(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4962993号
(P4962993)
(45)発行日　平成24年6月27日(2012.6.27)　(24)登録日　平成24年4月6日(2012.4.6)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 21/22 114D
G06F 11/22 (2006.01)　　G06F 11/22 340A

請求項の数 10　(全 16 頁)

(21)出願番号	特願2009-519507 (P2009-519507)
(86)(22)出願日	平成19年7月11日 (2007.7.11)
(65)公表番号	特表2009-544069 (P2009-544069A)
(43)公表日	平成21年12月10日 (2009.12.10)
(86)国際出願番号	PCT/US2007/015775
(87)国際公開番号	WO2008/008367
(87)国際公開日	平成20年1月17日 (2008.1.17)
審査請求日	平成22年7月9日 (2010.7.9)
(31)優先権主張番号	60/831,022
(32)優先日	平成18年7月14日 (2006.7.14)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	60/820,287
(32)優先日	平成18年7月25日 (2006.7.25)
(33)優先権主張国	米国 (US)

(73)特許権者　502188642
マーベル　ワールド　トレード　リミテッド
バルバドス国　ビービー１４０２７，セントマイケル、ブリトンズ　ヒル、ガンサイトロード、エル　ホライズン
(74)代理人　100104156
弁理士　龍華　明裕
(74)代理人　100118005
弁理士　飯山　和俊
(74)代理人　100143502
弁理士　明石　英也
(74)代理人　100138128
弁理士　東山　忠義

最終頁に続く

(54)【発明の名称】システムオンアチップ（ＳｏＣ）試験インタフェースセキュリティ

(57)【特許請求の範囲】
【請求項１】
プロセッサと、
イネーブルされている場合にだけ、前記プロセッサと通信する試験インタフェースと、
前記プロセッサ用のファームウェアを記憶する第１メモリと、
前記プロセッサ用の、前記プロセッサがブートした場合に前記第１メモリ内の予め定められた位置から前記ファームウェアの一部を前記プロセッサに読み込ませるブートコードを記憶する第２メモリと
レジスタ、前記予め定められた値を記憶する第３メモリ、および前記レジスタと前記第３メモリとの間の比較に基づいて、前記試験インタフェースをイネーブルするロジックを有する特定用途向け回路と
を備え、
前記試験インタフェースは、前記ファームウェアの前記一部が予め定められた値を有する場合にだけイネーブルされ、
前記ブートコードは、前記プロセッサに、前記ファームウェアの前記一部を前記レジスタに書き込ませる装置。
【請求項２】
前記試験インタフェースは、Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースを有する
請求項１に記載の装置。

【請求項３】
前記プロセッサは、前記ファームウェアの前記一部が前記予め定められた値を有するか否かを決定し、
前記プロセッサは、前記ファームウェアの前記一部が前記予め定められた値を有する場合に、前記試験インタフェースをイネーブルする請求項１または２に記載の装置。
【請求項４】
前記試験インタフェースは、イネーブルされている場合にだけ、前記特定用途向け回路と通信する請求項１から３の何れか１項に記載の装置。
【請求項５】
前記第１メモリ内の前記予め定められた位置に記憶された前記ファームウェアの前記一部はスクランブルされており、
前記装置は、
前記プロセッサが前記第１メモリ内の前記予め定められた位置から前記ファームウェアの前記一部を読み込んだ場合に、前記ファームウェアの前記一部をデスクランブルするデスクランブラ
をさらに備える請求項１から４の何れか１項に記載の装置。
【請求項６】
前記デスクランブルは、
Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ　（ＡＥＳ）プロセス、
Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ　（ＤＥＳ）プロセス、および
共有鍵プロセス
の少なくとも１つに従って実行される請求項５に記載の装置。
【請求項７】
前記第１メモリは、
ファームウェアメモリ
を有する請求項１から６の何れか１項に記載の装置。
【請求項８】
前記第２メモリは、
リードオンリーメモリ
を有する請求項１から７の何れか１項に記載の装置。
【請求項９】
請求項１から８の何れか１項に記載の装置を有する集積回路。
【請求項１０】
請求項９に記載の集積回路を備えるディスクプレーヤ。
【発明の詳細な説明】
【関連出願】
【０００１】
本出願は、２００７年１月１８日に出願された米国特許出願番号第１１／６５４８４１号、２００６年７月１４日に出願された米国仮特許出願番号第６０／８３１０２２号、および、２００６年７月２５日に出願された米国仮特許出願番号第６０／８２０２８７号の利益を主張し、その開示は、全てがここに参照として組み込まれる。
【技術分野】
【０００２】
本発明は、概して集積回路に関する。特に、本発明はシステムオンチップ（ＳｏＣ）試験インタフェースセキュリティに関する。
【背景技術】
【０００３】
集積回路技術の最近の進歩は、いわゆるシステムオンチップ（ＳｏＣ）集積回路を普及させた。そこでは、メモリ、および、単一の集積回路チップ上の特定用途向け回路のような他のハードウェアブロックとともに、プロセッサが組み込まれる。図１は、プロセッサ

１０２、不揮発性メモリ１０４、揮発性メモリ１０６、リードオンリーメモリ（ＲＯＭ）１０８、試験インタフェース１１０、および、特定用途向け回路１１２を備える従来技術としてのＳｏＣ１００を示す。

【０００４】

ＳｏＣ１００は、Ｊｏｉｎｔ Ｔｅｓｔ Ａｃｔｉｏｎ Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースのような、ＳｏＣ１００をデバッッギングおよび試験するのに用いる１つの試験インタフェース１１０を通常備える。試験インタフェース１１０は、一般にプロセッサ１０２および特定用途向け回路１１２に接続される。試験インタフェース１１０は、ＳｏＣ１００内の他の回路にも接続されることができる。例えば、ＳｏＣ１００は、不揮発性メモリ１０４に記憶されたファームウェアのプロセッサ１０２による実行をトレースするために用いることができる。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、試験インタフェース１１０は、開発中には有用な一方で、ひとたび実地で実用されると、アタッカがＳｏＣ１００に入り込む隙をも提供する。例えば、アタッカは、ＳｏＣ１００が内部に設けられたシステムのセキュリティを破るべくファームウェアをコピーまたは変更するために試験インタフェース１１０を使用することができる。ＳｏＣ１００は、いくつかのリソースへの不正アクセスを防ぐための秘密鍵のようなシークレットを用いることもできる。例えば、デジタルビデオディスク（ＤＶＤ）プレーヤ／バーナ内に設けられたＳｏＣ１００は、コピープロテクトされたＤＶＤのコピーをユーザが作成することを防ぐための秘密鍵を用いることができる。アタッカは、試験インタフェース１１０を用いて秘密鍵を取得して、コピープロテクトされたＤＶＤのコピーをＤＶＤプレーヤ／バーナを用いて作成することができる。

