

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6429167号
(P6429167)

(45) 発行日 平成30年11月28日 (2018.11.28)

(24) 登録日 平成30年11月9日 (2018.11.9)

(51) Int. Cl.		F I			
H04L	9/32	(2006.01)	H04L	9/00	673C
G06F	21/44	(2013.01)	H04L	9/00	673B
G06F	21/75	(2013.01)	G06F	21/44	
			G06F	21/75	

請求項の数 5 (全 32 頁)

(21) 出願番号	特願2015-52756 (P2015-52756)	(73) 特許権者	715002353
(22) 出願日	平成27年3月17日 (2015.3.17)		渡辺 浩志
(65) 公開番号	特開2016-174254 (P2016-174254A)		神奈川県横浜市緑区寺山町689番地1
(43) 公開日	平成28年9月29日 (2016.9.29)		グランシティレイディアント横浜四季の森
審査請求日	平成29年6月30日 (2017.6.30)		公園313号
		(74) 代理人	100067448
			弁理士 下坂 スミ子
		(72) 発明者	渡辺 浩志
			神奈川県横浜市緑区寺山町689-1-3
			13
		審査官	金沢 史明

最終頁に続く

(54) 【発明の名称】 電子装置ネットワークにおける物理的チップ認証方式

(57) 【特許請求の範囲】

【請求項1】

複数のネットワークユニットに分割され、少なくとも第一及び第二のネットワークユニットを含み、

前記第一のネットワークユニットが、第一の基幹サーバーと、前記第一のネットワークユニット内で前記第一の基幹サーバーにのみネット接続する第一の周辺装置群から構成され、

前記第二のネットワークユニットが、第二の基幹サーバーと、前記第二のネットワークユニット内で前記第二の基幹サーバーにのみネット接続する第二の周辺装置群から構成され、

前記第一及び第二の基幹サーバーは、互いにネット接続し、前記第一の基幹サーバーにネット接続する第一の周辺装置群と前記第二の基幹サーバーにネット接続する第二の周辺装置群とが、前記第一及び第二の基幹サーバーのネット接続を介して間接的に接続し、

前記第一のネットワークユニット内において、前記第一の基幹サーバーは、少なくとも一つの第一のパスコードと、前記第一の基幹サーバーとネット接続する第一の周辺装置群に属する個々の周辺装置に対応する複数の登録コードからなる第一の登録コードのリストを保持し、前記第一の登録コードは、前記第一のパスコードに対応して前記第一の周辺装置群に属する個々の周辺装置に固有の物理的な乱雑さを利用して発生したものを事前登録によって前記第一の基幹サーバーに保存したものであり、

前記第二のネットワークユニット内において、前記第二の基幹サーバーは、少なくとも

10

20

一つの第二のパスコードと、前記第二の基幹サーバーとネット接続する第二の周辺装置群に属する個々の周辺装置に対応する複数の登録コードからなる第二の登録コードのリストを保持し、前記第二の登録コードは、前記第二のパスコードに対応して前記第二の周辺装置群に属する個々の周辺装置に固有の物理的な乱雑さを利用して発生したものを事前登録によって前記第二の基幹サーバーに保存したものであり、

前記第一及び第二の周辺装置群に属する個々の周辺装置は、それぞれ異なるチップ認証装置を搭載し、

前記第一の周辺装置群に属するチップ認証装置は、前記第一の基幹サーバーから受信した前記第一のパスコードに対応して前記第一の周辺装置群に属する個々のチップ認証装置に固有の物理的乱雑さに基づいて生成された、それぞれ異なる出力信号を前記第一の基幹サーバーに送信し、

10

前記第二の周辺装置群に属するチップ認証装置は、前記第二の基幹サーバーから受信した前記第二のパスコードに対応して前記第二の周辺装置群に属する個々のチップ認証装置に固有の物理的乱雑さに基づいて生成された、それぞれ異なる出力信号を前記第二の基幹サーバーに送信し、

前記第一及び第二の基幹サーバーは、前記個々の出力信号を、前記第一及び第二の登録コードのリストと個々に比較し、対応する個々の周辺装置の正当性を評価し、

前記ネット接続は、前記複数の周辺装置に個々に入力するパスコードと前記登録コードの組み合わせによって構成される交信シリーズによって実現することを特徴とする電子装置のネットワーク。

20

【請求項 2】

請求項 1 記載の電子装置のネットワークであって、前記第一の周辺装置群に属する周辺装置は、同時に前記第二の周辺装置群にも含まれ、前記第一及び第二の基幹サーバーからそれぞれ異なる前記第一及び第二のパスコードを受信し、前記それぞれ異なる第一及び第二のパスコードの入力に対してそれぞれ異なる信号を出力し、前記第一及び第二の基幹サーバーに返信し、前記第一及び第二の基幹サーバーは、返信されてきた出力信号を前記第一及び第二の登録コードのリストとそれぞれ比較し、前記出力信号を返信してきた周辺装置の正当性を評価することを特徴とする電子装置のネットワーク。

【請求項 3】

請求項 1 記載の電子装置のネットワークであって、

30

前記第一の基幹サーバーは、前記第一のパスコードからなる第一の入力コードと前記第一の登録コードの対応表を保存し、前記第一の周辺装置群に属する個々の周辺装置は、前記第一の入力コードと前記第一の登録コードの対応表を内部メモリに保存することをそれぞれ禁止され、

前記第一の基幹サーバーは、前記第一の周辺装置群に属する周辺装置の前記内部メモリを個々に読み出し、前記第一の基幹サーバーに保存されている前記第一のパスコードと比較し、一致するコードが含まれているかどうかを判定し、

含まれていない場合、該周辺装置を公正と認可し、

含まれている場合、更に前記第一の登録コードの中に、前記周辺装置の内部メモリから個々に読み出して得た情報と一致するものがあるかどうか判定し、

40

含まれていない場合、該周辺装置を公正と認可し、

含まれている場合、該周辺装置を不正と認可する

検査工程を行い、

前記検査工程を、前記第一の周辺装置群に属する全ての周辺装置に対して行うことを特徴とする電子装置のネットワーク。

【請求項 4】

前記第一の周辺装置群に属するチップ認証装置は、それぞれ第一のビット線群及び第一のワード線群を含み、前記第一のビット線群は、それぞれ行番号を割り当てられた複数のビット線からなり、前記第一のワード線群は、それぞれ列番号を割り当てられた複数のワード線からなり、前記個々のビット線及びワード線の交差点に不揮発性メモリセルが配置

50

され、前記第一の入力コードは、前記第一のワード線群から順次選択する個々のワード線に対応する前記列番号の順列であり、前記列番号の順列に応じて順次選択されたワード線と、前記第一のビット線群に含まれる複数のビット線との交差点に配置され、

前記第一の周辺装置群に属するチップ認証装置は、前記第一のパスコードに対応して、列方向に並ぶ複数の不揮発性メモリセルから読み出されたデータの集合を前記行番号順に並べた列データを、更に、前記列番号の順列に従って行方向に並べた行列データを出力信号として出力し、

前記第一の基幹サーバーは、前記行列データを前記第一の登録コードのリストと比較し、該チップ認証装置を搭載する周辺装置の正当性を評価することを特徴とする請求項1記載の電子装置のネットワーク。

10

【請求項5】

前記第一のワード線群及び前記第一のビット線群からなるメモリセルアレイ上に分布する交差点に、前記行番号及び前記列番号の組み合わせからなるアドレスを割り当て、前記アドレス上に配置される複数の不揮発性メモリセルを一括消去し、一括書き込みし、続いて、前記複数の不揮発性メモリセルの閾電圧を個々に読み出し、前記閾電圧は前記アドレスに応じて前記メモリセルアレイ上に分布し、前記閾電圧の度数分布を獲得し、

前記閾電圧の度数分布は、第三のピークを有し、前記第三のピークの中央に属するアドレスをバッファに記録し、前記バッファに記録されたアドレスに対応する閾電圧を前記閾電圧の度数分布から排除し、前記第三のピークは、第一及び第二のピークに分割され、前記第一のピークに属するアドレスに第一の値を割り当て、前記第二のピークに属するアドレスに第二の値を割り当て、

20

前記第一の周辺装置群に属するチップ認証装置は、前記第一のパスコードに対応して列方向に並ぶアドレスと、前記バッファに記録したアドレスとを比較し、不一致の場合、該アドレスに割り当てられた前記第一或いは第二の値の集合を前記行番号順に並べた列データを、更に、前記列番号の順列に従って行方向に並べた行列データを出力信号として出力し、

前記第一の基幹サーバーは、前記行列データを前記第一の登録コードのリストと比較し、該チップ認証装置を搭載する周辺装置の正当性を評価することを特徴とする請求項4記載の電子装置のネットワーク。

【発明の詳細な説明】

30

【技術分野】

【0001】

本発明は、チップ間通信に用いる物理的チップ認証方式に関する。

【背景技術】

【0002】

21世紀に入り情報通信産業は飛躍的な進歩を遂げ、近年は更なる巨大マーケットを創出しつつある。情報端末のみならず、家電、家、車などすべてのモノがネットワークに接続するインターネット・オブ・シングス（Internet of Things, IoT）は既存のどの市場にも属さず、IoTの更に先を行くインターネット・オブ・エブリシング（Internet of Everything, IoE）にいたっては社会基盤そのものを変更する可能性を秘めている。

40

【0003】

技術的には、ネットに接続する最小単位（ノード）であるチップとチップの間の通信技術として捕らえることができるが、その数が数兆個から数十兆個にまで上る（Trillion Nodes）点でこれまでのネットワーク技術と異なる。世界人口を70億人とする、一人当たり数千個程度のノードに囲まれている計算になる。これらのチップは個人情報のみならず、個人の周辺にある機器の動作を制御するシステムも含んでいる。すべての個人がこれらすべてを常時きめ細かく管理することは現実的に不可能である。また、訓練を受けた専門家が中央管理するにしても数兆個ものノードを同時に管理するための計算機リソースは地球上に存在しない。仮に将来開発されたとしても、誰が責任を持ってその管理システムを扱うのか？一民間企業が勝手に行なうのは好ましくない。人間の能力を超える人工知能に

50

任せることも現状では良いとは言えないし、現実的でもない。

【0004】

管理できないとしたら何が問題になるか？大容量のL i イオン電池を搭載した自動運転車がハッキングされたらどうなるかを考えると理解しやすい。遠隔操作された多数の自動運転車が攻撃対象（ホワイトハウス、国会議事堂・・・）まで無人で移動し、そこでL i イオン電池を過充電させ大爆発を引き起こすことが可能となる。ある日突然ショッピングセンターの駐車場が大爆発を起こしたり、新幹線を正面衝突させたり、原子炉や航空管制システムを乗っ取られる危険と背中合わせになる。

【0005】

このような重要施設のネットワークは通常のインターネットからは非常に強力なファイアウォールで隔離されている（或いは物理的に隔離されている）から大丈夫だと考えるのは早計である。現実にはイランの核施設はS t u x n e tと呼ばれるマルウェアによる深刻な攻撃を受けた。（たとえば、非特許文献1参照。）

【0006】

S t u x n e t の感染経路は諸説あるが、もっとも有力なのはモバイル端末かU S Bメモリだと言われている。S t u x n e t は一度インターネットに解き放たれると何ヶ月もかけてターゲットのシステムに侵入するチャンスを伺う。途中強力なファイアウォールがあってもU S Bメモリやモバイル端末に侵入してファイアウォール内で接続されるまで待つ。接続された後はバックドアを開き、遠心分離器のP L C（programmable logic controller）を乗っ取り、遠隔操作を開始する。こうして、イランの核施設の1000台もの遠心分離器が急激な加速と減速を繰り返し破壊された。物理的に孤立したシステム内ならS t u x n e t 自身が遠心分離器を破壊させる。

【0007】

イランの核施設で破壊された遠心分離器は通常のネットワークからは遮断されていたが、メンテナンスのため機器の製造装置メーカーのモバイル端末と定期的に接続する必要があった。もし通常のネットワークとつながっていればこのような作業は必要ないが、遮断されているために返って必要な手順となる。また、S t u x n e t はターゲット以外に感染しても潜んでいるだけで何もしない。したがって、ウィルス対策ソフトで検知することは難しい。

【0008】

S t u x n e t による攻撃は、イランの核開発を遅らせイスラエルによるイランへの空爆を防ぐために行われたとも考えられている。しかしながら、恐ろしいことはS t u x n e t のソースコードがハッカーによって盗まれ、既に流出していることである。2014年に入り、S t u x n e t に良く似た性質を持つ新種のウィルスが発見されている。

【0009】

B a d U S Bと呼ばれるこのウィルスは、産業機器の制御プログラムであるP L Cの代わりにU S B機器を制御するファームウェアを乗っ取る。U S B機器は何かにつながって使用するものであり、そのための認証を内包している。この認証はファームウェアに含まれる。ファームウェアはU S B機器の制御チップに保存されているチップを制御するためのプログラムである。B a d U S Bはこの認証を盗み、このU S B機器が接続しているものには何もしない。たとえば、パソコンには感染しないが、パソコンを操作するために接続しているマウスやキーボードを乗っ取ることができる。このようにして地球の裏側にいるハッカーが他人のコンピューターを遠隔操作することができる。このとき、コンピュータには感染していないので、コンピュータのウィルス対策ソフトは何も検知できない。

【0010】

I o T / I o E では通信の最小単位（ノード）は機器の制御チップである。制御チップには制御プログラム（ファームウェア）が保存される。このファームウェアはそれぞれのチップを認識するために認証コードを内包する。上述した自動運転車を遠隔操作する新たな攻撃は、この認証コードを盗み自動運転車を遠隔操作するものである。

【0011】

今後9・11のような同時多発テロは遠隔操作により少数のハッカーグループによって引き起こされる可能性がある。このような新たな脅威は、従来のテロ対策やサイバーセキュリティ技術では防げない。

【先行技術文献】

【非特許文献】

【0012】

【非特許文献1】http://www.nikkei.com/article/DGXNASFK2602G_W2A221C1000000/

【非特許文献2】<http://www.nikkei.com/article/DGXMZ079858560Y4A111C1000000/>

【発明の概要】

【発明が解決しようとする課題】

10

【0013】

サイバーセキュリティ技術はソフトウェアによる中央管理が主流である。これは、セキュリティ技術に関する理解は人によりばらつきが多く、すべてのエンドユーザーに正しい運用管理を期待することは現実的にはほぼ不可能だからである。1000人が適正に運用していてもたった一人が適正に運用していなければセキュリティは脆弱になる。こうして、ネットワークを介したシステムのセキュリティは、十分訓練された管理者が十分信頼性の高いソフトウェアを使い中央管理することが望ましいとされている。中央管理はつまるところ、ネットワークを介したソフトウェアによる管理である。

【0014】

しかしながら、上述したように、IoT/IoEのビジネスモデルではノード数は数兆個にもなり、そもそも中央管理が難しい。その上、ネットワークに接続したノードのうちたった一つでも認証コードを乗っ取られればシステム全体（たとえば、自動運転車、航空管制システムなど）が脆弱になる。認証コードを使うのは、ネットワークが主にソフトウェアで制御されているからである。これが中央管理によるセキュリティの本質的限界である。

