(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7159190号
(P7159190)

(45)発行日　令和4年10月24日(2022.10.24)

(24)登録日　令和4年10月14日(2022.10.14)

(51)国際特許分類

Ｇ０６Ｆ　21/70　(2013.01)		Ｇ０６Ｆ	21/70
Ｇ０６Ｆ　21/62　(2013.01)		Ｇ０６Ｆ	21/62

ＦＩ

請求項の数　10　（全16頁）

(21)出願番号　特願2019-552241(P2019-552241)
(86)(22)出願日　平成29年12月6日(2017.12.6)
(65)公表番号　特表2020-514927(P2020-514927A)
(43)公表日　令和2年5月21日(2020.5.21)
(86)国際出願番号　PCT/US2017/064824
(87)国際公開番号　WO2018/174971
(87)国際公開日　平成30年9月27日(2018.9.27)
審査請求日　令和2年12月4日(2020.12.4)
(31)優先権主張番号　15/466,484
(32)優先日　平成29年3月22日(2017.3.22)
(33)優先権主張国・地域又は機関
米国(US)
前置審査

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195弁理士法人深見特許事務所
(72)発明者　バレンティノ，ラルフ・ピィ
アメリカ合衆国、９４０６５　カリフォルニア州、レッドウッド・ショアーズ、オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７
(72)発明者　ヘック，ジェームズ・エイ
アメリカ合衆国、９４０６５　カリフォルニア州、レッドウッド・ショアーズ、
最終頁に続く

(54)【発明の名称】　システム特徴をセキュアに分離するためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

システムであって、

１つまたは複数のシステム特徴の組の各々に対する信号のための信号状態の組を格納する不揮発性メモリを備え、

前記システムは、

（ａ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができないロックダウン状態と、

（ｂ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができる非ロックダウン状態とに構成可能なハードウェアと、

前記信号状態に基づき前記システム特徴の組の機能を構成する、ハードウェアロジックとを備え、

前記ロックダウン状態と前記非ロックダウン状態との間の変化は、前記システムの物理的操作なしに引き起こされることができず、

前記システムの前記物理的操作は、（ａ）前記システム内に備えられたマザーボード上の２つのピンを接続するためにジャンパを追加すること、または（ｂ）前記ジャンパを除去して、前記システム内に備えられたマザーボード上の２つのピンを切断することを備える、システム。

【請求項２】

システムであって、

１つまたは複数のシステム特徴の組の各々に対する信号のための信号状態の組を格納する不揮発性メモリを備え、
前記システムは、
（ａ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができないロックダウン状態と、
（ｂ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができる非ロックダウン状態とに構成可能なハードウェアと、
前記信号状態に基づき前記システム特徴の組の機能を構成する、ハードウェアロジックとを備え、
前記ロックダウン状態と前記非ロックダウン状態との間の変化は、前記システム内に備えられた信頼されたエンティティを介する前記システムの遠隔操作を用いて引き起こされることができる、システム。
【請求項３】
前記ハードウェアロジックは、前記非ロックダウン状態の間に再プログラムされることができ、前記ハードウェアロジックは、前記ロックダウン状態の間に再プログラムされることができない、請求項１または２に記載のシステム。
【請求項４】
前記ハードウェアロジックは、前記ロックダウン状態または前記非ロックダウン状態のいずれの間にも再プログラムされることができないハード化されたロジックを備える、請求項１または２に記載のシステム。
【請求項５】
前記システムは、前記ハードウェアが前記非ロックダウン状態にあるときに前記不揮発性メモリ内に格納された前記信号状態の組を変更するための機能を含む前記ハードウェアロジックの外部のコントローラをさらに備え、前記コントローラは、前記ハードウェアが前記ロックダウン状態にあるときに前記不揮発性メモリ内に格納された前記信号状態の組を変更することができない、請求項１から請求項４のいずれか１項に記載のシステム。
【請求項６】
前記コントローラは、ベースボード管理コントローラ（ＢＭＣ）である、請求項５に記載のシステム。
【請求項７】
前記コントローラは、前記ハードウェアが前記ロックダウン状態にあるときに前記不揮発性メモリ内に格納された前記信号状態の組を読み込むための機能を含む、請求項５に記載のシステム。
【請求項８】
前記不揮発性メモリは、前記ハードウェアロジックのみを介してアクセス可能である、請求項１から請求項７のいずれか１項に記載のシステム。
【請求項９】
方法であって、
システムのハードウェアロジックが、前記システムの不揮発性メモリに、１つまたは複数のシステム特徴の組の各々に対する信号のための信号状態の組を格納するステップと、
前記システムの物理的操作に基づいて無効信号または有効信号を伝送する信号伝送手段が、前記システムのハードウェアを、（ａ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができないロックダウン状態と、（ｂ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができる非ロックダウン状態との１つに構成するステップと、
前記システムの前記ハードウェアロジックが、前記信号状態に基づき前記システム特徴の組の機能を構成するステップとを備え、
前記ロックダウン状態と前記非ロックダウン状態との間の変化は、前記システムの前記物理的操作なしに引き起こされることができず、
前記システムの前記物理的操作は、（ａ）前記システム内に備えられたマザーボード上

の２つのピンを接続するためにジャンパを追加すること、または（ｂ）前記ジャンパを除去して、前記システム内に備えられたマザーボード上の２つのピンを切断することを備える、方法。

【請求項１０】

方法であって、

システムのハードウェアロジックが、前記システムの不揮発性メモリに、１つまたは複数のシステム特徴の組の各々に対する信号のための信号状態の組を格納するステップと、

前記システム内に備えられた信頼されたエンティティが、前記システムのハードウェアを、（ａ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができないロックダウン状態と、（ｂ）前記不揮発性メモリ内に格納された前記信号状態の組が変更されることができる非ロックダウン状態との１つに構成するステップと、

前記システムの前記ハードウェアロジックが、前記信号状態に基づき前記システム特徴の組の機能を構成するステップとを備え、

前記ロックダウン状態と前記非ロックダウン状態との間の変化は、前記システム内に備えられた前記信頼されたエンティティを介する前記システムの遠隔操作を用いて引き起こされることができる、方法。

