(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7200122号
(P7200122)

(45)発行日　令和5年1月6日(2023.1.6)

(24)登録日　令和4年12月23日(2022.12.23)

(51)国際特許分類
Ｇ０６Ｆ　21/57　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/57　３２０

請求項の数　12　（全17頁）

(21)出願番号　特願2019-552048(P2019-552048)
(86)(22)出願日　平成29年11月30日(2017.11.30)
(65)公表番号　特表2020-511727(P2020-511727A)
(43)公表日　令和2年4月16日(2020.4.16)
(86)国際出願番号　PCT/US2017/063915
(87)国際公開番号　WO2018/174969
(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7月15日(2020.7.15)
(31)優先権主張番号　15/466,514
(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)

(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　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、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　バレンティノ，ラルフ・ピィ
アメリカ合衆国、９４０６５ カリフォ
最終頁に続く

(54)【発明の名称】　信頼されたシステムファームウェア状態のリストアの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、
他の変更可能なコードを参照しない自己完結型のセキュアコードの組を備えるセキュアコードストアと、
オペレーションコードの組を備えるオペレーションコードストアと、
コントローラとを備え、前記コントローラは、
（ａ）前記システムが第１のハードウェア構成を有して構成されるときの前記セキュアコードの組の実行であって、前記セキュアコードの組の実行は、前記オペレーションコードストア内に格納された前記オペレーションコードの現在のバージョンを前記セキュアコードによって参照された前記オペレーションコードの置換バージョンで上書きすることを備え、前記コントローラと通信し、前記セキュアコードの前記実行のために必要ではない集積回路が、前記セキュアコードの組の実行の間、無効にされる、実行と、
（ｂ）前記システムが第２のハードウェア構成を有して構成されるときの前記オペレーションコードの組の実行であって、前記セキュアコードストアは、前記システムが前記第２のハードウェア構成を有して構成されるときに前記システムの１つまたは複数の他のコンポーネントから電気的に分離され、前記セキュアコードの組は、前記システムが前記第２のハードウェア構成を有して構成されるときにアクセスされることができない、実行とのうちの１つを、システム起動時に最初に実行するための機能を含み、
前記システムは、前記集積回路との通信を通してのみ機能する中央処理装置をさらに備え、

前記第１のハードウェア構成において前記集積回路が無効にされると、前記中央処理装置は無効にされる、システム。
【請求項２】
前記セキュアコードの組の前記実行は、
オペレーティングシステム、
ＢＩＯＳコードセット、
アプリケーション、
ＮＡＮＤフラッシュ、
不揮発性ストレージ、および、
プログラマブルロジックデバイス、のうちの１つまたは複数に対応するコードセットを削除することをさらに備える請求項１に記載のシステム。
【請求項３】
前記セキュアコードの組によって参照された前記オペレーションコードの前記置換バージョンは、前記セキュアコードストアの内部に格納される、請求項１または請求項２に記載のシステム。
【請求項４】
前記セキュアコードの組によって参照された前記オペレーションコードの前記置換バージョンは、前記セキュアコードストアの外部に格納される、請求項１または請求項２に記載のシステム。
【請求項５】
前記第１のハードウェア構成と前記第２のハードウェア構成との間の変更は、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の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、請求項５に記載のシステム。
【請求項７】
前記第１のハードウェア構成と前記第２のハードウェア構成との間の変更は、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、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８】
前記第２のハードウェア構成から前記第１のハードウェア構成への変更は、いずれのコードの実行によっても引き起こされることができない、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９】
前記集積回路は、フィールドプログラマブルゲートアレイを含む、請求項１から請求項８のいずれか１項に記載のシステム。
【請求項１０】
前記第１のハードウェア構成は、前記セキュアコードによって有効にされた前記システムの安全な回復に干渉する機能を含む１つまたは複数のデバイスを無効にする、請求項１から請求項８のいずれか１項に記載のシステム。
【請求項１１】
方法であって、
請求項１から請求項１０のいずれか１項に記載された前記コントローラの動作を備え、前記方法は、ハードウェアプロセッサを含む少なくとも１つのデバイスにおいて実行される、方法。
【請求項１２】
１つまたは複数のハードウェアプロセッサが実行すると請求項１から請求項１０のいず

