111に配置される画素群の中の、上下に隣接する2画素を示している。画素121および画素122は、互いに同じカラム（列）の連続する行の画素である。図7の例の場合、画素121および画素122に示されるように、各画素の回路には、光電変換素子並びに4つのトランジスタが用いられている。なお、各画素の回

路の構成は、任意であり、図7に示される例以外であってもよい。

[0061] 一般的な画素アレイには、カラム（列）毎に、画素信号の出力線が設けられる。画素アレイ部111の場合、1カラム（列）毎に、2本（2系統）の出力線が設けられる。1カラムの画素の回路は、1行おきに、この2本の出力線に交互に接続される。例えば、上から奇数番目の行の画素の回路が一方の出力線に接続され、偶数番目の行の画素の回路が他方の出力線に接続される。図7の例の場合、画素121の回路は、第1の出力線（VSL1）に接続され、画素122の回路は、第2の出力線（VSL2）に接続される。

[0062] なお、図7においては、説明の便宜上、1カラム分の出力線のみ示されているが、実際には、各カラムに対して、同様に2本ずつ出力線が設けられる。各出力線には、そのカラムの画素の回路が1行おきに接続される。

[0063] 選択部112は、画素アレイ部111の各出力線をADC113の入力に接続するスイッチを有し、制御部101に制御されて、画素アレイ部111とADC113との接続を制御する。つまり、画素アレイ部111から読み出された画素信号は、この選択部112を介してADC113に供給される。

[0064] 選択部112は、スイッチ131、スイッチ132、およびスイッチ133を有する。スイッチ131（選択SW）は、互いに同じカラムに対応する2本の出力線の接続を制御する。例えば、スイッチ131がオン（ON）状態になると、第1の出力線（VSL1）と第2の出力線（VSL2）が接続され、オフ（OFF）状態になると切断される。

[0065] 詳細については後述するが、固体撮像装置1においては、各出力線に対してADCが1つずつ設けられている（カラムADC）。したがって、スイッチ132およびスイッチ133がともにオン状態であるとする、スイッチ131がオン状態になれば、同カラムの2本の出力線が接続されるので、1画素の回路が2つのADCに接続されることになる。逆に、スイッチ131がオフ状態になると、同カラムの2本の出力線が切断されて、1画素の回路が1つのADCに接続されることになる。つまり、スイッチ131は、1つ

の画素の信号の出力先とするADC（カラムADC）の数を選択する。

[0066] 詳細については後述するが、このようにスイッチ131が画素信号の出力先とするADCの数を制御することにより、固体撮像装置1は、そのADCの数に応じてより多様な画素信号を出力することができる。つまり、固体撮像装置1は、より多様なデータ出力を実現することができる。

[0067] スイッチ132は、画素121に対応する第1の出力線（VSL1）と、その出力線に対応するADCとの接続を制御する。スイッチ132がオン（ON）状態になると、第1の出力線が、対応するADCの比較器の一方の入力に接続される。また、オフ（OFF）状態になるとそれらが切断される。

[0068] スイッチ133は、画素122に対応する第2の出力線（VSL2）と、その出力線に対応するADCとの接続を制御する。スイッチ133がオン（ON）状態になると、第2の出力線が、対応するADCの比較器の一方の入力に接続される。また、オフ（OFF）状態になるとそれらが切断される。

[0069] 選択部112は、制御部101の制御に従って、このようなスイッチ131～スイッチ133の状態を切り替えることにより、1つの画素の信号の出力先とするADC（カラムADC）の数を制御することができる。

[0070] なお、スイッチ132やスイッチ133（いずれか一方もしくは両方）を省略し、各出力線と、その出力線に対応するADCとを常時接続するようにしてもよい。ただし、これらのスイッチによって、これらの接続・切断を制御することができるようにすることにより、1つの画素の信号の出力先とするADC（カラムADC）の数の選択の幅が広がる。つまり、これらのスイッチを設けることにより、固体撮像装置1は、より多様な画素信号を出力することができる。

[0071] なお、図7においては、1カラム分の出力線に対する構成のみ示されているが、実際には、選択部112は、カラム毎に、図7に示されるのと同様の構成（スイッチ131～スイッチ133）を有している。つまり、選択部112は、各カラムについて、制御部101の制御に従って、上述したのと同様の接続制御を行う。

[0072] ADC 113は、画素アレイ部111から各出力線を介して供給される画素信号を、それぞれA/D変換し、デジタルデータとして出力する。ADC 113は、画素アレイ部111からの出力線毎のADC（カラムADC）を有する。つまり、ADC 113は、複数のカラムADCを有する。1出力線に対応するカラムADCは、比較器、D/A変換器（DAC）、およびカウンタを有するシングルスロープ型のADCである。

[0073] 比較器は、そのDAC出力と画素信号の信号値とを比較する。カウンタは、画素信号とDAC出力が等しくなるまで、カウント値（デジタル値）をインクリメントする。比較器は、DAC出力が信号値に達すると、カウンタを停止する。その後カウンタ1, 2によってデジタル化された信号をDATA1およびDATA2より固体撮像装置1の外部に出力する。

[0074] カウンタは、次のA/D変換のためデータ出力後、カウント値を初期値（例えば0）に戻す。

[0075] ADC 113は、各カラムに対して2系統のカラムADCを有する。例えば、第1の出力線（VSL1）に対して、比較器141（COMP1）、DAC 142（DAC1）、およびカウンタ143（カウンタ1）が設けられ、第2の出力線（VSL2）に対して、比較器151（COMP2）、DAC 152（DAC2）、およびカウンタ153（カウンタ2）が設けられている。図示は省略しているが、ADC 113は、他のカラムの出力線に対しても同様の構成を有する。

[0076] ただし、これらの構成の内、DACは、共通化することができる。DACの共通化は、系統毎に行われる。つまり、各カラムの互いに同じ系統のDACが共通化される。図7の例の場合、各カラムの第1の出力線（VSL1）に対応するDACがDAC 142として共通化され、各カラムの第2の出力線（VSL2）に対応するDACがDAC 152として共通化されている。なお、比較器とカウンタは、各出力線の系統毎に設けられる。

[0077] 定電流回路部114は、各出力線に接続される定電流回路であり、制御部101により制御されて駆動する。定電流回路部114の回路は、例えば、

MOS (Metal Oxide Semiconductor) トランジスタ等により構成される。この回路構成は任意であるが、図7においては、説明の便宜上、第1の出力線(VSL1)に対して、MOSトランジスタ161(LOAD1)が設けられ、第2の出力線(VSL2)に対して、MOSトランジスタ162(LOAD2)が設けられている。

[0078] 制御部101は、例えばユーザ等の外部から要求を受け付けて読み出しモードを選択し、選択部112を制御して、出力線に対する接続を制御する。また、制御部101は、選択した読み出しモードに応じて、カラムADCの駆動を制御したりする。さらに、制御部101は、カラムADC以外にも、必要に応じて、定電流回路部114の駆動を制御したり、例えば、読み出しのレートやタイミング等、画素アレイ部111の駆動を制御したりする。

[0079] つまり、制御部101は、選択部112の制御だけでなく、選択部112以外の各部も、より多様なモードで動作させることができる。したがって、固体撮像装置1は、より多様な画素信号を出力することができる。

[0080] なお、図7に示す各部の数は、不足しない限り任意である。例えば、各カラムに対して、出力線が3系統以上設けられるようにしてもよい。また、図7に示した、ADC132から出力される画素信号の並列数や、ADC132自体の数を増やすことで、外部に並列して出力される画素信号の数を増やしてもよい。

[0081] 以上、図7を参照して、本開示の一実施形態に係る固体撮像装置の機能構成の一例について説明した。

[0082] <1. 3. 単位画素の回路構成>

続いて、図8を参照して、単位画素の回路構成の一例について説明する。図8は、本開示の一実施形態に係る単位画素の回路構成の一例を示した図である。図8に示すように、本開示の一実施形態に係る単位画素121は、光電変換部、例えばフォトダイオードPDと、4つの画素トランジスタとを含む。4つの画素トランジスタは、例えば、転送トランジスタTr11、リセットトランジスタTr12、増幅トランジスタTr13、及び選択トランジ

スタTr14である。これらの画素トランジスタは、例えば、nチャンネルのMOSトランジスタにより構成され得る。

[0083] 転送トランジスタTr11は、フォトダイオードPDのカソードとフローティングディフュージョン部FDとの間に接続される。フォトダイオードPDで光電変換され、ここに蓄積された信号電荷（ここでは、電子）を、ゲートに転送パルス ϕ TRGが与えられることによってフローティングディフュージョン部FDに転送する。なお、参照符号Cfdは、フローティングディフュージョン部FDの寄生容量を模式的に示している。

[0084] リセットトランジスタTr12は、電源VDDにドレインが、フローティングディフュージョン部FDにソースがそれぞれ接続される。そして、フォトダイオードPDからフローティングディフュージョン部FDへの信号電荷の転送に先立って、ゲートにリセットパルス ϕ RSTが与えられることによってフローティングディフュージョン部FDの電位をリセットする。

[0085] 増幅トランジスタTr13は、フローティングディフュージョン部FDにゲートが、電源VDDにドレインが、選択トランジスタTr14のドレインにソースがそれぞれ接続される。増幅トランジスタTr13は、リセットトランジスタTr12によってリセットした後のフローティングディフュージョン部FDの電位をリセットレベルとして選択トランジスタTr14に出力する。さらに増幅トランジスタTr13は、転送トランジスタTr11によって信号電荷を転送した後のフローティングディフュージョン部FDの電位を信号レベルとして選択トランジスタTr14に出力する。

[0086] 選択トランジスタTr14は、例えば、増幅トランジスタTr13のソースにドレインが、垂直信号線9にソースがそれぞれ接続される。そして選択トランジスタTr14のゲートに選択パルス ϕ SELが与えられることによってオン状態となり、増幅トランジスタTr13から出力される信号を垂直信号線9に出力する。なお、この選択トランジスタTr14については、電源VDDと増幅トランジスタTr13のドレインとの間に接続した構成を採用することも可能である。

[0087] なお、本実施形態に係る固体撮像装置 1 を、積層型の固体撮像装置として構成する場合には、例えば、フォトダイオード及び複数の MOS トランジスタ等の素子が、図 2 の B または C におけるセンサダイ 23021 に形成される。また、転送パルス、リセットパルス、選択パルス、電源電圧は、図 2 の B または C におけるロジックダイ 23024 から供給される。また、選択トランジスタのドレインに接続される垂直信号線 9 から後段の素子は、選択トランジスタのドレインに接続される垂直信号線 9 から後段の素子は、ロジック回路 23014 に構成されており、ロジックダイ 23024 に形成される。

[0088] 以上、図 8 を参照して、単位画素の回路構成の一例について説明した。

[0089] 図 9 は、本実施形態に係る固体撮像装置 1 を用いた PUF の実施例を示す説明図である。この PUF は、増幅トランジスタ（図 8 に示した増幅トランジスタ T_{r13} ）の電圧値（電圧閾値）を物理パラメータとして利用している。そして、リセットトランジスタ（図 8 に示したリセットトランジスタ T_{r14} ）や選択トランジスタ（図 8 に示した選択トランジスタ T_{r12} ）の入力を High に上げることで、増幅トランジスタの電圧閾値のばらつきに相関したアナログ信号が垂直信号線 9 を流れ、ADC 113 に入力される。ADC 113 で AD 変換後のデジタル化された値（以下 PUF 値と呼ぶ）は、デジタルシステムのセキュアドメイン内にて、通常の PUF の用途である、デバイス毎にユニークな ID の生成や暗号化の際の鍵値として利用される。

[0090] 図 9 では、水平方向に 4 つの単位画素が示されている。また図 9 では、それぞれの単位画素に設けられる増幅トランジスタの電圧閾値（ $Amp-1 \ V_{th} \sim Amp-4 \ V_{th}$ ）のばらつきに相関したアナログ信号から PUF 値 $f(Amp-1 \ V_{th}) \sim f(Amp-4 \ V_{th})$ が生成される様子が示されている。