20

【0015】

本発明は上記事情に鑑みて成されたものであり、半導体デバイスによるノードの局所的認証管理を提供することを目的とする。

【課題を解決するための手段】

【0016】

30

本発明は、上記課題を解決するため、以下の手段を採用する。本発明に関わるチップ認証方式を用いるチップ認証装置は、複数のビット線と複数のワード線の交差点に配置した不揮発性メモリセルの集合体から構成され、少なくとも一つのワード線を選択する入力コードと、選択されたワード線に対応してビット線毎に読み出されたデータの集合からなる出力コードと、前記入力コードは、順次選択されるワード線の列番号の順列であり、前記出力コードは、前記入力コードにしたがって順次選択されるワード線に連なる不揮発性メモリセルの各データを行番号順に並べた列データを、更に、前記入力コードにしたがって順次選択されるワード線の列番号に従って並べたデータの集合であり、前記不揮発性メモリセルを一括消去し、一括書き込みし、続いて読み出して得た閾電圧分布の、中央のピークに属する不揮発性メモリセルに相当するアドレスを記録するバッファと、前記入力コードによって選択されたワード線に連なるアドレスと、前記バッファに記録したアドレスを比較し、一致した場合、該アドレスに相当するデータを、前記出力コードから削除する機能と、を備えていることを特徴とする。

40

【0017】

また、本発明に関わるチップ認証方式の製造方法は、半導体不揮発性メモリ装置のウェル工程とポリ工程の間に、ドナーイオンの打ち込みと、アクセプターイオンの打ち込む工程と、あるいは、半導体基板表面を櫛歯状に加工する工程と、誘電体膜製造工程の間に、前記半導体基板表面に作成された櫛歯状構造をスリミングするための熱酸化工程と、を備えていることを特徴とする。

【発明の効果】

50

【0018】

本発明によれば、新しいチップ認証方式を提供し、認証コードを盗むことによる制御チップ乗っ取りの危険性を低減することが可能となる。

【図面の簡単な説明】

【0019】

【図1】 従来の認証システムを搭載したチップの一例を示す図。

【図2】 本発明のチップ認証装置を搭載したチップの一例を示す図。

【図3】 本発明のチップ認証装置を搭載したチップを含む装置の接続方法の一例を示す図。

【図4】 外部I/Oを介して信号をやり取りする一例を示す図。

10

【図5】 本発明のチップ認証装置を搭載したチップを含む装置を、本発明のチップ認証装置と接続する装置に登録する方法の一例を示す図。

【図6】 正規の使用者が、本発明のチップ認証装置を搭載したチップを含む装置を、ネットワーク上で使用する方法の一例を示す図。

【図7】 遠隔攻撃者が、不正にネットワークに接続する方法の一例を示す図。

【図8】 遠隔攻撃者が、正規の装置の装置を攻撃する方法の一例を示す図。

【図9】 本発明のチップ認証装置を搭載したチップを含む周辺装置を、基幹サーバーに接続する方法の一例を示す図。

【図10】 基幹サーバーから、本発明のチップ認証装置を搭載したチップを含む周辺装置に共通パスコードを送信する方法の一例を示す図。

20

【図11】 本発明のチップ認証装置を搭載したチップを含む周辺装置から、認証コードを、基幹サーバーに送信する方法の一例を示す図。

【図12】 基幹サーバーから、本発明のチップ認証装置を搭載したチップを含む周辺装置に共通パスコードを送信する方法の一例を示す図。

【図13】 本発明のチップ認証装置を搭載したチップを含む周辺装置から、認証コードを、基幹サーバーに送信する方法の一例を示す図。

【図14】 複数の基幹サーバーと、本発明のチップ認証装置を搭載したチップを含む複数の周辺装置からなるネットワークの一例を示す図。

【図15】 複数の基幹サーバーが一つの周辺装置に接続する一例を示す図。

【図16】 本発明のチップ認証装置が満たすべき、出力の独立性の一例を示す図。

30

【図17】 本発明のチップ認証装置が満たすべき、入力 of 独立性の一例を示す図。

【図18】 本発明のチップ認証装置が満たすべき、出力信号の予測不可能性の一例を示す図。

【図19】 本発明のチップ認証装置が満たすべき、入出力信号の信頼性の一例を示す図。

【図20】 入力コードと登録コードの対応表の一例を示す図。

【図21】 周辺装置の正当性を検査するための作業工程の一例を示す図。

【図22】 不揮発性メモリセルアレイに割り振られたデータの一例を示す図。

【図23】 NAND型不揮発性メモリセルアレイの一例を示す図。

【図24】 NAND型不揮発性メモリセルアレイの第Pページを選択する方法の一例を示す図。

40

【図25】 NAND型不揮発性メモリセルアレイの第Sページを選択する方法の一例を示す図。

【図26】 NAND型不揮発性メモリセルアレイの第Pページと第Sページを選択する方法の一例を示す図。

【図27】 不揮発性メモリセルの集団を、一括消去・一括書き込みしたときの閾電圧の分布の一例を示す図。

【図28】 本発明の第二の実施形態に関する製造工程の一例を示す図。

【図29】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。

【図30】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。

【図31】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。

50

- 【図 3 2】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 3 3】 不揮発性メモリセルアレイの鳥瞰図。
【図 3 4】 不揮発性メモリセルアレイに関わる楕円状基板表面の鳥瞰図。
【図 3 5】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 3 6】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 3 7】 本発明の第二の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 3 8】 本発明の第三の実施形態に関する製造工程の一例を示す図。
【図 3 9】 本発明の第三の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 4 0】 本発明の第三の実施形態に関する、不揮発性メモリの閾電圧の分布を示す図。
【図 4 1】 本発明の第四の実施形態に関する、閾電圧の読み出し方法の一例を示す図。
【図 4 2】 本発明の第五の実施形態に関するチップの構成内容の一例を示す図。
【図 4 3】 本発明の第六の実施形態に関するチップの構成内容の一例を示す図。
【図 4 4】 本発明の第六の実施形態に関するチップの構成内容の一例を示す図。
【発明を実施するための形態】

【0020】

本発明に係る実施形態について、以下図面を参照して説明する。

【0021】

図 1 は、従来の典型的なチップ制御システムを説明する図面である。チップの機能を具現化する認証制御デバイス 3 は、ファームウェア 2 に含まれる認証コード (ID) 4 を必要に応じて読み出せるようになっている。たとえば、チップ 1 は、外部入力に応じて認証制御デバイス 3 が認証コード 4 を参照し、チップ 1 が正しい外部装置であることを主張する。ただし、これは主張するだけであって正しいことを証明するものではない。上述したように、認証コード (ID) 4 を盗めば他のチップがチップ 1 になりかわることが可能だからである。

【0022】

本発明では、図 2 に示すように、認証コード (ID) 4 と認証制御デバイス 3 からなる認証システム 6 を、本願のチップ認証装置 60 に置き換える。チップ認証装置 60 は外部入出力 50 から受け取るコール (入力信号) に応じて都度出力を発生するものであり、発生された出力信号は物理的乱雑さを利用して生成されるものである。また、入力信号を変えると出力信号も変わるという特徴を有している。図 3 のように、このチップ認証装置 60 を有するチップ 10 を搭載する第一の装置 71 が第二の装置 72 にネット接続されている場合を考えよう。

【0023】

図 4 のように、第二の装置 72 は、ネット接続された第一の装置 71 を認識するために信号 A、信号 B、信号 C、・・・を入力としてネット接続を介して第一の装置に搭載されるチップ認証装置 60 に与える。チップ認証装置 60 は、それぞれ信号 A1、信号 B1、信号 C1、・・・を出力としてネット接続を介して第二の装置に返す。ここで、第二の装置は、チップ 10 を搭載する第一の装置を、「信号 A の入力に対して信号 A1 の出力を返し、信号 B の入力に対して信号 B1 の出力を返し、信号 C の入力に対して信号 C1 の出力を返し、・・・」という装置であると認識する。これを交信シリーズ (A、B、C、・・・: A1、B1、C1、・・・) であらわす。あるいは、第二の装置 72 は第一の装置 71 を「信号 F の入力に対して信号 F1 の出力を返し、信号 A の入力に対して信号 A1 の出力を返し、信号 K の入力に対して信号 K1 の出力を返し、・・・」と認識する。これを交信シリーズ 80 (F、A、K、・・・: F1、A1、K1、・・・) であらわす。しかしながら、このような交信はすべての可能な入力信号に対して行わなくても良い。入力信号のパターンは無限にあり、特定の装置に対してそのすべてを行うことは不毛である。むしろ入力信号のパターン数が無限にあることは、第二の装置にネット接続しうる装置の数を無制限にすることに有用である。すなわち、第一の装置を第二の装置に最初にネット接続する際、第二の装置は第一の装置を登録することになる。この登録は、第二の装置の正規の使用者か、或いは、第二の装置の正規の使用者から正規に権限を委譲された者が行うこ

10

20

30

40

50

とが望ましい。登録時に任意に選ばれた入力信号102、たとえば、(R、L、A)と、第一の装置から返ってきた出力信号(R1、L1、A1)を第二の装置の内部メモリ302に保存する。このとき、登録に関わる通信シリーズは(R、L、A：R1、L1、A1)となる。更に具体的には、第二の装置に接続しうる装置は無数にあるので入力信号102のセットはあらかじめ固定することが望ましい。その場合、第一の装置が登録された通信シリーズ(R、L、A：R1、L1、A1)の替わりに(R1、L1、A1)を登録コード103とする。図5の例では、第一の装置71、第四の装置74、第五の装置75、・・・が、第二の装置に登録されている場合を説明している。たとえば、第四の装置は、入力信号(R、L、A)に対して、出力信号(R4、L4、A4)を第二の装置に返す。第五の装置は、入力信号(R、L、A)に対して、出力信号(R5、L5、A5)を第二の装置に返す。

10

【0024】

図6の例では、第二の装置の正規の使用者92が、所有する第一の装置を使ってネット接続を介して第二の装置72を操作する例を説明している。第一の装置と第二の装置は通信シリーズ80を用いてネットを介して通信し、連携して第二の装置72の正規使用者92の目的とする仕事を行う。ここで、第二の装置72の正規使用者92は、通信シリーズ80にいかなるコミットメントもしない。もしコミットメントをする場合、第二の装置72の管理・使用方法が煩雑になり、IoT/IoEの利便性が大きく損なわれることになる。具体的には、第二の装置が何らかの外部装置とネット接続するとき、まず第二の装置は入力信号102(R、L、A)をこの外部装置に送り、この外部装置から返って来た信号が登録コード202のどれか、(R1、L1、A1)、(R4、L4、A4)、(R5、L5、A5)・・・に一致するかどうかを確認すればよい。

20

【0025】

図7のように、遠隔攻撃者93が、第一の装置71を遠隔攻撃者93が所有する第三の装置73に不正に置き換える場合を考えよう。第三の装置73は、第一の装置71に内蔵されるチップ認証装置60を使用せずにこの通信シリーズ80を完全に模倣しなければならない。これが可能かどうかを見極めればよい。不可能であれば、本発明のチップ認証方式によって、装置の乗っ取りを防ぐことができると判明する。そのための前提条件として、第一の装置71を第三の装置73と不正に置き換えようとする者(遠隔攻撃者93)は、実際に第一の装置71を手にとることができないとする。これは、IoT/IoEにおいては自然な条件である。すなわち、IoT/IoEにおける乗っ取りは遠隔操作を前提にしているからである。遠隔攻撃者93の目的は、自分が手元に所有する第三の装置73を使って第二の装置72を遠隔操作することである。第一の装置を手元に奪取するためには、第二の装置に正規に接続する第一の装置71が存在する場所に赴き、秘密裏に奪取しなければならない。これは、攻撃をネット上で完結することができないことを意味する。すなわち、第二の装置の使用者に気づかれずに遠隔操作をすることができないのと同義である。第三の装置73と第二の装置72がネット接続されると、第二の装置はネット接続を介して第三の装置73を認識するために入力信号(R、L、A、・・・)をネット接続を介して第三の装置73に与える。第三の装置が出力信号(R3、L3、A3、・・・)をネット接続を介して第二の装置に返したとする。こうして、偽通信シリーズ(R、L、A、・・・：R3、L3、A3、・・・)が作成される。すなわち、遠隔攻撃者93は、偽通信シリーズ83を正規の通信シリーズ80に完全に一致させなければならない。ここで、入力コード102(R、L、A)と、この入力に対する返信(R3、L3、A3)からなる通信シリーズ(R、L、A：R3、L3、A3)は、偽通信シリーズ83の一例である。(R3、L3、A3)が(R1、L1、A1)と一致すれば、遠隔攻撃者93は第三の装置を第一の装置に置き換えて遠隔攻撃を成功できる。図5の例に従えば、遠隔攻撃者93は、(R3、L3、A3)を、第二の装置72の内部メモリ302に保存されている登録コード202のうちどれか一つと一致させれば良い。

30

40

【0026】

こうして、遠隔攻撃には基本的に二つの方法があることがわかる。第一の方法は、第二

50

の装置の内部メモリ302に保存されている情報から、入力コード102と、少なくとも登録コードのうちのどれか一つと、を盗み取ることである。たとえば、遠隔攻撃者93が登録コード202のうち、(R4、L4、A4)を盗み取ること成功したとする。このとき、遠隔攻撃者93は、所有する第三の装置73を第四の装置74に置き換えて第二の装置を不正に遠隔操作することができる。同様に、遠隔攻撃者93が登録コード202のうち、(R1、L1、A1)を盗み取ること成功したとする。このとき、遠隔攻撃者93は、所有する第三の装置73を第一の装置71に置き換えて第二の装置を不正に遠隔操作することができる。このような遠隔攻撃からシステムを守るため、システム管理者は第二の装置72の内部メモリ302を厳重に防御しなければならない。このため、内部メモリに入力コードや登録コードを保存する第二の装置72のような装置は、訓練を受けた専門家が常に最新のセキュリティ対策ソフトウェア技術を用いて厳重に保守することが望ましい。このように、第二の装置72はネットワークの中央に置かれ基幹的な役割を担い、セキュリティ管理者による中央管理下にあると仮定する。こうして、遠隔攻撃の第一の方法はほぼ防がれる。しかしながら、ネットワークに接続する装置が数兆個に上る場合、すべての装置を第二の装置72のように厳重に防御・保守することは現実的に不可能である。これは中央管理の限界を意味している。そこで、遠隔攻撃者93は、第二の装置72に接続する中央管理の行き届かない装置、図5の例では、第一の装置71、第四の装置74、第五の装置75・・・を遠隔攻撃することになる。これが遠隔攻撃の第二の方法である。しかしながら、第一の装置71は、入力コード102と登録コード202のペア(交信シリーズ)を認証コードとして内部メモリに保存しない。第四の装置74、第五の装置75等の、第二の装置にネット接続して使用することを目的とするほかの外部装置も同様である。これら外部装置(たとえば、図5の例では、第一の装置71、第四の装置74、第五の装置75、・・・)は、それぞれ相異なるチップ認証装置を搭載するチップを内蔵している。