れか１項に記載された前記コントローラの動作を実行させる命令を含む、プログラム。
【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、信頼されたシステムファームウェア状態をリストアすることに関する。
【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１５／４６６，５１４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
コンピュータシステムは典型的に、多くのコンポーネント、および多くのレイヤのソフトウェアを有する。コンピュータシステムのセキュリティは典型的に、レイヤ化されたアプローチを採用する。ベーシック入出力システム（ＢＩＯＳ）またはブートローダといったソフトウェアまたはファームウェアの第１の部分は、ソフトウェアの次の部分がロード等される前にそれを検証する。信頼のルートは、本質的に信頼され、他のコンポーネント内の信頼が確立されることができる基盤として機能するハードウェアまたはソフトウェアコンポーネントの組である。信頼のルートは、信頼のチェーンを確立するために使用される。一度システムの一部が信頼を失うと、信頼のチェーンは、破壊される。すべてのレベルのソフトウェアは疑わしく、新たな信頼のルートを再確立して構築することを困難にする。そのような信頼のチェーンの基礎にあるのは、典型的にファームウェアである。
【０００４】
ファームウェアは、制御、監視、および／またはデータ操作のために使用されるソフトウェアである。ファームウェアは、コンピューティングデバイスへとプログラムされ得る。ファームウェアは、不揮発性メモリデバイス内に格納され得る。ファームウェアは典型的に、デバイスの基本機能のみを含む。ファームウェアはしばしば、最も低いレベルのコードである。ファームウェアはしばしば、より高いレベルのソフトウェアにサービスを提供する。
【０００５】
従来、サーバは、ローカルのハードウェア上で動作され、信頼のチェーンは、比較的簡単に確立された。近年、サーバはますますクラウドモデルを使用し始めている。クラウドモデルでは、１つの企業は、物理サーバを別の企業からレンタルし得る。このサーバは、異なる顧客によって以前に使用されていた可能性がある。このことは、未知の履歴を有するサーバの状態において信頼を再確立するという新たな問題を生む。
【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】
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、通常オペレーションモード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、セキュアモード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、信頼されたシステムファームウェア状態のリストアの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．　通常オペレーションモードにあるシステム
３．　セキュアモードにあるシステム
４．　信頼されたシステムファームウェア状態のリストア
Ａ．　セキュアモードにないシステム
Ｂ．　セキュアモードにあるシステム
５．　サーバを信頼されたファームウェア状態にリストア
６．　リモート再構成
７．　その他、拡張
８．　ハードウェア概要
１．一般概要
１つまたは複数の実施形態は、信頼されたシステムファームウェア状態をリストアすることを含む。システムは、２つのコードストア内にコードを格納する。セキュアコードストア内に、システムは、自己完結型のセキュアコードの組を格納する。セキュアコードは、他の変更可能なコードを参照しない。オペレーションコードストア内に、システムは、オペレーションコードの組を格納する。
【００１１】
実施形態では、システムは、コントローラを含む。コントローラは、システムがセキュアモードにあるか通常オペレーションモードにあるかに依存してセキュアコードまたはオペレーションコードをシステム起動時に実行する。システムがセキュアモードにおいて構成されるときに、システムは、セキュアコードを実行する。セキュアモードでは、システムはまた、オペレーションコードストア内に格納されたオペレーションコードの現在のバージョンをセキュアコードによって参照されたオペレーションコードの置換バージョンで上書きする。
【００１２】
システムが通常オペレーションモードにおいて構成されるときに、システムは、オペレーションコードを実行する。通常オペレーションの間、セキュアコードストアは、システムの１つまたは複数の他のコンポーネントから電気的に分離される。セキュアコードは、システムが通常オペレーションモードにあるときにアクセスされることができない。
【００１３】
２．通常オペレーションモードにあるシステム
図１Ａは、１つまたは複数の実施形態に従う、通常オペレーションモードにあるシステムを示す。ベースボード管理コントローラ（ＢＭＣ）１１０は、システムを制御するためのコードを実行する。ブート選択機構１１６は、セキュアコードストア１２０、またはオペレーションコードストア１２２のいずれかに格納されたコードからＢＭＣをブートするかどうかを選択する。図１Ａに示されるように、システムは、不揮発性ストレージ１１２、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）１１４、バッファ１０４、および

ＣＰＵ並びに周辺電力制御１２４をさらに含む。１つまたは複数の実施形態では、システムは、図１Ａ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に示されたコンポーネントは、互いにローカルであり得またはリモートであり得る。図１Ａ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で実装され得る。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ることができる。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関して説明された動作は、代わりに別のコンポーネントによって実行され得る。

【００１４】

１つまたは複数の実施形態では、ＢＭＣ１１０は、システムを管理するコントローラである。ＢＭＣ上で実行するソフトウェアは、とりわけシステムの監視、システムの電源オンまたはオフ、およびオペレーティングシステムのインストールをすることができる。ＢＭＣは、システムが通常オペレーションモードにあるかセキュアモードにあるかを決定する能力を有するソフトウェアを含む。ＢＭＣは、チップセレクトゼロからのコードをフェッチするように構成され得る。チップセレクトゼロは、特定のコードストアを選択するＢＭＣ上の物理ピンである。ＢＭＣがこの例示的実施形態において使用されるが、当該分野で既知の任意の種類のコントローラは、同じ機能を行うために使用され得る。さらに、ＢＭＣ１１０は、不揮発性ストレージ１１２、ブート選択機構１１６、ＦＰＧＡ１１６、セキュアコードストア１２０、およびオペレーションコードストア１２２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、ＢＭＣ１１０は、不揮発性ストレージ１１２、ブート選択機構１１６、ＦＰＧＡ１１６、セキュアコードストア１２０、およびオペレーションコードストア１２２とは別個の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。ＢＭＣ１１０は、不揮発性ストレージまたはブート選択機構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る。