【発明の詳細な説明】

【技術分野】

【０００１】

技術分野

本発明は、コンピュータセキュリティに関する。特に、本発明は、１つまたは複数のシステム特徴の選択的分離に関する。

【０００２】

優先権

この出願は、２０１７年３月２２日に出願された米国仮出願第１５／４６６，４８４号の利益と優先権を主張し、その全体は、参照によりここに組み込まれる。

【背景技術】

【０００３】

背景

コンピューティングシステムは、多くのコンポーネントおよび特徴を含む。コンポーネントは、ユニバーサルシリアルバス（ＵＳＢ）といったインターフェース、不揮発性メモリといったハードウェア、およびリモートサーバ管理のために使用される管理コントローラといった統合されたデバイスを含む。特徴は、コンポーネントがターンオンにされもしくはターンオフにされているかどうか、コンポーネントがリセット状態に保持されているか、またはコンポーネントがクロックにアクセスし得るかといった、コンポーネントの一部または状態を含む。

【０００４】

これらのコンポーネントおよび特徴の各々は、潜在的な攻撃のベクトルとして参照され得、ここから無許可のエンティティがシステムにリモートに侵入し、システムを変更し得る。いくつかのこれらのコンポーネントは、あるユーザに対して非常に望ましくあり得、別のユーザによってセキュリティの懸念のために明確に禁止される。たとえば、あるユーザは、ＵＳＢインターフェースを必要とし得、一方、別のユーザは、セキュリティの理由のために彼女のシステム上にＵＳＢインターフェースを有することができない。

【０００５】

ソフトウェアベースの解決策は、周辺インターフェースに対してソフトウェアをアンロードすることまたは無効化することを含む。たとえば、ネットワークスタックまたはドライバは、アンロードされまたは無効にされ得る。しかし、ソフトウェア変更は、無許可の者によって、リモートにまたはシステム上の隠しソフトウェアの実行を通して覆され得る。暗号化、パスワード、およびドライバ認証といった適用された保護のレイヤにも関わらず、ソフトウェアベースの解決策は、リモートに覆されやすい。せいぜい、ソフトウェア

変更は、システムの侵入に成功するのをより困難にし、時間がかかるようにする。
【０００６】
このセクションにおいて記載されたアプローチは、特許請求可能なアプローチであり、既知のまたは特許請求されたアプローチとはかぎらない。したがって、特に明記しない限り、このセクションに記載されたアプローチのいずれかが、単にこのセクションに含まれているという理由だけで、先行技術として認められると想定されるべきではない。
【０００７】
図面の簡単な説明
実施形態は、添付の図面の図において限定ではなく例として示される。本開示における「ある」または「１つ」の実施形態への言及は、必ずしも同じ実施形態への言及ではなく、少なくとも一つを意味することに留意されたい。
【図面の簡単な説明】
【０００８】
【図１Ａ】１つまたは複数の実施形態に従う、ロックダウン状態にあるシステムを示す。
【図１Ｂ】１つまたは複数の実施形態に従う、非ロックダウン状態にあるシステムを示す。
【図２】１つまたは複数の実施形態に従う、信号状態の組を変更するための例示的動作の組を示す。
【図３】１つまたは複数の実施形態に従うシステムのブロック図を示す。
【発明を実施するための形態】
【０００９】
詳細な説明
以下の説明では、説明の目的で、完全な理解を提供するために多くの特定の詳細が述べられる。１つまたは複数の実施形態は、これらの特定の詳細なしで、実施されることができる。１つの実施形態で説明される特徴は、異なる実施形態で説明される特徴と組み合わせることができる。いくつかの例では、本発明を不必要に不明瞭にすることを避けるために、ブロック図形式を参照して既知の構造およびデバイスを説明する。
【００１０】
１．　一般概要
２．　ロックダウン構成にあるシステム
３．　非ロックダウン構成にあるシステム
４．　システム特徴の分離
５．　リモート再構成
６．　その他、拡張
７．　ハードウェア概要
【００１１】
１．一般概要
１つまたは複数の実施形態は、システム特徴を選択的におよびセキュアに分離することを含む。システムは、１つまたは複数の特徴を含む。１つまたは複数のこれらの特徴は、無効状態にあり得、または有効状態にあり得る。システムは、ロックダウン状態へと構成されることができ、その状態では特定のシステム特徴の無効にされた状態または有効にされた状態は、変えられることができない。
【００１２】
実施形態では、システムは、不揮発性メモリを含み、これは、システム特徴の各々に対する信号状態を備える信号状態の組を格納する。ロックダウン状態では、信号状態の組は、変更されることができない。システムはまた、非ロックダウン状態に構成されることができ、その状態では信号状態の組は、変更されることができる。ハードウェアロジックは、信号状態に基づきシステム特徴の機能を構成する。
【００１３】
本明細書に記載されおよび／または特許請求の範囲に記載される１つまたは複数の実施形態は、この一般概要セクションに含まれていない場合がある。

【００１４】
２．ロックダウン構成におけるシステム
図１Ａは、１つまたは複数の実施形態に従う、ロックダウン構成におけるシステムを示す。プログラマブルハードウェアロジック１１０は、不揮発性ストレージ１１６内に格納された信号状態１１８に基づき機能を実装する。システムはさらに、プログラミングインターフェース１０２、ロックダウンジャンパ１０４、ベースボード管理コントローラ（ＢＭＣ）１１２、および特徴１２０ａ－１２０ｎを含む。システムはさらに、マザーボード（図示されない）を含む。１つまたは複数の実施形態では、システムは、図１Ａ内に示されたコンポーネントよりも多いまたは少ないコンポーネントを含み得る。図１Ａ内に示されたコンポーネントは、互いにローカルにまたはリモートにあり得る。図１Ａ内に示されたコンポーネントは、ソフトウェアおよび／またはハードウェア内に実装され得る。各コンポーネントは、複数のアプリケーションおよび／またはマシンにわたって分散され得る。複数のコンポーネントは、１つのアプリケーションおよび／またはマシンへと組み合わされ得る。１つのコンポーネントに対して記載された動作は、代わりに別のコンポーネントによって行われ得る。
【００１５】
１つまたは複数の実施形態では、特徴（たとえば、特徴１２０ａ－１２０ｎ）は、デバイス、デバイスの一部、または２つ以上のデバイスの組み合わせを参照する。例示的デバイスは、ネットワークスタック、ドライバ、管理コントローラ、および拡張スロットを含む。デバイスの特徴は、デバイスへの電力、デバイスがリセット状態にあるかどうか、デバイスのクロック、およびデバイスの入力または出力を含む。
【００１６】
１つまたは複数の実施形態では、プログラマブルハードウェアロジック１１０は、集積回路（ＩＣ）に対応する。プログラマブルハードウェアロジックは、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、コンプレックスプログラマブルロジックデバイス（ＣＰＬＤ）、または任意の他の種類のプログラマブルロジックデバイス（ＰＬＤ）であり得る。
【００１７】
プログラマブルハードウェアロジック１１０は、特徴１２０ａ－１２０ｎ、プログラミングインターフェース１０２、バッファ１２２、データインターフェース１１４、および不揮発性ストレージ１１６に直接接続を介してまたはネットワークを介して通信可能に結合され得る。さらに、プログラマブルハードウェアロジック１１０は、ＢＭＣ１１２、不揮発性ストレージ１１６、および特徴１２０ａ－１２０ｎと同じコンピューティングシステム上に実装され得またはその上で実行し得る。代替的にまたは追加的に、プログラマブルハードウェアロジック１１０は、ＢＭＣ１１２、不揮発性ストレージ１１６、および特徴１２０ａ－１２０ｎとは別個のコンピューティングシステム上に実装されまたはその上で実行し得る。プログラマブルリードオンリーメモリ（ＰＲＯＭ）はまた、プログラマブルハードウェアロジックの機能を行い得る。
【００１８】
別の実施形態では、プログラム不可のハードウェアロジックは、プログラマブルハードウェアロジックの代わりに使用され得る。ハードウェアロジックは、ハード化されたロジックを含み得る。ハード化されたロジックは、システムがロックダウン状態または非ロックダウン状態にあるかどうかに関わらず、再プログラムされることができない。
【００１９】
実施形態では、プログラマブルハードウェアロジック１１０は、特徴１２０ａ－１２０ｎを制御するための機能を含む。プログラマブルハードウェアロジックは、特徴に、その特徴を有効または無効にする信号を伝送するための機能を含み得る。プログラマブルハードウェアロジックは、０（すなわち、ロー、または真ではない）または１（すなわち、ハイ、または真）を論理的に特定し得る。プログラマブルハードウェアロジックは、０または１を有効または無効信号にマップするための機能を含み得る。プログラマブルハードウ