【課題を解決するための手段】

【０００６】

概して、一側面において、この発明は、プロセッサと、イネーブルされている場合にだけ、プロセッサと通信する試験インタフェースと、プロセッサ用のファームウェアを記憶する第１メモリと、プロセッサ用のブートコードを記憶する第２メモリとを備え、プロセッサがブートした場合に、ブートコードはプロセッサに、第１メモリ内の予め定められた位置からファームウェアの一部を読み込ませ、試験インタフェースは、ファームウェアの一部が予め定められた値を有する場合にイネーブルされる装置、を特徴とする。

【０００７】

いくつかの実施態様において、試験インタフェースは、Ｊｏｉｎｔ Ｔｅｓｔ Ａｃｔｉｏｎ Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースを有する。いくつかの実施態様において、プロセッサはファームウェアの一部が予め定められた値を有するか否かを決定し、ファームウェアの一部が予め定められた値を有する場合に、プロセッサは試験インタフェースをイネーブルする。いくつかの実施態様は、レジスタと、予め定められた値を記憶する第３メモリと、レジスタと第３メモリとの間の比較に基づいて、試験インタフェースをイネーブルするロジックとを有する特定用途向け回路を備え、ブートコードは、プロセッサに、ファームウェアの一部をレジスタに書き込ませる。いくつかの実施態様において、試験インタフェースは、イネーブルされている場合にだけ、特定用途向け回路と通信する。いくつかの実施態様において、第１メモリ内の予め定められた位置に記憶されたファームウェアの一部はスクランブルされており、装置は、プロセッサが第１メモリ内の予め定められた位置からファームウェアの一部を読み込んだ場合に、ファームウェアの一部をデスクランブルするデスクランブラをさらに備える。いくつかの実施態様において、デスクランブルは、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＡＥＳ）プロセス、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＤＥＳ）プロセス、および共有鍵プロセスの少なくとも１つに従って実行される。いくつかの実施態様において、第１メモリは、ファームウェアメモリを有する。いくつかの実施態様において、第２メモ

リは、リードオンリーメモリを有する。いくつかの実施態様は、上記装置を有する集積回路を備える。いくつかの実施態様は、上記集積回路を備えるディスクプレーヤを備える。

【０００８】

概して、一側面において、この発明は、プロセッシング手段と、イネーブルされている場合にだけプロセッシング手段と通信する試験インタフェース手段と、プロセッッシング手段用のファームウェアを記憶する第１メモリ手段と、プロセッシング手段用のブートコードを記憶する第２メモリ手段とを備え、プロセッシング手段がブートした場合に、ブートコードは、第１メモリ内の予め定められた位置からファームウェアの一部をプロセッシング手段に読み込ませ、試験インタフェース手段は、ファームウェアの一部が予め定められた値を有する場合にだけイネーブルされる装置、を特徴とする。

【０００９】

いくつかの実施態様において、試験インタフェースは、Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ（ＪＴＡＧ）を有する。いくつかの実施態様において、プロセッシング手段は、ファームウェアの一部が予め定められた値を有するか否かを決定して、プロセッシング手段は、ファームウェアの一部が予め定められた値を有する場合に、試験インタフェース手段をイネーブルする。いくつかの実施態様は、データを記憶する第３メモリ手段と、予め定められた値を記憶する第４メモリ手段と、第３および第４メモリ手段の間の比較に基づいて、試験インタフェースをイネーブルするロジック手段とを備え、ブートコードは、プロセッシング手段に、ファームウェアの一部を第３メモリ手段に書き込ませる。いくつかの実施態様において、試験インタフェース手段は、試験インタフェースがイネーブルされている場合にだけ、ロジック手段と通信する。いくつかの実施態様において、第１メモリ手段内の予め定められた位置に記憶されたファームウェアの一部はスクランブルされており、装置は、プロセッシング手段が第１メモリ手段内の予め定められた位置からファームウェアの一部を読み込んだ場合に、ファームウェアの一部をデスクランブルするデスクランブラ手段をさらに備える。いくつかの実施態様において、デスクランブルは、Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ　（ＡＥＳ）プロセス、Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ　（ＤＥＳ）プロセス、および共有鍵プロセスの少なくとも１つに従って実行される。いくつかの実施態様は、上記装置を有する集積回路を備える。いくつかの実施態様は、上記集積回路を備えるディスクプレーヤを備える。

【００１０】

概して、一側面において、この発明は、プロセッサ、試験インタフェース、プロセッサ用のファームウェアを記憶する第１メモリ、および、プロセッサ用のブートコードを記憶する第２メモリを有する装置をオペレートする方法であって、ブートコードに従って、プロセッサがブートした場合に第１メモリ内の予め定められた位置からファームウェアの一部を読み込む段階と、ファームウェアの一部が予め定められた値を有するか否かを決定する段階と、ファームウェアの一部が予め定められた値を有する場合にだけ、試験インタフェースをイネーブルする段階とを備え、試験インタフェースは、イネーブルされている場合にだけプロセッサと通信する方法、を特徴とする。

【００１１】

いくつかの実施態様において、装置は、レジスタ、および、予め定められた値を記憶する第３メモリを有し、方法は、ブートコードに従って、ファームウェアの一部をレジスタに書き込む段階と、レジスタと第３メモリとの間の比較に基づいて、試験インタフェースをイネーブルする段階とをさらに備える。いくつかの実施態様において、装置は、レジスタおよび第３メモリを有する特定用途向け回路をさらに有し、記試験インタフェースは、イネーブルされている場合にだけ、特定用途向け回路と通信する。いくつかの実施態様において、第１メモリ内の予め定められた位置に記憶されたファームウェアの一部はスクランブルされており、方法は、第１メモリ内の予め定められた位置からファームウェアの一部を読み込んだ場合に、ファームウェアの一部をデスクランブルする段階をさらに備える。いくつかの実施態様において、デスクランブルする段階は、Ａｄｖａｎｃｅｄ　Ｅｎｃ

ｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＡＥＳ）プロセス、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＤＥＳ）プロセス、および共有鍵プロセスの少なくとも１つに従って実行される。