【００１５】

実施形態では、セキュアコードストア１２０は、セキュアコードが格納されたシステム内の位置である。セキュアコードストアは、たとえば、フラッシュメモリ、ハードドライブ上の物理位置、または仮想メモリアドレスであり得る。セキュアコードストア１２０は、複数の異なるストレージユニットおよび／またはデバイスを含み得る。複数の異なるストレージユニットおよび／またはデバイスは、同じ種類であってもまたは同じ物理サイトに配置されてもよくまたはそうでなくてもよい。通常オペレーションモードでは、セキュアコードストアは、ブート選択機構およびシステムの残りの部分から電気的に分離される（分離１１８）。セキュアコードストア内に格納されたセキュアコードは、通常オペレーションの間、変更されることができない。セキュアコードは、他の変更可能なコードを参照しない。セキュアコードストアは、オペレーションコードの置換バージョンをさらに格納する。

【００１６】

実施形態では、オペレーションコードストア１２２は、オペレーションコードが格納されたシステム内の位置である。オペレーションコードストアは、たとえば、フラッシュメモリ、ハードドライブ上の物理位置、または仮想メモリアドレスであり得る。オペレーションコードストア１２２は、複数の異なるストレージユニットおよび／またはデバイスを含み得る。複数の異なるストレージユニットおよび／またはデバイスは、同じ種類であってもまたは同じ物理サイトに配置されてもよくまたはそうでなくてもよい。オペレーションコードストアは、ブート選択機構１１６に結合される。オペレーションコードストアは、ブート選択機構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る。たとえば、オペレーションコードストアは、シリアルペリフェラルインタフェースバス（ＳＰＩ）によってブート選択機構に結合され得る。オペレーションコードストアは、システムがセキュアモードにあるかまたはオペレーションモードにあるかどうかに関わらずブート選択機構に結合される。オペレーションコードストア内に格納されたオペレーショ

ンコードは、通常オペレーションの間、システムを実行するために使用されるコードである。オペレーションコードは、システム上の最も低いレベルのコードであり得る。

【００１７】

実施形態では、ブート選択機構１１６は、ＢＭＣによって使用されるブートデバイスを制御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。ＢＭＣは、上述のようにチップセレクトゼロにマップされたアドレスからコードをフェッチするよう構成され得る。ブート選択機構は、ＢＭＣによってチップセレクトゼロにおいて何が見られるかを操作するための機能を含み得る。ブート選択機構は、システムがセキュアモードにあるかまたはオペレーションモードにあるかに依存して、セキュアコードストアまたはオペレーションコードストアのいずれかに対しチップセレクトゼロを指し示す。オペレーションモードでは、セキュアコードストアは、アクセス不可であり、そのためＢＭＣは、セキュアコードストアからブートすることもそこにアクセスすることもできない。オペレーションモードでは、ＢＭＣは、オペレーションコードストアまたはセキュアコードストアとは異なる別のストア（図示しない）からブートし得る。

【００１８】

実施形態では、バッファ１０４は、セキュアジャンパとＢＭＣとの間に結合された１方向バッファである。バッファは、逆駆動を阻止するための機能を含む。バッファが１方向であるという理由で、信号は、そのインタフェースに沿ってＢＭＣへとのみ伝送されることができ、そこから伝送されることはできない。バッファ１０４は、データがＢＭＣに伝送されるときに一時的にデータを格納するための機能をさらに含み得る。

【００１９】

実施形態では、不揮発性ストレージ１１２は、システムによって使用されるデータを格納する機能を含む。不揮発性ストレージは、不揮発性メモリであり、システムが電源オフのときにそこに内容が保存される。不揮発性ストレージは、たとえばリードオンリーメモリ（ＲＯＭ）、プログラマブルリードオンリーメモリ（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１１２は、複数の異なるストレージユニットおよび／またはデバイスを含み得る。複数の異なるストレージユニットおよび／またはデバイスは、同じ種類であってもまたは同じ物理サイトに配置されてもよくまたはそうでなくてもよい。不揮発性ストレージは、ＢＭＣに直接接続またはネットワークを介して通信可能に結合される。

【００２０】

実施形態では、ＦＰＧＡ１１４は、プログラマブルロジックブロックのアレイを備える集積回路である。ＦＰＧＡは、ＣＰＵ、周辺電力、アドインカード、およびネットワークといったコンポーネントの状態を制御するための機能を含む。たとえば、ＦＰＧＡは、デバイスへの電力を制御し得る。ＦＰＧＡは、ＣＰＵおよび周辺電力制御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る。

【００２１】

実施形態では、ＣＰＵおよび周辺電力制御１２４は、ＦＰＧＡに通信可能に結合される。ＣＰＵは、ソフトウェアを実行するためにシステムによって使用されるプロセッシングユニットである。ＣＰＵは、ソフトウェアに基づき命令を実行し得る。周辺電力制御は、ＣＰＵおよび／またはシステム全体への電力を制御し得る。

【００２２】

通常オペレーションモードでは、セキュアジャンパは、マザーボード上に設置されない。結果として、システム内に備えられるマザーボード上の２つのピンは、電気的に分離される。通常オペレーションでは、信号は、ＦＰＧＡ、ＢＭＣ（バッファ１０４を介して）、およびブート選択機構に送信される。