ェアロジックの構成は、少なくとも部分的に、不揮発性ストレージ１１６内に格納された信号状態１１８によって規定され得る。プログラマブルハードウェアロジックは、信号状態１１８と特徴１２０ａ－１２０ｎのそれぞれの特徴の有効性との間のマッピングを格納し得る。追加的に、プログラマブルハードウェアロジックは、不揮発性ストレージ内の信号状態を変更するための機能を含み得る。

【００２０】

図１Ａでは、図１Ａ内の特徴１２０ａ－１２０ｎを指し示す矢印で示されるように、特徴１２０ａ－１２０ｎは無効にされる。特徴は、プログラマブルハードウェアロジックから受信された特定の信号に応じて無効にされる。たとえば、特徴は、ハードドライブの電源であり得る。プログラマブルハードウェアロジックは、ハードドライブへの電力を無効にするための信号を伝送し得る。ハードドライブへの電力およびハードドライブそれ自体は、動作不能にレンダリングされる。特徴は、ロックダウンモードなどで必ずしもすべて無効にされることを要さない。各デバイスは、所望のセキュリティモデルに依存して選択的に無効または有効にされ得る。たとえば、特徴ａおよび特徴ｂは、有効にされ得、特徴ｎは、無効にされ得る。別の例として、すべての特徴は、有効にされ得る。

【００２１】

実施形態では、プログラミングインターフェース１０２は、プログラマブルハードウェアロジック１１０を構成するための命令を伝送するように構成されるハードウェアおよび／またはソフトウェアを含む。プログラミングインターフェースは、プログラマブルハードウェアロジックに命令を伝送し、プログラマブルハードウェアロジックのハードウェアロジックを変更するための機能を含み得る。プログラミングインターフェースは、任意の種類のインターフェースであり得、限定しない一例として、シリアルバス（Ｊｏｉｎｔ Ｔｅｓｔ Ａｃｔｉｏｎ Ｇｒｏｕｐ（ＪＴＡＧ）バスなど）、パラレルインターフェイス、または汎用入出力（ＧＰＩＯ）である。

【００２２】

プログラミングインターフェースは、プログラムマブルハードウェアロジックを構成するための命令を含むコードを含むプロセッシングユニットに接続され得る。追加的にまたは代替的に、プログラミングインターフェースは、ユーザ入力を受信するために通信可能に結合され得る。ユーザ入力は、たとえば、コードを受信するためのコマンドライン、またはアプリケーションプログラミングインターフェイス（ＡＰＩ）から受信され得る。

【００２３】

実施形態では、不揮発性ストレージ１１６は、信号状態の組を格納するための機能を含む。不揮発性ストレージは、スタティックランダムアクセスメモリであり、システムが電源オフのときに内容がそこに保存される。したがって、システムの電源がオンオフされても、不揮発性ストレージ内に格納された設定は、保たれる。不揮発性ストレージは、例えば、読み取り専用メモリ（ＲＯＭ）、プログラム可能な読み取り専用メモリ（ＰＲＯＭ）、フラッシュメモリ、ハードディスクドライブ、または磁気テープであり得る。不揮発性ストレージ１１６は、プログラマブルハードウェアロジック１１０のみに直接接続され、そうでなければシステムから分離される。不揮発性ストレージは、プログラムマブルハードウェアロジックによってのみ変更されることができる。

【００２４】

実施形態では、信号状態１１８は、不揮発性ストレージ１１６に格納される。信号状態は、所与の信号に対して可能な離散的な値である。信号状態は、有効／無効テーブルとして格納され得る。有効／無効テーブルは、特定の特徴を有効または無効にするかどうかを決定するために使用されるべき設定を格納する。信号状態は、たとえば、１（ハイ）または０（ロー）であり得る。プログラマブルハードウェアロジックは、信号状態を変更し得る。信号状態を保持する不揮発性ストレージがプログラマブルハードウェアロジックのみに結合され、そうでなければシステムから分離されるので、信号状態は、プログラマブルハードウェアロジックからの命令なしに変更されることができない。

【００２５】

実施形態では、ＢＭＣ１１２は、プログラマブルハードウェアロジック１１０を通して不揮発性ストレージ１１６をプログラムするための機能を含むコントローラである。ＢＭＣは、電力制御、故障検出、および送信アラートといった機能を行うことによってシステムを監視し管理するための機能を含む。ＢＭＣは、システム特徴内の故障を検出し得、その結果、信号状態を再プログラムしてその特徴を無効にする。ＢＭＣは、プログラマブルハードウェアロジック１１０にデータインターフェース１１４を介して結合される。ＢＭＣの代わりに、外部コントローラまたはホストは、不揮発性ストレージをプログラムするために使用され得る。