[0091] 図 10 は、PUF が読み出されてから AD 変換を終えるまでの間に生じるサイドチャネルリークの具体例を示す説明図である。サイドチャネルリークとして、第一に、信号線を通る電磁界が考えられる。この電磁界の振幅

と増幅トランジスタの電圧閾値とに相関があることが予想される。サイドチャネルリークとして、第二に、A/D変換の動作中に発生する電磁界も考えられる。この電磁界の時系列パターンが増幅トランジスタの電圧閾値のばらつきに相関を持つことが想定される。例えば、シングルスロープA/D変換方式の場合では、コンパレータの反転するタイミングとPUF値とに相関関係がある。従って、攻撃者はコンパレータの反転するタイミングを、コンパレータ付近から発する電磁界などのサイドチャネルリークから取得することでPUF値を推定することが、原理的には可能である。

[0092] そこで、本開示の実施の形態に係る固体撮像装置1は、攻撃者によるPUF値の推定を極めて困難にするため、PUF値の推定には至らない電気信号を信号線に流し、A/D変換を実行する。PUF値の推定には至らない電気信号を出力するための読み出しを、以下「ダミーPUF読み出し」と呼ぶことにする。ダミーPUF読み出しに対する、PUF値の推定には至る電気信号を出力するための読み出しを単に「PUF読み出し」または「本物のPUF読み出し」と呼ぶことにする。

[0093] 図11は、本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読み出しについて説明する説明図である。仮にSelect-1により指定できる増幅トランジスタをPUFとして定めるとする。その場合、ダミーPUF読み出しとして、Select-2やSelect-3で指定した増幅トランジスタに対する読み出しを実行すると、似たような信号ではあるが、PUFとして定めた増幅トランジスタとは違う増幅トランジスタであるため、PUF値の推定には至らない電気信号を信号線に流し、A/D変換を行うことができる。

[0094] このダミーPUF読み出しは攻撃者を攪乱させるために積極的に使うことができる。攻撃者がダミーPUF読み出しと、本物のPUF読み出しを区別できない前提に立てば、例えサイドチャネルリークが測定可能なレベルで起こっていたとしても、攻撃者はPUF値を得ることができない。この前提は様々なPUFで妥当であると考えられる。

[0095] 本開示の実施の形態に係る固体撮像装置1が実行するダミーPUF読み出

しは、P U Fとして採用されている行とは別の行を読み出すような読み出しであってもよいが、行単位処理に制約されないA D変換構造を持つイメージセンサのようなアレイ型センサであれば、P U Fとして採用されている領域とは別の領域を読み出すような読み出しであってもよい。

[0096] 図12は、本開示の実施の形態に係る固体撮像装置1が実行するダミーP U F読み出しについて説明する説明図である。図12では、固体撮像装置1が画素単位で読み出し処理可能な構造を有しているものとする。また図12では、各画素の構成のみを図示し、各画素からの出力線は省略している。本開示の実施の形態に係る固体撮像装置1は、本物のP U F読み出しを、実線で囲まれた単位画素を対象とし、ダミーP U F読み出しを、破線で囲まれた単位画素を対象としてもよい。

[0097] 本開示の実施の形態に係る固体撮像装置1は、P U Fとして採用されている行または領域と、P U Fとして採用されていない行または領域とで、アナログ信号同士の演算を行い、A D変換を実行しても良い。アナログ信号同士の演算には、例えばアナログドメインでの加算や減算があり得る。

[0098] ダミーP U F読み出しの方法はアーキテクチャに依存するため、全てを列挙することは不可能である。しかし、ダミーP U F読み出しの方法に共通するポイントは、秘密情報として選定されていないが、物理パラメータの種類として同等のものを読み出すことで、本物のP U F読み出しと同じような波形のサイドチャネルリークを生成し、攻撃者を攪乱させることができる、ということである。

[0099] さらに、A D変換の動作中に発生するサイドチャネルリークが攻撃者の観点から最も有用であると判断される場合には、本開示の実施の形態に係る固体撮像装置1は、ダミーP U F読み出しとして、本物のP U F読み出しであっても、A D変換器の動作設定を変えることでサイドチャネルリークを変化・変調させるという手法を実行しうる。具体的には、例えば、ダイナミックレンジを変化させる手法により、サイドチャネルリークを変化・変調させる手法がある。このA D変換器の動作設定を変える手法は、ダミーP U F読

み出しのために冗長な回路構成を持つ必要がないことを示している。

[0100] ただ、システムの起動毎に同じパターンでダミー読み出しを行うと、攻撃者は、起動を繰り返して出力を解析することで、ダミーPUF読み出しと本物のPUF読み出しとを区別することができるようになる可能性がある。

[0101] そこで、本開示の実施の形態に係る固体撮像装置1は、ダミーPUF読み出しと本物のPUF読み出しとの区別をさらに困難にするために、起動毎にダミーPUF読み出しの方法、パターン、設定を変化させてもよい。本開示の実施の形態に係る固体撮像装置1は、起動毎にダミーPUF読み出しの方法、パターン、設定を変化させるために、起動毎に変化するランダム情報を利用して良い。このランダム情報は、十分なエントロピーを持つ乱数発生器が生成した乱数が使用されうる。ランダム情報を利用して起動毎にダミーPUF読み出しの方法、パターン、設定（例えば上述のAD変換器の動作設定）を変化させることで、本開示の実施の形態に係る固体撮像装置1は、攻撃者による本物のPUF読み出しの推測を極めて困難にさせることができる。

[0102] 具体的には、本開示の実施の形態に係る固体撮像装置1は、以下の関数 f を実装する。実装形態はアナログ、デジタルを問わないが、乱数が持つエントロピーを十分活用できる程度には f の出力は多岐に富む必要がある。

ダミーPUF読み出しパターン = f (乱数)

[0103] 図13は、本開示の実施の形態に係る固体撮像装置1が実装する関数 f の具体的な形態を示す説明図である。関数 f は、例えば数百ビット程度以上の乱数の各ビットに、図13に示すような意味を与え、また固体撮像装置1がそのように解釈するように設計する。図13に示した例では、本物のPUF読み出しと、ダミーPUF読み出しとを含んだ一連の読み出しの中で、本物のPUF読み出しを1回、ダミーPUF読み出しをN回の、計 $N+1$ 回の読み出しが実行されることを意味する。そして、本物のPUF読み出しが実行されるタイミングや、それぞれの読み出しで選択される行（または領域）も、乱数により決定される。もちろん、図13に示した関数 f の形態は一例に

過ぎないことはいうまでも無く、意味の与え方は実装に依存されるものである。実装に依存されるとは、例えば行単位での読み出ししか出来ないアレイなのか、画素単位、領域単位での読み出しが可能なアレイなのか、A/D変換器の設定を変更できるよう実装されているのか、等に応じて関数 f の意味が変わりうることを指す。

[0104] 図14は、本開示の実施の形態に係る固体撮像装置1が関数 f を実行することによる読み出しの設定例を示す説明図である。図14では、固体撮像装置1は、1回目の起動では240回のダミーPUF読み出しを実行し、3回目で本物のPUF読み出しを実行することが示されている。固体撮像装置1は、2回目の起動では400回のダミーPUF読み出しを実行し、99回目で本物のPUF読み出しを実行する。固体撮像装置1は、3回目の起動では440回のダミーPUF読み出しを実行し、221回目で本物のPUF読み出しを実行する。固体撮像装置1は、4回目の起動では150回のダミーPUF読み出しを実行し、45回目で本物のPUF読み出しを実行する。

[0105] 本開示の実施の形態に係る固体撮像装置1は、このように起動のたびにサイドチャネルリークの時系列パターンを変化させることが出来る。サイドチャネルリークの時系列パターンが変化することで、攻撃者は、どの時点のサイドチャネルリークが本物のPUF読み出しに対応するものであるのかを推定することが、極めて困難になる。そして、関数 f の定義は固体撮像装置1の使用用途に応じて柔軟に変えることができる。例えば、ダミーPUF読み出し回数に割り当てるビット数を増やすと、攻撃の困難度は上がる。ダミーPUF読み出し回数に割り当てるビット数を減らすと、一連の読み出しに要する時間が短くなる。従って、攻撃の困難度を高めたい場合は、ダミーPUF読み出し回数に割り当てるビット数を増やし、ある程度の攻撃の困難度を担保しつつ、読み出しの時間を短くしたい場合は、ダミーPUF読み出し回数に割り当てるビット数を減らすことが考えられる。

[0106] 図13では、関数 f の形態として読み出し回数や読み出しタイミングが設定されていたが、本開示は係る例に限定されるものではなく、A/D変換器の

動作設定についても乱数を利用することが出来る。

[0107] 関数 f を固体撮像装置 1 のテープアウト時に完全に決定しても良いし、セキュアな不揮発メモリ（例えば、後述の記憶部 206）に関数 f の一部のパラメータを保持することで、ある程度の柔軟性を持たせても良い。このように関数 f の一部のパラメータを不揮発メモリに保持することで、デバイス毎に異なる関数 f を実行して、異なる生成パターンで乱数を生成することが出来る。

[0108] 本実施形態における「起動」の定義について触れる。通常は PUF の読み出しは電源 ON 1 回につき 1 回でよいと考えられるため、ほとんどの場合において「起動」＝「システム電源 ON」である。一方で、1 回の電源 ON で複数回 PUF 読み出しを行う場合もある。この場合は、読み出し前に乱数を新たに発生させることで、攻撃の難易度を上げることができる。

[0109] 上述した動作を実行するための、本開示の実施の形態に係る固体撮像装置 1 の機能構成例について説明する。図 15 は、本開示の実施の形態に係る固体撮像装置 1 の機能構成例を示す説明図である。

[0110] 図 15 に示したように、本開示の実施の形態に係る固体撮像装置 1 は、読み出し制御部 202 と、画素アレイ部 204 と、記憶部 206 と、AD 変換部 208 と、固有値計算部 210 と、暗号化部 212 と、通信制御部 214 と、を含んで構成される。

[0111] 読み出し制御部 202 は、所定の入力クロック及びデータに基づいて、後述の画素アレイ部 204 を駆動させるための信号を生成して、画素アレイ部 204 を駆動させる。読み出し制御部 202 は、例えば、図 1 を用いて説明した固体撮像装置 1 の構成における制御回路 8、垂直駆動回路 4、水平駆動回路 6 を含みうる。また読み出し制御部 202 は、図 2 に示した制御回路 230 13 に設けられ得る。

[0112] 読み出し制御部 202 は、上述したように、本物の PUF 読み出しと、ダミー PUF 読み出しとを実行する。読み出し制御部 202 は、本物の PUF 読み出しと、ダミー PUF 読み出しとを実行する際に、上述したように関数

fを実行する。

[0113] 画素アレイ部204は、所定の行及び列からなる単位画素が配列されており、ソースフォロワ回路でデータを出力するよう構成されている。画素アレイ部204における各画素の回路構成は例えば図8に示したものである。画素アレイ部204は、読み出し制御部202により駆動されてアナログ信号を出力する。画素アレイ部204は、本開示のアナログデバイスの一例として機能しうる。

[0114] 記憶部206は、様々なデータやプログラムを記憶しうる記憶デバイスで構成される。例えば、記憶部206は、乱数を生成するための所定の関数fの一部のパラメータを保持する。

[0115] AD変換部208は、画素アレイ部204から各出力線を介して供給される画素信号を、それぞれA/D変換し、デジタルデータとして出力する。AD変換部208は、画素アレイ部111からの出力線毎のADC（カラムADC）を有する。つまり、AD変換部208は、複数のカラムADCを有する。1出力線に対応するカラムADCは、比較器、D/A変換器（DAC）、およびカウンタを有するシングルスロープ型のADCである。

[0116] AD変換部208は、読み出しの際に読み出し制御部202によって設定が変更されうる。読み出し制御部202によってAD変換部208の設定が変更されることで、攻撃者によるPUF値の推測を困難にさせることができる。画素アレイ部204及びAD変換部208は、本開示のデバイス部の一例として機能しうる。

