(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5246580号
(P5246580)

(45)発行日　平成25年7月24日(2013.7.24)　(24)登録日　平成25年4月19日(2013.4.19)

(51)Int.Cl.		F I		
G06K 17/00	(2006.01)	G06K	17/00	F
G06F 11/00	(2006.01)	G06F	9/06	630A
H01L 21/02	(2006.01)	H01L	21/02	Z
G06K 19/07	(2006.01)	G06K	17/00	L
G06K 19/00	(2006.01)	G06K	19/00	H

請求項の数 31　外国語出願　(全 22 頁)　最終頁に続く

(21)出願番号　特願2010-212501 (P2010-212501)
(22)出願日　平成22年9月22日 (2010.9.22)
(65)公開番号　特開2011-108225 (P2011-108225A)
(43)公開日　平成23年6月2日 (2011.6.2)
審査請求日　平成22年9月24日 (2010.9.24)
(31)優先権主張番号　12/592,212
(32)優先日　平成21年11月20日 (2009.11.20)
(33)優先権主張国　米国 (US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　シャヒザデー、シャーロク
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

最終頁に続く

(54)【発明の名称】商品パッケージのマイクロエレクトロニクスシステムの無線周波数再構成

(57)【特許請求の範囲】
【請求項１】
物品であって、
無線周波数識別タグ（ＲＦＩＤタグ）と、
前記ＲＦＩＤタグに連結されたハードウェアリソースと、
前記ハードウェアリソースをアップビンまたはダウンビンする無線周波数（ＲＦ）通信機能と
を備え、
前記ＲＦＩＤタグは、前記ハードウェアリソースに関して固有の暗号化識別子とキャッシュされたユニットレベルのトレーサビリティデータ（ＵＬＴデータ）とを有し、
前記ＵＬＴデータは、製造日、製造場所（ｆａｂ）、利用された機器、処理フロー、ウェハサイトの起点、クロック速度、電力消費、キャッシュサイズ、命令セット、およびビン分割のうち少なくとも３つを含む物品。
【請求項２】
前記ＲＦＩＤタグは前記ハードウェアリソースと一体的に設けられる請求項１に記載の物品。
【請求項３】
前記ＲＦＩＤタグは前記ハードウェアリソースと一体的に設けられ、
前記物品はさらに、
前記ハードウェアリソースが上に設けられ、前記ＵＬＴデータに含まれている搭載基板

と、
前記搭載基板上に設けられ、前記ハードウェアリソースに連結されたＲＦアンテナと
をさらに備える請求項１に記載の物品。
【請求項４】
シリアルバスを介して連結された前記ハードウェアリソースと前記ＲＦＩＤタグとが設けられた搭載基板と、
前記搭載基板上に設けられ、前記ＲＦＩＤタグに連結されたＲＦアンテナと
をさらに備える請求項１に記載の物品。
【請求項５】
無線周波数識別タグ（ＲＦＩＤタグ）を含むシステムが、前記システムのハードウェアリソースへのアップビンまたはダウンビンと互換性を有するか否かを判断する段階と、
前記ハードウェアリソースを遠隔データベースに対して認証する段階と、
前記ＲＦＩＤタグにて遠隔システムからの前記ハードウェアリソースをアップビンまたはダウンビンせよとの無線周波数命令（ＲＦ命令）を受信する段階と、
前記ＲＦ命令に基づいて第１の機能を持つ前記ハードウェアリソースをプログラミングする段階とを備え、
前記ハードウェアリソースをプログラミングする段階は、前記プログラミングする段階の前と異なる前記ハードウェアリソースの第２の機能をリリースする段階を有する方法。
【請求項６】
前記第２の機能のリリースは、前記ハードウェアリソースのアップビンまたはダウンビンのいずれか１つである請求項５に記載の方法。
【請求項７】
前記判断する段階は、第１の判断する段階であって、前記認証する段階は第１の認証する段階であって、前記受信する段階は第１の受信する段階であって、前記プログラミングする段階は第１のプログラミングする段階であって、前記方法はさらに、
前記システムが前記システムの前記ハードウェアリソースへの再構成と互換性を有するか否かを判断する、後続の判断を行う段階と、
前記ハードウェアリソースを遠隔データベースに対して認証する、後続の認証を行う段階と、
遠隔システムからの、後続して前記ハードウェアリソースを再構成せよとのＲＦ命令を受信する、後続の受信を行う段階と、
前記ＲＦ命令に基づいて前記ハードウェアリソースをプログラミングする、後続のプログラミングを行う段階とを備える請求項５に記載の方法。
【請求項８】
前記判断する段階は、第１の判断する段階であって、前記認証する段階は第１の認証する段階であって、前記受信する段階は第１の受信する段階であって、前記プログラミングする段階は第１のプログラミングする段階であって、前記方法はさらに、
前記システムが前記システムの前記ハードウェアリソースへの再構成と互換性を有するか否かを判断する、後続の判断を行う段階と、
前記ハードウェアリソースを遠隔データベースに対して認証する、後続の認証を行う段階と、
遠隔システムからの、後続して前記ハードウェアリソースを再構成せよとのＲＦ命令を受信する、後続の受信を行う段階と、
前記ＲＦ命令に基づいて前記ハードウェアリソースをプログラミングする、後続のプログラミングを行う段階とを備え、
前記ハードウェアリソースは第２の機能を含み、
前記ハードウェアリソースをプログラミングする、前記後続のプログラミングを行う段階は、前記後続のプログラミングを行う段階の前と比較して向上した前記ハードウェアリソースの後続する機能をリリースする段階を有する請求項５に記載の方法。
【請求項９】