【００２３】

セキュアジャンパの無い通常オペレーションでは、システムは、ＦＰＧＡ有効信号１０６を生成する。ＦＰＧＡ有効信号は、ＦＰＧＡを有効にする。ＦＰＧＡ有効信号がアクティブであるとき、ＦＰＧＡは、動作可能である。ＦＰＧＡは、それ自体に内部変更を加え

得る。ＦＰＧＡは、命令をＣＰＵおよび周辺電力制御に伝送し得る。通常オペレーションモードでは、ＦＰＧＡは、たとえば、ＣＰＵへの電力を制御し得る。

【００２４】

セキュアジャンパ無しに、システムはまた、通常オペレーションモードがアクティブであるとＢＭＣが決定し得るようにＢＭＣへの信号を生成する。さらに、セキュア信号は、ブート選択機構１１６に伝送される。セキュア信号は、オペレーションコードストア１２２がＢＭＣのためのブートデバイスであるように、ブート選択機構のブート選択ロジックに影響を及ぼす。

【００２５】

通常オペレーションモードでは、セキュアコードストア１２０は、ブート選択機構、およびシステムの残りの部分から分離される（分離１１８）。セキュアコードストアは、ブート選択機構への接続を絶つことにより、またはセキュアコードストアへの電力を切断することにより、物理的に分離され得る。セキュアコードストアが分離されるときに、それは、システムの残りの部分によってアクセスされることができない。通常オペレーションモードでは、セキュアコードストアは、変更されることができない。

【００２６】

システムは、１つまたは複数のオペレーティングシステム、ＢＩＯＳコードセット、およびアプリケーション（図示されない）をさらに備え得る。

【００２７】

３．セキュアモードにあるシステム

図１Ｂは、１つまたは複数の実施形態に従う、セキュアモードにあるシステムを示す。ＢＭＣ１１０、バッファ１０４、不揮発性ストレージ１１２、ブート選択機構１１６、セキュアコードストア１２０、オペレーションコードストア１２２、ＦＰＧＡ１１４、およびＣＰＵおよび周辺電力制御１２４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、以下に記す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、セキュアジャンパ１０２が挿入された結果、セキュアな状態にある。１つまたは複数の実施形態では、システムは、図１Ｂにおいて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１Ｂに示されたコンポーネントは、互いにローカルであり得またはリモートであり得る。図１Ｂ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で実装され得る。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ることができる。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関して説明された動作は、代わりに別のコンポーネントによって実行され得る。

【００２８】

実施形態では、セキュアジャンパ１０２は、システムのマザーボード上の２つのピン間に配置されることができる物理的短絡デバイスである。セキュアジャンパは、１つの側で接地される。他の側で、セキュアジャンパは、ＢＭＣ１１０にバッファ１０４を介して結合される。セキュアジャンパが挿入されるとき、セキュアジャンパは、２つのピンを電気的に接続し、システムマザーボードの構成を変更させる。セキュアジャンパが配置されるとき、ＢＭＣに接続された回路は、セキュア信号を伝送するように構成される。

【００２９】

セキュアジャンパの配置は、ボード上のチップ選択ハードウェアロジックを変更させ、ＢＭＣのブートデバイスを、ブート選択機構１１６を介して変更する。セキュアジャンパは、マザーボード上のハードウェアをトリガして、サービスプロセッサに取り付けられたコードストアを再構成し、ブートデバイスを実質的に変更する。追加的に、セキュアジャンパ１０２が挿入されたとき、セキュア信号は、アサートされる。セキュア信号は、ＦＰＧＡ、ＢＭＣ（バッファ１０４を介して）、およびブート選択機構に送信される。セキュアジャンパが設置され、システムは、セキュアモードにある。

【００３０】

ＦＰＧＡに送信されたセキュア信号は、ＦＰＧＡ無効信号（１２６）をトリガする。ＦＰＧＡ無効信号は、命令をＦＰＧＡに伝送し、ＦＰＧＡ全体を無効にする。ＦＰＧＡ無効信号は、ＦＰＧＡが任意の他のデバイスを実行することまたはそれと通信することを阻止する。ＦＰＧＡ無効化信号は、システムがセキュアモードにある間、ＦＰＧＡ内部の信頼できないエンティティによる干渉からシステムをセキュアにする。ＦＰＧＡは、信頼されたファームウェア状態をリストアする処理に対する干渉を一切引き起こし得ない。

【００３１】

実施形態では、ＦＰＧＡは、ＣＰＵおよび周辺電力制御１２４に接続される。ＦＰＧＡが無効にされるとき、ＣＰＵおよび周辺電力制御は、それらがＦＰＧＡとの通信を通してのみ機能することができるので、次いで無効にされる。セキュアモードでは、ＣＰＵおよび周辺電力制御は、無効にされ、システムの残りの部分から論理的に分離される。