[0117] 固有値計算部210は、AD変換部208から送られるデジタル信号に基づき、固体撮像装置1に固有の値（PUF値）を計算する。固有値計算部210は、PUF値として所定のビット長を有する値を生成する。固有値計算部210は、固体撮像装置1のPUF値を計算すると、その固有値を暗号化部212に送る。固有値計算部210が生成したPUF値は、暗号化部212における暗号化処理で用いられるシード、または鍵そのものとなり得る。

[0118] PUF値の計算方法は特定のものに限定されるものではない。例えば、A

D変換後のデジタル値を任意の方法で連結することでPUF値が計算されても良く、複数の画素に対してAD変換後のデジタル値に対する演算を行い、その演算結果を連結することでPUF値が計算されても良い。

[0119] 暗号化部212は、固有値計算部210が生成したPUF値を用いて、データの暗号化処理を実行する。暗号化部212は、例えば図2に示したロジック回路23014に設けられ得る。具体的には、暗号化部212は、固有値計算部210が生成したPUF値をシードまたは鍵そのものとして用いてデータの暗号化処理を行う。暗号化の対象となるのは、PUF値そのもの、画像情報、画像情報に基づく特徴量、などがありうる。固有値計算部210が生成した固有値を用いて暗号化処理を行うことで、固体撮像装置1は、データを極めてセキュアに暗号化することが出来る。

[0120] 通信制御部214は、データを固体撮像装置1の外部に送信する。通信制御部214は、撮像データを出力する場合と、暗号化部212が暗号化したデータを出力する場合とで異なる処理を行っても良い。

[0121] 本開示の実施の形態に係る固体撮像装置1は、係る構成を有することで、物理パラメータとして実現されているPUFがAD変換完了までに発しうるサイドチャネルリークを最小化し、攻撃者による攻撃を困難化することが可能とすることが出来る。

[0122] [1. 3. 動作例]

続いて本開示の実施の形態に係る固体撮像装置1の動作例を説明する。図16は、本開示の実施の形態に係る固体撮像装置1の動作例を示す流れ図である。図16に示した流れ図は、固体撮像装置1が起動してから、アナログの電気信号からPUF値を生成するまでの流れを示したものである。

[0123] 固体撮像装置1は、起動後に読み出しの設定を行う（ステップS102）。読み出しの設定は、例えば読み出し制御部202が実行する。読み出しの設定としては、ダミーPUF読み出しの回数や画素アレイ部204からの読み出し位置、本物のPUF読み出しのタイミングや画素アレイ部204からの読み出し位置、AD変換部208のAD変換の設定などがあり得る。また

固体撮像装置 1 は、読み出しの設定の際に乱数発生器が生成した乱数を用いても良い。また固体撮像装置 1 は、読み出しの設定の際に記憶部 206 に記憶された情報を用いても良い。

[0124] 固体撮像装置 1 は、読み出しの設定を行うと、その読み出しの設定に基づいた一連の読み出しの実行を行う（ステップ S104）。一連の読み出しの実行は、例えば読み出し制御部 202 が実行する。

[0125] 固体撮像装置 1 は、一連の読み出しを実行すると、本物の PUF 読み出しであれば、読み出しに基づいて PUF 値の生成を実行する（ステップ S106）。PUF 値の生成は、例えば固有値計算部 210 が実行する。ここで、固有値計算部 210 はダミー読み出しによるダミー PUF 値の生成も行っても良い。これにより、デジタル回路でのサイドチャネルリークを最小化することが可能となる。

[0126] 本開示の実施の形態に係る固体撮像装置 1 は、このような一連の動作を実行することで、物理パラメータとして実現されている PUF が AD 変換完了までに発しうるサイドチャネルリークを最小化し、攻撃者による攻撃を困難化することが可能とすることが出来る。

[0127] [1. 4. 変形例]

続いて本実施形態のダミー PUF 読み出しの変形例を説明する。図 17～19 は、本開示の実施の形態に係る固体撮像装置 1 が実行するダミー PUF 読み出しの変形例を示す説明図である。

[0128] 本実施形態にかかる固体撮像装置 1 は、ダミー PUF 読み出しとして、例えば図 17 において実線で囲ったように、離れている少なくとも 2 つの行を読み出し、その読み出した結果を加算する動作を行っても良い。また本実施形態にかかる固体撮像装置 1 は、ダミー PUF 読み出しとして、例えば図 18 において実線で囲ったように、隣接する少なくとも 2 つの行を読み出し、その読み出した結果を加算する動作を行っても良い。本実施形態にかかる固体撮像装置 1 は、ダミー PUF 読み出しとして、例えば図 19 において実線で囲ったように、列単位で異なる行の画素を読み出す動作を行っても良い。

[0129] また、図 1 7 ～ 1 9 に示した例の他にも、本実施形態にかかる固体撮像装置 1 は様々な読み出しを実行しうる。例えば、本実施形態にかかる固体撮像装置 1 は、図 1 7 に示した読み出しと図 1 8 に示した読み出しとを組み合わせ、隣接する少なくとも 2 つの行を読み出した結果を複数加算する動作を実行しても良い。また本実施形態にかかる固体撮像装置 1 は、図 1 7 または図 1 8 に示した読み出しと、図 1 9 に示した読み出しとを組み合わせ、列単位で異なる行の画素を読み出したものを 2 つ以上加算した動作を実行したり、列単位で異なる、隣接する少なくとも 2 つの行の画素を読み出したものを 2 つ以上加算した動作を実行したりしても良い。

[0130] そして本実施形態にかかる固体撮像装置 1 は、この変形例においても、本物の P U F 読み出しやダミー P U F 読み出しの設定を乱数に基づき決定してもよい。

[0131] < 2. まとめ >

以上説明したように本開示の実施の形態によれば、物理パラメータとして実現されている P U F が A D 変換完了までに発しうるサイドチャネルリークを最小化し、攻撃者による攻撃を困難化することが可能な固体撮像装置 1 を提供することができる。

[0132] 本明細書の各装置が実行する処理における各ステップは、必ずしもシーケンス図または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処理する必要はない。例えば、各装置が実行する処理における各ステップは、フローチャートとして記載した順序と異なる順序で処理されても、並列的に処理されてもよい。

[0133] また、各装置に内蔵される C P U、R O M および R A M などのハードウェアを、上述した各装置の構成と同等の機能を発揮させるためのコンピュータプログラムも作成可能である。また、該コンピュータプログラムを記憶させた記憶媒体も提供されることが可能である。また、機能ブロック図で示したそれぞれの機能ブロックをハードウェアで構成することで、一連の処理をハードウェアで実現することもできる。

[0134] 以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

[0135] また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

[0136] なお、以下のような構成も本開示の技術的範囲に属する。

(1)

規則的に配置されるアナログデバイスを有するデバイス部と、
前記デバイス部の固有情報を生成する第1の読み出しと、前記デバイス部の固有情報を生成しない第2の読み出しと、を混在させた読み出しを実行する読み出し制御部と、
を備える、制御装置。

(2)

前記読み出し制御部は、前記デバイス部に対する読み出し位置を異ならせることで前記第1の読み出しと前記第2の読み出しとを混在させる、前記(1)に記載の制御装置。

(3)

前記デバイス部から出力されるアナログ値をデジタル値に変換するAD変換部をさらに備え、

前記読み出し制御部は、前記AD変換部の設定を異ならせることで前記第1の読み出しと前記第2の読み出しとを混在させる、前記(1)または(2)に記載の制御装置。

(4)

前記読み出し制御部は、ランダムに生成されるランダム情報に基づいて前記第 1 の読み出しと前記第 2 の読み出しとを混在させる、前記（１）～（３）のいずれかに記載の制御装置。

（５）

前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する読み出し位置を決定する、前記（４）に記載の制御装置。

（６）

前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する前記第 2 の読み出しの回数を決定する、前記（４）または（５）に記載の制御装置。

（７）

前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する前記第 1 の読み出しのタイミングを決定する、前記（４）～（６）のいずれかに記載の制御装置。

（８）

前記デバイス部から出力されるアナログ値をデジタル値に変換する A/D 変換部をさらに備え、

前記読み出し制御部は、前記ランダム情報に基づいて前記 A/D 変換部に対する設定を決定する、前記（４）～（７）のいずれかに記載の制御装置。

（９）

前記ランダム情報は、前記固有情報を生成する処理以前に生成される、前記（４）～（８）のいずれかに記載の制御装置。

（１０）

前記ランダム情報を生成するための関数の少なくとも一部のパラメータを記憶する記憶部をさらに備える、前記（４）～（９）のいずれかに記載の制御装置。

（１１）

前記読み出し制御部は、前記読み出しの区間において、前記第 1 の読み出

しは一度だけ実行する、前記（１）～（１０）のいずれかに記載の制御装置。

（１２）

規則的に配置されるアナログデバイスを有するデバイス部の固有情報を生成する第１の読み出しと、前記デバイス部の固有情報を生成しない第２の読み出しと、を混在させた読み出しを実行することを含む、制御方法。

（１３）

ランダム情報を生成し、

前記ランダム情報に基づいて、複数の行を含む画素アレイの所定の行を読み出し、

前記所定の行の読み出しに基づいて、デバイスの固有情報を生成し、

前記所定の行以外の行の読み出しに基づいて、ダミー情報を生成する読み出し方法。

（１４）

前記ランダム情報に基づいて、前記複数の行を読み出す順番を制御する

前記（１３）に記載の読み出し方法。

（１５）

前記デバイスの固有情報は、PUF値である

前記（１３）に記載の読み出し方法。

（１６）

前記デバイスの固有情報は、半導体製造中に発生する物理変数と関連する

前記（１３）に記載の読み出し方法。

（１７）

前記ランダム情報は、前記画素アレイを含む撮像装置が電源オンされたときに生成される

前記（１３）に記載の読み出し方法。

（１８）

前記ランダム情報は、前記撮像装置の駆動回路に基づいて生成される

前記（１７）に記載の読み出し方法。

（１９）

前記デバイスの固有情報と前記ダミー情報とを結合する

前記（１３）に記載の読み出し方法。

（２０）

ランダム情報を生成し、

前記ランダム情報に基づいて、複数の行を含む画素アレイの所定の行を読み出し、

前記所定の行の読み出しに基づいて、デバイスの固有情報を生成し、

前記所定の行以外の行の読み出しに基づいて、ダミー情報を生成する

コンピュータプログラム。

（２１）

プロセッサと、

前記プロセッサによって実行可能なプログラムを格納するメモリと、

を有し、

前記プログラムは、

ランダム情報を生成し、

前記ランダム情報に基づいて、複数の行を含む画素アレイの所定の行を読み出し、

前記所定の行の読み出しに基づいて、デバイスの固有情報を生成し、

前記所定の行以外の行の読み出しに基づいて、ダミー情報を生成する

読み出し装置。

符号の説明

- [0137] 1 : 固体撮像装置
2 : 画素
3 : 画素アレイ
4 : 垂直駆動回路
5 : カラム信号処理回路

- 6 : 水平駆動回路
- 7 : 出力回路
- 8 : 制御回路
- 9 : 垂直信号線
- 10 : 水平信号線
- 11 : 半導体基板
- 12 : 入出力端子

請求の範囲

- [請求項1] 規則的に配置されるアナログデバイスを有するデバイス部と、
前記デバイス部の固有情報を生成する第1の読み出しと、前記デバイス部の固有情報を生成しない第2の読み出しと、を混在させた読み出しを実行する読み出し制御部と、
を備える、制御装置。
- [請求項2] 前記読み出し制御部は、前記デバイス部に対する読み出し位置を異ならせることで前記第1の読み出しと前記第2の読み出しとを混在させる、請求項1に記載の制御装置。
- [請求項3] 前記デバイス部から出力されるアナログ値をデジタル値に変換するA/D変換部をさらに備え、
前記読み出し制御部は、前記A/D変換部の設定を異ならせることで前記第1の読み出しと前記第2の読み出しとを混在させる、請求項1に記載の制御装置。
- [請求項4] 前記読み出し制御部は、ランダムに生成されるランダム情報に基づいて前記第1の読み出しと前記第2の読み出しとを混在させる、請求項1に記載の制御装置。
- [請求項5] 前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する読み出し位置を決定する、請求項4に記載の制御装置。
- [請求項6] 前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する前記第2の読み出しの回数を決定する、請求項4に記載の制御装置。
- [請求項7] 前記読み出し制御部は、前記ランダム情報に基づいて前記デバイス部に対する前記第1の読み出しのタイミングを決定する、請求項4に記載の制御装置。
- [請求項8] 前記デバイス部から出力されるアナログ値をデジタル値に変換するA/D変換部をさらに備え、
前記読み出し制御部は、前記ランダム情報に基づいて前記A/D変換