【００１２】

概して、一側面において、この発明は、プロセッサ、試験インタフェース、プロセッサ用のファームウェアを記憶する第１メモリ、および、プロセッサ用のブートコードを記憶する第２メモリを有する装置をオペレートするためのプロセッサ上で実行可能なコンピュータプログラムであって、ブートコードに従って、プロセッサがブートした場合に第１メモリ内の予め定められた位置からファームウェアの一部を読み込むための命令と、ファームウェアの一部が予め定められた値を有するか否かを決定するための命令と、ファームウェアの一部が予め定められた値を有する場合にだけ、試験インタフェースをイネーブルするための命令とを備え、試験インタフェースは、イネーブルされている場合にだけプロセッサと通信するコンピュータプログラム、を特徴とする。いくつかの実施態様において、装置は、レジスタ、および、予め定められた値を記憶する第３メモリを有しており、コンピュータプログラムは、ブートコードに従って、ファームウェアの一部をレジスタに書き込むための命令と、レジスタと第３メモリとの間の比較に基づいて、試験インタフェースをイネーブルするための命令とを備える。いくつかの実施態様において、装置は、レジスタおよび第３メモリを有する特定用途向け回路をさらに有し、試験インタフェースは、イネーブルされている場合にだけ、特定用途向け回路と通信する。いくつかの実施態様において、第１メモリ内の予め定められた位置に記憶されたファームウェアの一部はスクランブルされており、コンピュータプログラムは、第１メモリ内の予め定められた位置からファームウェアの一部を読み込んだ場合に、ファームウェアの一部をデスクランブルするための命令をさらに備える。いくつかの実施態様において、デスクランブルは、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＡＥＳ）プロセス、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ （ＤＥＳ）プロセス、および共有鍵プロセスの少なくとも１つに従って実行される。

【００１３】

１以上の実施の詳細が、添付の図および以下の説明に記載される。他の特徴は、その説明および図から、そして請求項から明らかである。

【図面の簡単な説明】

【００１４】

【図１】従来技術のシステムオンアチップ（ＳｏＣ）を示す図である。

【図２】この発明のいくつかの実施形態において、プロセッサが認証コードをチェックするＳｏＣを示す図である。

【図３】この発明のいくつかの実施形態において、図３のＳｏＣのためのプロセスを示す図である。

【図４】この発明のいくつかの実施形態において、特定用途向け回路が認証コードをチェックするＳｏＣを示す図である。

【図５】この発明のいくつかの実施形態において、図５のＳｏＣのためのプロセスを示す図である。

【図６Ａ】この発明の様々な典型的な実装を示す図である。

【図６Ｂ】この発明の様々な典型的な実装を示す図である。

【図６Ｃ】この発明の様々な典型的な実装を示す図である。

【図６Ｄ】この発明の様々な典型的な実装を示す図である。

【図６Ｅ】この発明の様々な典型的な実装を示す図である。

【図６Ｆ】この発明の様々な典型的な実装を示す図である。

【図６Ｇ】この発明の様々な典型的な実装を示す図である。

【発明を実施するための形態】

【００１５】

本明細書で用いられる各参照番号の桁は、参照番号が最初に現れる図の番号を示す。

この発明の実施形態は、複数のシステムオンアチップ（ＳｏＣ）集積回路用の複数の試験インタフェースに対するセキュリティを提供する。ＳｏＣは、試験インタフェース、１つのプロセッサ、プロセッサ用のファームウェアを記憶する１つのファームウェアメモリ、および、プロセッサ用のブートコードを記憶する１つのリードオンリーメモリを有する。試験インタフェースは、試験インタフェースがイネーブルされている場合にだけプロセッサと通信する。試験インタフェースは、Ｊｏｉｎｔ Ｔｅｓｔ Ａｃｔｉｏｎ Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースとして実装されてよい。プロセッサがブートした場合に、ブートコードは、プロセッサに、ファームウェアメモリ内の予め定められた位置からファームウェアの一部を読み込ませる。試験インタフェースは、プロセッサに読み込まれたファームウェアの一部が予め定められた認証コードを含む場合にだけ、イネーブルされる。

【００１６】

この発明の実施形態に従って実装された複数のＳｏｃにおいて、認証コードは、ＳｏＣの開発フェーズの間においてファームウェアメモリ内に記憶されることができる。それにより、ＳｏＣの試験およびデバッグのために試験インタフェースがイネーブルにされる。その後、製造のためにファームウェアから認証コードが削除されることができ、それにより試験インタフェースがディセーブルされる。

【００１７】

いくつかの実施形態において、プロセッサは、ファームウェアの一部が認証コードを含むか否かを決定して、ファームウェアの一部が認証コードを含む場合に、試験インタフェースをイネーブルする。他の実施形態においては、ファームウェアの一部が認証コードを含むか否かを、特定用途向け回路が決定する。特定用途向け回路は、例えばデジタルビデオディスク（ＤＶＤ）プレーヤ／バーナなどをコントロールする、デバイスコントローラおよび類似のものであってよい。特定用途向け回路は、１つのレジスタ、認証コードを記憶する１つのメモリ、および１つのコンパレータを有する。ブートコードは、プロセッサに、ファームウェアの一部をレジスタに書き込ませる。コンパレータは、レジスタと更なるメモリとの間の比較に基づき、試験インタフェースをイネーブルする。

【００１８】

特定用途向け回路が認証コードをチェックする実施形態においては、ＳｏＣの製造者は認証コードを知る必要がなく、このため、製造するＳｏＣのための認証コードを保守しセキュアにする責務から解放される。これらの実施形態において、顧客（例えば、ＳｏＣを含む電子デバイスの製造者）は、認証コードを含んでいない複数のＳｏＣを購入することができ、その後、試験およびデバッグするために試験インタフェースをイネーブルすべく、認証コードを複数のＳｏＣに入力することができる。例えば、特定用途向け回路内のメモリは、１つのワンタイムプログラマブルメモリとして実装されてよい。顧客は、メモリに認証コードを焼き、認証コードをファームウェアに記録もする。顧客が複数のＳｏＣを出荷する場合に、顧客は認証コードをファームウェアから単に削除し、それにより試験インタフェースをディセーブルする。

【００１９】

いくつかの実施形態において、ファームウェアメモリに記憶されたファームウェアのいくつかまたは全てが、１つのスクランブリングプロセスに従ってスクランブルされる。これらの実施形態は、プロセッサがファームウェアメモリからファームウェアを読み込んだ場合に１つのデスクランブリングプロセスに従ってファームウェアをデスクランブルする、１つのデスクランブラを含む。スクランブリングおよびデスクランブリングプロセスは、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）プロセス、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＤＥＳ）プロセス、共有鍵プロセス、および類似のものを含むことができる。これらの実施形態において、アタッカが試験インタフェースを通じてどうにかしてＳｏＣにアクセスすることができたとしても、アタッカはファームウェアをデスクランブルするという問題にさらに直面するだろう。