【００３２】

セキュア信号は、分離を無効にすることによってセキュアコードストアがＢＭＣに接続されることをさらに引き起こす。ＢＭＣ１１０は、不揮発性ストレージまたはブート選択機構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る。たとえば、セキュアコードストアは、ブート選択機構にシリアルペリフェラルインタフェースバス（ＳＰＩ）によって結合され得る。セキュア信号は、セキュアコードストアがＢＭＣのためのブートデバイスとなるようにブート選択ロジックに影響を及ぼす。オペレーションコードストアは、実質的に、補助ストレージデバイスとなる。システムは、物理的にシステムを操作すること、セキュアジャンパを挿入または除去することのみによって、セキュアモードへとまたはそれから再構成されることができる。システムは、任意のコードの実行によってセキュアモードへとまたはそれから再構成されることができない。

【００３３】

上述のように、ブート選択機構は、システムがセキュアモードにあるかまたはオペレーションモードにあるかに依存して、セキュアコードストアまたはオペレーションコードストアのいずれかに対してチップセレクトゼロを指し示す。セキュアモードでは、セキュアコードストアおよびオペレーションコードストアの両方がブート選択機構に接続されるとき、ブート選択機構は、セキュアコードからブートするように構成される。

【００３４】

４．信頼されたシステムファームウェア状態のリストア

図２は、１つまたは複数の実施形態に従い、信頼されたファームウェア状態をリストアするための例示的動作の組を示す。図２に示される1つまたは複数の動作は、変更、再配置、または完全に省略され得る。したがって、図２に示される特定の一連の動作は、１つまたは複数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。

【００３５】

まず、システムは、起動する（動作２０２）。システム起動は、システムの１つまたは複数のデバイスに電力を供給することを含み得る。システム起動は、ソフトウェアに基づき、１つまたは複数のデバイスをブートすることを含み得る。コントローラ（たとえば、ＢＭＣ）は、選択されたコードストア内に格納されたコードに基づきブートする。

【００３６】

選択されたコードストアは、システムのハードウェア構成に基づく。システムは、セキュアモードにあるか、セキュアモードにはないかのいずれかである（動作２０４）。システムがセキュアモードにあるかどうかは、セキュアジャンパが挿入され、マザーボード上の２つのピンを接続するかどうかによって決定されるので、ハードウェアロジックの問題である。代替的にまたは追加的に、システムは、セクション６において以下に説明するように、セキュアモードへとまたはそれからリモートに構成され得る。ハードウェアロジックの結果、システムは、１つまたは複数の信号を伝送する。信号に基づき、システムコンポーネントは、実質的なモードを決定することができる。

【００３７】

Ａ．セキュアモードにないシステム

システムがセキュアモードにない場合、コントローラは、電気的に分離されたセキュアコードへのアクセス無しにオペレーションコードを実行する（動作２２０）。オペレーションコードを実行することは、オペレーションコードをオペレーションコードストアから取得することを含み得る。コントローラは、オペレーションコードをオペレーションコードストアから、たとえば、バスを介して、またはセキュアなネットワーク上で物理的に取得し得る。オペレーションコードを実行することは、オペレーションコードを解釈することをさらに含み得る。オペレーションコード内の命令に基づき、コントローラは、一連の動作を実行し得る。たとえば、コントローラは、オペレーションコードストアから取得された命令に基づき、システムのプロセッシングユニットの温度を監視し得る。

【００３８】

コントローラは、通常オペレーションモードではオペレーションコードストアからブートする。セキュアジャンパが無く、セキュアコードは、電気的に分離される。セキュアコードの電気的分離は、セキュアコードストアとブート選択機構との間の接続を物理的に絶つことによって達成され得る。たとえば、セキュアジャンパの不存在は、セキュアコードストアとブート選択機構とを接続する配線を切断する。

【００３９】

セキュアジャンパが無く、ブート選択機構のハードウェアロジックは、オペレーションコードストアをコントローラのためのブートデバイスとして選択するように構成される。ブート選択機構は、オペレーションコードストアがチップセレクトゼロにあるという命令を送信することによってブートデバイス情報をコントローラに伝送し得る。コントローラは、チップセレクトゼロからブートするように構成される。コントローラはしたがって、セキュアモードではないときにオペレーションコードストアからブートする。

【００４０】

追加的に、セキュアジャンパ無しに、コントローラにマザーボードから送信された信号は、コントローラによって入力信号として受信される。この入力信号は、コントローラロジックが、それがセキュアモードで動作していないという決定をすることを可能とする。

【００４１】

Ｂ．セキュアモードにあるシステム

システムがセキュアモードにある場合、コントローラは、セキュアコードを実行する（動作２１０）。セキュアコードを実行することは、セキュアコードをセキュアコードストアから取得することを含み得る。コントローラは、セキュアコードをセキュアコードストアから、たとえば、バスを介して、またはセキュアなネットワーク上で物理的に取得し得る。セキュアコードを実行することは、セキュアコードを解釈することをさらに含み得る。セキュアコード内の命令に基づき、コントローラは、一連の動作を実行し得る。たとえば、コントローラは、セキュアコードストアの命令に基づき、特定のデバイス上へ格納されたソフトウェアおよび／またはメモリを削除し得る。