部に対する設定を決定する、請求項 4 に記載の制御装置。

[請求項9] 前記ランダム情報は、前記固有情報を生成する処理以前に生成される、請求項 4 に記載の制御装置。

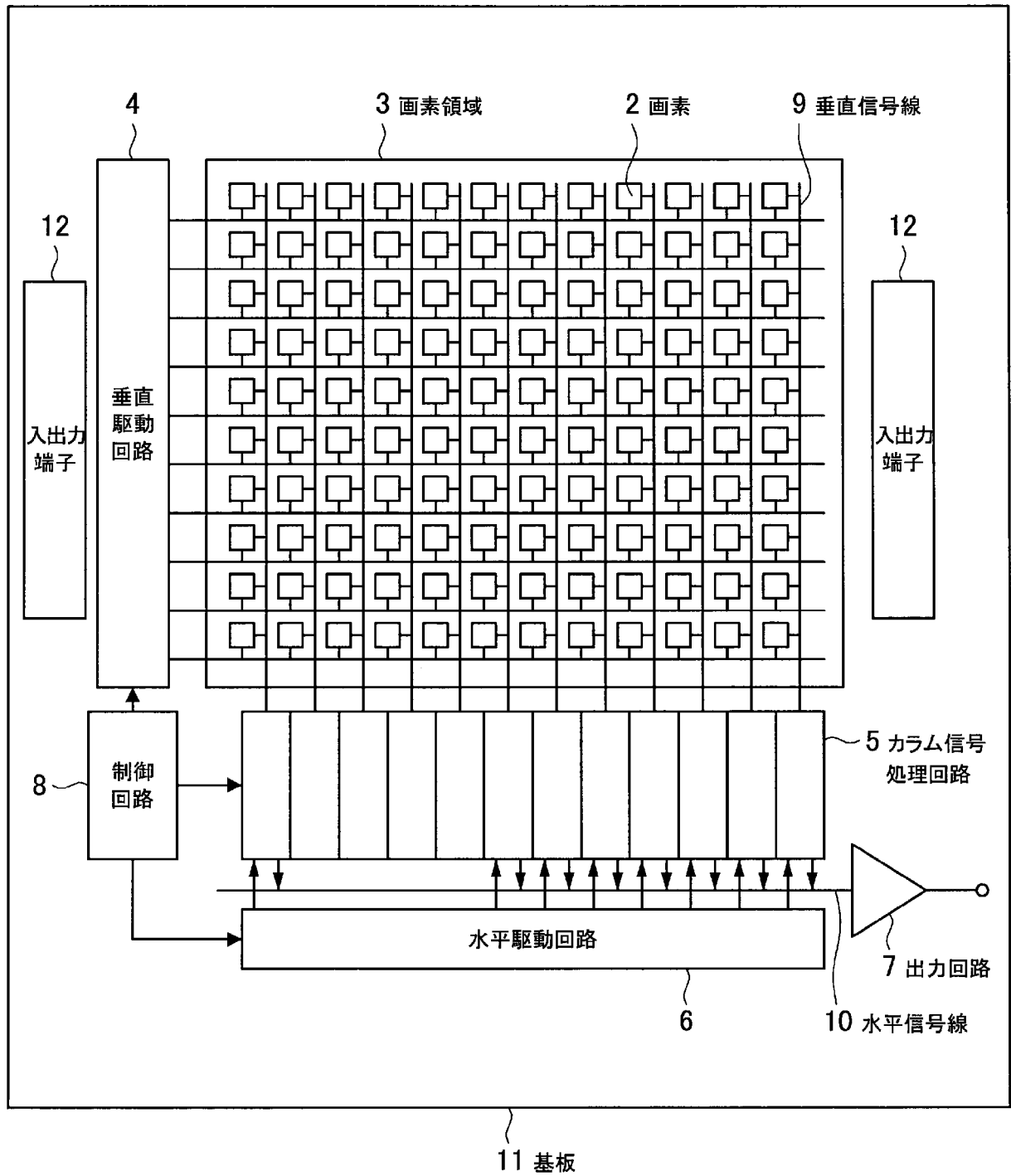
[請求項10] 前記ランダム情報を生成するための関数の少なくとも一部のパラメータを記憶する記憶部をさらに備える、請求項 4 に記載の制御装置。

[請求項11] 前記読み出し制御部は、前記読み出しの区間において、前記第 1 の読み出しは一度だけ実行する、請求項 1 に記載の制御装置。

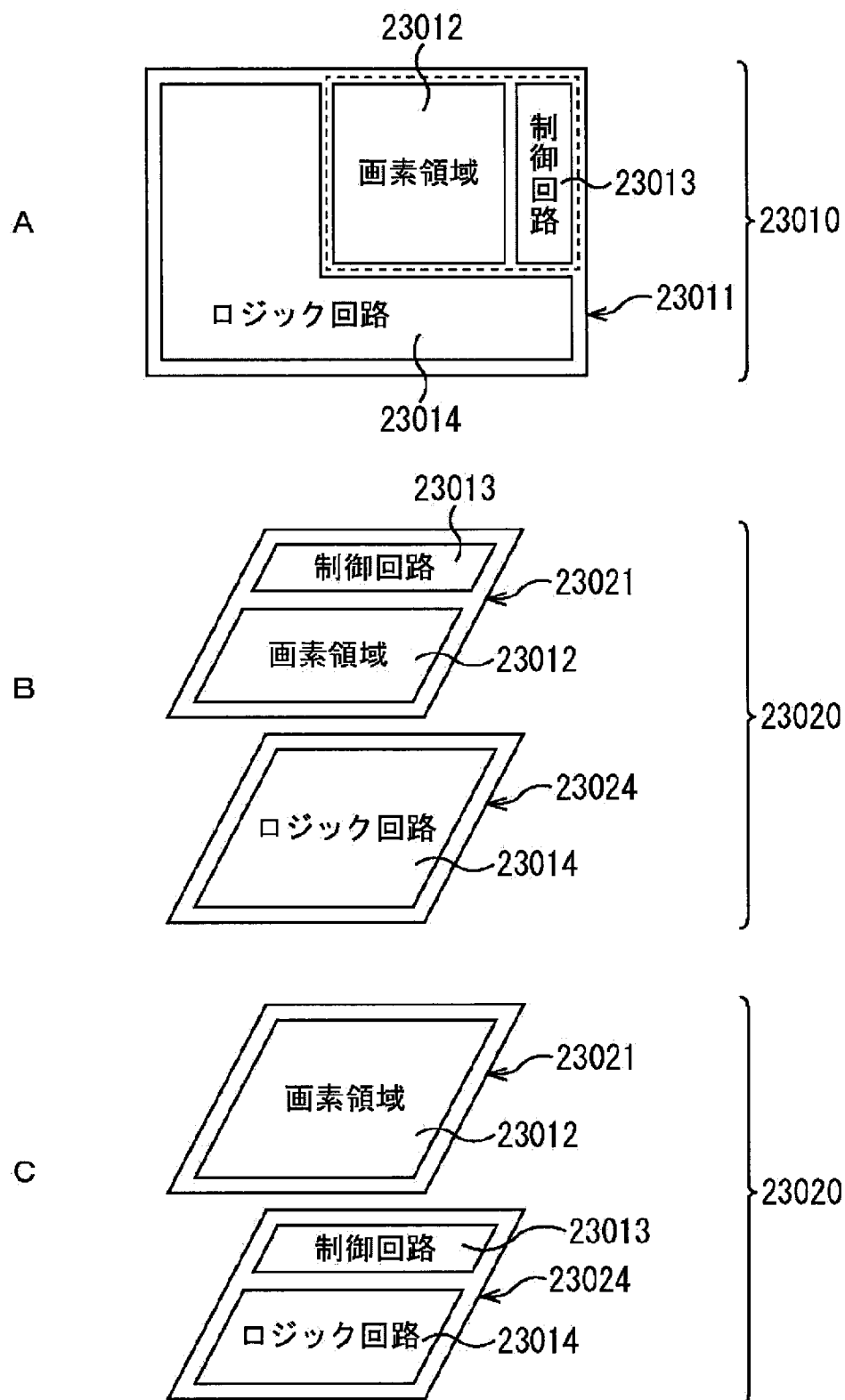
[請求項12] 規則的に配置されるアナログデバイスを有するデバイス部の固有情報を生成する第 1 の読み出しと、前記デバイス部の固有情報を生成しない第 2 の読み出しと、を混在させた読み出しを実行することを含む、制御方法。

[図1]