前記ハードウェアリソースは第１の機能を含み、
前記ハードウェアリソースをプログラミングする段階は、前記プログラミングする段階の前と比較して向上した前記ハードウェアリソースの第２の機能をリリースする段階を有し、
前記方法はさらに、
前記ハードウェアリソースの利用をモニタする段階と、
前記ハードウェアリソースの機能を前記第１の機能に戻す段階とを備える請求項５に記載の方法。
【請求項１０】
前記ハードウェアリソースは第１の機能を含み、
前記ハードウェアリソースをプログラミングする段階は、前記プログラミングする段階の前と比較して向上した前記ハードウェアリソースの第２の機能をリリースする段階を有し、
前記方法はさらに、
前記ハードウェアリソースの利用をモニタする段階と、
前記ハードウェアリソースの機能を、前記第１の機能とも前記第２の機能とも異なる第３の機能に変更する段階とをさらに備える請求項５に記載の方法。
【請求項１１】
前記ハードウェアリソースは複数のハードウェアリソースのうちの１つであり、
前記複数のハードウェアリソースのプログラミングを同時に行う請求項５から１０のいずれか一項に記載の方法。
【請求項１２】
前記ハードウェアリソースは複数のハードウェアリソースのうちの１つであり、
前記複数のハードウェアリソースのプログラミングを前記複数のハードウェアリソースの一部について行う請求項５から１０のいずれか一項に記載の方法。
【請求項１３】
前記ハードウェアリソースは異種の複数のハードウェアリソースのうちの１つであり、
前記プログラミングする段階は、
少なくとも１つの第１のハードウェアリソースに、より多くの機能をリリースするべく、第１の機能に応じて前記少なくとも１つの第１のハードウェアリソースをプログラミングする第１のプログラミング段階と、
少なくとも１つの第２のハードウェアリソースに、より多くの機能をリリースするべく、後続する機能に応じて前記少なくとも１つの第２のハードウェアリソースをプログラミングする第２のプログラミング段階とを有する請求項５に記載の方法。
【請求項１４】
ハードウェアリソースの製造をデータベースに、および、前記ハードウェアリソースに前記ハードウェアリソースに連結されたＲＦＩＤタグを利用して固有暗号化識別子とともに記録する段階と、
前記ハードウェアリソースの性能を特徴付ける段階と、
前記ハードウェアリソースをビン分割する段階と、
前記ハードウェアリソースをダウンビンする段階と、
外部の機器製造業者（ＯＥＭ）との間で構築された販売または評価に関する契約の下で前記ハードウェアリソースが出荷された後、前記契約に関するアップビンまたはダウンビンのライセンスを送信する段階と
を備え、
前記ＲＦＩＤタグは、ユニットレベルのトレーサビリティデータ（ＵＬＴデータ）を有し、
前記ＵＬＴデータは、製造日、製造場所（ｆａｂ）、利用された機器、処理フロー、およびウェハ上の前記ハードウェアリソースのウェハサイトの起点位置のうち少なくとも３つを含む方法。