【００２６】

実施形態では、データインターフェース１１４は、ＢＭＣ１１２がプログラマブルハードウェアロジック１１０内のデータを変化させることを可能とする通信インターフェースである。データインターフェースは、命令をプログラマブルハードウェアロジックに伝送し、不揮発性ストレージ１１６内に格納された１つまたは複数の信号状態１１８を変更し得る。データインターフェースは、任意の種類のインターフェースであり得、限定しない一例として、シリアルバス（たとえば、インターインテグレーテッドサーキット（Ｉ２Ｃ））、パラレルインターフェイス、または汎用入出力（ＧＰＩＯ）通信インターフェースである。

【００２７】

実施形態では、ロックダウンジャンパ１０４は、マザーボード上の２つのピンを接続するために挿入され得る短い長さの導電体である。ロックダウンジャンパは、マザーボードに挿入されまたはそこから除去され得、回路を開閉する。図１Ａでは、ロックダウンジャンパが配置される。ロックダウンジャンパが挿入されるとき、システムは、ロックダウンモードにある。ロックダウンジャンパが配置された状態で、０（ロー）信号は、伝送される。代替的に、システムは、ロックダウンジャンパが配置されたときに１（ハイ）信号が伝送されるように構成され得る。ロックダウンジャンパが配置された状態でどちらの信号が送信されるように構成されようとも、その信号は、無効を意味するようにプログラムされる。無効信号は、システム上で実行する任意のソフトウェアによって変更されることができない。無効信号は、ロックダウンジャンパを物理的に除去することによってのみ変更されることができる。無効信号１０６、１２４は、ロックダウンジャンパが配置されたときに送信される。

【００２８】

無効信号１０６は、分離バッファ１０８を制御する。プログラミングインターフェース１０２は、プログラマブルハードウェアロジック１１０に分離バッファ１０８を通して接続する。無効信号は、プログラミングインターフェースがプログラマブルハードウェアロジックの内容を変更することを阻止する。無効１０６は、ロックダウンジャンパのみを通して制御されることが可能である。ロックダウンジャンパは、プログラミングインターフェースを物理的に中断して、プログラマブルハードウェアロジックを分離する。ロックダウンジャンパが配置されたときに、プログラミングインターフェースの電気的分離が存在する。

【００２９】

無効信号１０６は、ロックダウンジャンパからプログラミングインターフェース１０２へとバッファ１０８を介して伝送される信号である。無効信号１０６は、プログラミングインターフェースがプログラマブルハードウェアロジックと通信し、および／またはこれを構成することを無効にする。無効信号は、必要な電力および／または接続をアクティベート解除することによって通信を阻止し得る。ロックダウンジャンパが存在するとき、プログラミングインターフェースは、プログラマブルハードウェアロジックを変更することができない。

【００３０】

無効１２４は、ロックダウンジャンパからプログラマブルハードウェアロジック１１０へと、バッファ１２２を介して伝送される信号である。無効１２４は、プログラマブルハ

ードウェアロジック１１０の入力に、データインターフェース１１４に送信される。無効信号がアクティブであるとき、データインターフェースは、信号状態１１８を変更しないように論理的に分離される。無効１２４は、信号状態１１８へのアクセスを有するプログラマブルハードウェアロジック１１０の部分に送信される通信を遮断することによって、ＢＭＣが不揮発性ストレージを変更することを阻止する。結果として、不揮発性ストレージは、書き込み保護される。無効信号は、データインターフェースの書き込みのみを無効にし得、読み込みを無効にしない。この場合、ＢＭＣは、不揮発性ストレージ内に格納された値を依然として読み込むことができるが、その内部の任意の値を変更することができない。

【００３１】

バッファ１２２は、プログラマブルハードウェアロジック１１０からの逆駆動を阻止するための機能を含む１方向バッファである。バッファ１２２は、プログラマブルハードウェアロジックからの信号がロックダウンジャンパからの信号を変えることを阻止する。バッファ１２２は、データがプログラマブルハードウェアロジックに伝送されるときにデータを一時的に格納する機能をさらに含み得る。

【００３２】

別のバッファであるバッファ１２６は、プログラマブルハードウェアロジック１１０の内部に置かれる。バッファ１２６は、ロジックバッファとして機能する。バッファ１２６は、１方向バッファであり得、逆駆動を阻止する。バッファ１２６は、プログラマブルハードウェアロジックが無効信号を変更することを阻止するための機能を含む。バッファ１２６は、データがプログラマブルハードウェアロジックからおよび／またはそこへと伝送されるときに、データを一時的に格納するための機能をさらに含み得る。

【００３３】

３．非ロックダウン構成にあるシステム

図１Ｂは、１つまたは複数の実施形態に従う、非ロックダウン構成にあるシステムを示す。プログラミングインターフェース１０２と、ＢＭＣ１１２と、データインターフェース１１４と、バッファ１０８、１２２、１２６と、プログラマブルハードウェアロジック１１０と、不揮発性ストレージ１１６と、信号状態１１８と、特徴１２０ａ－１２０ｎとは、上述のセクション２において図１Ａを参照して説明されたが、以下に記述するように異なって実装されまたは異なって動作し得る。図１Ｂでは、システムは、非ロックダウン状態にある。ロックダウンジャンパは、非ロックダウン状態において挿入されない。図１Ｂ内に示されたコンポーネントは、互いにローカルにまたはリモートにあり得る。図１Ｂ内に示されたコンポーネントは、ソフトウェアおよび／またはハードウェア内に実装され得る。各コンポーネントは、複数のアプリケーションおよび／またはマシンにわたって分散され得る。複数のコンポーネントは、１つのアプリケーションおよび／またはマシンへと組み合わされ得る。１つのコンポーネントに対して記載された動作は、代わりに別のコンポーネントによって行われ得る。

【００３４】

ロックダウンジャンパが挿入されないとき、システムは、非ロックダウンモードにある。ロックダウンジャンパが無い状態で、システムは、１（ハイ）信号を伝送する。代替的に、システムは、ロックダウンジャンパが配置されていないときに０（ロー）信号を伝送し得る。いずれの場合にも、０または１それぞれは、有効信号に対応する。ロックダウンジャンパが配置されていない状態で、システムは、有効信号１３０、１３２を生成する。

【００３５】

有効信号１３０は、ロックダウンジャンパからプログラミングインターフェース１０２にバッファ１０８を介して伝送される信号である。有効信号１３０は、プログラミングインターフェースを有効にしてプログラマブルハードウェアロジックと通信し、および／またはこれを構成する。有効信号は、必要な電力および／または接続をアクティベートすることによって通信を可能とし得る。ロックダウンジャンパが無いときに、プログラミングインターフェースは、プログラマブルハードウェアロジックを変更することができる。