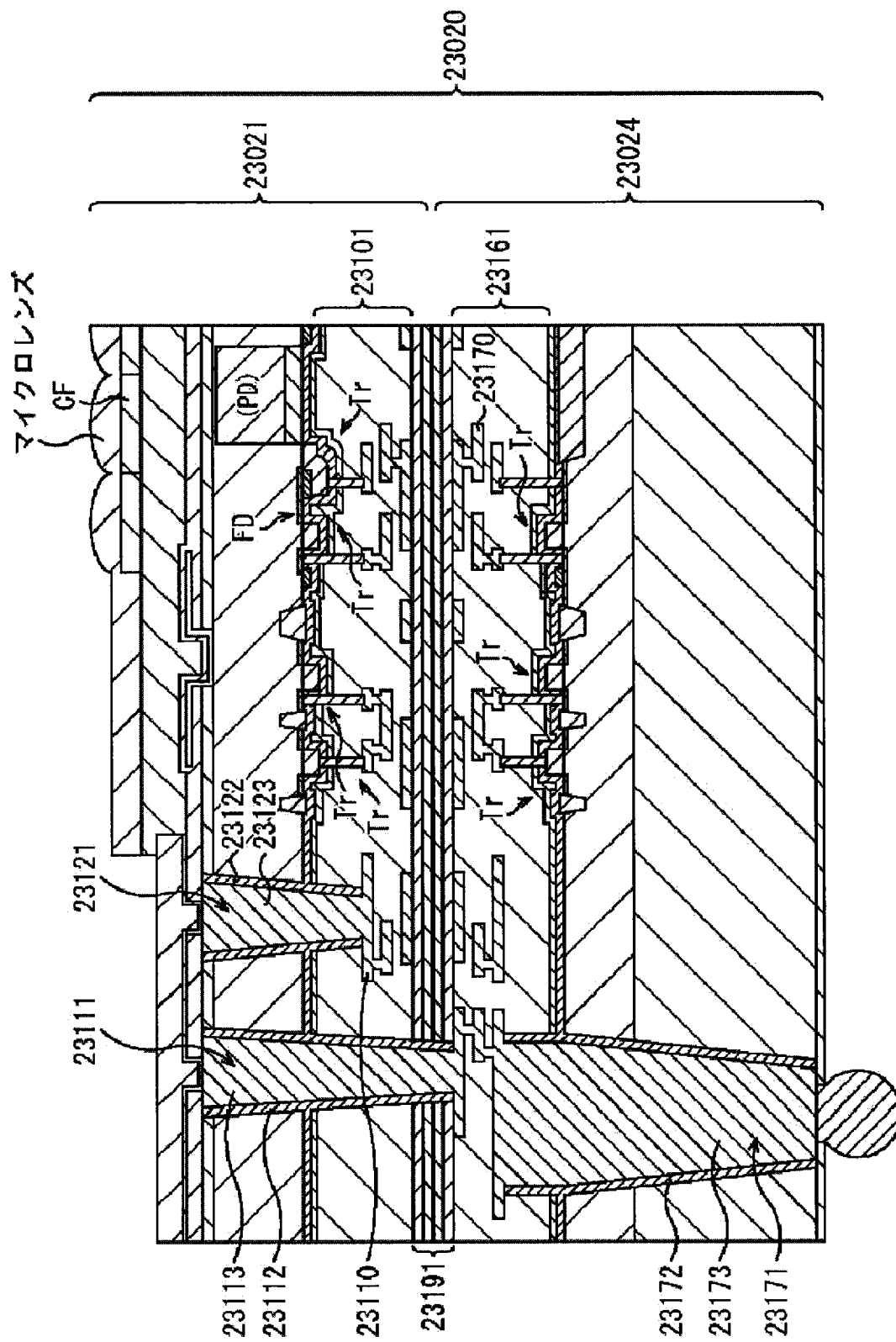
1 固体撮像装置



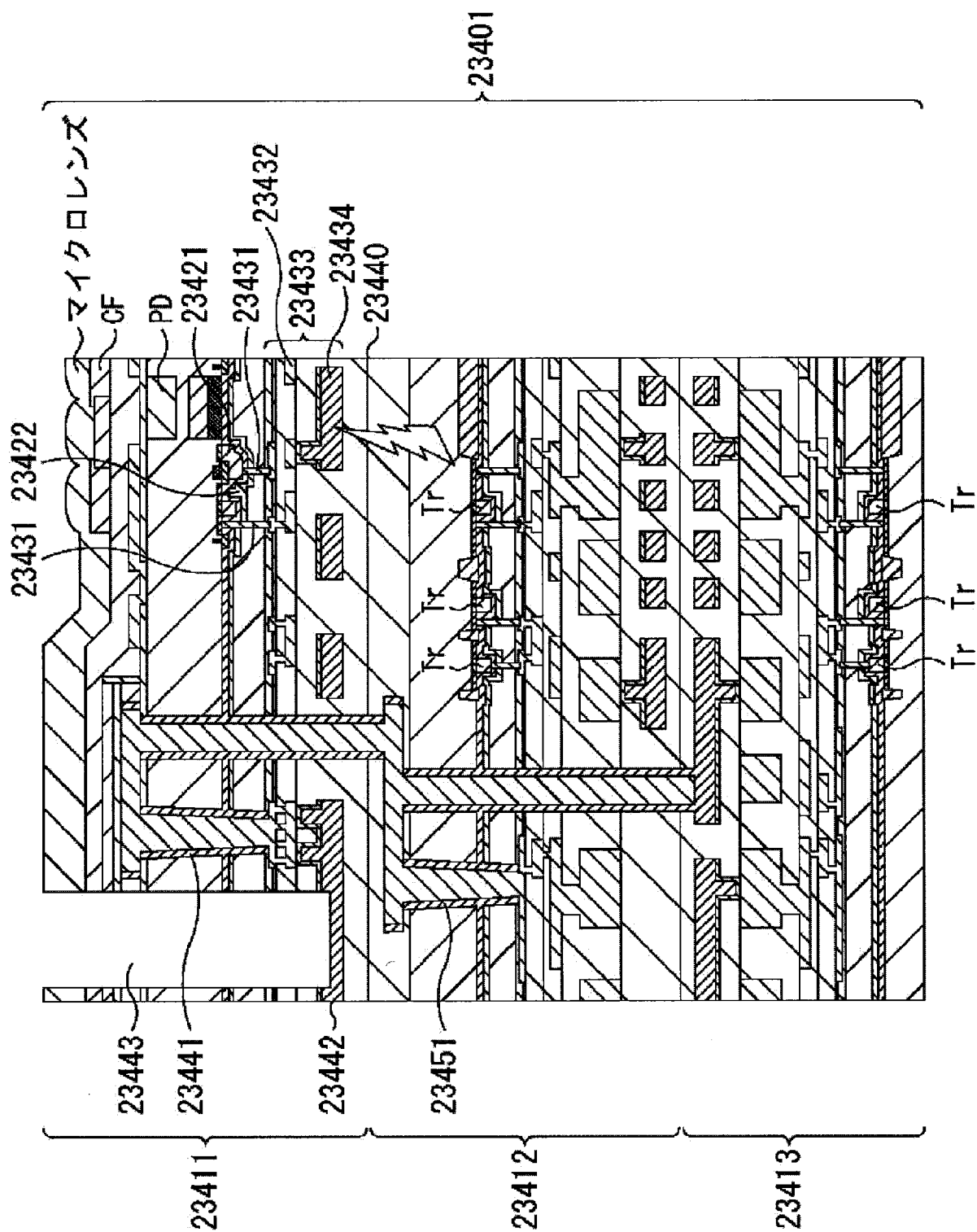
[図2]



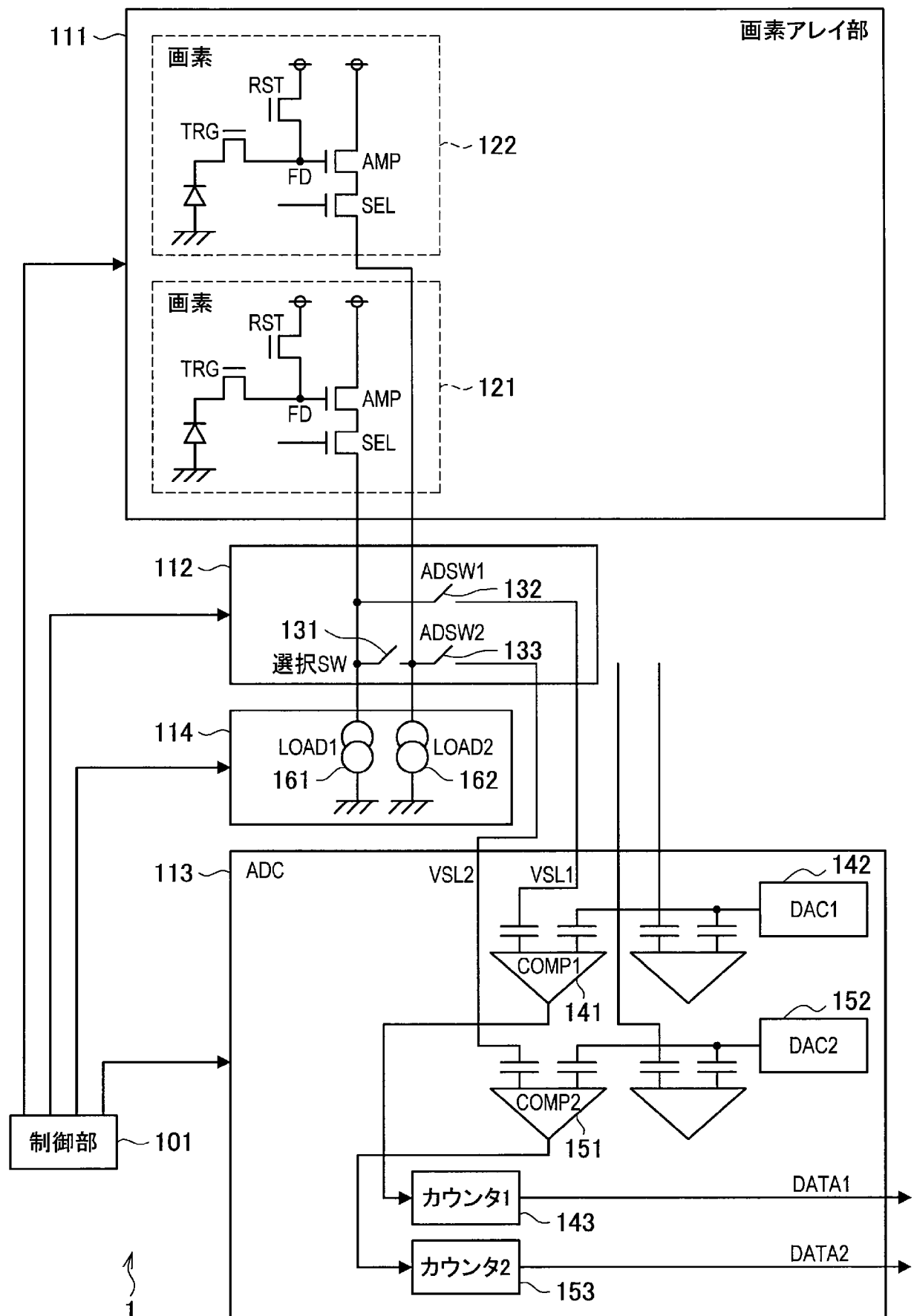
[図3]



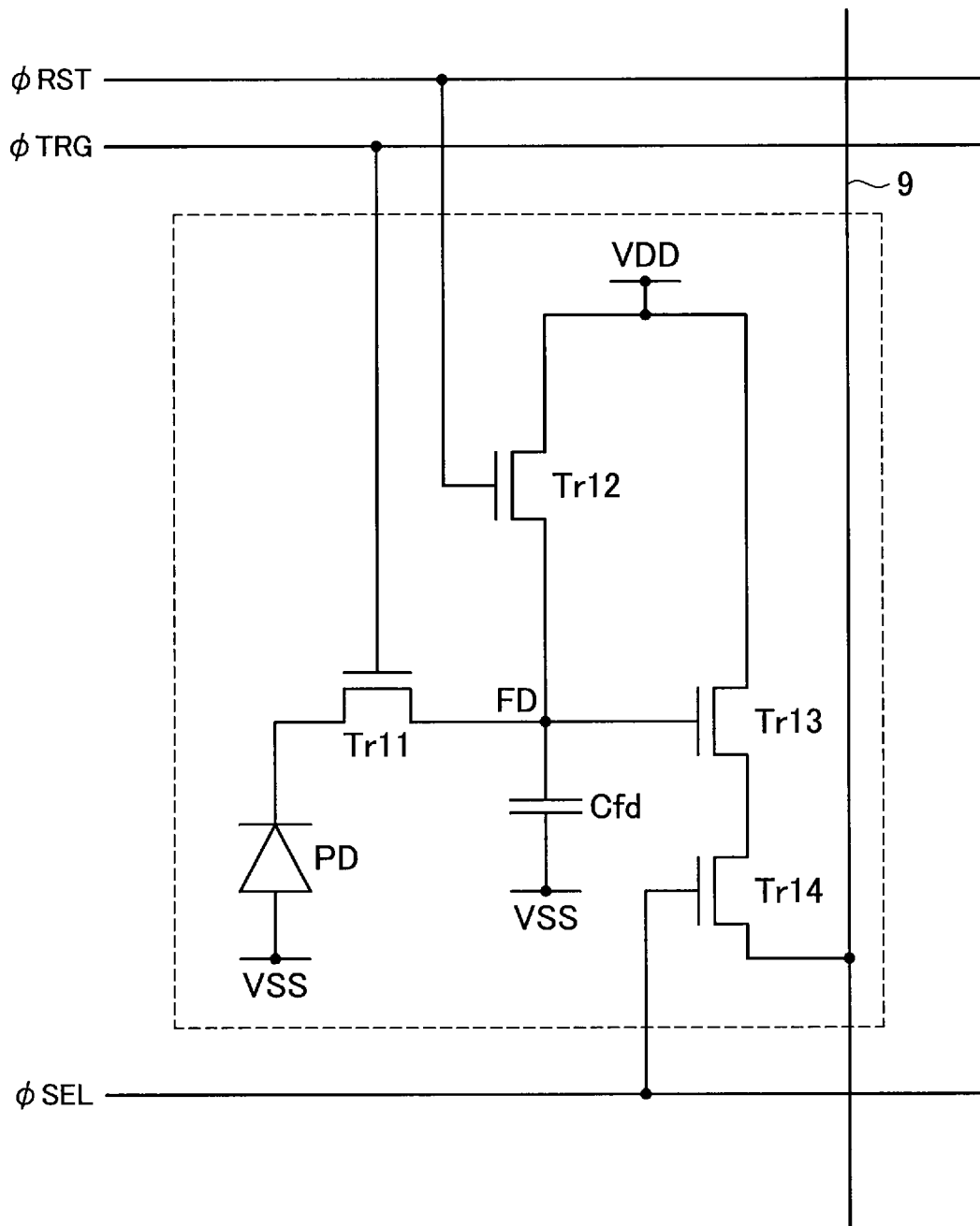
[図6]