【請求項１５】
無線周波数（ＲＦ）通信により前記ハードウェアリソースをアップビンする段階をさらに備える請求項１４に記載の方法。
【請求項１６】
無線周波数（ＲＦ）通信により前記ハードウェアリソースをダウンビンする段階をさらに備える請求項１４または１５に記載の方法。
【請求項１７】
前記ハードウェアリソースへの記録には、前記ハードウェアリソースと一体部である無線周波数識別（ＲＦＩＤ）タグへの記録が含まれる請求項１４から１６のいずれか一項に記載の方法。
【請求項１８】
前記ハードウェアリソースへの記録には前記ＲＦＩＤタグへの記録が含まれ、
前記ＲＦＩＤタグは、前記ハードウェアリソースが上に設けられている搭載基板上に設けられ、前記搭載基板はさらに前記ＲＦＩＤタグに記録されたＵＬＴデータも含む請求項１４から１６のいずれか一項に記載の方法。
【請求項１９】
前記ハードウェアリソースのアップビンまたはダウンビンは、専ら無線周波数（ＲＦ）ＲＦ通信により行われる請求項１４から１８のいずれか一項に記載の方法。
【請求項２０】
前記ハードウェアリソースのアップビンまたはダウンビンは、部分的に無線周波数（ＲＦ）ＲＦ通信により、および、部分的に物理的に連結されたコンポーネントからの電力支援により行われる請求項１４から１８のいずれか一項に記載の方法。
【請求項２１】
前記ハードウェアリソースを出荷する段階の前に、前記ハードウェアリソースをディセーブルする段階を備える請求項１４から２０のいずれか一項に記載の方法。
【請求項２２】
前記ＯＥＭを前記ハードウェアリソースに記録する段階と、
前記出荷する段階の前に、前記ハードウェアリソースをディセーブルする段階と、
前記ＯＥＭに、前記ハードウェアリソースが前記ＯＥＭに向けられたものであったか否かを判断させる段階と、
前記判断させる段階の結果が肯定的なものである場合に、前記ＯＥＭに前記ハードウェアリソースをアンロックさせる段階とをさらに備える請求項１４から２０のいずれか一項に記載の方法。
【請求項２３】
市場で定められているハードウェアリソースのダウンビンまたはアップビン要件の変更を観察する段階と、
アップビン要件の変更に関して前記契約に関するアップビンまたはダウンビンのライセンスを利用できる旨の通知を送信する段階と
をさらに備える請求項１４から２２のいずれか一項に記載の方法。
【請求項２４】
ウェハ上に第１の複数のハードウェアリソースを製造する段階と、
製造日、製造場所（ｆａｂ）、利用された機器、処理フロー、シンギュレーション前のウェハ上の前記第１の複数のハードウェアリソースの各々のダイサイトの位置のうち少なくとも３つを含む前記第１の複数のハードウェアリソースの製造を、データベースに、および、前記第１の複数のハードウェアリソースの各々に固有の暗号化識別子とともに記録する段階と、
前記第１の複数のハードウェアリソースの各々の性能を特徴付ける段階と、
前記第１の複数のハードウェアリソースをビン分割する段階と、
前記第１の複数のハードウェアリソースのうち、暗号化固有識別子を含む無線周波数識別タグ（ＲＦＩＤタグ）に連結されている少なくとも１つのハードウェアリソースを含む