【００２０】

図２は、この発明の実施形態において、ＳｏＣ２００内のプロセッサ２０２が認証コードをチェックするＳｏＣ２００を示す。ＳｏＣ２００は、プロセッサ２０２と、試験インタフェース２０４がイネーブルされている場合にだけプロセッサ２０２と通信する試験インタフェース２０４と、プロセッサ２０２用のファームウェア２０８を記憶するファームウェアメモリ２０６と、プロセッサ２０２用のブートコード２１２を記憶するリードオンリメモリ（ＲＯＭ）２１０とを有する。以下に詳細に説明されるように、試験インタフェース２０４がイネーブルされている場合に、試験インタフェース２０４は、プロセッサ２０２および特定用途向け回路２１６に接続され、また、ＳｏＣ２００内の他の複数の回路にも接続されてよい。試験インタフェース２０４は、Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースまたは類似のものとして実装されてよい。ファームウェアメモリ２０６は、不揮発性メモリまたは類似のものとして実装されてよい。

【００２１】

ＳｏＣ２００は概して、１つのランダムアクセスメモリ（ＲＡＭ）２１４および１つの特定用途向け回路２１６を有してもよい。例えば、ＳｏＣ２００がＤＶＤプレーヤのようなディスクプレーヤをコントロールすることを目的とする場合、特定用途向け回路２１６は１つのディスクコントローラおよび１つの読み込みチャネルを含むことができる。当然に、他の実装では、他の種類の複数の特定用途向け回路を含むことができる。

【００２２】

いくつかの実施形態において、例えば上述したように、ファームウェア２０８はスクランブルがかけられており、ＳｏＣ２００は、ファームウェア２０８がファームウェアメモリ２０６から読み込まれた場合にファームウェア２０８の全てまたは一部をデスクランブルする１つのデスクランブラ２１８を含む。説明される複数の実施形態においてＳｏＣ２００の複数の要素がある構成で表されるが、他の実施形態では他の構成をとることができることが、本明細書で提供された開示および教示に基づいて当業者に明らかであろう。例えば、ＳｏＣ２００の複数の要素は、ハードウェア、ソフトウェア、またはそれらのコンビネーションで実装することができる。

【００２３】

図３は、この発明の実施形態に係る、図３のＳｏＣ２００のプロセスを示す。説明される複数の実施形態においてプロセス３００の複数の要素がある構成で表されるが、他の実施形態では他の構成をとることができることが、本明細書で提供された開示および教示に基づいて当業者に明らかであろう。

【００２４】

関連技術分野でよく知られているように、例えばＳｏＣ２００への電力を切断して投入したり、プロセッサ２０２にリセット信号を加えたり、同様のことをすることで、プロセッサ２０２がブートされる（ステップ３０２）。ブートされたとき、プロセッサ２０２は、ＲＯＭ２１０に記憶されているブートコード２１２の実行を開始する（ステップ３０４）。ブートコード２１２は、プロセッサ２０２に、ファームウェアメモリ２０６内の予め定められた位置からファームウェア２０８の一部を読み込ませ（ステップ３０６）、ファームウェア２０８の一部が適正な認証コードを含むか否かを決定させる（ステップ３０８）。例えば、認証コードはＲＯＭ２１０に記憶されることができ、プロセッサ２０２は、その認証コードを、ファームウェアメモリ２０６内の予め定められた位置から読み込まれたファームウェア２０８の一部と比較する。

【００２５】

ファームウェア２０８が適正な認証コードを含む場合（ステップ３１０）には、プロセッサ２０２は、例えばイネーブル信号２２０をアサートすることにより、試験インタフェース２０４をイネーブルする（ステップ３１２）。そうでない場合には、プロセッサ２０２は、例えばイネーブル信号２２０を無効にすることにより、試験インタフェース２０４をディセーブルする（ステップ３１４）。イネーブルされた場合、試験インタフェース２０４は、試験デバイスのような外部デバイスと、プロセッサ２０２との間の通信、いくつかの実施形態では特定用途向け回路２１６のようなＳｏＣ２００内の他の複数の回路との

通信を、許可する。

【００２６】

図４は、この発明の実施形態に従って、ＳｏＣ４００内の特定用途向け回路４１６が認証コードをチェックするＳｏＣ４００を示す。ＳｏＣ４００は、プロセッサ４０２と、試験インタフェース４０４がイネーブルされている場合にだけプロセッサ４０２と通信する試験インタフェース４０４と、プロセッサ４０２用のファームウェア４０８を記憶するファームウェアメモリ４０６と、プロセッサ用のブートコード４１２を記憶するリードオンリメモリ（ＲＯＭ）４１０とを有する。試験インタフェース４０４は、以下に説明するように、試験インタフェース４０４がイネーブルされた場合に、プロセッサ４０２および特定用途向け回路４１６と接続されてよく、ＳｏＣ４００内の他の複数の回路とも接続されてよい。試験インタフェース４０４は、Ｊｏｉｎｔ　Ｔｅｓｔ　Ａｃｔｉｏｎ　Ｇｒｏｕｐ（ＪＴＡＧ）インタフェースまたは類似のものとして実装されてよい。ファームウェアメモリ４０６は、不揮発性メモリまたは類似のものとして実装されてよい。ＳｏＣ４００は概して、１つのランダムアクセスメモリ（ＲＡＭ）４１４を有してもよい。

【００２７】

ＳｏＣ４００は、特定用途向け回路４１６も有する。例えば、ＳｏＣ４００がＤＶＤプレーヤのようなディスクプレーヤをコントロールすることを目的とする場合、特定用途向け回路４１６は１つのディスクコントローラおよび１つの読み込みチャネルを含むことができる。当然に、他の実装では、他の種類の複数の特定用途向け回路を含むことができる。特定用途向け回路４１６は、レジスタ４２２、メモリ４２４、およびコンパレータ４２６を有する。メモリ４２４は、１つのワンタイムプログラマブルメモリとして実装されてよい。

【００２８】

いくつかの実施形態において、例えば上述したように、ファームウェア４０８はスクランブルがかけられており、ＳｏＣ４００は、ファームウェア４０８がファームウェアメモリ４０６から読み込まれた場合にファームウェア４０８の全てまたは一部をデスクランブルする１つのデスクランブラ４１８を含む。説明される複数の実施形態においてＳｏＣ４００の複数の要素がある構成で表されるが、他の実施形態では他の構成をとることができることが、本明細書で提供された開示および教示に基づいて当業者に明らかであろう。例えば、ＳｏＣ４００の複数の要素は、ハードウェア、ソフトウェア、またはそれらのコンビネーションで実装することができる。

【００２９】

図５は、この発明の実施形態において、図５のＳｏＣ４００のための処理を示す。説明される複数の実施形態においてＳｏＣ５００の複数の要素がある構成で表されるが、他の実施形態では他の構成をとることができることが、本明細書で提供された開示および教示に基づいて当業者に明らかであろう。