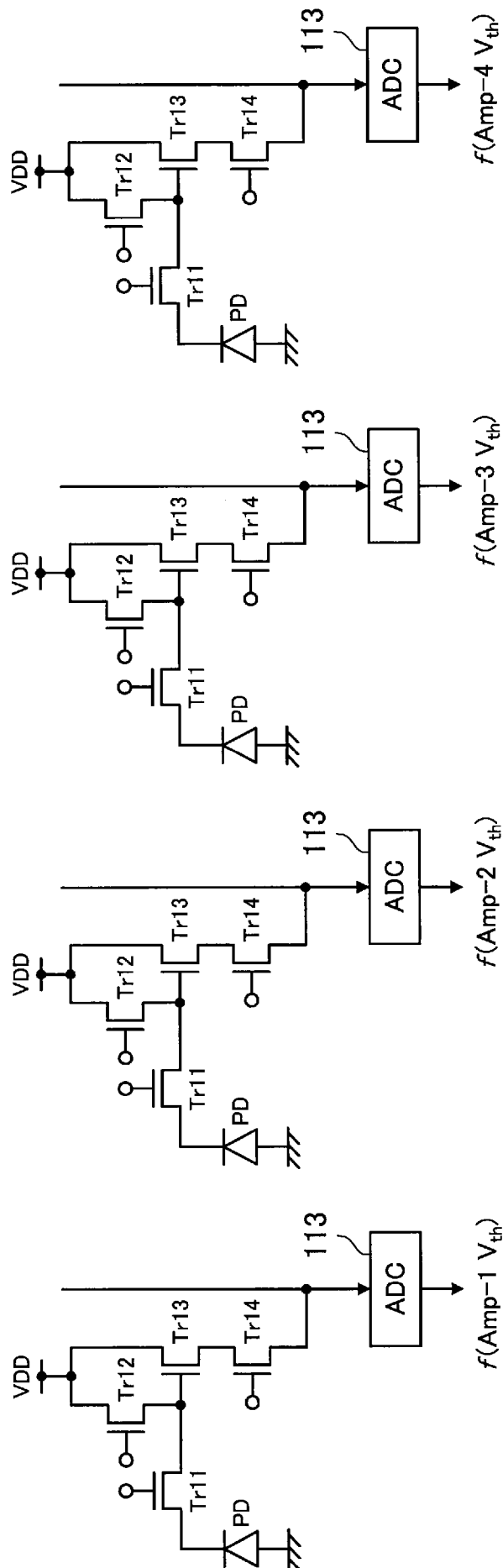
[図7]



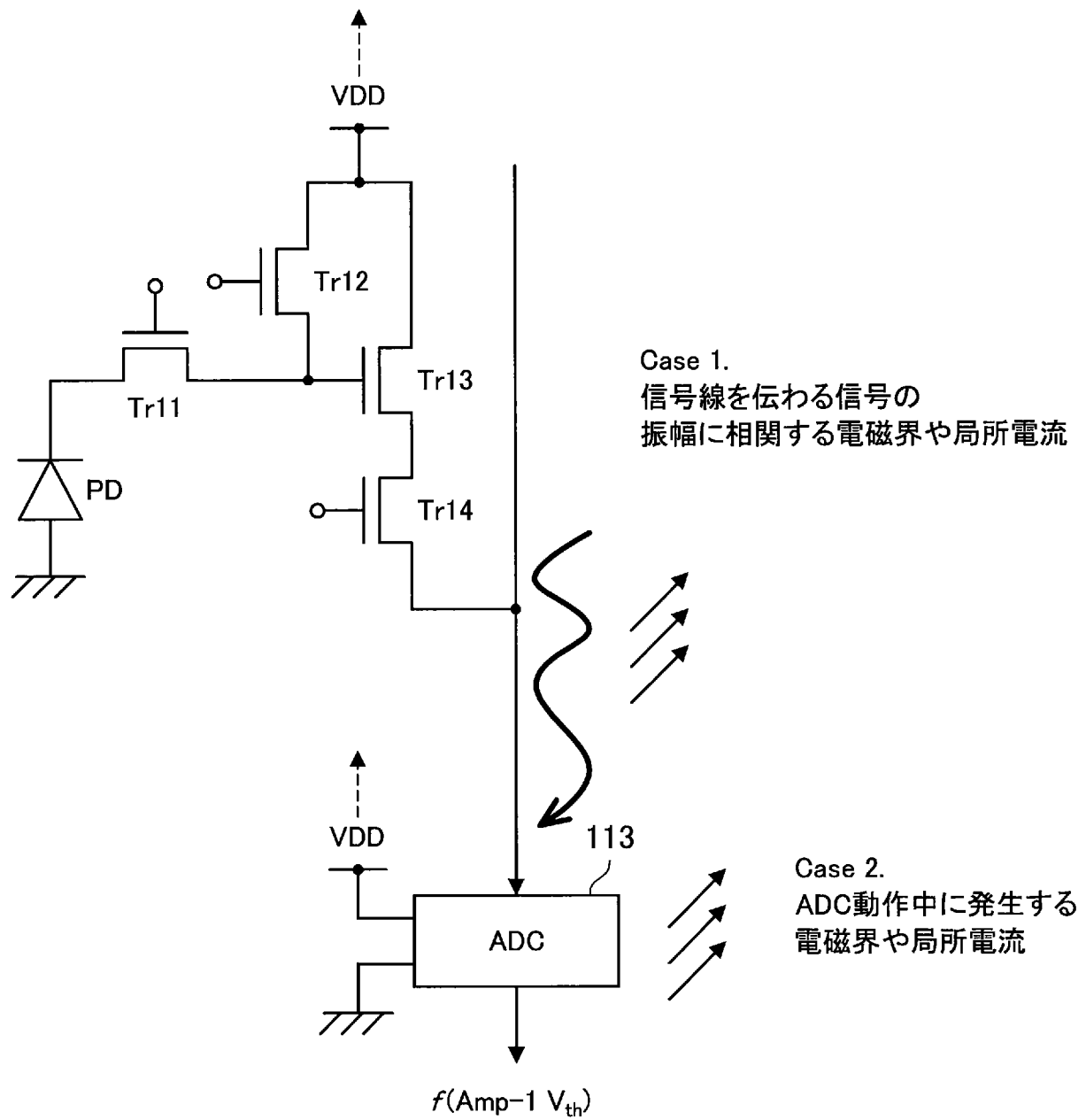
[図8]

121

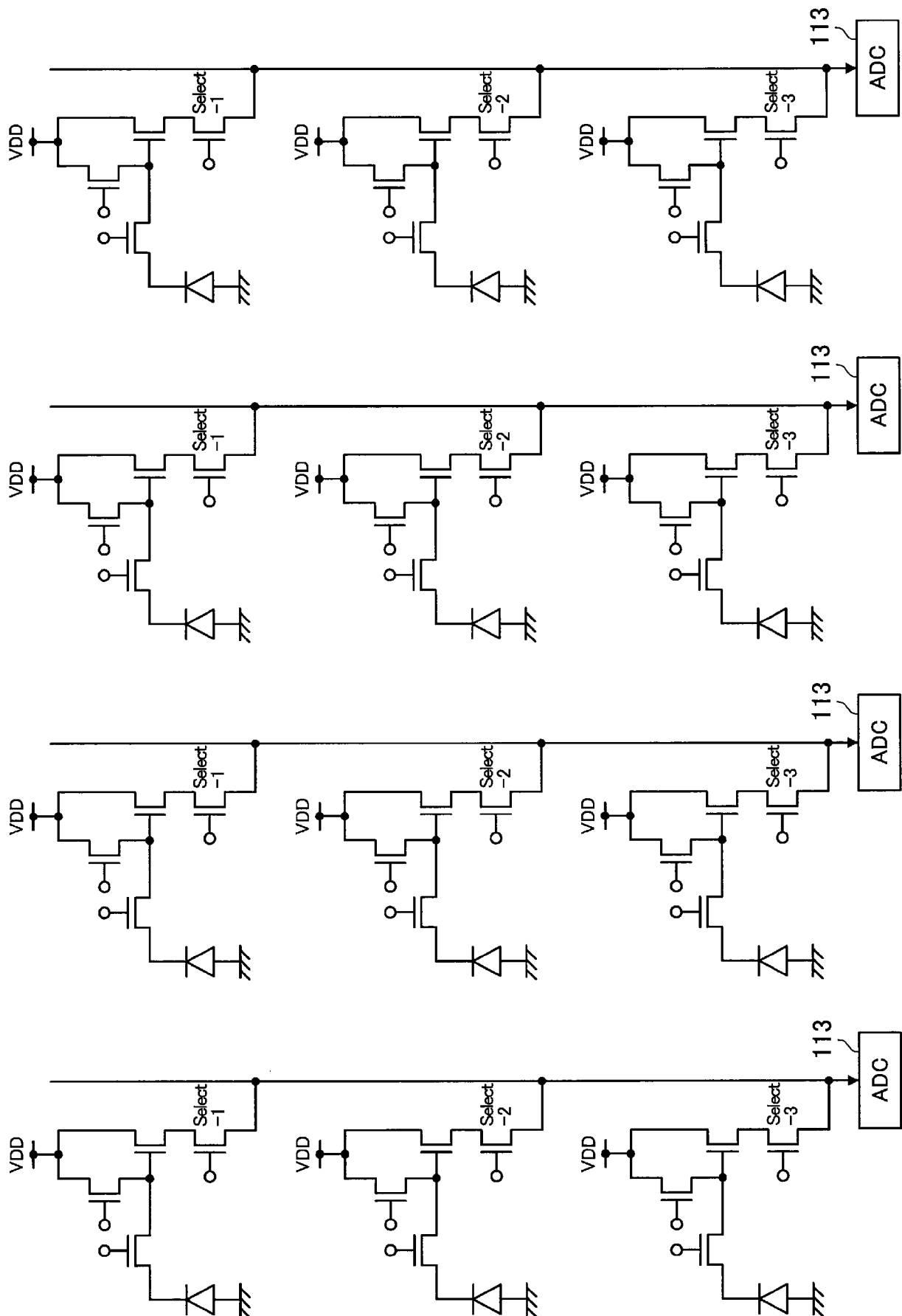
[図9]