【００３６】
有効１３２は、ロックダウンジャンパからプログラマブルハードウェアロジック１１０へとバッファ１２２を介して伝送される信号である。有効信号１３２は、データインターフェース１１４が有効にされることを引き起こす。有効信号は、必要な電力および／または接続をアクティベートすることによってデータインターフェースを有効にし得る。ＢＭＣは、データインターフェース１１４を介して、プログラマブルハードウェアロジック１１０を介した不揮発性ストレージへの読み込みおよび書き込みの両方をし得る。ロックダウンジャンパが挿入されないとき、プログラマブルハードウェアロジックは、不揮発性ストレージ内の信号状態を変更することができる。
【００３７】
４．　システム特徴の分離
図２は、１つまたは複数の実施形態に従う、システム特徴を分離するための例示的動作の組を示す。図２において示された１つまたは複数の動作は、変形され、再配置され、またはすべて削除され得る。従って、図２に示される特定の動作シーケンスは、１つ以上の実施形態の範囲を限定するものとして解釈されるべきではない。
【００３８】
実施形態では、システムは、システム特徴の組に対する信号状態を格納する（動作２０２）。信号状態は、所与のデバイスに対応するビットを変更することによって不揮発性ストレージ内に格納され得る。プログラマブルハードウェアロジックは、ＢＭＣから命令を受信し、特定の信号状態を格納し得る。プログラマブルハードウェアロジックは、ＢＭＣからの命令を受信したことに応答して、プログラマブルハードウェアロジック内に格納された信号状態を変更し得る。
【００３９】
たとえば、ＢＭＣは、システムを攻撃から強化するために所与の特徴が無効にされるべきと決定し得る。ＢＭＣは、データインターフェースを介して、特徴を無効にするための命令を伝送し得る。要求に応答して、プログラマブルハードウェアロジックは、そのデバイスに対応するテーブルエントリ内に１または０の信号状態を格納するように不揮発性ストレージに命令する。
【００４０】
プログラマブルハードウェアロジックは、信号状態に基づきシステム特徴の機能を構成する。（動作２０４）。プログラマブルハードウェアロジックは、信号状態を、システム特徴を有効または無効にするための命令に変換するために、マッピングを使用し得る。ハードウェアロジックは、対応する命令をシステム特徴に伝送する。特徴が無効にされる場合、特徴は、システムの残りの部分から分断されおよび／または機能することを阻止される。特徴が有効にされた場合、特徴は、機能しおよび／またはシステムの残りの部分と通信し得る。
【００４１】
システムは、それがロックダウン構成にあるかまたは非ロックダウン構成にあるかで異なる振る舞いをし得る（２０６）。システムがロックダウン構成にあるかどうかは、ハードウェアロジックの問題であり、ロックダウンジャンパがマザーボードへと挿入されるかされないかによって決定される。代替的にまたは追加的に、システムは、セクション５において以下に説明するように、リモートでロックダウンまたは非ロックダウン構成へとされることができる。
【００４２】
システムがロックダウン構成にある場合、システムは、信号状態が変更されることを禁止する（動作２１０）。ロックダウン構成では、ロックダウンジャンパは、挿入され、このことは、無効信号を生成し、ハードウェアロックを実効的に作成する。無効信号は、プログラマブルハードウェアロジックへのプログラミングインターフェースを遮断する。ハードウェアロックは、プログラマブルハードウェアロジックの更新を阻止する。ソフトウェアは、信号状態を覆すことができない。無効信号はまた、ＢＭＣからプログラマブルハ

ードウェアロジックへのデータインターフェースを遮断する。データインターフェースを無効にすることは、ソフトウェアが不揮発性ストレージ内に格納された信号状態を変更することをプログラマブルハードウェアロジックが可能とするのを阻止する。無効信号は、プログラマブルハードウェアロジックがその内部ハードウェアロジックを変更するのをさらに禁止する。プログラマブルハードウェアロジック内のハードウェアロジックの再構成を阻止することは、プログラマブルハードウェアロジックが信号状態を直接的に変更することを阻止する。

【００４３】

システムがロックダウン構成にない場合（システムは非ロックダウン状態にある場合）、システムは、信号状態が変更されることを可能とする（動作２２０）。非ロックダウン構成では、ロックダウンジャンパは、挿入されず、このことは、有効信号がプログラマブルハードウェアロジックに伝送されることを引き起こす。この有効信号は、ソフトウェアが不揮発性ストレージ内に格納された信号状態を変更することを可能とするのを、プログラマブルハードウェアロジックに可能とする。有効信号はまた、プログラミングインターフェースに伝送される。この有効信号は、ソフトウェアがプログラマブルハードウェアロジックを変更することを可能とする。

【００４４】

たとえば、システムは、１つの特徴、たとえばドライバに対する信号状態を含む。不揮発性ストレージは、ドライバに対する１という信号状態を格納する。プログラマブルハードウェアロジックは、ドライバに対応するこの１という信号状態を取得する。プログラマブルハードウェアロジックは、取得された信号状態に応答して、１を有効信号にマップする。プログラマブルハードウェアロジックは、有効信号をドライバに伝送する。

【００４５】

ロックダウンジャンパは、挿入されない。システムは、非ロックダウン状態にある。この状態では、有効信号は、プログラマブルハードウェアロジックへのプログラミングインターフェースに伝送される。有効信号は、ハードウェアロジックを変更するためにソフトウェアを有効にする。たとえば、プログラミングインターフェースからの命令は、プログラマブルハードウェアロジックに直接的に命令し、ドライバを無効にするためにその内部ロジックを再構成する。

【００４６】

非ロックダウンモードでは、有効信号はまた、ＢＭＣへのデータインターフェースに伝送される。この有効信号は、プログラマブルハードウェアロジックにデータインターフェースを介して命令を送信することによって、不揮発性ストレージ内の信号状態を変更するためにＢＭＣを有効にする。

【００４７】

たとえば、ＢＭＣは、ドライバが攻撃を受けやすいと決定し得、その信号状態を０に設定する。プログラマブルハードウェアロジックがドライバのための信号状態を参照するとき、それは、信号状態が０であると分かる。プログラマブルハードウェアロジックは、無効信号をドライバに送信するためにそのハードウェアを再構成する。そして、ドライバは無効にされる。

【００４８】

ドライバが無効に維持されることを確実にするため、システムとの物理対話が必要とされる。管理者は、ロックダウンジャンパをシステムのマザーボード上の２つのピンの間に挿入する。ロックダウンジャンパの挿入は、システムをロックダウンモードにさせる。