【００４２】

セキュアジャンパがマザーボードへと挿入された状態で、マザーボードは、セキュア信号を伝送するように構成される。セキュア信号は、ブート選択機構、コントローラ、およびＦＰＧＡに送信される。

【００４３】

ブート選択機構に送信されたセキュア信号は、ブート選択ロジックに影響を及ぼす。セキュア信号は、セキュアコードストアがブート選択機構に結合され、もはや無効とされないようにすることを引き起こす。セキュアコードは、コントローラからもはや分離されない。

【００４４】

さらに、セキュアジャンパが挿入されるとき、ブート選択機構のハードウェアロジックは、セキュアコードストアをコントローラのためのブートデバイスとして選択するように構成される。ブート選択機構は、セキュアコードストアからブートするようにシステムを構成する。セキュアコードストアおよびオペレーションコードストアの両方がセキュアモ

ードではブート選択機構に接続されるが、ブート選択機構は、コントローラにセキュアコードストアからブートするように命令する。ブート選択機構は、ブートデバイス情報をコントローラに伝送し得る。ブート選択機構は、セキュアコードストアがチップセレクトゼロにあるという通知をコントローラに伝送し得る。コントローラは、常時チップセレクトゼロからブートするように構成される。コントローラはしたがって、セキュアモードにあるときにセキュアコードストアからブートする。

【００４５】

システムまた、セキュア信号をコントローラに伝送する。コントローラは、セキュア信号を、逆駆動できない入力信号として受信する。セキュアジャンパとコントローラとの間のインタフェースに沿うバッファの配置は、コントローラが信号をセキュアジャンパに向かって戻すように送信することを阻止する。コントローラは、セキュア信号を変更することができない。セキュア信号を受信したために、コントローラロジックは、それがセキュアモードにおいて動作していると分かる。

【００４６】

追加的に、システムは、ＦＰＧＡ無効信号をＦＰＧＡに伝送する。ＦＰＧＡ無効信号は、ＦＰＧＡの動作を阻止する。ＦＰＧＡ無効信号は、ＦＰＧＡへの電力またはクロックを切断することによってＦＰＧＡが無効にされることを引き起こし得る。ＦＰＧＡ無効信号は、他のデバイスからＦＰＧＡを分離することによってＦＰＧＡが無効にされることを引き起こし得る。無効にされたとき、ＦＰＧＡは、システムの任意のデバイスの状態に影響を及ぼすことができない。ＦＰＧＡは、信頼されたファームウェア状態をリストアする処理に対する干渉を一切引き起こし得ない。

【００４７】

セキュアモードでは、コントローラは、１つまたは複数のコードセットを削除する（動作２１２）。コントローラは、命令を信頼されないすべてのデバイスに伝送し、その内部に格納されたコードおよび／またはメモリを削除する。コントローラは、周辺サービスプロセッサ、ＮＡＮＤフラッシュ、不揮発性ストレージ、またはＦＰＧＡに格納されたコードセットを含み得る、すべてのプログラム可能なメモリが削除されることを引き起こす。コントローラは、オペレーティングシステムおよび／またはＢＩＯＳコードセットといったコードセットを削除し得る。

【００４８】

次に、コントローラは、オペレーションコードの現在のバージョンをセキュアコードによって参照されたオペレーションコードの置換バージョンで上書きする（動作２１４）。セキュアコードは、オペレーションコードセットを、セキュアコードストア内に隔離されて維持されていた元のオペレーションコードセットのバージョンで置換する命令を含み得る。代替的に、オペレーションコードセットは、元のオペレーションコードセットの一部で置換され得る。オペレーションコードセットは、ブートローダで置換され得る。上述のステップは、任意の他のファームウェアを要さずに実行されることができる。一度動作が完了すると、システム全体は、真新しく（クリーンに）され、信頼されたファームウェア状態へとリストアされる。

【００４９】

たとえば、ユーザは、セキュアジャンパが配置された状態でシステムを電源オンにする。システムは、セキュアモードにある。セキュアモードでは、ＦＰＧＡ無効信号は、ＦＰＧＡに送信され、ＦＰＧＡ、ＣＰＵ、および周辺電力制御を無効にする。

【００５０】

システムはまた、セキュア信号をブート選択機構に伝送し、それがセキュアコードストアの分離を無効にすることをもたらす。セキュア信号は、ブート選択機構内のブート選択ロジックに影響を及ぼす。セキュアモードでは、セキュアコードストアは、コントローラのためのブートデバイスになる。

【００５１】

システムはまた、セキュア信号をコントローラに伝送する。コントローラは、セキュア

信号を、逆駆動されることができない入力信号として受信する。セキュア信号を受信したため、コントローラロジックは、それがセキュアモードにおいて動作していると分かる。

【００５２】

セキュアコードストアは、コントローラに不揮発性ストレージ、ＦＰＧＡ、およびオペレーションコードストア上のコードセットを削除するよう命令するコードを含む。セキュアコードストアは、システムにオペレーションコードストア内のコードをオペレーションコードの真新しいバージョンで置換するよう命令するコードをさらに含む。一定期間の動作後に、オペレーションコードストア内のオペレーションコードは、変えられ得、信頼されない可能性がある。コントローラは、セキュアコードからの命令に応じて、コードを削除し置換する。