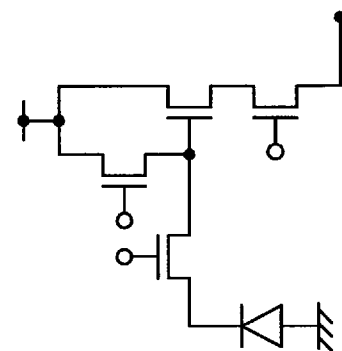
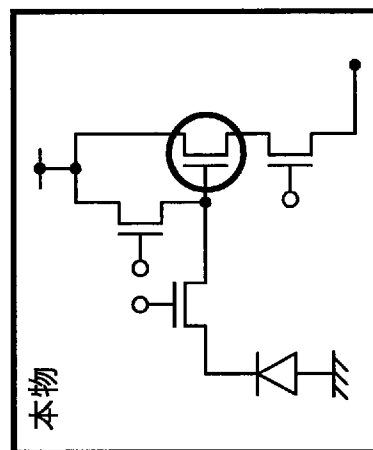
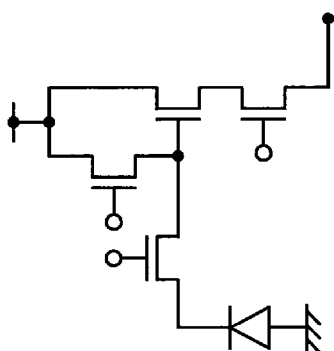
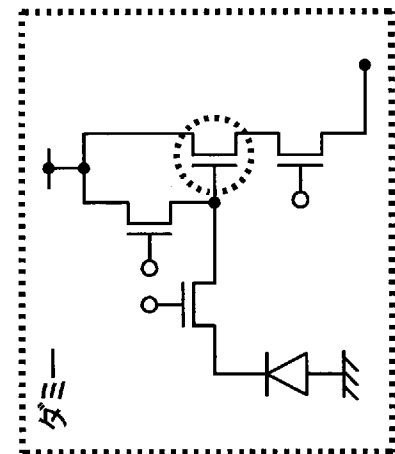
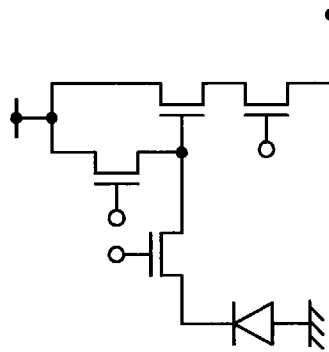
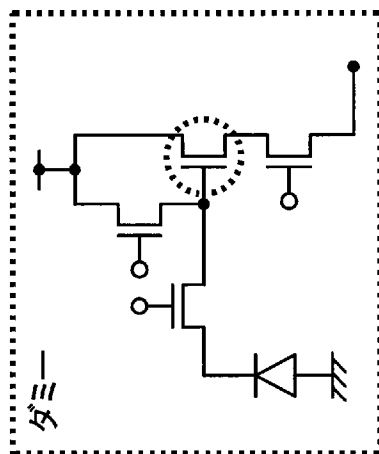
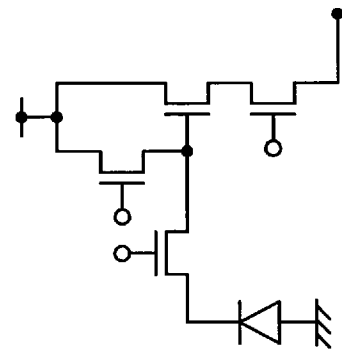
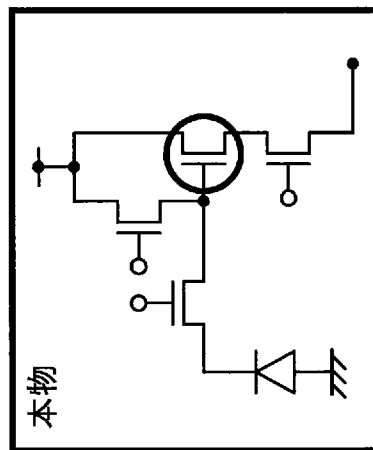
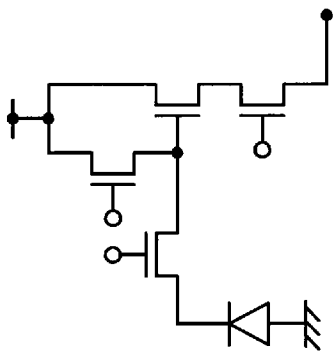
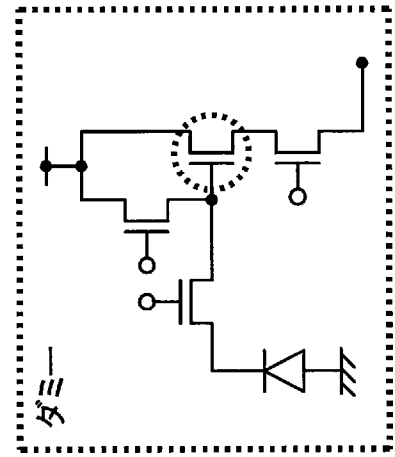
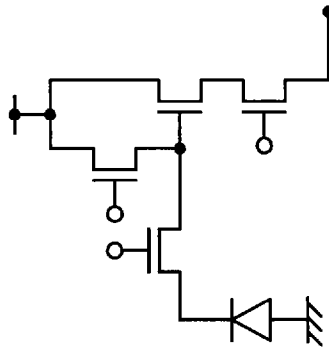
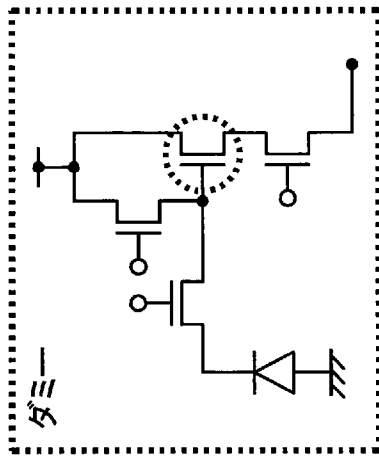
[図10]



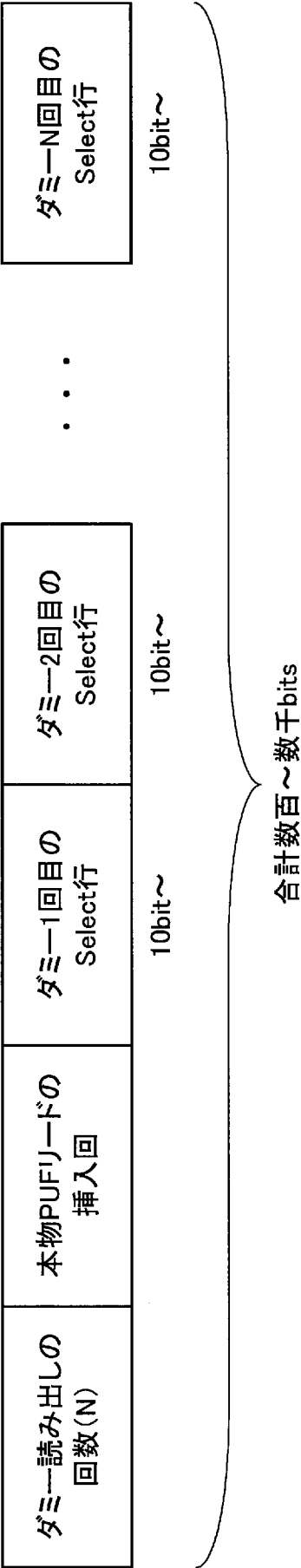
[図11]



[図12]



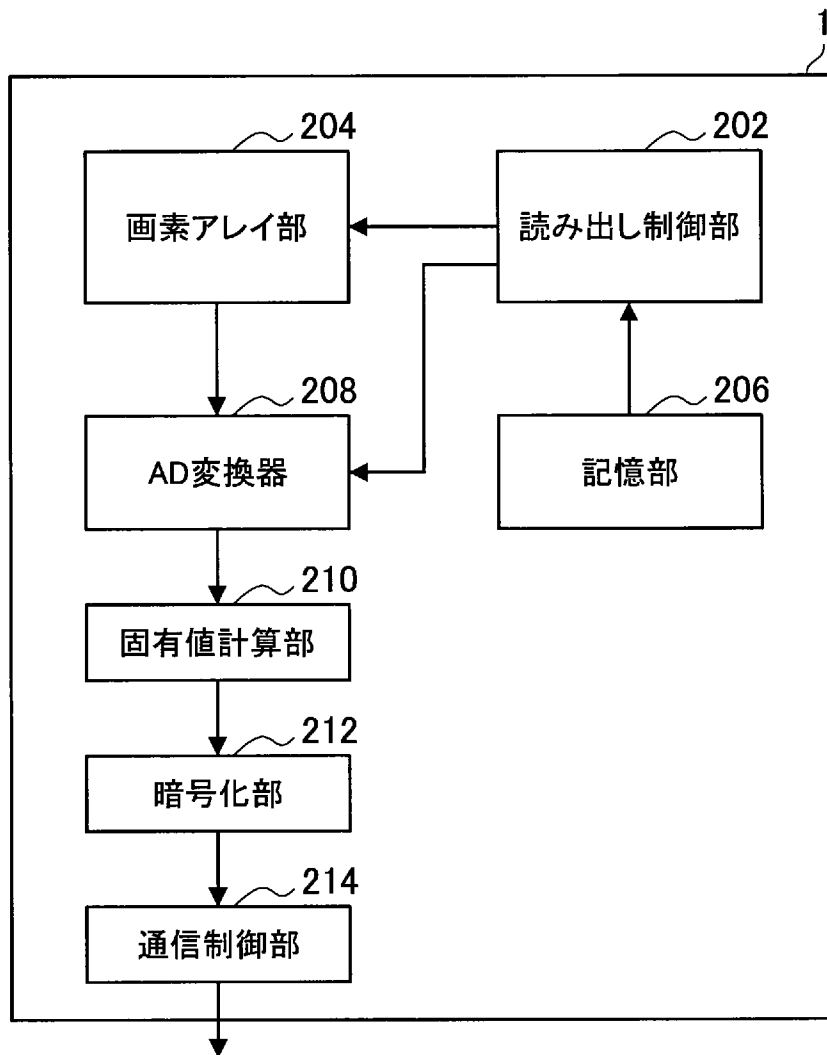
[図13]



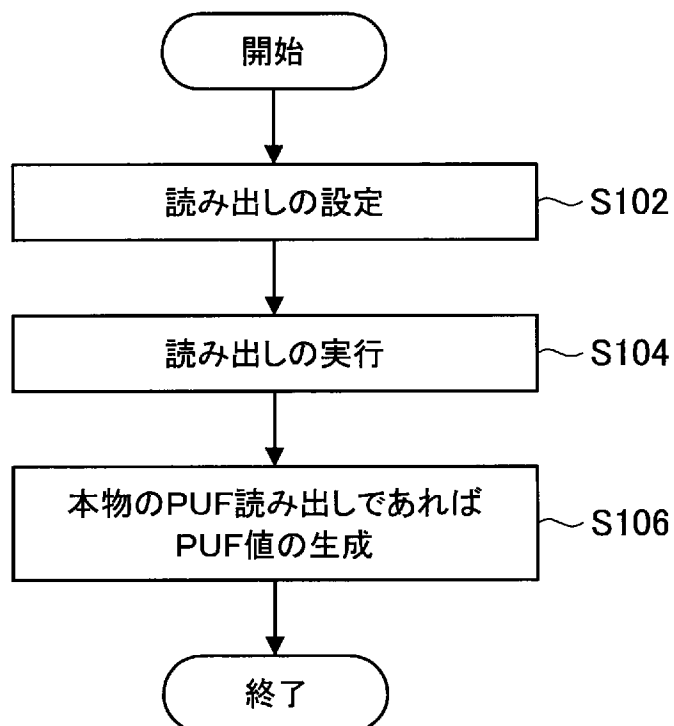
[図14]

1回目の起動	240	3	1000	1500	...	200		
2回目の起動	400	99	2020	455	...	2105	...	1123
3回目の起動	440	221	39	776	...	5	...	323
4回目の起動	150	45	543	...	211			540