【００４９】

ロックダウン状態では、システムは、無効信号をプログラマブルハードウェアロジックに伝送する。この無効信号は、プログラマブルハードウェアロジックの変更を阻止する。ソフトウェアは、プログラマブルハードウェアロジックに、そのハードウェアロジックを再構成してドライバを有効にするよう命令することができない。

【００５０】

システムは、プログラマブルハードウェアロジックへの無効信号をＢＭＣへのデータインターフェースにさらに伝送する。この無効信号は、ＢＭＣが不揮発性ストレージ内に格納された信号状態をプログラマブルハードウェアロジック１１０の機能を変えることによって調整することを阻止する。ＢＭＣは、プログラマブルハードウェアロジックにドライバのための信号状態を（ドライバを有効にする）１に変化させるよう命令することができない。不揮発性ストレージは、書き込み保護され、変更されることができない。

【００５１】

そして、どのソフトウェアもプログラマブルハードウェアロジックまたは不揮発性ストレージ内の信号状態を再構成することができない。ドライバは、ロックダウンジャンパが物理的に除去され、信号状態が再構成されない限り、無効に維持される。

【００５２】

５．リモート再構成

実施形態では、システムは、ロックダウン状態へとまたはそれからリモートに再構成されることができる。ロックダウンは、ジャンパを用いてアサートされる必要はない。この場合、ロックダウンは、システム内の信頼されたエンティティを使用してアサートされ、これは、システムのリモート管理を可能とする。

【００５３】

無許可のリモート再構成を阻止するために、システムは、信頼されたエンティティを含む。信頼されたエンティティは、たとえば、独自のプライベートインタフェースを有するアドインカードであり得る。信頼されたカードは、システムの残りの部分から分離され、信頼されたユーザまたはデバイスによってのみ制御下に維持される。信頼されたカードは、簡易なマイクロコントローラ上で動作し得、それが信頼された状態にあることを検証するのを容易にする。信頼されたエンティティは、システム内の信号をシステムのセキュリティモデルとは独立に操作する。たとえば、信頼されたエンティティは、有効または無効信号を操作することができ、または信頼されたエンティティは、システムへの電力を操作することができる。

【００５４】

信頼されたエンティティは、セキュアなジャンパの代わりにシステムロジックに接続される。信頼されたエンティティは、外部ソースからの命令を受信することができる。信頼されたエンティティはそして、有効または無効信号の伝送を上述のように制御し得る。

【００５５】

実施形態では、信頼されたエンティティは、リモートインタフェースに信頼されたリモート接続を介して通信可能に結合される。信頼されたリモート接続は、システムに接続された任意の他のインターフェースに対してプライベートである。信頼されたリモート接続は、シリアルインタフェース、および／またはプライベートネットワークのみに接続するネットワーク接続であり得る。リモートインタフェースを使用することによって、認可されたユーザは、ハードウェア構成をセキュアモードへとまたはそれから変え得る。

【００５６】

６．その他、拡張

実施形態は、ハードウェアプロセッサを含み、本明細書に記載および／または添付の特許請求の範囲のいずれかに列挙される動作のいずれかを実行するように構成される１つまたは複数のデバイスを有するシステムに向けられる。

【００５７】

実施形態では、非一時的なコンピュータ可読記憶媒体は、１つまたは複数のハードウェアプロセッサによって実行されると、本明細書に記載されたおよび／または請求項のいずれかに記載された動作を実行させる命令を含む。

【００５８】

本明細書で説明される特徴および機能の任意の組み合わせは、１つまたは複数の実施形態に従って使用され得る。上述の明細書において、実施形態は、実装ごとに異なり得る多数の特定の詳細を参照して説明されてきた。したがって、明細書および図面は、限定的な

意味ではなく、例示的な意味で考えられるべきである。本発明の範囲の唯一かつ排他的な指標および本出願人が本発明の範囲とすることを意図するものは、本出願から発行される特許請求の範囲の文言通りおよび均等の範囲であり、そのような特許請求の範囲は、特定の形式において後の訂正を含む。

【００５９】

７．ハードウェア概要

１つの実施形態に従って、ここで説明される技法は、１つまたは複数の特定用途のコンピューティングデバイスによって実装される。特定用途コンピューティングデバイスは、技法を実行するために有線であり得、または技法を実行するために永続的にプログラムされた１つまたは複数の特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、またはネットワーク処理ユニット（ＮＰＵ）といったデジタル電子デバイスを含み得、またはファームウェア、メモリ、他のストレージ、または組み合わせにおけるプログラム命令に従って技法を実行するようにプログラムされた１つまたは複数の汎用ハードウェアプロセッサを含み得る。そのような特定用途コンピューティングデバイスは、カスタム有線ロジック、ＡＳＩＣ、ＦＰＧＡ、またはＮＰＵをカスタムプログラミングと組み合わせて、技法を実現し得る。特定用途コンピューティングデバイスは、デスクトップコンピュータシステム、ポータブルコンピューターシステム、ハンドヘルドデバイス、ネットワークデバイス、または技法を実装するための有線および／またはプログラムロジックを組み込んだ任意の他のデバイスであり得る。

【００６０】

たとえば、図３は、本発明の実施形態がその上に実装され得るコンピュータシステム３００を示すブロックダイアグラムである。コンピュータシステム３００は、情報を通信するためのバス３０２または他の通信機構、および情報を処理するためにバス３０２と結合されたハードウェアプロセッサ３０４を含む。ハードウェアプロセッサ３０４は、たとえば、汎用マイクロプロセッサであり得る。コンピュータシステム３００はまた、プロセッサ３０４によって実行される情報および命令を格納するためにバス３０２に結合されたランダムアクセスメモリ（ＲＡＭ）または他の動的ストレージデバイスなどのメインメモリ３０６を含む。メインメモリ３０６はまた、プロセッサ３０４によって実行される命令の実行中に一時変数または他の中間情報を格納するために使用され得る。そのような命令は、プロセッサ３０４がアクセス可能な非一時的記憶媒体に格納されると、コンピュータシステム３００を、命令において特定された動作を実行するようにカスタマイズされた特定用途マシンにする。

【００６１】

コンピュータシステム３００は、プロセッサ３０４に対する静的情報および命令を格納するためにバス３０２に結合された読み出し専用メモリ（ＲＯＭ）３０８または他の静的ストレージデバイスをさらに含む。磁気ディスクまたは光ディスクなどの記憶装置３１０が提供され、情報および命令を格納するためにバス３０２に結合される。