【００５３】

この時点で、オペレーションコードストアは、真新しいコードを含むが、不揮発性ストレージおよびＦＰＧＡ上のコードは、置換されていない。これらのデバイス上のコードを置換するために、ユーザは、システムを通常オペレーションモードに再構成する。オペレータは、セキュアジャンパを物理的に除去する。セキュアジャンパの除去は、マザーボード上の接続を再構成する。

【００５４】

ブート選択ハードウェアロジックは、セキュアコードストアを分離するように再構成される。システムは、信号をコントローラおよびブート選択機構に伝送し、これによりコントローラは、オペレーションコードストア内のオペレーションコードからブートする。システムは、ＦＰＧＡ有効信号をＦＰＧＡに伝送する。ＦＰＧＡは、ＦＰＧＡ有効信号の受信に応答して有効にされる。

【００５５】

今、オペレーションコードストアは、コントローラに接続され、セキュアコードストアは、コントローラに接続されない。コントローラは、オペレーションコードストア内のオペレーションコードからブートする。セキュアコードストアは、システムから分離され、信頼を失われ得ない。

【００５６】

５．サーバを信頼されたファームウェア状態にリストア

例として、システムは、サーバを信頼されたファームウェア状態にリストアするための動作を実行する。まず、オペレータは、システムを電源オフにし、セキュアジャンパを挿入する。オペレータは、電源をオンにし、ＢＭＣをブートさせる。

【００５７】

ＢＭＣは、ＢＭＣがセキュアモードにあり、セキュアコードストアからブートすると認識する。ＢＭＣは、すべての外部インタフェースからの入力を無効にし、システムの１つまたは複数のデバイスを無効にする。ＢＭＣは、すべての信頼されないデバイスおよび／またはセキュアコードの実行のために必要ではないすべてのデバイスを無効にし得る。ＢＭＣは、オペレーションコードストアを、マザーボードＦＰＧＡ、不揮発性メモリ（たとえば、ＮＡＮＤ）、および任意の他の書き込み可能なストア等、アクセスを有するすべての不揮発性ストレージを削除し得る。ＢＭＣは、セキュアコードストアの内容を使用してオペレーションコードストアを再構築する。

【００５８】

このプロセスの間に、ＢＭＣは、その状況を表示する。セキュアモードでは、システムは、オペレーティングシステムまでブートしない。ＢＭＣは、セキュアモードのすべてのステップが完了するまでＬＥＤを点滅させることでこれを通知する。一度セキュアモードにおけるステップが完了されると、ＢＭＣは、サーバが信頼された状態にリストアされたことを、ＬＥＤを変化させシリアルコンソールにメッセージを表示することによって通知する。

【００５９】

オペレータは、電源をオフにし、ジャンパを除去する。ジャンパが配置されることなく

システムが電源オンされたときに、システムは、有効信号を無効信号の代わりに送信する。有効信号の伝送は、ブート選択機構がセキュアコードストアを分離および保護し、オペレーションコードストアをブートデバイスとして構成することを引き起こす。

【００６０】

ＢＭＣは、オペレーションコードストア内の新たな信頼されたコードからブートする。ＢＭＣは、まだ使用されていないファームウェアイメージをロードする。まだ使用されていないファームウェアイメージは、ネットワーク接続を介してウェブサーバから、またはＤＶＤを通して等、任意の信頼されたソースからロードされることができる。ＢＭＣは、ＢＩＯＳ、ＦＰＧＡ、および不揮発性メモリといったすべての残りファームウェアの既知の良好なコピーを再インストールする。これは、通常のファームウェア更新手順を通して行われることができる。システムはオペレーション状態に戻り、新たにリストアされた信頼のルートから動作することができる。

【００６１】

６．リモート再構成

実施形態では、システムは、セキュアモードへとまたはそれからリモートに構成されることができる。セキュア信号は、ジャンパを用いてアサートされる必要はない。この場合、セキュア信号は、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。

【００６２】

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、セキュア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。