【0027】

ここで、図8のように、遠隔攻撃者93が第一の装置71を遠隔攻撃する場合を考えよう。まず、遠隔攻撃者93は、第一の装置71の内部メモリーに不正にアクセスし、登録コード及び入力コードに関する情報(交信シリーズ)を盗み取ろうとする。しかしながら、第一の装置はそもそもそのような情報を内部メモリーに保存していないので、この攻撃は必ず失敗に終わる。次に、遠隔攻撃者93は、適当に選んだ信号(X、Y、Z)を第一の装置71に入力し、(X1、Y1、Z1)の返信を得る。(X、Y、Z)が、第二の装置72が用いる入力コード102(R、L、A)と異なる場合、返信(X1、Y1、Z1)は登録コード202の(R1、L1、A1)とは異なる。こうして、第二の遠隔攻撃も失敗に終わる。ここで問題なのは、遠隔攻撃者93が適当に選んだ信号セット(X、Y、Z)が、たまたま第二の装置72の内部メモリ102に保存した入力コード102(R、L、A)に一致することである。このような偶然を防ぐため、入力コードの要素数を十分多くし、更に第二の装置72の管理者以外には非公開とすることである。この情報は、第二の装置72の管理者によって厳重に守られるべきである。また、時より変更することが望ましい。この変更を行った場合、第二の装置72に接続する装置の再登録を行うことが必要になる。このような再登録を行う頻度を減らすために、入力コードの要素数は可能な限り多くするように管理することが必要である。このように、入力コードは、パスコードとして振舞う。

【0028】

この入力コードは、さまざまな周辺装置への認証IDを検査するために共通して使うことが望ましい。この場合、おのこの周辺装置へのアクセスに個別に必要なものではない。このような事情から、本発明で説明する入力コードを以下“共通パスコード”と呼ぶことにする。

【0029】

上記第二の装置72が計算機(パソコン等)の場合、これに接続する第一の装置71、第四の装置74、第五の装置75は、計算機に接続して用いられる周辺装置となる。たと

えば、マウス、キーボード、マイクロホン、などである。上述したとおり、計算機本体は最新のウィルス対策ソフトを使用して管理者が責任を持って管理することが前提となる。本件に関わる発明は、周辺装置（マウス、キーボード、マイクロホン等）の置き換え（乗っ取り）から計算機本体を守ることが目的となる。これによって計算機本体を守ることが目的とするウィルス対策ソフトが守りきれない周辺装置を遠隔攻撃から守ることができる。

【0030】

上記第二の装置72がネットワークサービスの中心的機能を担う基幹サーバーの場合、これに接続する第一の装置71、第四の装置74、第五の装置75などを、基幹サーバーに対して周辺装置とみなすことができる。図9は、一つの基幹サーバー400に、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430、・・・がネット接続する例を示している。たとえば、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430・・・は、このネットワークサービスを利用するエンドユーザーの端末である。たとえば、スマートフォン、タブレット、計算機端末、スマート家電のリモコン、自動運転者の操作パネル、あるいはその他ウェアラブル端末等である。上述したとおり、基幹サーバーは、十分に訓練を受けた専門家が最新のセキュリティソフトウェアを駆使して責任を持って管理することが前提となる。本件に関わる発明は、エンドユーザーの端末（スマートフォン、タブレット、計算機端末、その他ウェアラブル端末等）の置き換え（乗っ取り）から基幹サーバーへの不正アクセスを防ぐことが目的となる。これによって、十分に訓練を受けた専門家が最新のセキュリティソフトウェアを駆使しても守りきれない、ネットワーク上に無数に存在する情報端末を遠隔攻撃から守ることができる。

【0031】

上記第二の装置72がクラウドセンシングサービスの中心的機能を担うデータセンターの場合、これに接続する第一の装置71、第四の装置74、第五の装置75は、このデータセンターが必要とするデータを取得するセンサーである。センサーの数は無数であり、広い範囲に設置される。したがって、その一つ一つを中央管理で遠隔攻撃から守ることは現実的に不可能である。このようなセンサーの例は、GPS、ウィルスモニター、温度計、地震計、LEDソケット型可視光通信デバイス、バイオセンサー、各種スマートメーターなど無数にある。上述したとおり、データセンターは、十分に訓練を受けた専門家が最新のセキュリティソフトウェアを駆使して責任を持って管理することが前提となる。本件に関わる発明は、このようなセンサーの置き換え（乗っ取り）からデータセンターへの不正アクセスを防ぐことが目的となる。これによって、十分に訓練を受けた専門家が最新のセキュリティソフトウェアを駆使しても守りきれない、クラウドセンシングのためのネットワーク上に無数に存在するセンサーを遠隔攻撃から守ることができる。

【0032】

ここで、本発明の特徴の一つとして、中央管理の行き届かない周辺装置（たとえば、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430・・・）は、前記共通パスコードのような入力データを保存しないことがあげられる。このように、認証通信のために必要なデータ（たとえば、共通パスコード）を保存する“基幹サーバー”と保存しない“周辺装置”に分けることが特徴となる。同時に、認証通信のために必要なデータ（たとえば、共通パスコード）を保存する“基幹サーバー”は中央管理し、認証通信のために必要なデータ（たとえば、共通パスコード）を保存しない“周辺装置”には本発明のチップ認証方式を搭載することを特徴とする。

【0033】

上記共通パスコードは、第一の基幹サーバー1400に少なくとも一つ保存され、周辺装置を認識する際に周辺装置に送られる。たとえば、図10のように、第一の基幹サーバー1400は第一の共通パスコード1410を、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430に送る。これらの周辺装置は、第一の基幹サーバーを「第一の共通パスコード1410を送ってくるもの」として認識する。図11に示すように、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430は、この第一の共

通パスコード1410の入力に対応し、それぞれ、第一の認証4101、第二の認証4201、第三の認証4301を、第一の基幹サーバー1400に返す。第一の基幹サーバー1400は、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430を、「第一の共通パスコード1410に対して、それぞれ第一の認証4101、第二の認証4201、第三の認証4301を返すもの」と認識する。同様に、図12のように、第二の基幹サーバー2400は、第二の共通パスコード2410を、第一の周辺回路410、第二の周辺装置420、第三の周辺装置430に送る。これらの周辺装置は、第二の基幹サーバーを「第二の共通パスコード2410を送ってくるもの」として認識する。図13に示すように、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430は、この第二のパスコード2410の入力に対応し、それぞれ、第四の認証4102、第五の認証4202、第六の認証4302を、第二の基幹サーバー2400に返す。第二の基幹サーバー2400は、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430を、「第二の共通パスコード2410に対して、それぞれ第四の認証4102、第五の認証4202、第六の認証4302を返すもの」と認識する。言うまでも無く、第一の共通パスコード1410と第二の共通パスコード2410は異なる。第一の認証4101、第二の認証4201、第三の認証4301、第四の認証4102、第五の認証4202、第六の認証4302のうちどの二つの認証も同じではない。

【0034】

実際のネットワークでは、周辺装置は無数にあり、しかも基幹サーバーは一つに限らない。たとえば、図14では、二つの基幹サーバー（第一の基幹サーバー1400、第二の基幹サーバー2400）と五つの周辺装置（第一の周辺装置410、第二の周辺装置420、第三の周辺装置430、第四の周辺装置440、第五の周辺装置450）からなるネットワークを例示している。第一の基幹サーバー1400を中心に、第四の周辺装置440と第五の周辺装置450とで一つのネットワークユニットを構成し、第二の基幹サーバー2400と、第一の周辺装置410、第二の周辺装置420、及び第三の周辺装置430とでもう一方のネットワークユニットを構成する。これらのネットワークユニットは、互いに、第一の基幹サーバー1400と第二の基幹サーバー2400とのみで接続している。さらに、第四の周辺装置440および第五の周辺装置450は、第一の基幹サーバー1400とのみ接続し、第一の周辺装置410、第二の周辺装置420、及び第三の周辺装置430は、第二の基幹サーバー2400とのみ接続している。本発明の特徴は、このような複数の基幹サーバーと複数の周辺装置からなるネットワークにおいて、基幹サーバー同士は直接通信が可能であるが、周辺装置同士は直接通信をしないことが上げられる。これは、中央管理の行き届かない周辺装置では、共通パスコードのような入力データを保存しないためである。その代わりに、周辺装置同士は、基幹サーバーを介して間接的に通信する。たとえば、第一の周辺装置410と第二の周辺装置420は、第二の基幹サーバー2400を介して間接的に通信可能である。第四の周辺装置440と第五の周辺装置450は、第一の基幹サーバー1400を介して、間接的に通信可能である。第三の周辺装置430と第四の周辺装置440は、互いにネット上で連結している第一の基幹サーバー1400と第二の基幹サーバー2400とを介して、間接的に通信可能である。こうして、本発明によれば、中央管理のためのリソースを基幹サーバーにのみ集中させることが可能となる。図14の具体的な例としては、たとえば、自動運転車とスマートハウスが上げられる。たとえば、第一の基幹サーバー1400、第四の周辺装置440、および第五の周辺装置450からなるネットワークユニットは、共に一つの自動運転車を構成する部品であるとする。同時に、第二の基幹サーバー2400、第一の周辺装置410、第二の周辺装置420、第三の周辺装置430からなるネットワークユニットは、一つのスマートハウスの部品であるとする。災害時自動運転車のバッテリーがスマートハウスのバッテリーを補完するような場合、たとえば、スマートハウスのバッテリーの状況を把握するためのセンサー（たとえば、第四の周辺装置440）が自動運転車に搭載されている。このように、第四の周辺装置440は、第一の基幹サーバー1400と第二の基幹サーバー2400のどちらともネット接続することになる。

10

20

30

40

50

【0035】

図15に示すように、本発明を用いたネットワークでは、一つの周辺装置（たとえば第一の周辺装置410）が複数の基幹サーバー（たとえば、第一の基幹サーバー1400、第二の基幹サーバー2400、第三の基幹サーバー3400）と接続することも認められる。その中で、たとえば、第一の基幹サーバー1400と第二の基幹サーバー2400は直接通信可能であるが、第一の基幹サーバー1400も第二の基幹サーバー2400も、第三の基幹サーバー3400とは直接通信していないものとする。ここで、第三の基幹サーバー3400が遠隔攻撃者でないという証明はない。このため、第一の周辺装置410に通信認証に関するデータ（共通パスコード）を保存しないことは重要である。このように、本発明のチップ認証方式を用いることによって、この問題に対処することができる。

10

【0036】

第一の基幹サーバー1400は、第一の共通パスコード1410を有し、第二の基幹サーバー2400は、第二の共通パスコード2410を有し、第三の基幹サーバー3400は、第三の共通パスコード3410を有するものとする。すなわち、第一の周辺装置410は、第一の基幹サーバー1400を「第一の共通パスコード1410を入力してくるもの」と認識し、第二の基幹サーバー2400を「第二の共通パスコード2410を入力してくるもの」と認識し、第三の基幹サーバー3400を「第三の共通パスコード3410を入力してくるもの」と認識する。これらの入力に対し、第一の基幹サーバー1400は、第一の周辺装置410を「第一の認証11を返すもの」と認識し、第二の基幹サーバー2400は、第一の周辺装置410を、「第二の認証12を返すもの」と認識し、第三の基幹サーバー3400は、第一の周辺装置410を、「第三の認証13を返すもの」と認識する。ここで、通信認証に関するデータ（共通パスコード、あるいは、共通パスコードに対応して返信する認証データ等）は、基幹サーバーに保存され、周辺装置には保存しない。周辺装置には、本発明のチップ認証装置を搭載する。

20

【0037】

次に、本発明で提案するチップ認証方式が満たすべき条件について述べておこう。

【0038】

《出力の独立性》

まず、二つのチップ認証装置に同じ入力信号を入力したときの動作を特定する。図16に示すように、二つの異なる第一のチップ認証装置21と第二のチップ認証装置22に対して、同じ入力信号（入力信号Q）を入力する。このとき、第一のチップ認証装置21は出力信号Aを出力する。第二のチップ認証装置22は出力信号Bを出力する。このとき、出力信号Aと出力信号Bとは異なる。このように、入力信号が同一であってもチップ認証装置が異なる場合出力信号はそれぞれ異なる。この性質は、共通パスコードを使う例（図10、図11、図12、図13）に必要な条件である。すなわち、同じパスコードをそれぞれ異なるチップ認証装置を搭載する周辺装置に入力信号として入力しても、それぞれの周辺装置から返って来る出力信号は周辺装置毎に相異なる。たとえば、図10のように、第一の共通パスコード1410を、それぞれ異なるチップ認証装置を内蔵する第一の周辺装置410、第二の周辺装置420、第三の認証装置430に与えたとき、これらの周辺装置から返って来る出力信号は、図11に示すように、それぞれ第一の認証4101、第二の認証4201、第三の認証4301となる。ここで、第一の認証4101、第二の認証4201、第三の認証4301の内どの二つも相異なる。図12、及び、図13の例も同様に説明できる。

30

40

【0039】

《入力の独立性》

反対に、同一のチップ認証装置に異なる入力信号を入力すると、それぞれ相異なる出力信号を出力する。たとえば、図17に示すように、チップ認証装置60に入力信号Cを入力すると出力信号Aを出力する。同じチップ認証装置60に入力信号Dを入力すると出力信号Bを出力する。ここで、出力信号Aと出力信号Bは、入力信号Cと入力信号Dが異なる

50

る限り、それぞれ相異なる出力信号である。この性質は、図15のように、異なる基幹サーバーからそれぞれ異なるパスコードを入力信号として同一の周辺装置に入力し、それぞれ基幹サーバーが相異なる認証を該周辺装置から出力信号として受け取る場合に必要な条件である。具体的には、第一の基幹サーバー1400が第一の共通パスコード1410を第一の周辺装置410に入力し、第一の周辺装置410が第一の認証11を第一の基幹サーバー1400に出力し、第二の基幹サーバー2400が第二の共通パスコード2410を第一の周辺装置410に入力し、第一の周辺装置410が第二の認証12を第二の基幹サーバー2400に出力し、第三の基幹サーバー3400が第三の共通パスコード3410を第一の周辺装置410に入力し、第一の周辺装置410が第三の認証13を第三の基幹サーバー3400に出力する、ような場合である。

10

【0040】

すなわち、図14は（入力の独立性）の条件と（出力の独立性）の条件を同時に満たすネットワーク構造の一例となっている。ほとんどの場合、実際には、基幹サーバーの数は2より大きく、周辺装置の数は5より大きい。図14は、もっとも簡単な一例に過ぎない。