第２の複数のハードウェアリソースを契約義務により組み立てる段階と、
前記少なくとも１つのハードウェアリソースをダウンビンする段階と、
前記契約の下で前記ハードウェアリソースが出荷された後に、前記ＲＦＩＤタグを利用して前記ハードウェアリソースをプログラミングする段階とを備える方法。
【請求項２５】
前記ハードウェアリソースをプログラミングする段階は、
マイクロコード命令により行われる動的ヒューズを利用して前記ハードウェアリソースを永久的にプログラミングする段階を有する請求項２４に記載の方法。
【請求項２６】
無線周波数識別タグ（ＲＦＩＤタグ）と、
前記ＲＦＩＤタグに連結されたハードウェアリソースと、
前記ハードウェアリソースをアップビンまたはダウンビンする無線周波数（ＲＦ）通信機能と、
前記ハードウェアリソースに連結された外部メモリと
を備え、
前記ＲＦＩＤタグは、前記ハードウェアリソースに関して固有の暗号化識別子とキャッシュされたユニットレベルのトレーサビリティデータ（ＵＬＴデータ）とを有し、
前記ＵＬＴデータは、製造日、製造場所（ｆａｂ）、利用された機器、処理フロー、ウェハサイトの起点、クロック速度、電力消費、キャッシュサイズ、命令セット、およびビン分割のうち少なくとも３つを含むコンピューティングシステム。
【請求項２７】
前記コンピューティングシステムは、携帯電話機、ページャ、ポータブルコンピュータ、デスクトップコンピュータ、および、双方向ラジオのうちいずれか１つの一部である請求項２６に記載のコンピューティングシステム。
【請求項２８】
対象システム、コンピュータおよび遠隔データベース用のプログラムであって、
前記コンピュータに、前記対象システムが前記対象システムのハードウェアリソースへのアップビンまたはダウンビンと互換性を有するか否かを、前記対象システムの無線周波数識別タグ（ＲＦＩＤタグ）と通信することにより、判断する手順を実行させ、
前記コンピュータに、前記ハードウェアリソースを前記遠隔データベースに対して認証する手順を実行させ、
前記対象システムに、前記コンピュータおよび前記遠隔データベースを含む遠隔システムから前記ハードウェアリソースを再構成せよとのＲＦ命令を受信する手順を実行させ、
前記対象システムに、ＲＦプログラミングする前と異なる前記ハードウェアリソースの第２の機能をリリースする手順を実行させることを含み、前記ＲＦ命令に基づいて前記ＲＦＩＤタグにより、前記対象システムに、第１の機能を持つ前記ハードウェアリソースを前記ＲＦプログラミングする手順を実行させるためのプログラム。
【請求項２９】
前記遠隔システムに、前記対象システムへ確認命令を提供する手順をさらに実行させるためのプログラムであり、
前記確認命令は、前記対象システムに対するアップビンまたはダウンビンが成功したことを確認するためのものである請求項２８に記載のプログラム。
【請求項３０】
前記遠隔データベースに、アップビンまたはダウンビンが成功したことが確認できると、前記対象システムに対する前記アップビンまたはダウンビン分の勘定書を請求する手順を実行させ、
前記遠隔システムに、前記対象システムと前記アップビンまたはダウンビンとに関する情報をセキュアなデータベースに記録する手順をさらに実行させる請求項２８または２９に記載のプログラム。
【請求項３１】

前記遠隔データベースに、前記対象システムから受信した暗号鍵に従ってプログラミング命令を暗号化した形で準備して送信する手順をさらに実行させる請求項２８から３０のいずれか一項に記載のプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
開示される実施形態は、半導体マイクロエレクトロニクスデバイスおよびその再構成方法に係る。
【背景技術】
【０００２】
特にパーソナルコンピュータ（ＰＣ）、サーバ、携帯情報端末（ＰＤＡ）、および携帯電話機を含む多くのプロセッサベースのシステムが、ハードウェアコンポーネントとソフトウェアコンポーネントとの組み合わせを含む。通常のシステムは、処理動作の大半を扱うＣＰＵ（中央処理装置）と通称されるマイクロプロセッサを、例えばメモリおよびその他の記憶媒体、チップセットおよびその他の処理デバイス、入出力（Ｉ／Ｏ）デバイス等の関連コンポーネントとともに含む。エンドユーザは通常これらシステムを様々な処理、娯楽、通信、およびその他のアクティビティに利用する。
【０００３】
製造段階では、プロセッサベースのシステムは、しばしば任意の意図された用途よりも多くの演算機能を有する。
【図面の簡単な説明】
【０００４】
実施形態を実行する方法の理解を助けるべく、上で要約した様々な実施形態のうち特定のものを、添付図面を参照しながら記載する。これら図面の示す実施形態は必ずしも実寸に即しておらず、本発明の範囲を制限するものとして捉えられるべきではない。一部の実施形態は添付図面を参照してさらに簡略化されたり、さらに詳細に説明されたりする場合がある。
【図１】例示的な実施形態における物品を含む概略図である。
【図２ａ】一実施形態における方法の概略図である。
【図２ｂ】一実施形態におけるさらなるイベントの後の図２ａに示す方法の概略図である。
【図２ｃ】一実施形態におけるさらなるイベントの後の図２ｂに示す実施形態の概略図である。
【図３】例示的な実施形態における搭載基板の立面断面図である。
【図４】複数の実施形態における方法のフロー図である。
【図５】例示的な実施形態におけるシステムのブロック図である。
【発明を実施するための形態】
【０００５】
開示する実施形態は、無線周波数識別（ＲＦＩＤ）タグを複数含み、その各々が固有の識別子を有する。ＲＦＩＤタグは、ハードウェアリソースのクエリ、アンロック、および再構成のために、データおよびコマンドの配信メカニズムで利用される。ＲＦＩＤタグに格納される情報には、ハードウェアリソースの処理系譜および性能機能が含まれる。ＲＦＩＤタグの不揮発性ＲＡＭ（ＮＶＲＡＭ）に格納される制御命令よび方法は、ハードウェアリソースの設定を読み出したり、再構成したりする用途に利用される。マイクロコードで駆動されるファームウェアも、シリアルバス等の物理接続によるＲＦＩＤタグリーダおよびプログラマとして利用することができる。
【０００６】
同様の構成を同様の接尾辞により示した箇所もある図面について言及する。様々な実施形態の構造をより明確に示すべく、ここに含まれる図面は集積回路の構造を図形で示した