【００３０】

関連技術分野でよく知られているように、例えばＳｏＣ４００への電力を切断して投入したり、プロセッサ４０２にリセット信号を加えたり、同様のことをすることで、プロセッサ４０２がブートされる（ステップ５０２）。ブートされたとき、プロセッサ４０２は、ＲＯＭ４１０に記憶されているブートコード４１２の実行を開始する（ステップ５０４）。ブートコード４１２は、プロセッサ４０２に、ファームウェアメモリ４０６内の予め定められた位置からファームウェア４０８の一部を読み込ませ（ステップ５０６）、ファームウェア４０８のその一部を特定用途向け回路４１６内のレジスタ４２２に書き込ませる（ステップ５０８）。

【００３１】

これらの実施形態において、認証コードはメモリ４２４に記憶される。コンパレータ４２６は、レジスタ４２２とメモリ４２４との間の比較に基づき、試験インタフェース４０４をイネーブルする。具体的には、メモリ４２４が適正な認証コードを格納している場合（ステップ５１０）には、コンパレータ４２６は、例えばイネーブル信号４２０をアサー

トすることにより、試験インタフェース４０４をイネーブルする（ステップ５１２）。そうでない場合には、コンパレータ４２６は、例えばイネーブル信号４２０を無効にすることにより、試験インタフェース４０４をディセーブルする（ステップ５１４）。イネーブルされた場合、試験インタフェース４０４は、試験デバイスのような外部デバイスと、プロセッサ４０２との間の通信、いくつかの実施形態では特定用途向け回路４１６のようなＳｏＣ４００内の他の複数の回路との通信を、許可する。

【００３２】

図６Ａ－６Ｇは、この発明の様々な典型的な実装を示す図である。図６Ａを参照すると、この発明は、ハードディスクドライブ６０１に実装されることができる。この発明は、図６Ａにおいて６０２で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方を実装することができる。いくつかの実施態様において、ＨＤＤ６０１内のシグナルプロセッシングおよび／またはコントロール回路６０２および／または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、および／または、磁気記録媒体６０３に出力される、および／または磁気記録媒体６０３から受信されたデータのフォーマットを実行することができる。

【００３３】

ＨＤＤ６０１は、ホストデバイス（図示せず）（例えば、コンピュータ、携帯情報端末のようなモバイルコンピューティングデバイス、セルラフォン、メディアまたはＭＰ３プレーヤなど）、および／または他のデバイスと、１以上の有線または無線の通信リンク６０４を介して通信することができる。ＨＤＤ６０１は、メモリ６０５（例えば、ランダムアクセスメモリ（ＲＡＭ）、フラッシュメモリのような低レイテンシの不揮発性メモリ、リードオンリメモリ（ＲＯＭ）、および／または他の適切な電子データストレージ）に接続されることができる。

【００３４】

図６Ｂを参照すると、この発明は、デジタル多目的ディスク（ＤＶＤ）ドライブ６０６に実装されることができる。この発明は、図６Ｂにおいて６０７で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方、および／またはＤＶＤドライブ６０６の大容量データストレージを実装することができる。ＤＶＤ６０６内のシグナルプロセッシングおよび／またはコントロール回路６０７または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、および／または、光記録媒体６０８に出力される、および／または光記録媒体６０８から受信されたデータのフォーマットを実行することができる。いくつかの実施形態において、シグナルプロセッシングおよび／またはコントロール回路６０７、および／またはＤＶＤ６０６内の複数の回路（図示せず）は、エンコーディングおよび／またはデコーディングおよび／またはＤＶＤドライブに関連する他のいかなる信号処理機能のような他の機能を実行することができる。

【００３５】

ＤＶＤドライブ６０６は、出力デバイス（図示せず）（例えばコンピュータ、テレビジョンまたは他のデバイス）と、１以上の有線または無線の通信リンク６０９を介して通信することができる。ＤＶＤ６０６は、不揮発式でデータを記憶する大容量データストレージ６１０と通信することができる。大容量データストレージ６１０は、ハードディスクドライブ（ＨＤＤ）を含むことができる。ＨＤＤは、図６Ａで示された構成を有することができる。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。ＤＶＤ６０６は、メモリ６１１（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。

【００３６】

図６Ｃを参照すると、この発明は、高精細テレビジョン（ＨＤＴＶ）６１２に実装されることができる。この発明は、図６Ｃにおいて６１３で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方、ＨＤＴＶ６１２のＷＬ

ＡＮインタフェースおよび／または大容量データストレージを実装することができる。ＨＤＴＶ６１２は、有線または無線フォーマットでＨＤＴＶ入力信号を受け取って、ディスプレイ６１４用のＨＤＴＶ出力信号を生成する。いくつかの実施形態において、ＨＤＴＶ６１２のシグナルプロセッシング回路および／またはコントロール回路６１３、および／または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、データのフォーマット、および／または、要求される他のタイプのいかなるＨＤＴＶ処理を実行することができる。

【００３７】

ＨＤＴＶ６１２は、光および／または磁気記録媒体のように、不揮発式でデータを記憶する大容量データストレージ６１５と通信することができる。少なくとも１つのＨＤＤは図６Ａで示した構成を有してよく、少なくとも１つのＤＶＤは図６Ｂで示した構成を有してよい。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。ＨＤＴＶ６１２は、メモリ６１６（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。ＨＤＴＶ６１２は、ＷＬＡＮネットワークインタフェース６１７を通じたＷＬＡＮ接続をサポートすることもできる。

【００３８】

図６Ｄを参照すると、この発明は、ビークル６１８のコントロールシステム、ＷＬＡＮインタフェース、および／またはビークルコントロールシステムの大容量データストレージを実装する。いくつかの実施形態において、この発明は、パワートレインコントロールシステム６１９を実装する。パワートレインコントロールシステム６１９は、１以上のセンサ（例えば、温度センサ、圧力センサ、回転センサ、気流センサ、および／または他のいかなる適切なセンサ）から入力を受け取り、および／または、１以上の出力コントロール信号（例えば、エンジンオペレーティングパラメータ、トランスミッションオペレーティングパラメータ、および／または他のコントロール信号）を生成する。

【００３９】

この発明は、ビークル６１８の他のコントロールシステム６２２にもまた実装されてよい。コントロールシステム６２２は、同様に入力センサ６２３から信号を受け取ることができ、コントロール信号を１以上の出力デバイス６２４に出力できてよい。いくつかの実施形態において、コントロールシステム６２２は、アンチロックブレーキングシステム（ＡＢＳ）、ナビゲーションシステム、テレマチクスシステム、ビークルテレマチクスシステム、レーンデパーチャシステム、アダプティブクルーズコントロールシステム、ビークルエンターテイメントシステム（ステレオ、ＤＶＤ、コンパクトディスクなど）の一部であってよい。さらに他の実施形態が考えられる。