【0041】

《出力の予測不可能性》

図18に示すように、 n 個の入力信号 $Q_1 - Q_n$ を同一のチップ認証装置60に与えたとき、それぞれの入力信号に対し出力信号 $R_1 - R_n$ が得られることを知っているものとする。このとき、 n 個の $Q_1 - Q_n$ のいずれとも異なる入力信号 Q_{n+1} を同一のチップ認証装置60に与えずに、これを与えたときに得られるはずの出力信号 R_{n+1} を、 (Q_1, R_1) 、 (Q_2, R_2) 、 $\dots$ 、 (Q_n, R_n) のセットから予測することは不可能である。ただし、 n は2以上の整数とする。チップ認証装置60が、何らかのアルゴリズムによって出力を生成している場合、すなわち、ソフトウェアによって認証を返す場合、ほぼ必ずこの条件は破られる。したがって、チップ認証装置60は物理的乱雑さを利用して出力信号を生成しなければならない。あるいは、物理的乱雑さを利用して生成した信号を、あらかじめ保存して用いることが必要である。ただし、物理的乱雑さを利用して生成した信号を保存するために膨大なメモリ領域が必要となる。

20

【0042】

《入出力の信頼性》

図19に示すように、実際には、入力信号 Q を制御する回路に関わる制御不能のノイズなどにより、入力信号 Q には入力信号誤差 ΔQ (31)が混入する。これに対し、入力信号誤差 ΔQ (31)及び出力信号を制御する回路に関わる制御不能のノイズなどにより、出力信号 R には出力信号誤差 ΔR (32)が混入する。このとき、二つの異なる入力信号（たとえば、 Q_1 および Q_2 ）の差の絶対値は、入力信号誤差 ΔQ (31)の絶対値の最大値より大きいものとする。ここで、入力信号 Q_1 に対する出力信号 R_1 と、入力信号 Q_2 に対する出力信号 R_2 との間の差の絶対値は、出力信号誤差 ΔR (32)の絶対値の最大値より大きくなければならない。

30

【0043】

本発明に関わるチップ認証方式は、上述した（出力の独立性）、（入力の独立性）、（出力の予測不可能性）、及び、（入出力の信頼性）の、4つすべてを同時に満たしていない。

40

【0044】

《検査》

本発明が実施される以前から稼動しているネットワークをIoTなどに発展させる場合には、既に基幹サーバーに接続している周辺装置を、本発明によるチップ認証装置を搭載したチップで構成された周辺装置に置き換えて行かねばならない。ここで、この置き換えが確実に行われたかどうか検査することが必要になる。あるいは、本発明のチップ認証装置を搭載していないチップを採用した周辺装置が一部でも不正に登録されていないかどうか検査することが必要である。ここで説明する検査は、基幹サーバーの保守点検の一部と

50

して随時行うことが可能である。また、周辺装置の登録時にも行うことが望ましい。

【0045】

この検査のためにもっとも有効な方法は、中央管理下にある基幹サーバーを使って検査対象となる周辺装置を実際に遠隔攻撃することである。検査対象となる周辺装置を構成するチップは、本発明のチップ認証装置を用いていない場合、内蔵メモリに共通パスコードと登録コードの対応表(図20参照)を保存していなければならない。本発明のチップ認証装置を搭載したチップの内蔵メモリには、このようなコードは保存されていない。図20のようなコード対応表を正規に保存しているのは、本発明に関するネットワークでは、基幹サーバーだけである。図9にある、入力コード402と登録コード403の組あわせがそれである。図9の入力コード402が図20の入力コード42に対応し、図9の登録コード403が図20の登録コード43に対応している。

10

【0046】

具体的な検査作業の流れを図21を用いて説明する。第一に、検査する周辺装置の内蔵メモリを読み出す。ここで読み出されたコードの中に、基幹サーバーに入力コード402として保存されている入力コードの中に一致するものがあるかどうかを調べる。不一致の場合、検査した周辺装置を公正なものとして承認する。一致する場合、更に基幹サーバーに登録コード403として保存されている登録コードの中に一致するものがあるかどうか調べる。一致した場合、検査した周辺装置を不正品として判定する。一致しない場合、公正として承認する。

20

【0047】

本実施形態に関わるチップ認証方式を用いるネットワークを構成するすべての装置は、たとえば、図14のように、訓練を受けたセキュリティ専門家が保守・管理する基幹サーバー(たとえば、1400、2400)のグループと、前記セキュリティ専門家が管理できない周辺装置(たとえば、410、420、430、440、450)のグループに分けられる。ここで、周辺装置同士はお互いに直接に接続せず、基幹サーバーとのみ接続可能とする。こうして、一つの基幹サーバーとそれに直接接続する複数の周辺装置からなるネットワークユニットを構成する。基幹サーバーは、基幹サーバー同士と任意に接続可能であり、周辺装置同士は、基幹サーバーを介して間接的に接続可能である。こうして、各ネットワークユニット同士も接続可能である。図14は、二つのネットワークユニットが互いの基幹サーバー同士の接続によって連携したネットワークの一例である。実際には、もっと多数の基幹サーバー、すなわち、もっと多数のネットワークユニットから構成されるネットワークも実現可能である。各周辺装置には、すべて異なるチップ認証装置が搭載されている。図10及び図12に示すように、基幹サーバー(1400、2400)は、それぞれ固有の共通パスコード(1410、2410)を少なくとも一つずつ保有する。図9に示すように、それぞれの基幹サーバーが出力する共通パスコードは、基幹サーバーの内蔵メモリに入力コード(たとえば、402)として厳重に保管される。図11及び図13に示すように、共通パスコード(1410、2410)を入力された周辺装置(410、420、430)は、同じ共通パスコードに対しておのおの固有の認証(4101、4201、4301)、及び、(4102、4202、4302)を基幹サーバー(1400、2400)にそれぞれ返信する。ここで返信される認証はすべてお互いに異なることが必要である。そのため、周辺装置に搭載される、本発明のチップ認証装置は、図16に示すように、(出力の独立性)を満たさなければならない。図9に示すように、基幹サーバーは、周辺装置から返信されてきた出力信号(認証コード)を、入力コード(たとえば、402)のそれぞれに対応する形で内蔵メモリに厳重に保管する登録コード(たとえば、403)と便宜比較する。図15に示すように、一つの周辺装置が複数の基幹サーバーと接続することが許される。この場合、一つの周辺装置(たとえば、410)は、複数の共通パスコード(たとえば、1410、2410、3410)を入力され、それぞれ異なる入力に対して、それぞれ異なる認証(たとえば、11、12、13)を出力しなければならない。そのため、周辺装置に搭載される、本発明のチップ認証装置は、図17に示すように、(入力の独立性)を満たさなければならない。

30

40

50

【0048】

続いて、本発明に関するチップ認証装置に関する条件を考える。まず、チップ認証装置をプログラムで構成する場合、入力コードに対する出力信号（認証コード）の作成は、かならずある種のアルゴリズムを用いて行われることになる。したがって、遠隔攻撃者（たとえば、93）がこのアルゴリズムを解読した場合、入力コードさえ判っていれば、たとえば図20のように、登録コードを偽造することが可能となる。こうして、この遠隔攻撃者は周辺装置の一部を乗っ取り、基幹サーバーに不正アクセスすることが可能となる。このような不正行為を防ぐため、本発明のチップ認証装置は、図18に示すように、（出力の予測不可能性）を満たさなければならない。しかしながら、プログラムがアルゴリズムで設計されている限り、どのようなプログラムも（出力の予測不可能性）を満たすことができない。これは、プログラムにより完全な乱数を発生することが不可能であることと同じ事情である。このように、チップ認証装置は、物理的乱雑さを活用したものでなければならない。

10

【0049】

前記のようなチップ認証装置は、半導体チップ内に他の機能を持つモジュールと一緒に混載してもよいし、または、チップ認証機能のみを持つ半導体チップとして単独で製造しても良い。また、チップ認証装置は、入力コード（共通パスコード）を受け取る度に、物理的乱雑さに基づいて出力信号（認証コード）を発生することが望ましい。しかしながら、十分大きなメモリ容量を確保できるなら、別途物理乱数発生装置によって発生しておいた信号コードを内部メモリに格納しておくことでも同様の効果を得ることができる。ただし、この場合でも、共通パスコードだけは周辺装置のメモリに保存してはならない。いずれにしろ、チップ認証装置そのものが半導体チップで実現される電子装置である。また、前記ネットワークは、構成要素である周辺装置、基幹サーバーが半導体チップから構成される電子装置のネットワークである。

20

【実施例1】

【0050】

本発明に関するチップ認証装置は、半導体不揮発性メモリ上に構成することが可能である。まず、物理乱数発生装置を用い、“1”と“0”のランダムな組み合わせを生成する。たとえば、“1”を黒、“0”を白として、これを不揮発性メモリのメモリセルアレイに書き込むと、図22のような白と黒がランダムに配置した市松模様ができる。この不揮発メモリアレイが、図23のようなNAND型だとしよう。図24のように、ソース選択ゲート704およびドレイン選択ゲート705をオンとし、ワード線701の中から第P列のワード線を選択して読み出し電圧を印加し、非選択ワード線にバス電圧を印加すると、各々のビット線702に応じて、上の行から“1”と“0”からなる配列が生成する。図22の例では、上から（白白黒白白黒白白黒・・・）が出力されることとなる。これは、図24において、第Pページ（第P列）のデータが上から（0010010001・・・）が出力されることと同一である。ここで、用いる不揮発性メモリはNOR型であってもかまわない。しかしながら、ページ毎に（列毎に）各々のビット線702を同時に読み出すことのできるNAND型は、読み出す動作の単純さとスピードの点で、NOR型より有利になる。ここで、第P列（第Pページ）を選択するというのは、チップ認証装置への入力である。ただし、入力は第P列だけを指定するものではない。第P列を選択した後、図25では、一例として、第S列を選択する。出力は、図22の例から、（黒黒白白黒黒白白白白・・・）となる。すなわち、（1101010000・・・）が出力される。続いて、特に図示しないが、一例として、第T列を選択すると（001010011101010・・・）が出力される。これを繰り返し、（P、S、T、・・・）が順に入力される。ここで、（P、S、T、・・・）は、図5及び図9などで説明した入力コード（102、402）に相当する。こうして、上記の“1”と“0”の配列が合成されて出力される。たとえば、（0010010001・・・）（1101010000・・・）（001010011101010・・・）が出力される。これを周辺装置から発信される認証コードとみなし、図9のように、入力コード（P、S、T、・・・）402に関連して基

30

40

50

幹サーバー 400 に保存されている登録コード 403 と比較すればよい。

【0051】

図 26 のように、入力コードとして、第 P 列と第 S 列を同時に選択することもある。また、3 つ以上の列を同時に選択することも可能である。しかしながら、一般に、組み合わせより順列の方が場合の数が多く、一つか二つ程度の信号を順々に入力する入力コードの方が好ましい。このような入力コードは、図 5 及び図 9 のように、基幹サーバーなどに厳重に保管され、共通パスコードとして基幹サーバーと周辺機器との間の交信に使用される。

【0052】

本実施の形態では、図 22 のように、不揮発性メモリアレイにデータが書き込まれている。しかしながら、入力コード（共通パスコード）は、読み出す列（NAND 型ではページ）を指定しているだけなので、周辺装置のメモリのどの領域にも保存されることはない。上述したように、図 6 に示される交信シリーズ 80 は、入力コードと認証コード（あるいは、登録コード）の組み合わせで出来ている。そのため、遠隔攻撃者は、チップ認証装置のメモリアレイに保存されているデータを盗み読みしても、入力コードと登録コードの両方からなる交信シリーズを再現することが出来ない。

10

【0053】

図 22 のように、不揮発性メモリアレイに書き込まれたデータであっても、物理乱数発生装置を用いて生成したデータであるため、データが十分大きければ、どのようなアルゴリズムを持ってしても解読することはほぼ不可能である。こうして、（出力の予測不可能性）も担保することが可能となる。

20

【0054】

物理乱数発生装置を用いて生成した乱数データをメモリセルアレイに書き込むのは、本発明の第一の実施形態のチップ認証装置を搭載するチップを初期化するときに行う。この初期化は、工場集荷時にも、販売時にも、認証機関による認証時にも、エンドユーザー自身が使い始めるときにも、行うことができる。

【実施例 2】

【0055】

本発明に関するチップ認証装置を具現化する半導体装置の一例は、複数個の不揮発性半導体メモリセルの集団を用いて構成することができる。

30

【0056】

まず、通常の量産レベルの製造ラインで製造された、複数個の不揮発性メモリセルの集団を、一括消去する。次に、一括書き込みする。この後読み出すことによって、閾電圧（ V_t ）の分布を得ることが出来る。通常の量産レベルの製造ラインで製造された不揮発性メモリセルの閾電圧（ V_t ）の分布は、このような方法で読み出せば、たとえば、図 27 の点線のように、幅 3 V 程度の分布を示すことが知られている。

【0057】

次に、図 28 のように、通常の量産レベルの製造ラインの製造レシピを一部変更する。通常の量産レベルの製造工程に含まれる、ウェル工程 901 とトンネル膜工程 902 の間に、低エネルギー・チャンネル・イオン打ち込み法により、ウェル全体にドナーとアクセプターを同程度の濃度で浅く打ち込むチャンネルドープ工程 900 を挟み、その後トンネル膜工程 902 とポリ工程 903 を経て通常の量産レベルの製造ラインに戻る。この結果、いくつかのメモリセルでは、ドナーイオンがソース側拡散層近くにより多く分布し、 V_t が減少する。一方、他のいくつかのメモリセルでは、アクセプターイオンがドレイン側拡散層付近により多く分布し、 V_t が高くなる。こうして、一括消去、一括書き込みの後に読み出すことで得られる図 27 の V_t 分布は、図 29 のように 3 つのピークを持つ分布に広がる。左側に、ドナーによって V_t が低くなったセルの集団が多く含まれる。右側に、アクセプターによって V_t が高くなったセルの集団が多く含まれる。反対に、中央の点線で示した分布は図 27 より低くなる。3 つのピークからなる分布の幅は、およそ 4 V 程度となる。ここで、中央の点線の分布は、本発明に関するドナーとアクセプターのイオン打

40

50

ち込みによらない分布であり、分布が幅を持つ原因は、通常の量産レベルの製造ラインで製造されたメモリセルの分布と同様である。すなわち、配線遅延などの不確定要因、トンネル膜中にできるトラップによる不確定要因、ゲートパターンニングやトンネル膜厚などの製造上の不確定要因などである。このうち、トラップ要因の不確定さは、書き込みと消去を繰り返したり、そのまま放置したり、熱を加えたりするうちに変化することが知られており、閾電圧の分布を制御する上で大きな問題となっている。一方、本発明に関する、ドナーとアクセプターのチャンネル・イオン打ち込みによる分布の変化（図29の左と右のピーク）は、チャンネル中のイオンの分布によるものなので、上述したトラップとは関係がない。したがって、書き込み・消去するうちに変化することも少なく、放置している内に変化することも少なく、また、熱を加えることによって変化することも少ない。その上、チャンネル内でのドナーイオンやアクセプターイオンの分布という、物理的乱雑さによって閾電圧分布を新たに付与する。たとえば、図29において、右の分布が、チャンネル中のドレイン拡散層側に分布したアクセプター（負のイオン）によるものである。左に分布したものが、チャンネル中のソース拡散層側に分布したドナー（正のイオン）によるものである。