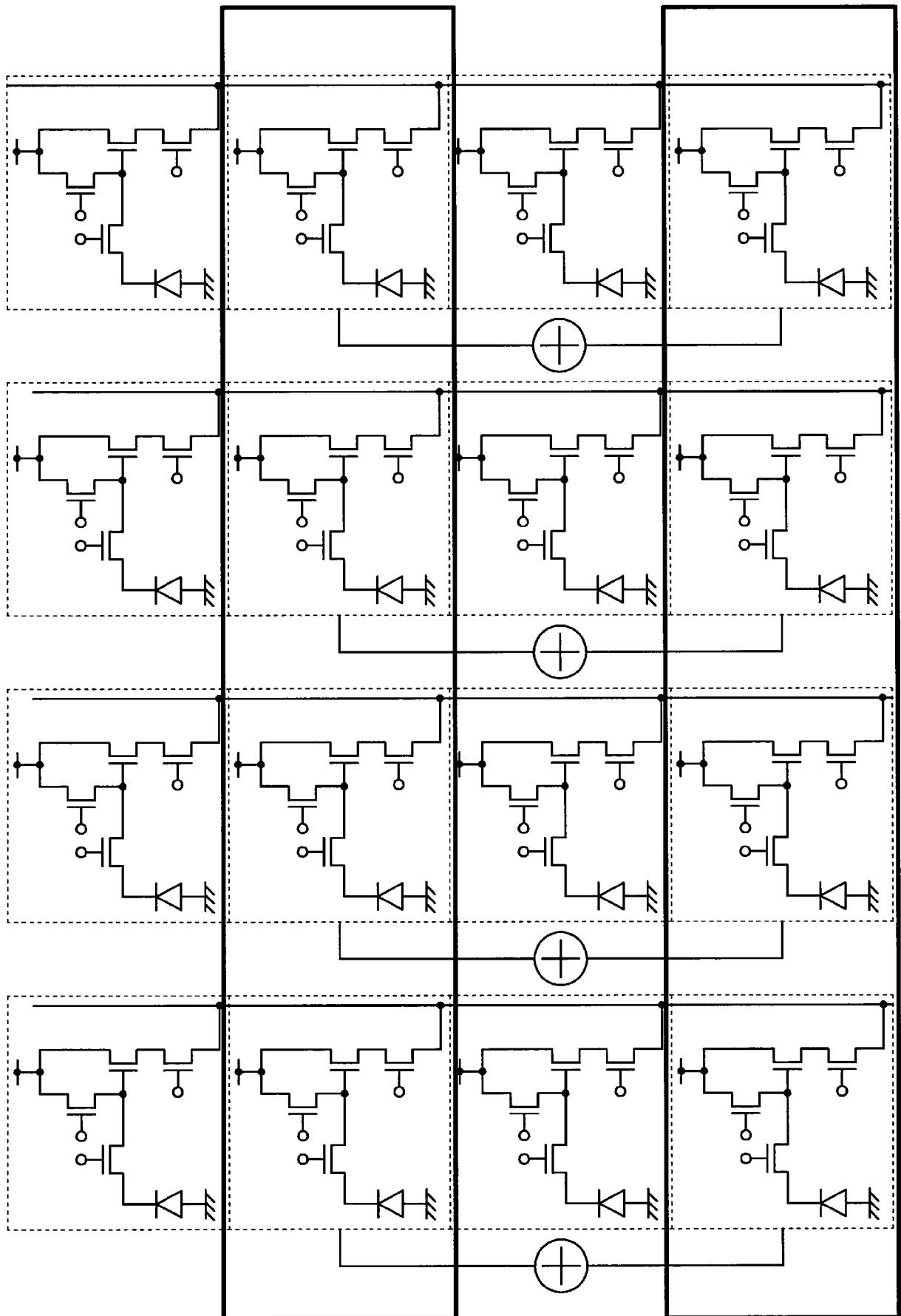
[図15]



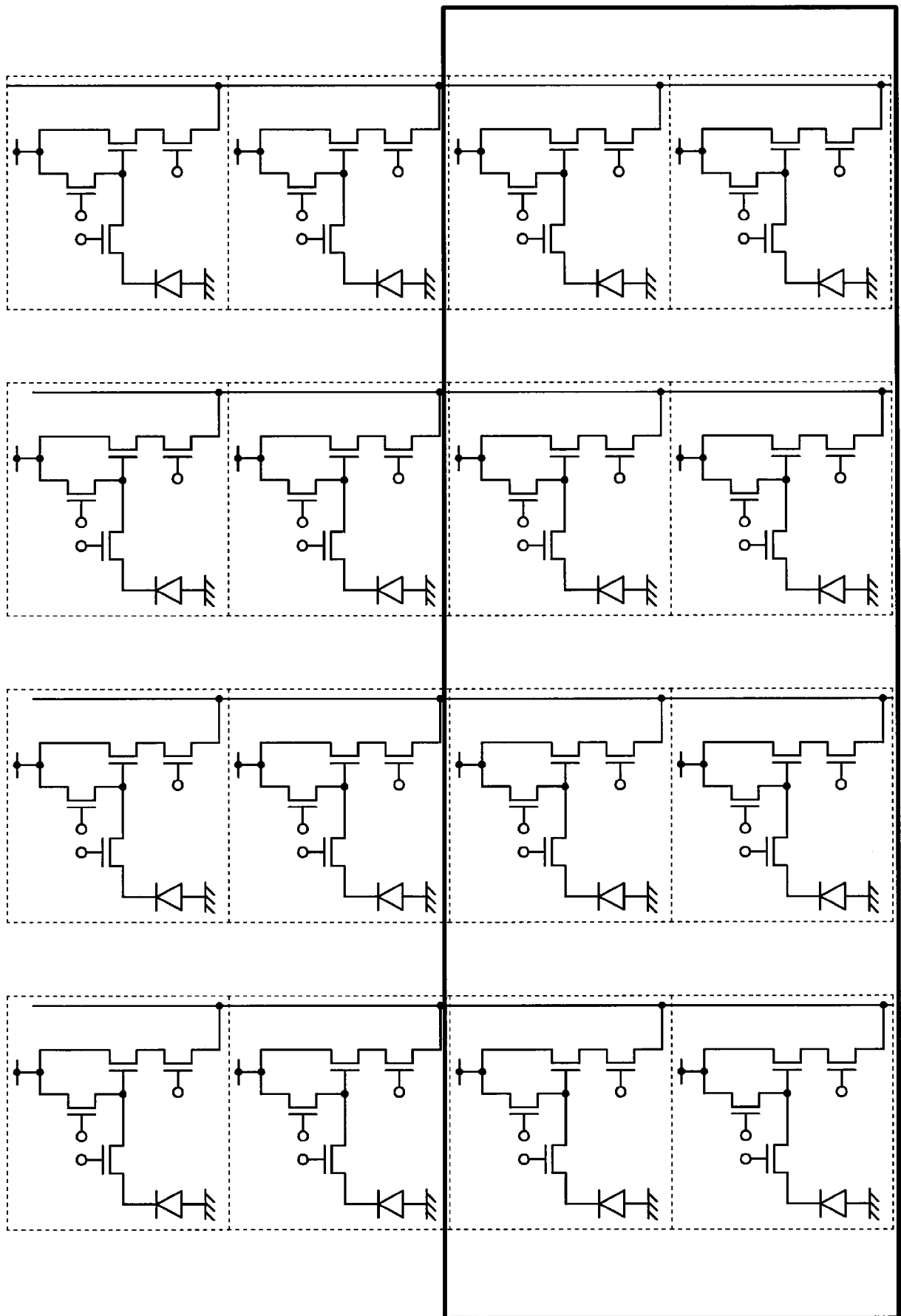
[図16]



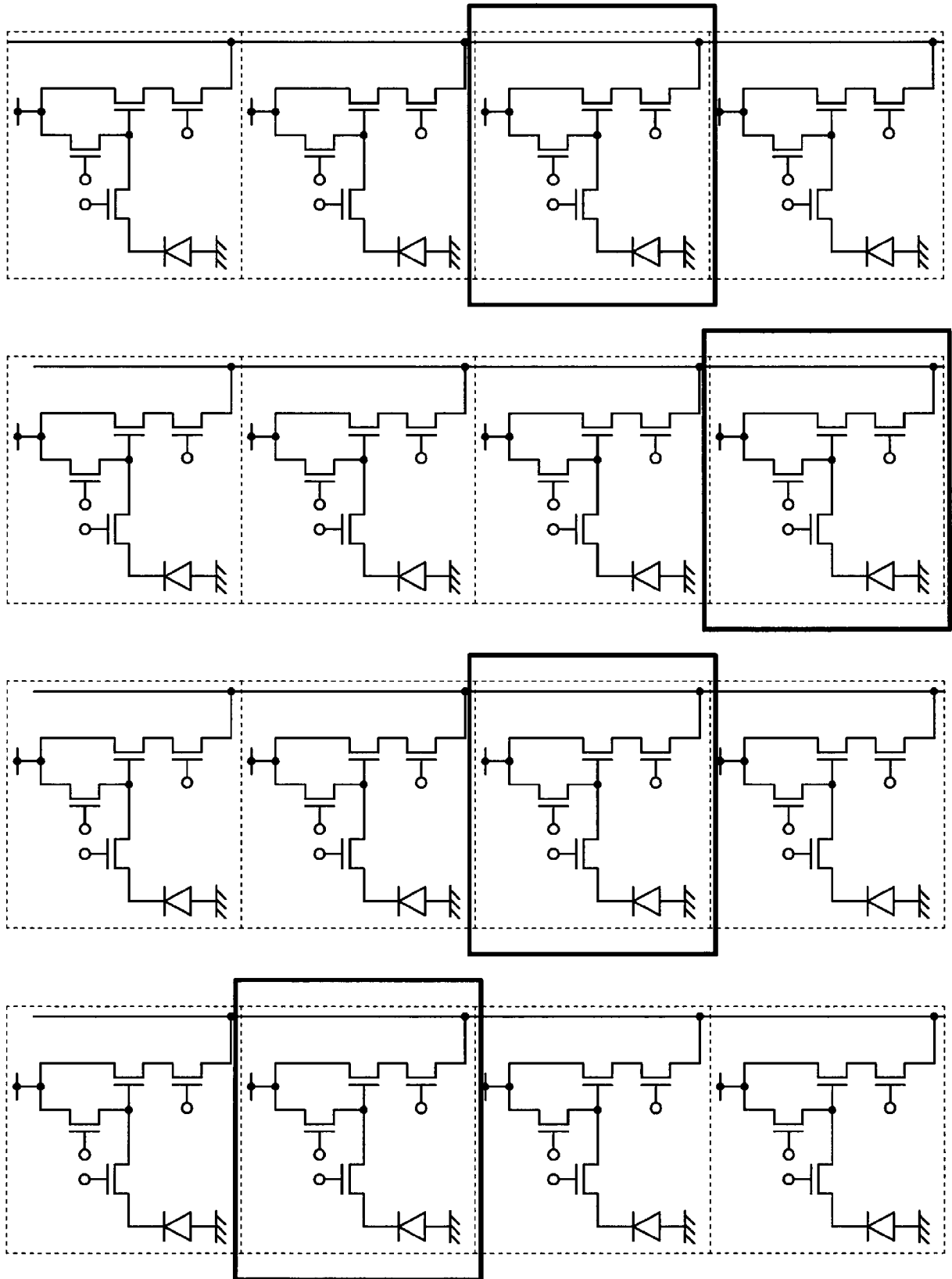
[図17]



[図18]



[図19]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/039869

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/73 (2013.01) i, G06F21/75 (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)

Int.Cl. G06F21/73, G06F21/75

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 1971-2019

Registered utility model specifications of Japan 1996-2019

Published registered utility model applications of Japan 1994-2019

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	WO 2016/167076 A1 (BRILLNICS INC. et al.) 20 October 2016, paragraphs [0066]-[0073], [0075], fig. 13, 15 & US 2018/0115723 A1, paragraphs [0090]-[0098], [0101], fig. 13, 15 & CN 107852471 A	1-2, 4-7, 9-12 3, 8
Y A	JP 2016-81522 A (THE BOEING COMPANY) 16 May 2016, abstract & US 2016/0103626 A1, abstract & EP 3007093 A1 & CN 105512055 A & TW 201633152 A	1-2, 4-7, 9-12 3, 8



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

09.01.2019

Date of mailing of the international search report

22.01.2019

Name and mailing address of the ISA/

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku,

Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/039869

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9135453 B2 (SHEN-ORR, C. et al.) 15 September 2015, abstract & GB 2494731 A & WO 2013/035006 A1 & CN 103748826 A	1-12

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/73(2013.01)i, G06F21/75(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. G06F21/73, G06F21/75

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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	WO 2016/167076 A1（ブリルニクス インクほか）2016.10.20, 段落 [0066]-[0073], [0075], 図 13, 15 & US 2018/0115723 A1, paragraphs [0090]-[0098], [0101], figures 13, 15 & CN 107852471 A	1-2, 4-7, 9-12 3, 8
Y A	JP 2016-81522 A（ザ・ボーイング・カンパニー）2016.05.16, [要 約] & US 2016/0103626 A1, ABSTRACT & EP 3007093 A1 & CN 105512055 A & TW 201633152 A	1-2, 4-7, 9-12 3, 8

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

09.01.2019

国際調査報告の発送日

22.01.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

平井 誠

5 S

9071

電話番号 03-3581-1101 内線 3546

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
A	US 9135453 B2 (SHEN-ORR, Chaim et al.) 2015.09.15, ABSTRACT & GB 2494731 A & WO 2013/035006 A1 & CN 103748826 A	1-12