【００４０】

パワートレインコントロールシステム６１９は、不揮発式でデータを記憶する大容量データストレージ６２５と通信することができる。大容量データストレージ６２５は、光／磁気ストレージデバイス（例えばハードディスクドライブ（ＨＤＤ）および／またはＤＶＤドライブ）を含むことができる。少なくとも１つのＨＤＤは図６Ａで示された構成を有することができ、少なくとも１つのＤＶＤは図６Ｂで示された構成を有することができる。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。パワートレインコントロールシステム６１９は、メモリ６２６（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。パワートレインコントロールシステム６１９は、ＷＬＡＮネットワークインタフェース６２７を通じたＷＬＡＮ接続をサポートすることもできる。コントロールシステム６２２は、大容量データストレージ、メモリ、および／またはＷＬＡＮインタフェース（いずれも図示せず）を含むこともできる。

【００４１】

図６Ｅを参照すると、この発明は、セルラアンテナ６２９を含むセルラフォン６２８に

実装される。この発明は、図６Ｅにおいて６３０で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方、セルラフォン６２８のＷＬＡＮインタフェースおよび／または大容量データストレージを実装することができる。いくつかの実施態様において、セルラフォン６２８は、マイクロホン６３１、オーディオ出力６３２（例えばスピーカおよび／またはオーディオ出力ジャック）、ディスプレイ６３３および／または入力デバイス６３４（例えばキーパッド、ポインティングデバイス、ボイスアクチュエーション、および／または他の入力デバイス）を含むことができる。セルラフォン６２８内のシグナルプロセッシングおよび／またはコントロール回路６３０、および／または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、および／または、他のセルラフォン機能を実行することができる。

【００４２】

セルラフォン６２８は、光および／または磁気記録媒体（例えば、ハードディスクドライブ（ＨＤＤ）および／またはＤＶＤドライブ）のように、不揮発式でデータを記憶する大容量データストレージ６３５と通信することができる。少なくとも１つのＨＤＤは図６Ａで示した構成を有してよく、少なくとも１つのＤＶＤは図６Ｂで示した構成を有してよい。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。セルラフォン６２８は、メモリ６３６（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。セルラフォン６２８は、ＷＬＡＮネットワークインタフェース６３７を通じたＷＬＡＮ接続をサポートすることもできる。

【００４３】

図６Ｆを参照すると、この発明は、セットトップボックス６３８に実装されることができる。この発明は、図６Ｆにおいて６３９で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方、セットトップボックス６３８のＷＬＡＮインタフェースおよび／または大容量データストレージを実装することができる。セットトップボックス６３８は、ブロードバンドソースのようなソースから信号を受け取って、テレビジョンおよび／またはモニタのようなディスプレイ６４０、および／または他のビデオおよび／またはオーディオ出力デバイスに適した、スタンダードおよび／またはハイデフィニション・オーディオ／ビデオ信号を出力する。セットトップボックス６３８のシグナルプロセッシングおよび／またはコントロール回路６３９および／または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、および／または、他のいかなるセットトップボックス機能を実行することができる。

【００４４】

セットトップボックス６３８は、不揮発式でデータを記憶する大容量データストレージ６４３と通信することができる。大容量データストレージ６４３は、光および／または磁気ストレージデバイス（例えば、ハードディスクドライブ（ＨＤＤ）および／またはＤＶＤドライブ）を含むことができる。少なくとも１つのＨＤＤは図６Ａで示した構成を有してよく、少なくとも１つのＤＶＤは図６Ｂで示した構成を有してよい。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。セットトップボックス６３８は、メモリ６４２（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。セットトップボックス６３８は、ＷＬＡＮネットワークインタフェース６４３を通じたＷＬＡＮ接続をサポートすることもできる。

【００４５】

図６Ｇを参照すると、この発明は、メディアプレーヤ６４４に実装されることができる。この発明は、図６Ｇにおいて６４５で一般に識別されるシグナルプロセッシングおよび／またはコントロール回路のいずれかまたは双方、メディアプレーヤ６４４のＷＬＡＮインタフェースおよび／または大容量データストレージを実装することができる。いくつかの実施形態において、メディアプレーヤ６４４はディスプレイ６４６、および／または、キーパッド、タッチパッドなどのようなユーザ入力６４７を有してよい。いくつかの実施

形態において、メディアプレーヤ６４４は、メニュー、ドロップダウンメニュー、アイコン、および／またはディスプレイ６４６および／またはユーザ入力６４７を通じたポイントアンドクリックインタフェースを典型的に利用するグラフィカルユーザインタフェース（ＧＵＩ）を用いることができる。メディアプレーヤ６４４は、スピーカおよび／またはオーディオ出力ジャックのようなオーディオ出力６４８を有することができる。メディアプレーヤ６４４内のシグナルプロセッシングおよび／またはコントロール回路６４５および／または他の複数の回路（図示せず）は、データ処理、コーディングおよび／または暗号化、演算、および／または、他のいかなるメディアプレーヤ機能を実行することができる。

【００４６】

メディアプレーヤ６４４は、圧縮されたオーディオおよび／またはビデオコンテンツのようなデータを不揮発式で記憶する大容量データストレージ６４９と通信することができる。いくつかの実施形態において、圧縮されたオーディオファイルは、ＭＰＥＧフォーマットまたは他の適切な圧縮オーディオおよび／またはビデオフォーマットに準拠したファイルを含む。大容量データストレージは、光／磁気ストレージデバイス（例えばハードディスクドライブ（ＨＤＤ）および／またはＤＶＤドライブ）を含むことができる。少なくとも１つのＨＤＤは図６Ａで示された構成を有することができ、少なくとも１つのＤＶＤは図６Ｂで示された構成を有することができる。ＨＤＤは、およそ１．８インチより小さい径の１以上のプラッタを持つ小型ＨＤＤであってよい。メディアプレーヤ６４４は、メモリ６５０（例えば、ＲＡＭ、ＲＯＭ、フラッシュメモリのような低レイテンシの不揮発性メモリ、および／または他の適切な電子データストレージ）に接続されることができる。メディアプレーヤ６４４は、ＷＬＡＮネットワークインタフェース６５１を通じたＷＬＡＮ接続をサポートすることもできる。上記に説明した実施形態に加えて、さらに他の実施形態が考えられる。