10

【0058】

図30は、図29の分布から中央の幅3V程度に相当するセルを取り除いたものである。取り除かれたセルのアドレスは、バッファなどに保存する。遠隔攻撃者がこのバッファを盗み読みしても、入力コードに関する十分な情報は得られない。

【0059】

20

わずかであるが、図30の破線で示すように、本実施形態に関するドナーとアクセプターのイオン打ち込みによらない分布が残っている。この分布のうちの一部のセルは、書き込みと消去を繰り返す内、あるいは、放置している内、あるいは、熱を加えたりする内に閾電圧が変化し、更にその一部は、図31に点線で示すように、中央のギャップに裾野を引いて侵入して来る。しかしながら、本実施形態では、元々3Vほどの広いギャップを確保していたので、図32のように、まだ2Vほどギャップが残っている。選択したワード線（選択した列あるいはページ）にこのギャップ内に相当する読み出し電圧を印加し、非選択ワード線にパス電圧を印加したとき、ビット線に電流が流れればビット線と選択ワード線の交差点にあるセルは“黒”（すなわち、“1”）、流れなければ選択したワード線とビット線の交差点にあるセルは“白”（すなわち、“0”）とみなす。読み出し電圧のばらつきを考えても、2Vという、このギャップの広さは、黒と白を区別するのに十分である。図19で説明した（入出力の信頼性）を担保するために、このギャップ幅を十分に広くとる必要がある。

30

【0060】

このように、本実施形態においては、チャンネルドープ工程900によるドナーイオンとアクセプターイオンの分布のばらつきを利用して、図22に示すようなランダムな市松状のパターンを生成できる。このように、どのようなアルゴリズムも使用せず、半導体の製造工程における制御不能の物理的乱雑さを活用することによって、実現が可能となる。

【0061】

図33は、NAND型不揮発メモリのセル構造の鳥瞰図である。基板504の表面は櫛歯状に加工され、表面にアクティブエリア505が平行して紙面前後に配列されている。これと直交して、図23のワード線701に直結する制御ゲート501が左右に伸び、ポリ間誘電体膜502を挟んでアクティブエリア505の先端を包みこんでいる。アクティブエリア505先端部の手前と制御ゲートの反対側には拡散層503がある。図34は、図33から制御ゲート501及びポリ間誘電体膜502を剥ぎ取ったものである。アクティブエリア505の幅AAは、デバイスの微細化と共に小さくなる。現在最先端では、AAは20nm以下にまで微細化されている。

40

【0062】

微細化と共にAAが狭くなるにつれ、図29に対応する、ドナーイオンによるピークとアクセプターイオンによるピークの間のギャップは広がる。その一例を図35に示す。前

50

述の例のように、間の3 V程度を中抜きし、中抜きされたメモリセルのアドレスをバッファに保存する。このアドレスデータは、パスコードとは関係ないので、遠隔攻撃者に盗み読まれても問題ない。上述のように、トラップ起因の染み出しを考慮すると、図36のようになる。これは、上の例の図31に対応する。元々のギャップが広いと、図31に比べると、点線で示すギャップへの染み出しは減少する。結果として、図37に示すように、白分布と黒分布の間のギャップは、トラップ起因によるV_t変化を考慮しても、たとえば、2.5 Vほどになる。これは、図32の例の2 Vより拡大している。こうして、デバイスの微細化により、本実施形態の効果は顕著になることが判る。通常のメモリセルでは、ばらつきを抑えることが目標になるが、本実施形態では、逆に、微細化と共に増大する物理的乱雑さを積極的に活用するのである。

10

【実施例3】**【0063】**

図38は、第三の実施形態の特徴を現すスリミング工程950を説明するものである。通常の製造プロセスにおけるポリ工程（浮遊ゲート）903及び基板表面を櫛歯状に加工するシャロー・トレンチ・イソレーション（STI）工程951に続き、スリミング工程950を挟み、その後ポリ間誘電体膜工程952とポリ工程（制御ゲート）953と続き、通常の製造工程も戻る。たとえば、スリミング工程950は熱酸化プロセスの一種である。

【0064】

図39は、本実施形態の特徴であるスリミング工程950によって得られる閾電圧の分布である。スリミング工程950により、アクティブエリア505の幅AAが更に狭くなる。その結果、ドナーイオンによるピークとアクセプターイオンによるピークの変動が更に大きくなり、図39のように、3つのピークがそれぞれ孤立するように分布する。ここで、第二の実施形態と同様の方法で中央4 Vに相当するセルの分布を中抜きすると、図40のようになる。ギャップ幅は4 V程度となり、図37に比べて更に広くなる。こうして、本実施形態の特徴であるスリミング工程950を用いることにより、（入出力の信頼性）を更に引き出すことが可能となる。

20

【実施例4】**【0065】**

アクティブエリア505の幅AAが十分狭くない場合、読み出し時に混入するノイズにより、読み出すたびに同じセルの出力が白と黒の間を変化することがある。あるいは、バッファに保存されていないアドレスであっても、白にも黒にも属さない場合が生じる可能性がある。このような場合、図41に示すように、まず測定するセルを選択し、このセルの測定を複数回（たとえばN）繰り返し、白が出る回数がN/2より大きければ白とみなし、黒の出る回数がN/2より多ければ黒とみなし、どちらでもなければ、当該セルのアドレスをバッファに保存し、別のセルを選択する、という操作が必要になる。ただし、Nは2より大きい自然数である。

30

【実施例5】**【0066】**

図42に示すように、上述した第一から第四の実施形態の内、一つ、もしくは、複数の特徴を併せ持つチップ認証モジュール600と、このチップ認証モジュール600と外部との通信を開く外部I/O500と、このチップ認証モジュール600のみと通信をするその他の機能を有するモジュール800とを、混載するチップ100からなる半導体装置。これは、混載型チップ認証装置となる。

40

【実施例6】**【0067】**

図30、図36、および、図40のように、閾値分布の中抜きをする方法は次のように説明できる。たとえば、チップ認証機能のみを有するスタンドアローン型のチップ認証装置の場合、図43のように、中抜きすると決めたセルのアドレスをバッファ90に記録し、入力されたパスコードが順次選択するページに連なるメモリセルのアドレスを個々に

50

バッファに記録されたアドレスと比較し、両者が一致した場合、対応するアドレスから読み出されたデータを出力コードに含めないことによって実現することができる。チップ認証機能以外の機能も有する混載型のチップ認証装置の場合、図44のように、中抜きすると決めたセルのアドレスをバッファ90に記録し、入力されたパスコードが順次選択するページに連なるメモリセルのアドレスを個々にバッファに記録されたアドレスと比較し、両者が一致した場合、対応するアドレスから読み出されたデータを出力コードに含めないことによって実現することが出来る。

【0068】

この発明によれば、電子装置のネットワークを、周辺装置と、周辺装置の登録状況を管理する基幹サーバーとに分割し、基幹サーバーはソフトウェアによる中央管理とし、中央管理の手が行き届かない周辺装置には物理的チップ認証装置を搭載し、システム全体のセキュリティをソフトウェアとハードウェアでシェアすることにより、周辺装置への遠隔攻撃を効率よく未然に防ぐことが可能となる。

10

【0069】

なお、本発明の技術範囲は上記実施の形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲において種々の変更を加えることが可能である。

【産業上の利用可能性】

【0070】

中央管理の行き届かない周辺装置を無数に抱えるネットワークの装置間認証を、どのようなアルゴリズムにもよらずにチップレベルで安全に実現することが可能となる。

20

【符号の説明】

【0071】

- 1、10、100、400 チップ
- 2 ファームウェア
- 3 認証制御デバイス
- 4 認証コード（ID）
- 5、50、500 外部入出力装置（I/O）
- 6 認証システム（従来例の一例）

- 11、12、13 認証
- 21、22、60 本願に関わるチップ認証装置

30

- 31 入力信号誤差
- 32 出力信号誤差
- 42 入力コード
- 43 登録コード
- 60 チップ認証装置
- 71 第一の装置
- 72 第二の装置
- 73 第三の装置
- 74 第四の装置
- 75 第五の装置
- 80 交信シリーズ
- 83 偽交信シリーズ
- 90 バッファ
- 92 第二の装置の正規使用者
- 93 遠隔攻撃者

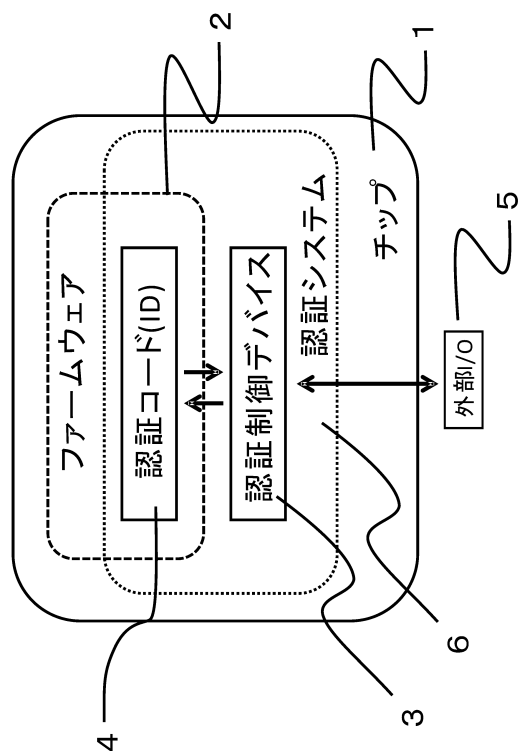
- 102、402 入力コード
- 202、403 登録コード
- 302、401 内部メモリ
- 400、1400、2400、3400 基幹サーバー
- 410、420、430、440、450 周辺装置

40

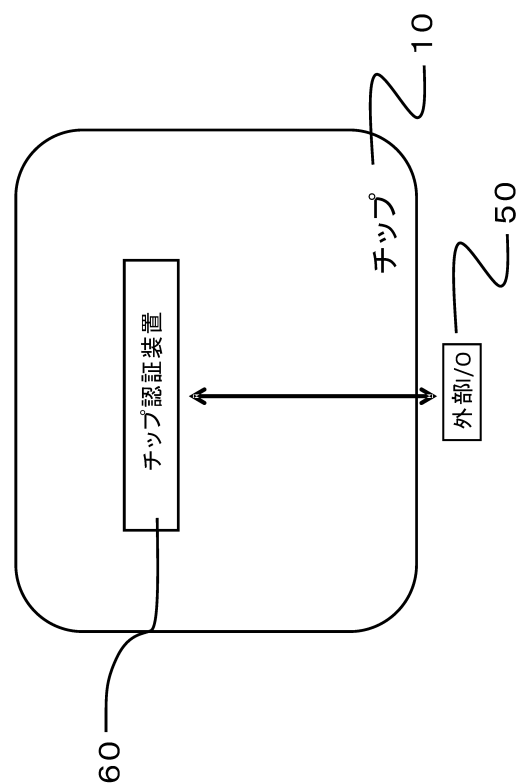
50

501	制御ゲート	
502	ポリ間誘電体膜	
503	拡散層	
504	基板	
505	アクティブエリア	
600	チップ認証モジュール	
701	ワード線	
702	ビット線	
703	ソース線	
704	ソース選択ゲート	10
705	ドレイン選択ゲート	
800	その他のモジュール	
900	チャネルドープ工程	
901	ウェル工程	
902	トンネル膜工程	
903	ポリ工程（浮遊ゲート）	
950	スリミング工程	
951	STI工程	
952	ポリ間誘電体膜工程	
953	ポリ工程（制御ゲート）	20
1410、2410	共通パスコード	
4101、4201、4301、4102、4202、4302	認証	