【００６２】

コンピュータシステム３００は、情報をコンピュータユーザに表示するために、バス３０２を介して陰極線管（ＣＲＴ）などのディスプレイ３１２に結合され得る。英数字および他のキーを含む入力デバイス３１４は、情報およびコマンド選択をプロセッサ３０４に伝達するためにバス３０２に結合される。別の種類のユーザ入力デバイスは、方向情報およびコマンド選択をプロセッサ３０４に伝達し、ディスプレイ３１２上のカーソル移動を制御するためのマウス、トラックボール、またはカーソル方向キーなどのカーソル制御３１６である。この入力デバイスは典型的に、第１軸（ｘなど）および第２軸（ｙなど）の２つの軸において２つの自由度があり、デバイスが平面内の位置を特定可能にする。

【００６３】

コンピュータシステム３００は、カスタマイズされた有線ロジック、１つまたは複数のＡＳＩＣまたはＦＰＧＡ、ファームウェアおよび／またはプログラムロジックを使用して本明細書に記載の技法を実装し、これらはコンピュータシステムと組み合わせてコンピュ

ータシステム３００を特定用途マシンにするまたはプログラムする。一実施形態によれば、本明細書の技法は、プロセッサ３０４がメインメモリ３０６に含まれる１つまたは複数の命令の１つまたは複数のシーケンスを実行したことに応答して、コンピュータシステム３００によって実行される。そのような命令は、ストレージデバイス３１０などの別の記憶媒体からメインメモリ３０６に読み込まれ得る。メインメモリ３０６に含まれる命令のシーケンスの実行により、プロセッサ３０４は本明細書に記載の処理ステップを実行する。代替実施形態では、ソフトウェア命令の代わりに、またはそれと組み合わせて、有線回路を使用することができる。

【００６４】

本明細書で使用される「記憶媒体」という用語は、マシンを特定の方法で動作させるデータおよび／または命令を記憶する任意の非一時的媒体を指す。そのような記憶媒体は、不揮発性媒体および／または揮発性媒体を含み得る。不揮発性媒体は、たとえば、ストレージデバイス３１０などの光ディスクまたは磁気ディスクが含まれる。揮発性媒体は、メインメモリ３０６などの動的メモリを含む。記憶媒体の一般的な形態は、たとえば、フロッピー（登録商標）ディスク、フレキシブルディスク、ハードディスク、ソリッドステートドライブ、磁気テープ、または他の磁気データ記憶媒体、ＣＤ－ＲＯＭ、その他の光学データ記憶媒体、穴のパターンを備えた物理媒体、ＲＡＭ、ＰＲＯＭ、およびＥＰＲＯＭ、フラッシュＥＰＲＯＭ、ＮＶＲＡＭ、その他のメモリチップまたはカートリッジ、連想メモリ（ＣＡＭ）、およびＴｅｒｎａｒｙ　Ｃｏｎｔｅｎｔ－Ａｄｄｒｅｓｓａｂｌｅ　Ｍｅｍｏｒｙ（ＴＣＡＭ）を含む。

【００６５】

記憶媒体は、伝送媒体と別のものであるが、これと組み合わせて使用されることができる。伝送メディアは、記憶媒体間の情報の送信に関与する。たとえば、伝送媒体は、バス３０２を構成するワイヤを含む同軸ケーブル、銅線、光ファイバーを含む。伝送媒体は、電波および赤外線データ通信中に生成される音波などの音響波または光波の形態を取ることができる。

【００６６】

さまざまな形態の媒体が、実行のためにプロセッサ３０４に１つまたは複数の命令の１つまたは複数のシーケンスを運ぶことに関与し得る。たとえば、命令は、初期的にリモートディスクの磁気ディスクまたはソリッドステートドライブで実行されることができる。リモートコンピュータは、命令を動的メモリにロードし、モデムを使用して電話回線で命令を送信することができる。コンピュータシステム３００に対してローカルなモデムは、電話線でデータを受信し、赤外線送信機を使用してデータを赤外線信号に変換することができる。赤外線検出器は、赤外線信号で運ばれるデータを受信でき、適切な回路は、データをバス３０２に配置することができる。バス３０２は、データをメインメモリ３０６に運び、プロセッサ３０４は、そこから命令を取り出して実行する。メインメモリ３０６によって受信された命令は、プロセッサ３０４による実行の前または後のいずれかに、ストレージデバイス３１０に任意に格納され得る。

【００６７】

コンピュータシステム３００はまた、バス３０２に結合された通信インターフェース３１８を含む。通信インターフェース３１８は、ローカルネットワーク３２２に接続されたネットワークリンク３２０に結合する双方向データ通信を提供する。例えば、通信インターフェース３１８は、統合サービスデジタルネットワーク（ＩＳＤＮ）カード、ケーブルモデム、衛星モデム、または対応する種類の電話回線へのデータ通信接続を提供するモデムであり得る。別の例として、通信インターフェース３１８は、互換性のあるＬＡＮへのデータ通信接続を提供するローカルエリアネットワーク（ＬＡＮ）カードであり得る。無線はまた、実装され得る。そのような実装では、通信インターフェース３１８は、さまざまな種類の情報を表すデジタルデータストリームを運ぶ電気信号、電磁信号、または光信号を送受信する。

【００６８】

ネットワークリンク３２０は、典型的に、１つまたは複数のネットワークを介して他のデータデバイスへのデータ通信を提供する。たとえば、ネットワークリンク３２０は、ローカルネットワーク３２２を介してホストコンピューター３２４またはインターネットサービスプロバイダー（ＩＳＰ）３２６によって運営されるデータ機器への接続を提供することができる。ＩＳＰ３２６は、今日一般に「インターネット」３２８と呼ばれる世界規模のパケットデータ通信ネットワークを通じてデータ通信サービスを次いで提供する。ローカルネットワーク３２２およびインターネット３２８は両方とも、デジタルデータストリームを運ぶ電気信号、電磁信号または光信号を使用する。コンピュータシステム３００へとまたはそこへとデジタルデータを搬送する、さまざまなネットワークを介した信号、およびネットワークリンク３２０および通信インターフェース３１８を介した信号は、伝送媒体の例示的な形態である。

【００６９】

コンピュータシステム３００は、ネットワーク（複数可）、ネットワークリンク３２０、および通信インターフェース３１８を通じて、メッセージを送信し、プログラムコードを含むデータを受信することができる。インターネットの例では、サーバ３３０は、インターネット３２８、ＩＳＰ３２６、ローカルネットワーク３２２、および通信インターフェース３１８を介して、アプリケーションプログラムに要求されたコードを送信する。