【００４７】

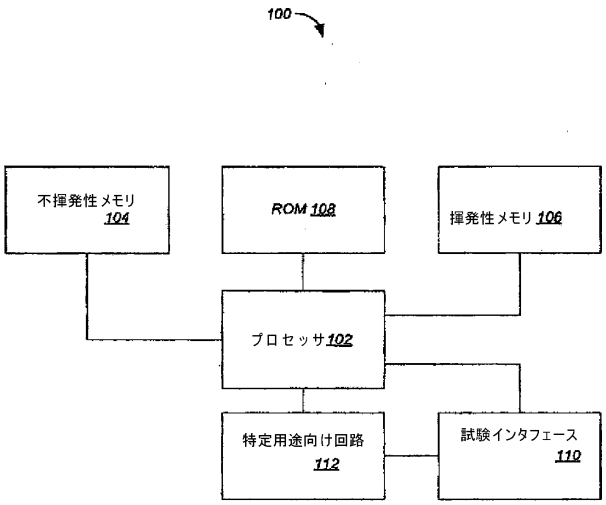
この発明の実施形態は、デジタル電子回路で、またはコンピュータハードウェア、ファームウェア、ソフトウェア、またはそれらのコンビネーションで実装することができる。この発明の装置は、プログラマブルプロセッサによる実行のための機械読み込み可能な記録媒体内に実体的に実現されたコンピュータプログラムプロダクト内に実装することができる。この発明の方法ステップは、この発明の機能を実行する命令のプログラムを実行しているプログラマブルプロセッサによって、入力データに対してオペレートし出力を生成することで実行されることができる。この発明は、プログラマブルシステム上で実行可能な、１以上のコンピュータプログラムに有利に実装されることができる。このプログラマブルシステムは、データおよび命令をデータストレージシステムから受け取り、データおよび命令をデータストレージシステムに送信する、データストレージシステムに結合された少なくとも１つのプログラマブルプロセッサ、少なくとも１つの入力デバイス、および、少なくとも１つの出力デバイスを有することができる。それぞれのコンピュータプログラムは、高レベル手続き型またはオブジェクト指向型のプログラミング言語、若しくは必要であればアッセンブラまたはマシン語で実装されることができる。いずれの場合でも、言語はコンパイル型またはインタープリタ型言語であってよい。適切なプロセッサは、一例として汎用および専用マイクロプロセッサの双方を含む。概してプロセッサは、リードオンリーメモリおよび／またはランダムアクセスメモリから命令およびデータを受け取るだろう。概してコンピュータは、データファイルを記憶する１以上の大容量ストレージデバイスを含むだろう。そのようなデバイスは、内部ハードディスクおよびリムーバブルディスクのような磁気ディスク、光磁気ディスク、および光ディスクを含むだろう。コンピュータプログラム命令およびデータを実体的に実現するのに適したストレージデバイスは、全ての形式の不揮発性メモリ（一例として、ＥＰＲＯＭ、ＥＥＰＲＯＭ、およびフラッシュメモリデバイスのような半導体メモリデバイスを含む）、内部ハードディスクおよびリムーバブルハードディスクのような磁気ディスク、光磁気ディスク、およびＣＤ－ＲＯＭディスクを含むことができる。上記はいずれもＡＳＩＣ（特定用途向け集積回路）によ

り補完されるかＡＳＩＣに組み込まれることができる。

【００４８】

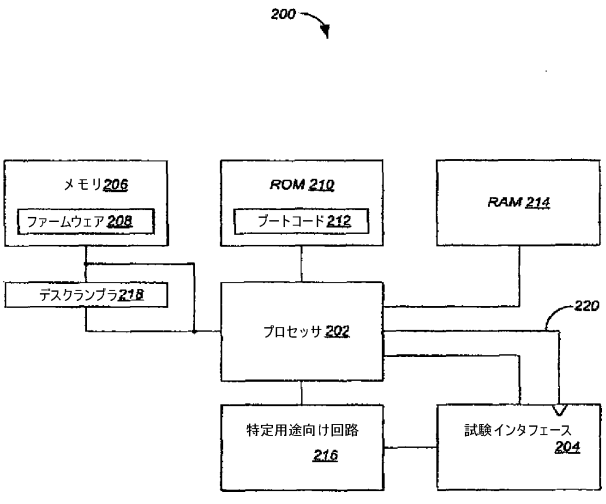
この発明の数々の実施形態が説明された。それにもかかわらず、この発明の要旨と範囲から逸脱することなく、さまざまな変更がなされ得ることが理解される。したがって、他の実施形態が、以下の請求項の範囲内にある。