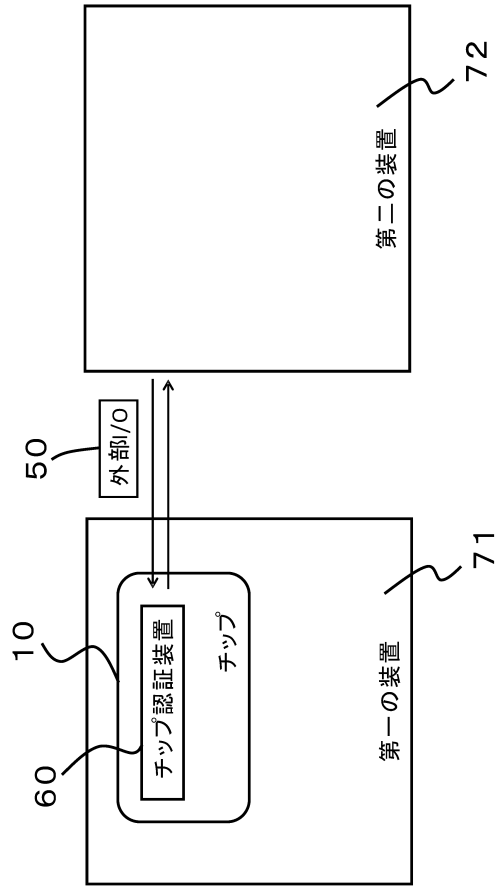
【図1】



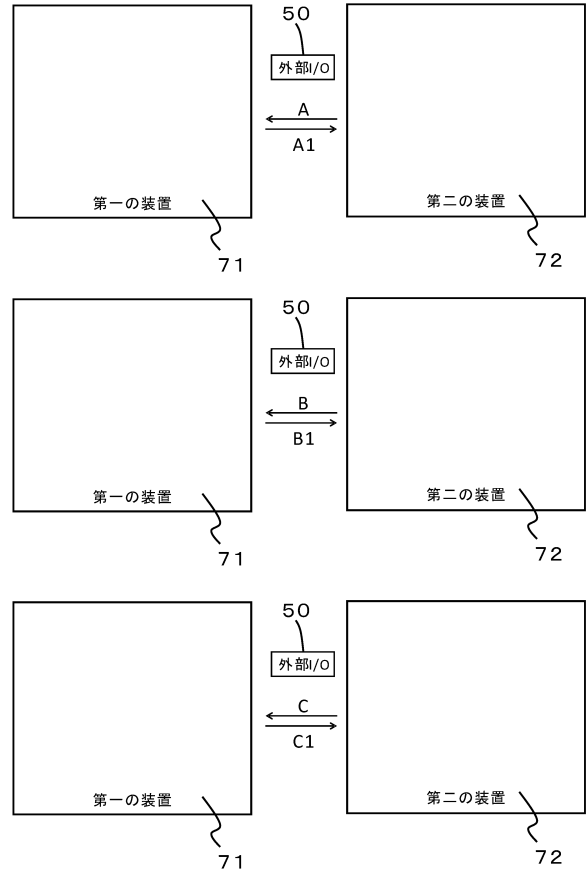
【図2】



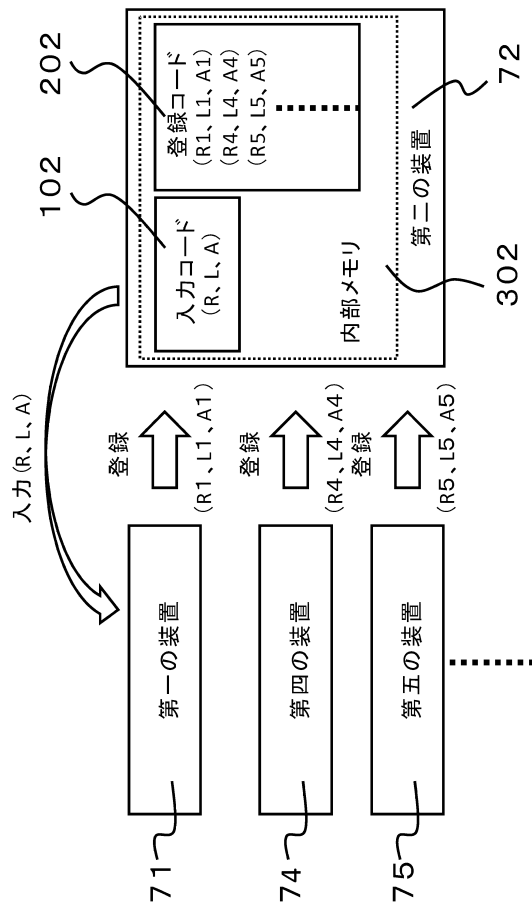
【図 3】



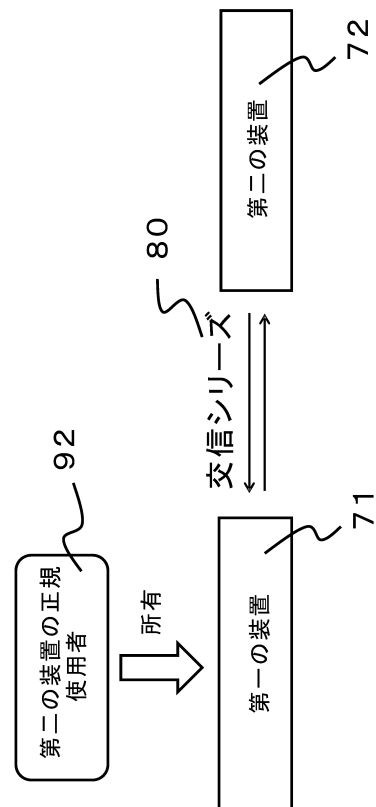
【図 4】



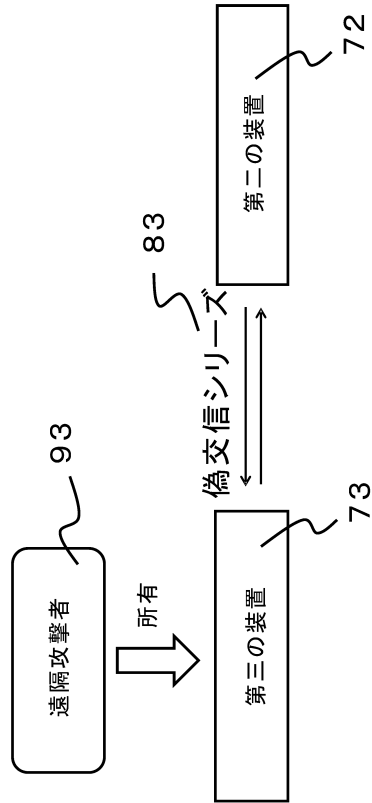
【図 5】



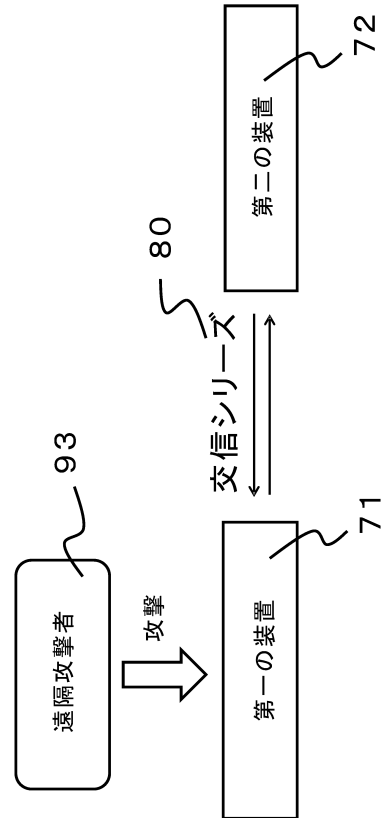
【図 6】



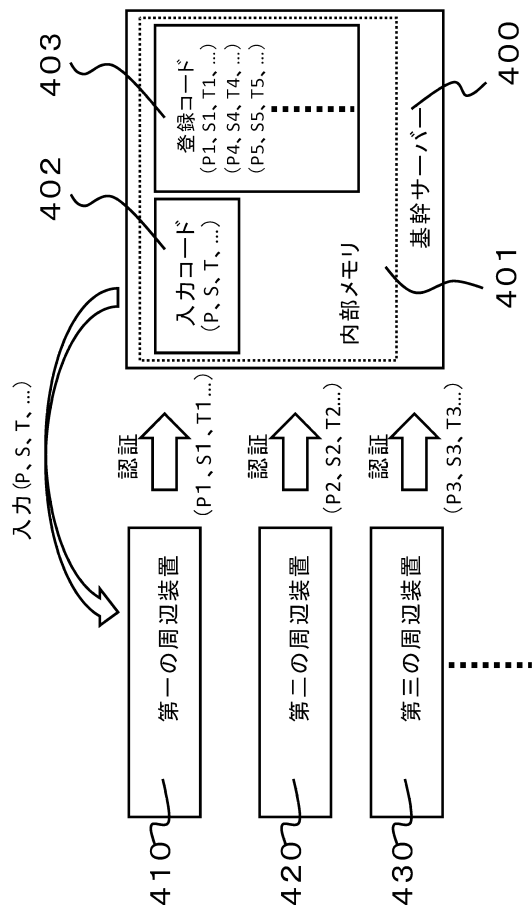
【図 7】



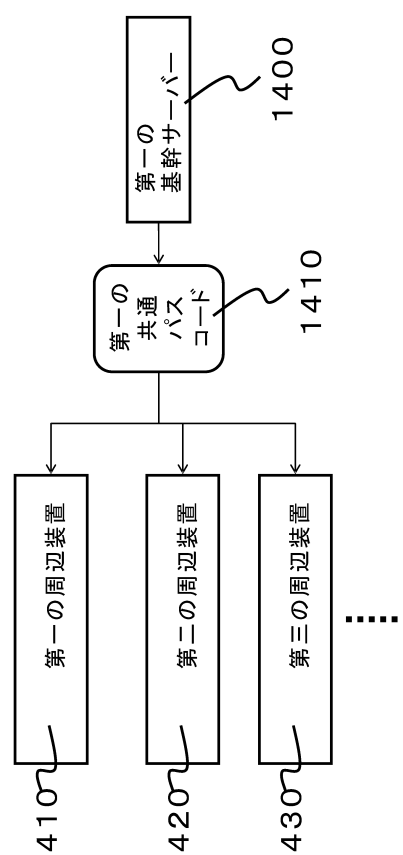
【図 8】



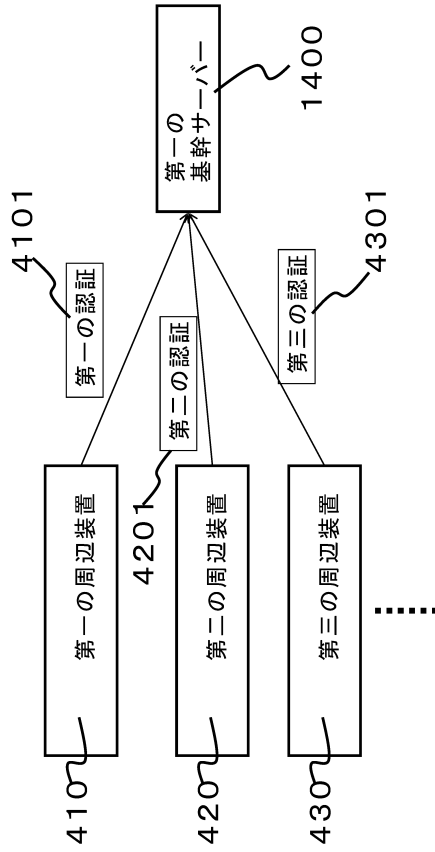
【図 9】



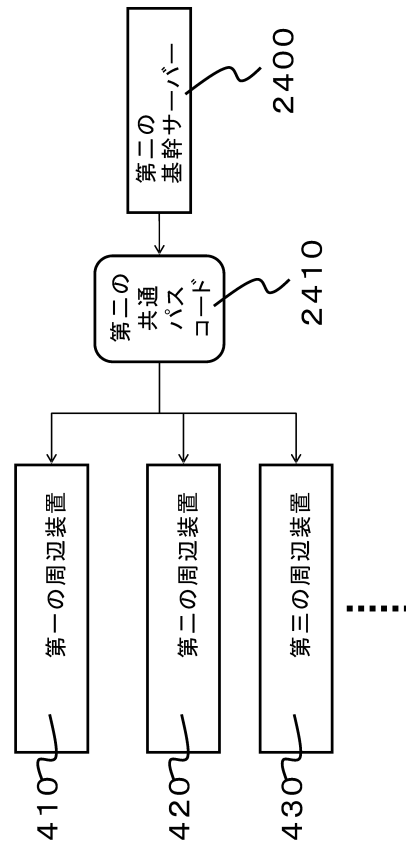
【図 10】



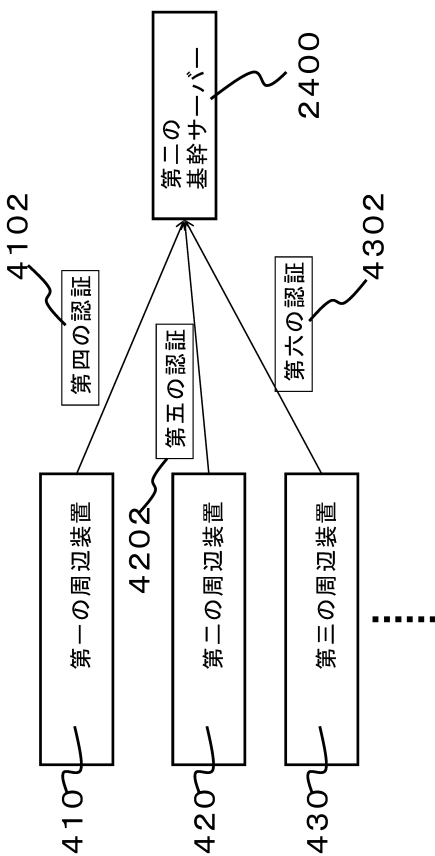
【図 1 1】



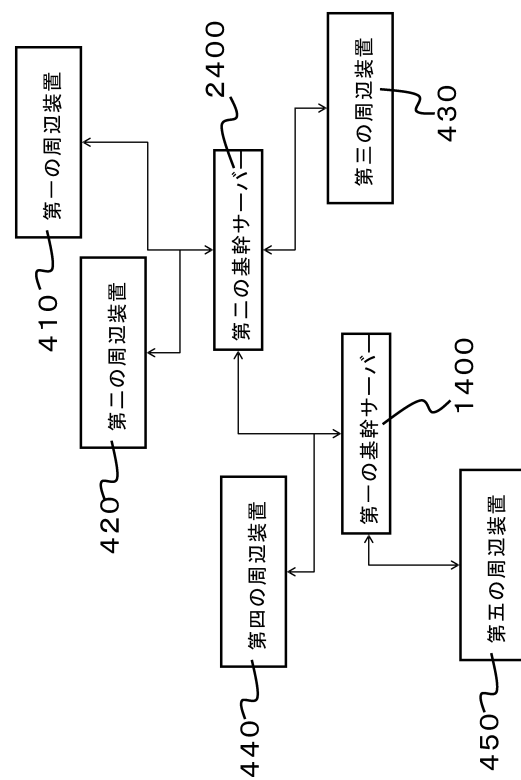
【図 1 2】



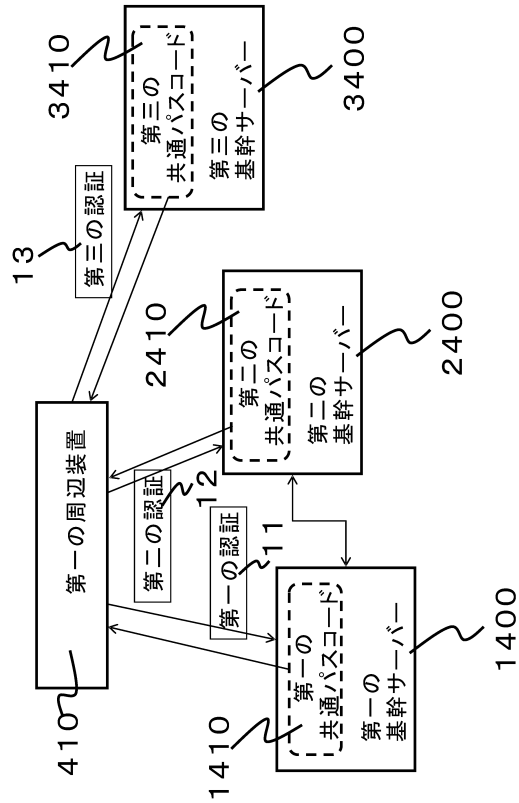
【図 1 3】



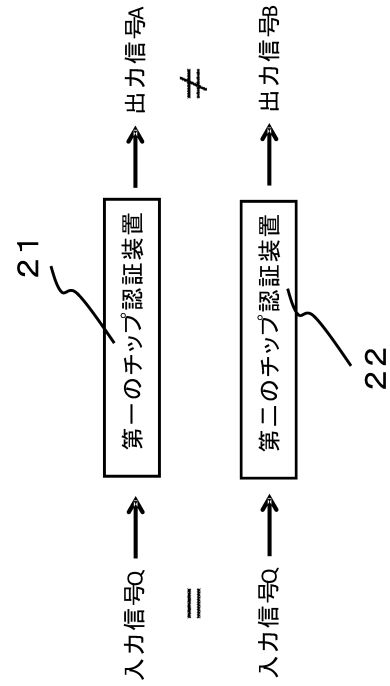
【図 1 4】



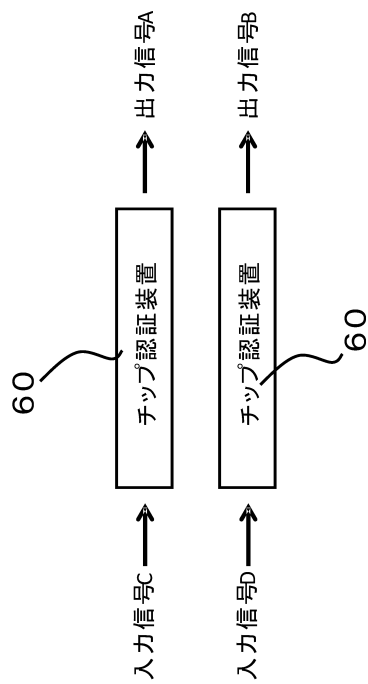
【図 15】



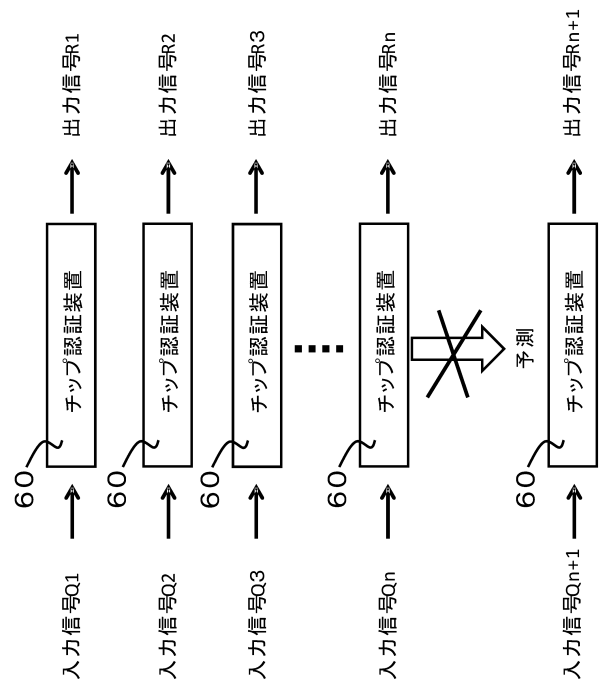
【図 16】



【図 17】



【図 18】



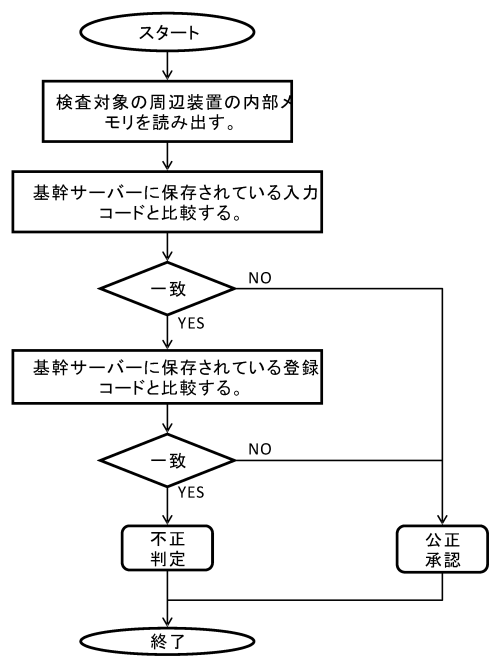
【図 19】



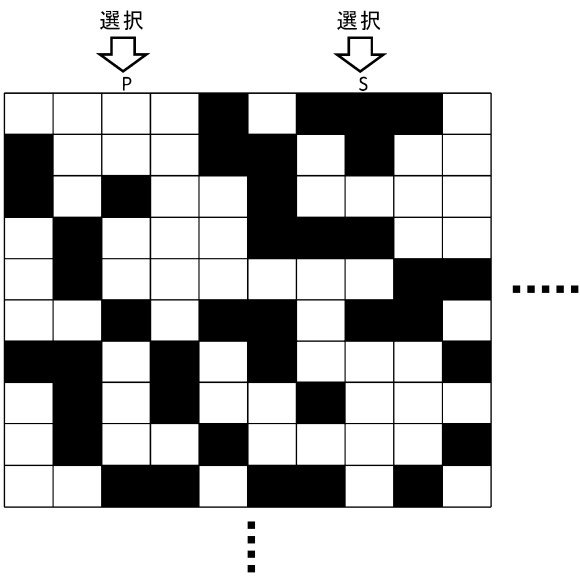
【図 20】

入力コード 42	RTSDEDDTAG!\$&D(!	oq& QX5'Xj*!e{ CY
	OD\$zD)X#pgd[_&x*n	C(Y6;sHWLnplL+5P[+@
	LJ/z5J@e\$g9mhd0/9Mx	p;A18;6Nd[ic8a"+.SO
	_p]Q 9ecbe{2leq=!?E	wG;x'5@/O(GM";ODS+K
	u+x~53cvmjfyvZ"GzI#	Tw[F\sk8!a"hKlgFIN~
	■ ■ ■	■ ■ ■