【００６３】

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、セキュア信号の伝送を上述のように制御し得る。

【００６４】

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。

【００６５】

７．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。

【００６６】

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。

【００６７】

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。

【００６８】

８．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。

【００６９】

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。

【００７０】

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。

【００７１】

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。

【００７２】

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。

【００７３】

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。

【００７４】

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。

【００７５】

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。

【００７６】

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。

【００７７】

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。

【００７８】

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。

【００７９】

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。

【００８０】

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】

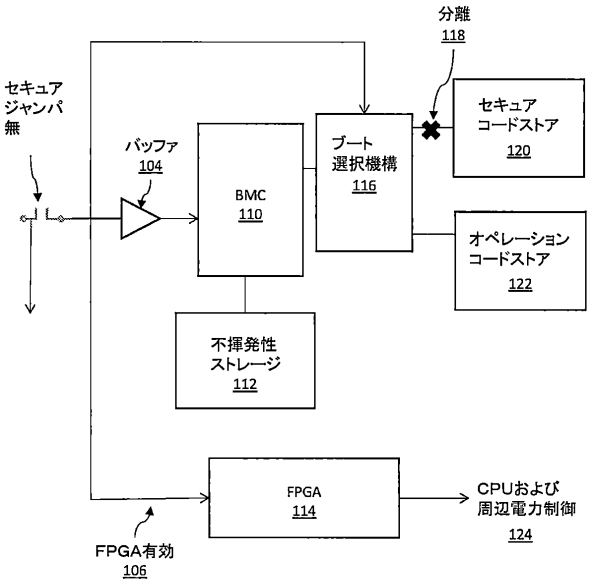


FIG. 1A

【図１Ｂ】

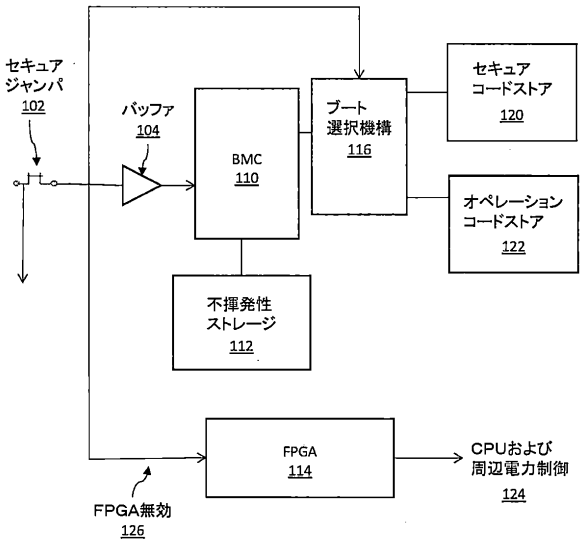


FIG. 1B

【図２】

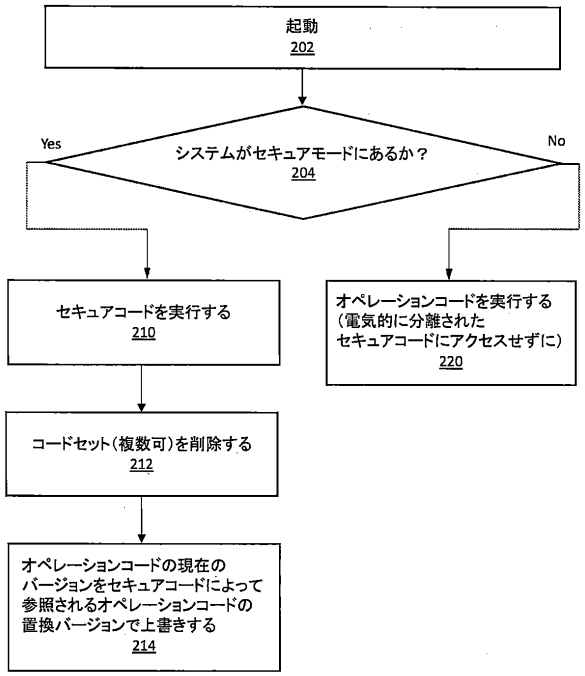
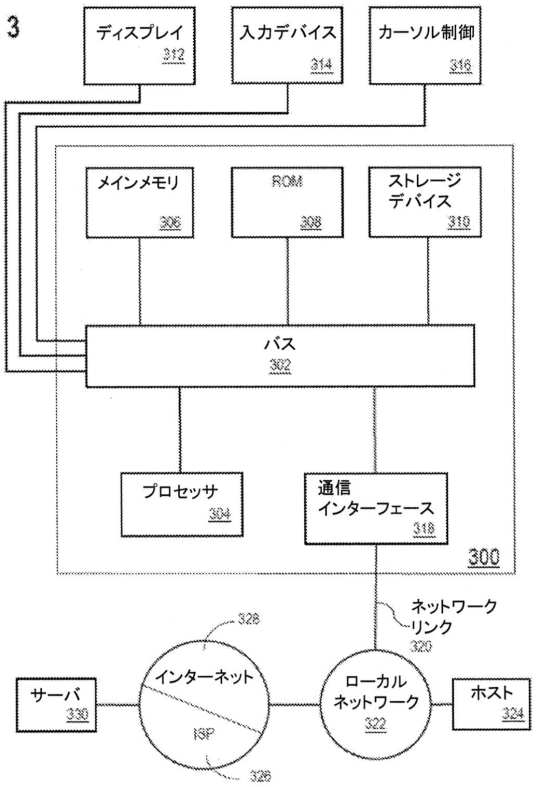


FIG. 2

【図３】

FIG. 3



フロントページの続き

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　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　宮司 卓佳

(56)参考文献
特開２０１３－１６４８４２（ＪＰ，Ａ）
特開２００９－２１１３３９（ＪＰ，Ａ）
特開平０９－３３０２７２（ＪＰ，Ａ）
特開２００６－０８１２４６（ＪＰ，Ａ）
米国特許出願公開第２００４／０１３９３５７（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０１１０３７９（ＵＳ，Ａ１）
米国特許出願公開第２０１２／００７９２６０（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０３０６６２３（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７