【図１】

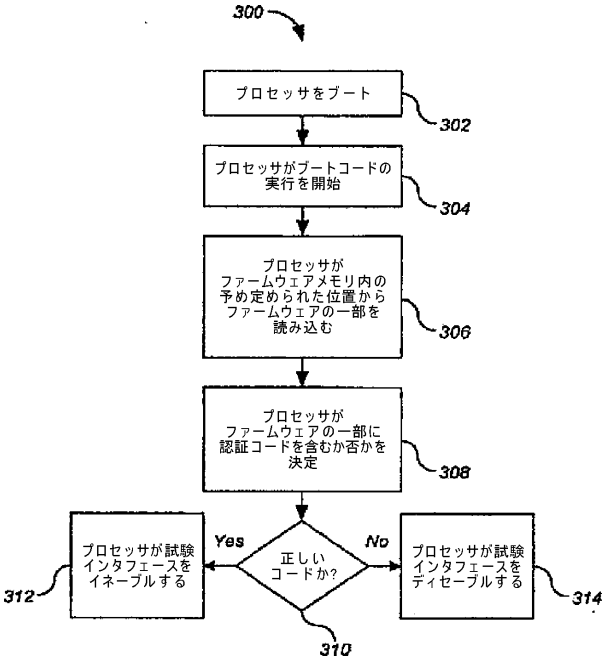


従来技術

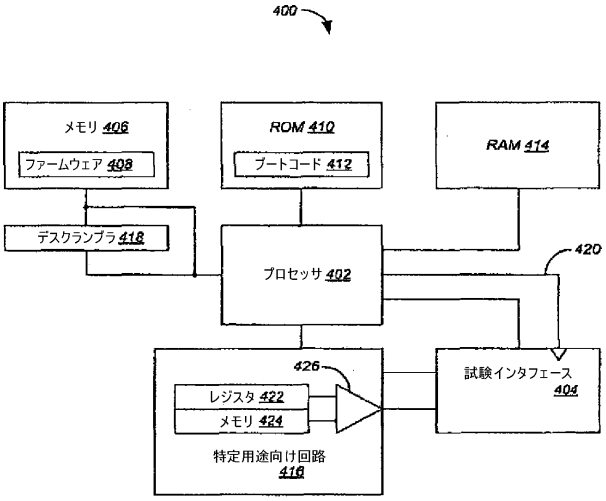
【図２】



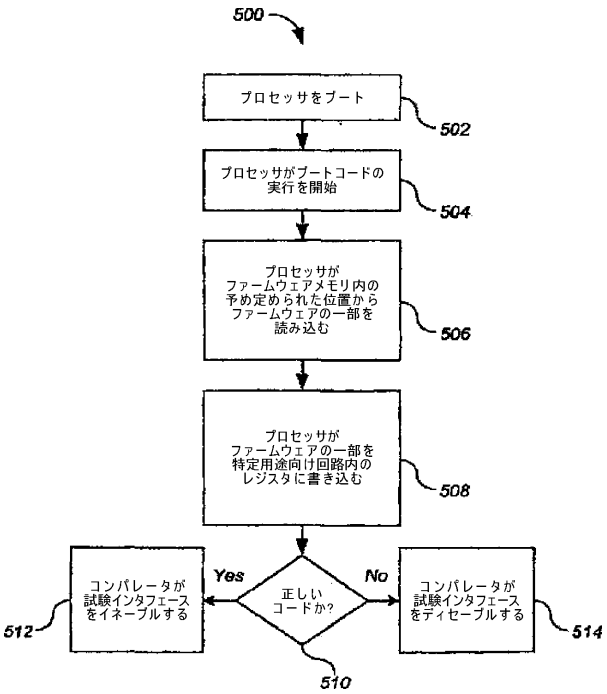
【図３】



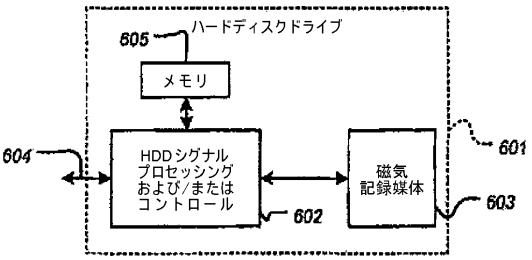
【図４】



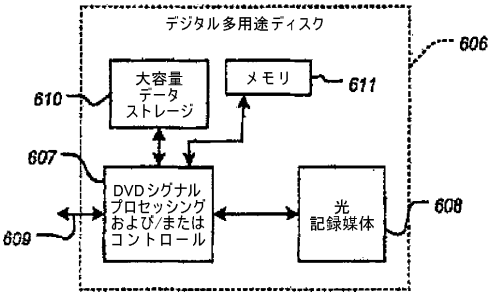
【図５】



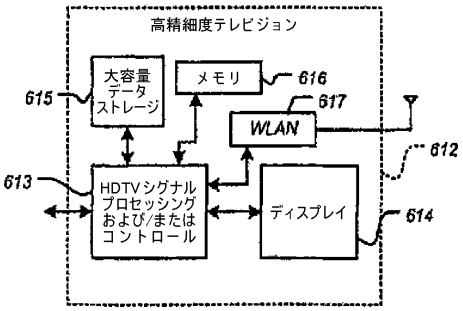
【図６Ａ】



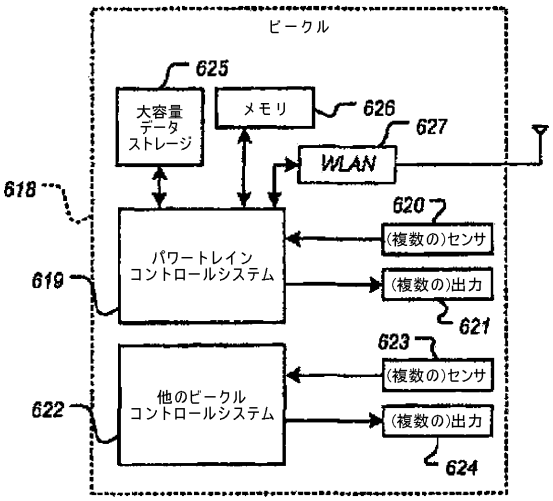
【図６Ｂ】



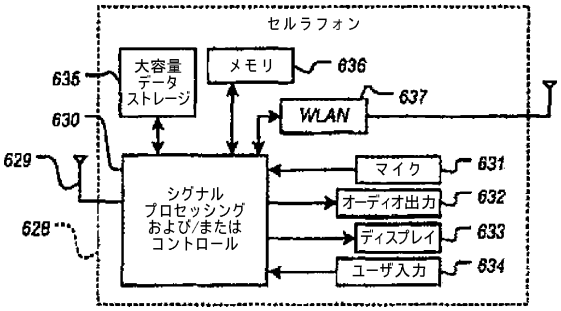
【図６Ｃ】



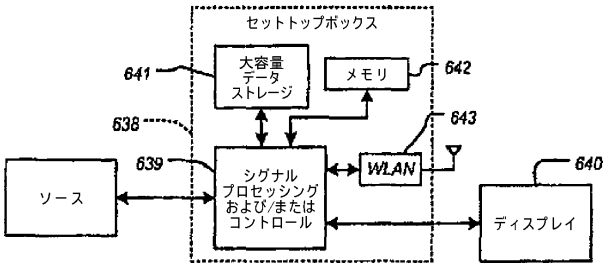
【図６Ｄ】



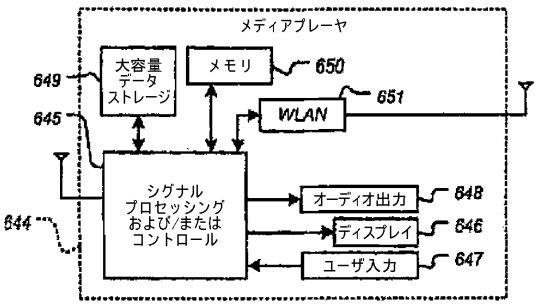
【図６Ｅ】



【図６Ｆ】



【図６Ｇ】



フロントページの続き

(31)優先権主張番号　11/654,841
(32)優先日　平成19年1月18日(2007.1.18)
(33)優先権主張国　米国(US)

(74)代理人　100112520
弁理士　林　茂則
(74)代理人　100156591
弁理士　高田　学
(72)発明者　フェン、ウェイシ
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ、マーベル　レーン　５４８８
マーベル　セミコンダクター　インコーポレイテッド内

審査官　後藤　彰

(56)参考文献　特開２００６－１０７０４０（ＪＰ，Ａ）
特開２００６－　１１９８７（ＪＰ，Ａ）
特開２００２－３５８１３７（ＪＰ，Ａ）
特開２００２－３４１９５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/22
G06F　11/22