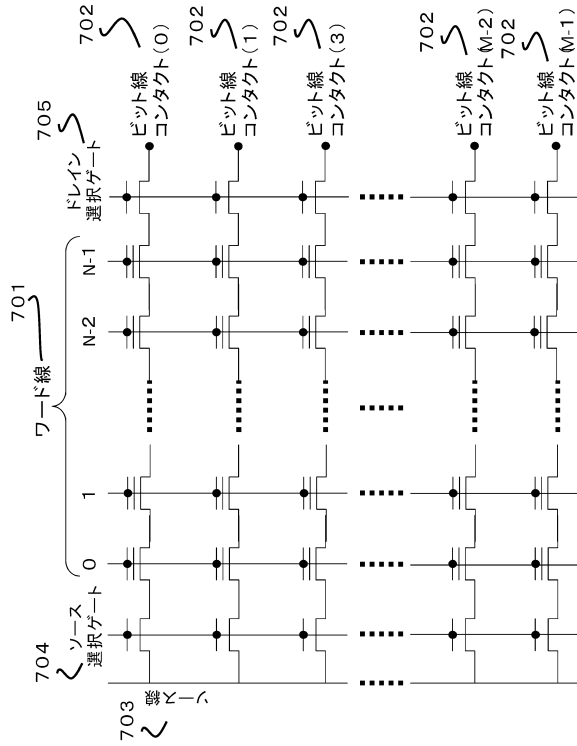
【図 21】



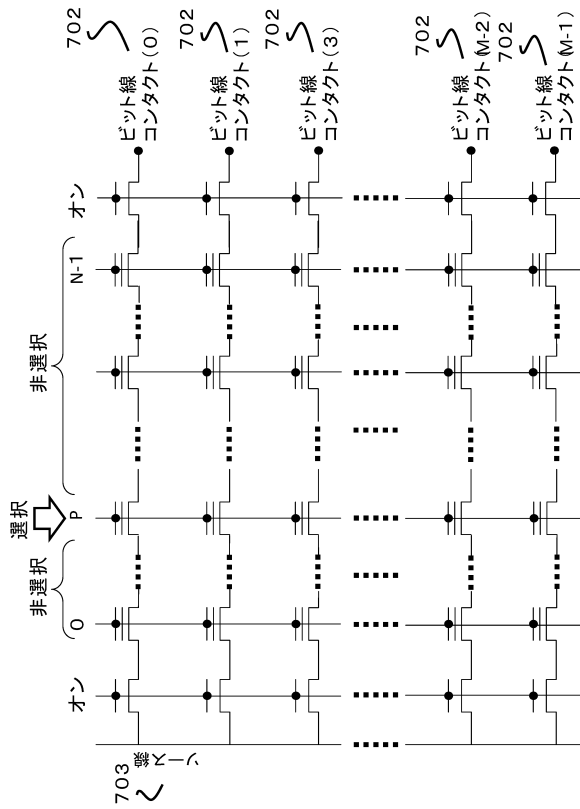
【図 22】



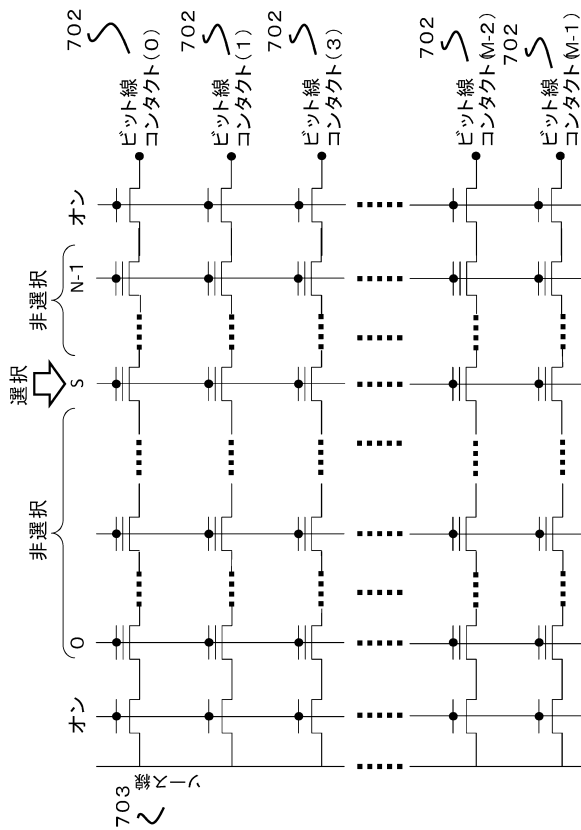
【図 2 3】



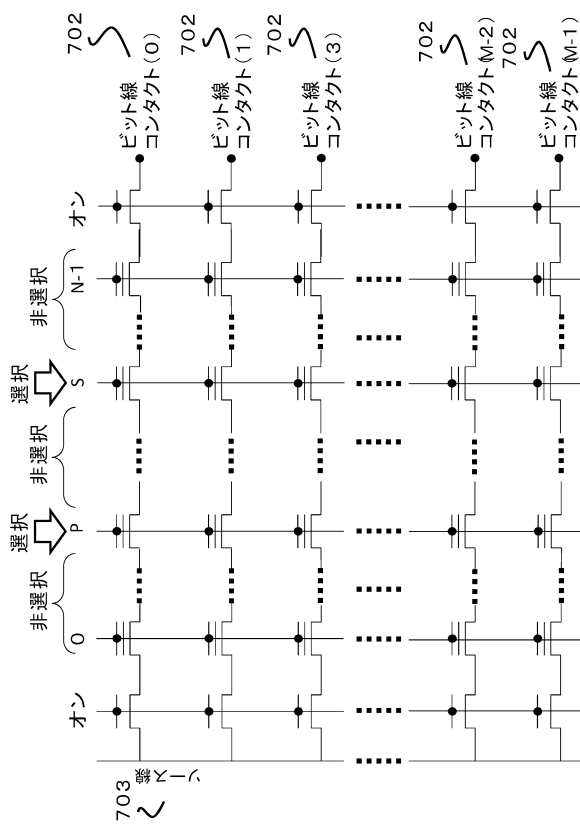
【図 2 4】



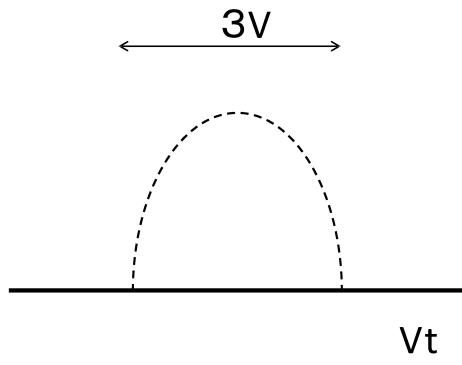
【図 2 5】



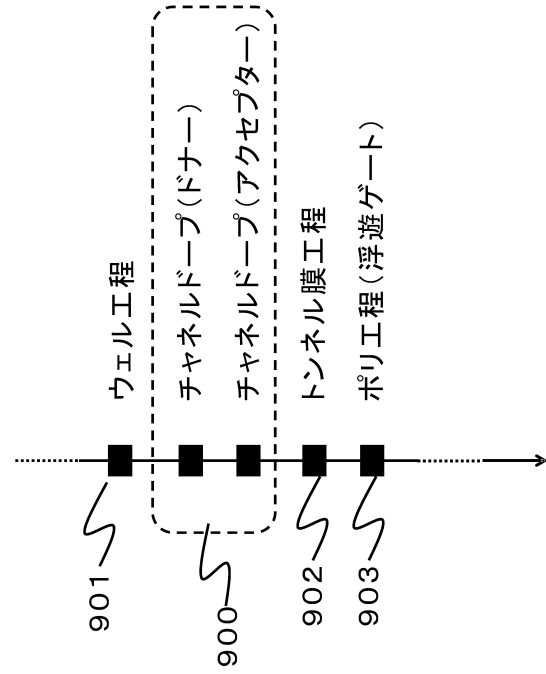
【図 2 6】



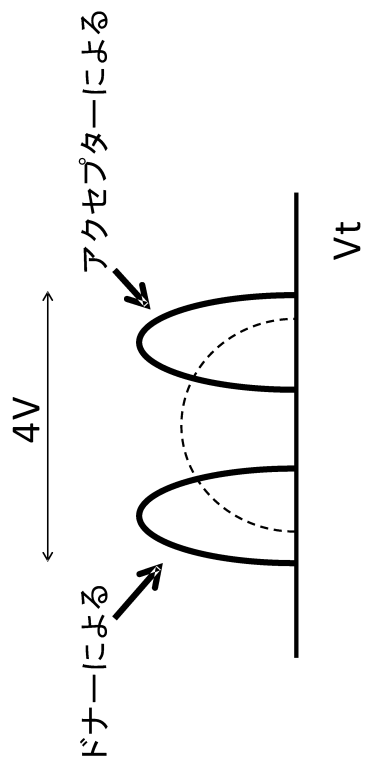
【図 27】



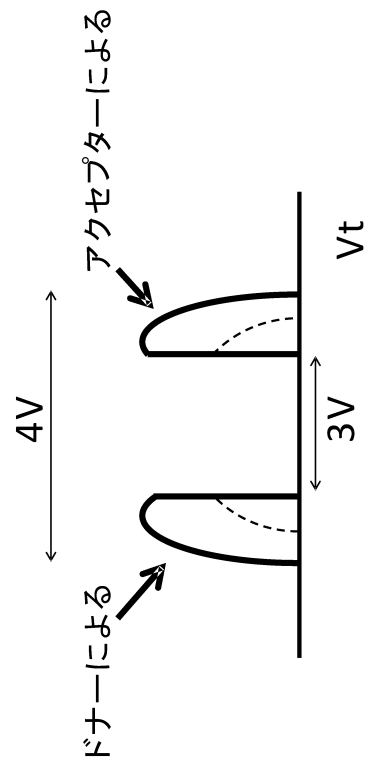
【図 28】



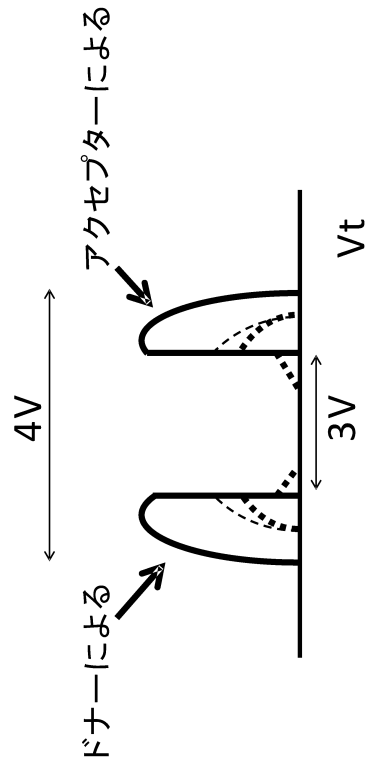
【図 29】



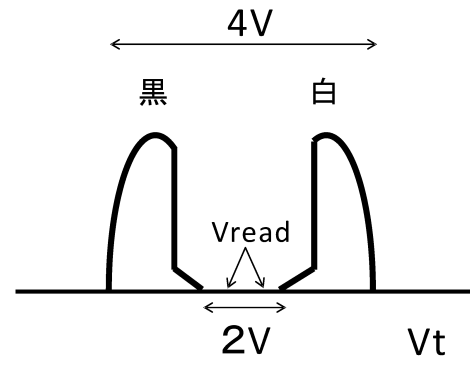
【図 30】



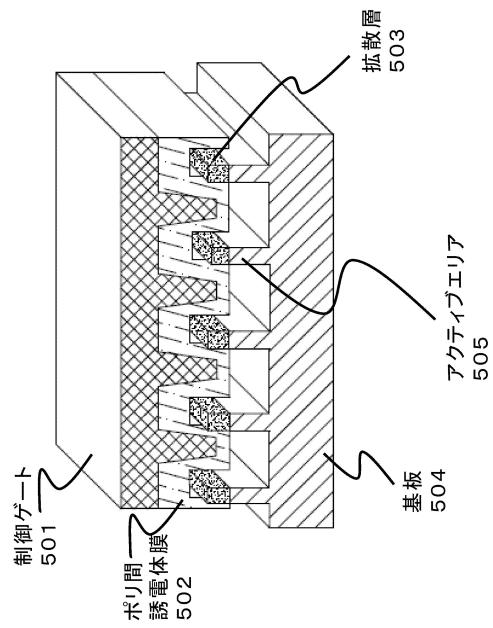
【図 3 1】



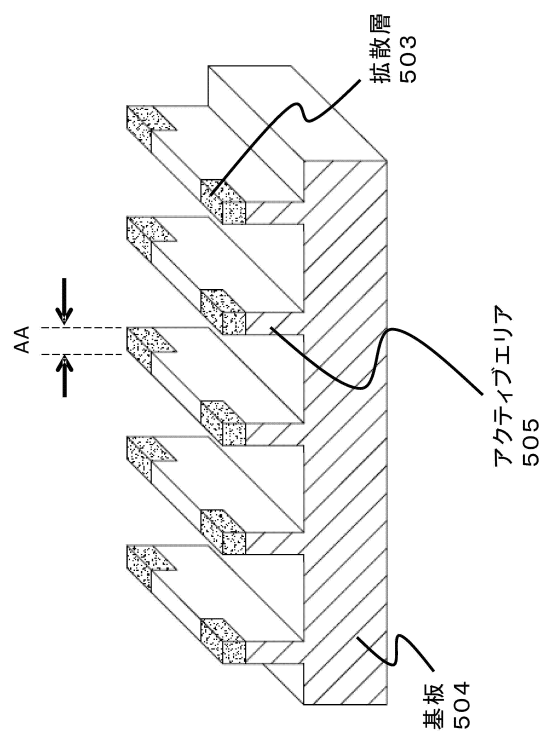
【図 3 2】



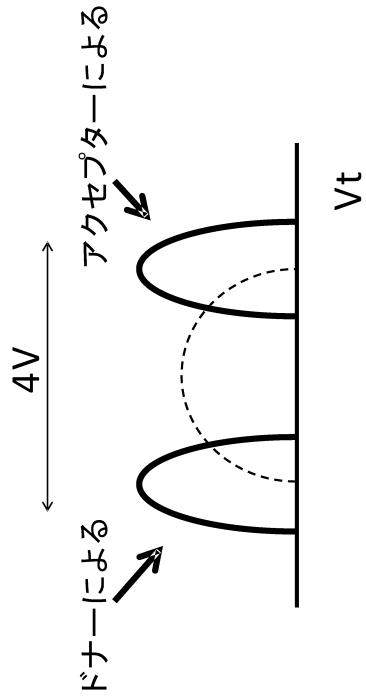
【図 3 3】



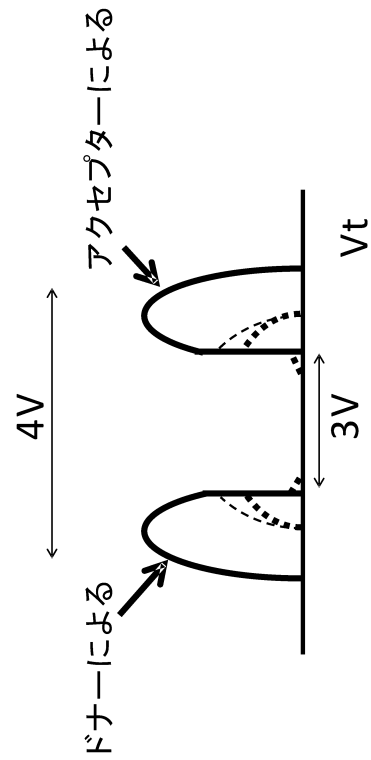
【図 3 4】