【００７０】

受信されたコードは、プロセッサ３０４が受信されたときにそれによって実行され、および／または後で実行するためにストレージデバイス３１０または他の不揮発性ストレージに格納され得る。

【００７１】

上述の明細書では、本発明の実施形態は、実装ごとに異なり得る多数の特定の詳細を参照して説明されてきた。したがって、明細書と図面は、限定的な意味ではなく、例示的な意味で考えられるべきである。本発明の範囲の唯一かつ排他的な指標および本出願人が本発明の範囲とすることを意図するものは、本出願から発行される特許請求の範囲の文言通りおよび均等の範囲であり、そのような特許請求の範囲は、特定の形式において後の訂正を含む。

【図面】

【図１Ａ】

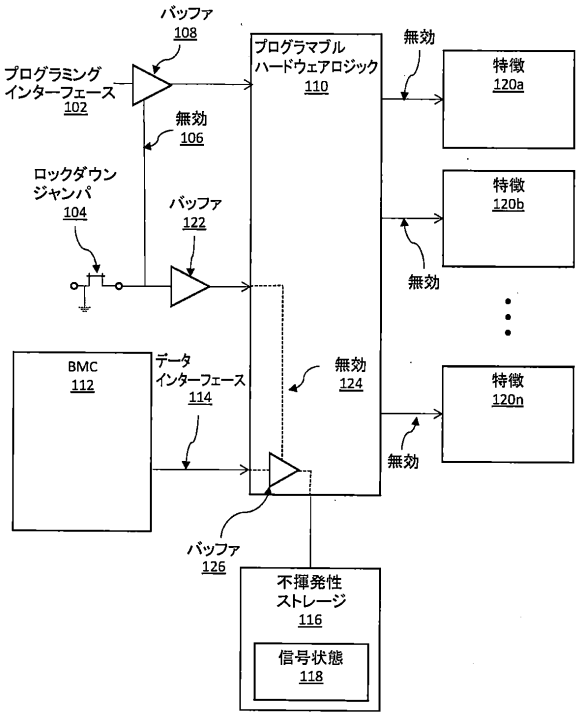


FIG. 1A

【図１Ｂ】

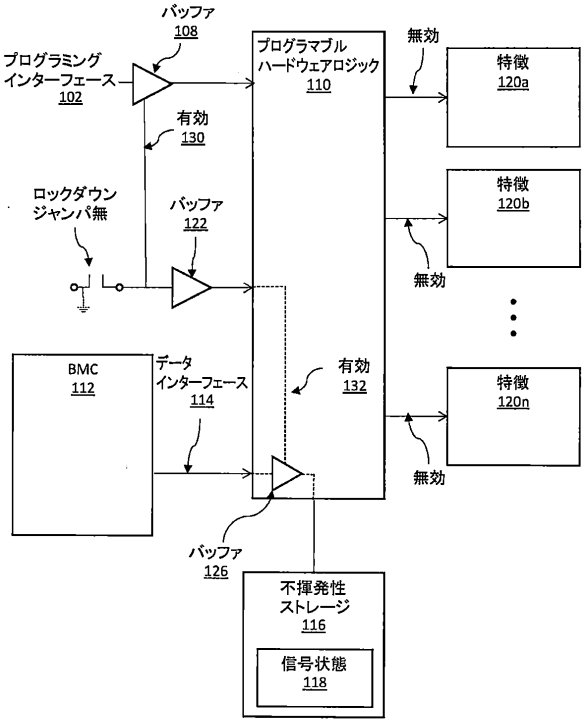


FIG. 1B

【図２】

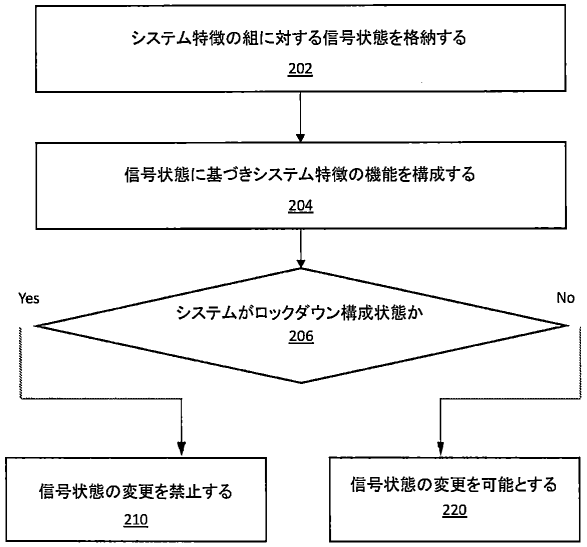
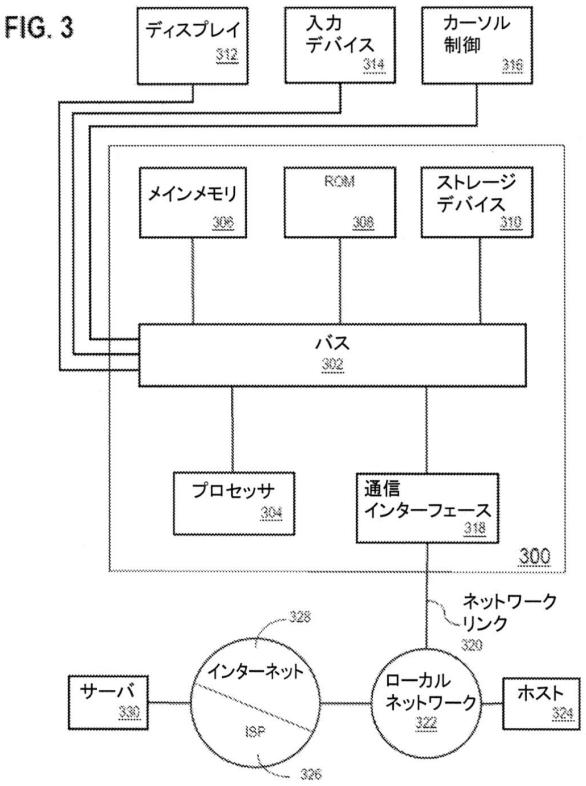


FIG. 2

【図３】



フロントページの続き

オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７
(72)発明者　ハートウェル，デイビッド・ダブリュ
アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・ショアーズ、オラクル・パークウェイ、５００、エム／エス・５・オゥ・ピィ・７

審査官　小林 秀和
(56)参考文献　特開２００８－３０５４０１（ＪＰ，Ａ）
特開２０００－２６７８４７（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／７０
Ｇ０６Ｆ　２１／６２