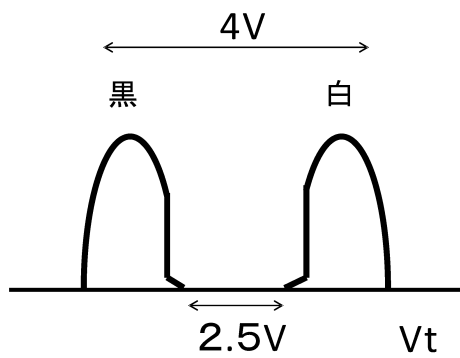
【図 3 5】



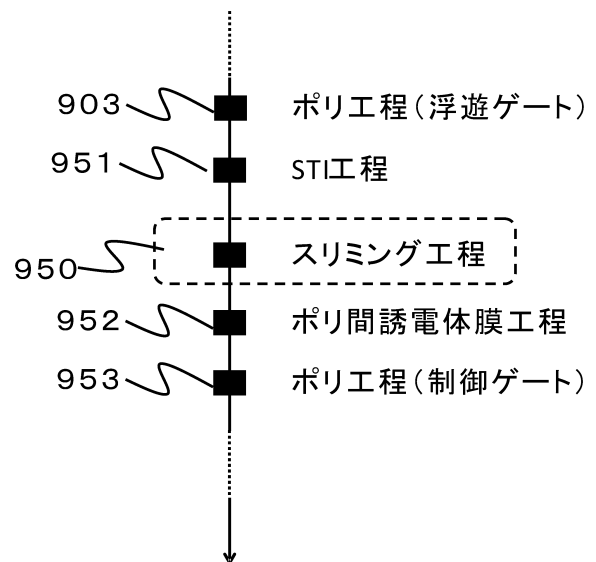
【図 3 6】



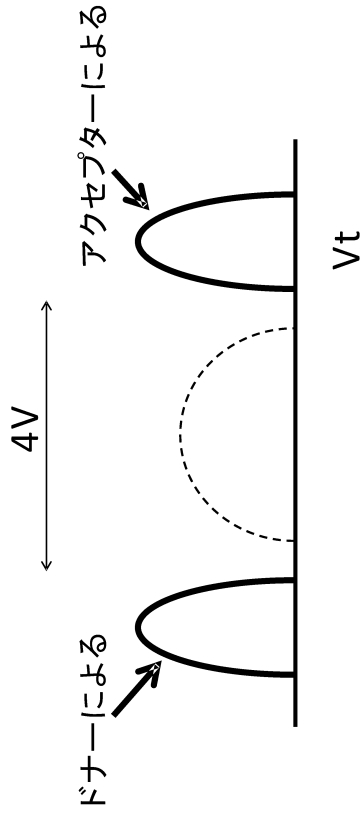
【図 3 7】



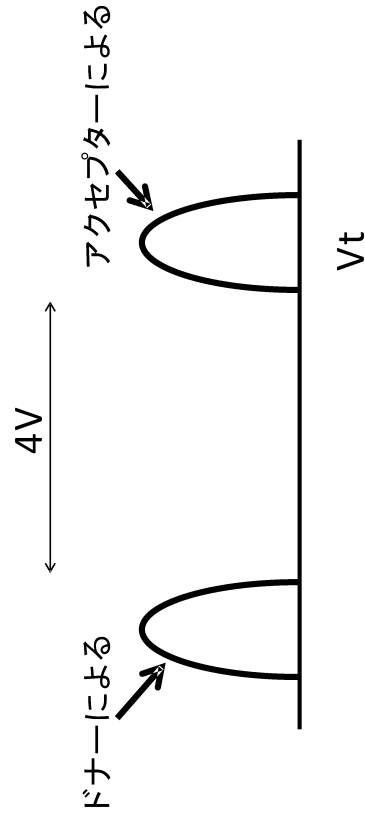
【図 3 8】



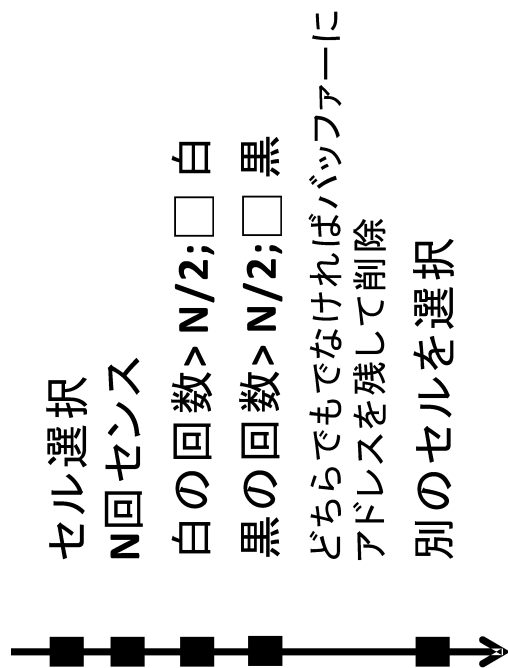
【図 3 9】



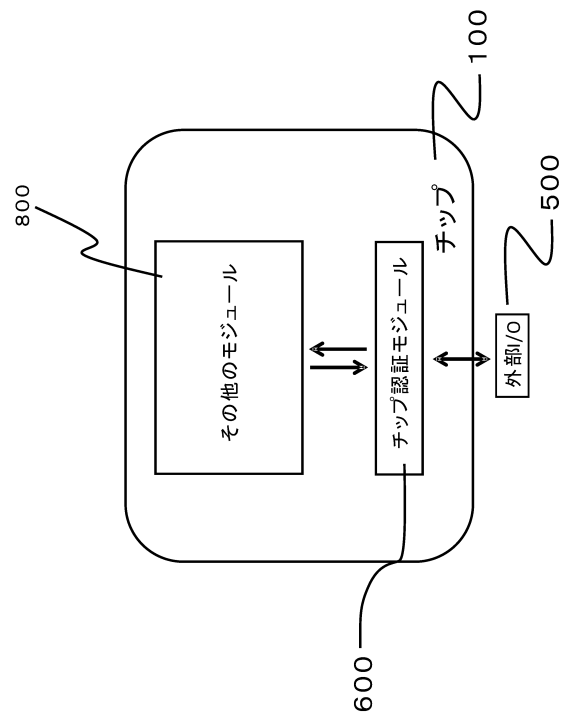
【図 4 0】



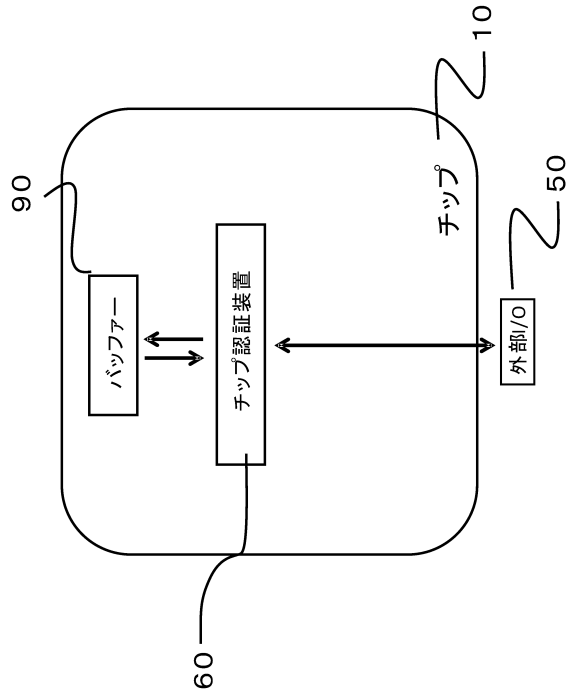
【図 4 1】



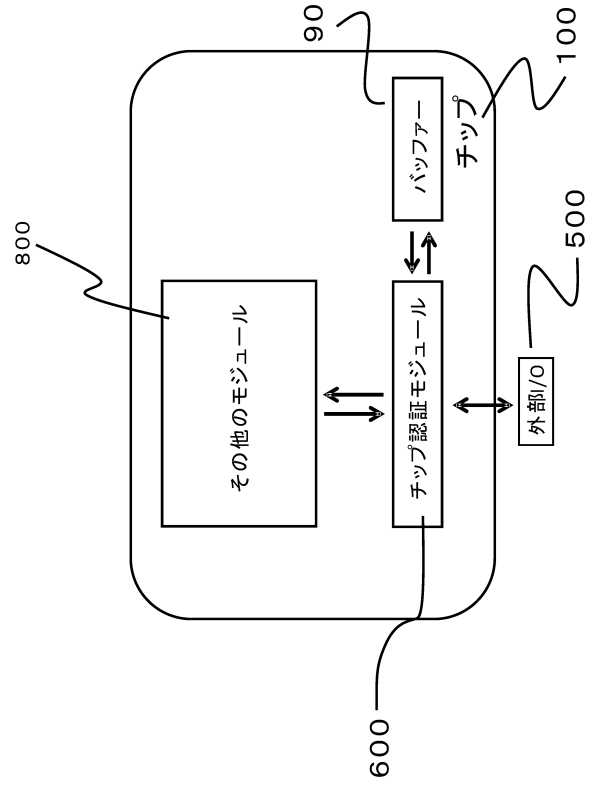
【図 4 2】



【図 4 3】



【図 4 4】



フロントページの続き

(56)参考文献 特開2015-036257 (JP, A)
特開2010-226603 (JP, A)
特開2008-085547 (JP, A)
特開2014-053675 (JP, A)
米国特許出願公開第2009/0083833 (US, A1)
米国特許出願公開第2014/0279532 (US, A1)
特開2011-198317 (JP, A)
特表2009-531977 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/00- 9/38
G06F 21/44
G06F 21/75