ものである。従って顕微鏡写真におけるもの等の、製造される構造の実際の外見はこれと異なるかもしれないが、これも例示する実施形態の請求される構造を含む。さらに、図面は例示する実施形態の理解に必要な構造のみを示す場合がある。従来技術として公知のさらなる構造は、図面を明瞭に保つ目的から含めていない場合がある。プロセッサチップおよびメモリチップを同じ文章で言及している場合があっても、これらが同じ構造であると理解されるべきではない。

【０００７】

図１は、例示的な実施形態における物品を含む概略図１００である。マイクロプロセッサ等のハードウェアリソース１１０が搭載基板１１２に連結されている。一実施形態では、ハードウェアリソース１１０は、Ａｔｏｍ（登録商標）、Ｃｅｌｅｒｏｎ（登録商標）、Ｃｏｒｅ（登録商標）等のインテルコーポレーション社製のマイクロプロセッサである。一実施形態では、ハードウェアリソース１１０は、スマートフォン等用の処理およびその他の機能を含むシステムオンチップ（ＳＯＣ）である。一実施形態では、ハードウェアリソース１１０は、メモリチップまたはメモリモジュールである。一実施形態では、ハードウェアリソース１１０はチップセットまたはチップセットの１要素である。

【０００８】

ＲＦＩＤタグ１１４も搭載基板１１２に配設され、一実施形態においてはシリアルバス１１６でハードウェアリソース１１０に連結される。一実施形態では、ＲＦＩＤタグは半導体基板内に形成される。ＲＦＩＤタグ１１４は、銅製ループ１１８等のＲＦＩＤアンテナ１１８を利用する。一実施形態では、ＲＦＩＤアンテナは、特定用途向けに調節されたダイポール構造を有する。

【０００９】

ＲＦＩＤアンテナ１１８は、本実施形態では搭載基板１１２上のループとして示される。一実施形態では、ＲＦＩＤアンテナは、搭載基板１１２がコンポーネントパッケージングとして搭載されたマザーボード上に設けられる。一実施形態では、ＲＦＩＤアンテナは、より大きな基板に連結されたコンポーネントパッケージングである搭載基板を含む筐体上に設けられる。一実施形態では、ＲＦＩＤアンテナは、ＲＦＩＤタグが配設されるシステムのシェルに統合される。例えば、スマートフォンの外部シェルは、シェルと一体部として成型されるＲＦＩＤアンテナを有する。

【００１０】

一実施形態では、ＲＦＩＤタグ１１４は、特定のハードウェアリソース１１０に関する固有識別子を有する。ＲＦＩＤタグ１１４は、さらに、ハードウェアリソース１１０および搭載基板１１２の相乗作用に関するデータを格納している。

【００１１】

ＲＦＩＤタグ１１４、シリアルバス１１６、およびＲＦＩＤアンテナ１１８は、ハードウェアリソース１１０の無線周波数（ＲＦ）通信機能と称される場合がある。しかし一実施形態では、ＲＦ通信機能はハードウェア（シリコン内）と一体的に設けられ、少なくともＲＦＩＤタグ１１４およびシリアルバス１１６の機能がハードウェアリソース１１０の半導体材料に統合される。

【００１２】

ファームウェアを有するドングル等のアンテナ１２０が、コンピューティングシステム１２２に連結されたＲＦＩＤリーダデバイスに連結され、コンピューティングシステム１２２は、セキュアなデータベース１２４に連結される。コンピューティングシステム１２２は一般的なデスクトップコンピュータとして示されるが、ハードウェアリソース１１０に配線で接続されたものではない任意の適切なコンピューティングシステムであってよい。一実施形態では、ハードウェアリソース１１０は、コンピューティングシステム１２０から１１０へのクエリを受けて固有の暗号化識別子を有するＲＦＩＤタグ１１４に対するライセンスを発行してもらうことにより、ＲＦＩＤタグ１１４を介してセキュアなデータベース１２４に対して認証される。セキュアなデータベース１２４は（さらに遠隔サーバ１２４とも称される）、ＲＦ通信によりハードウェアリソース１１０またはシステム内の

別のコンポーネントに書き込まれるライセンスを発行する。

【００１３】

一実施形態では、ハードウェアリソース１１０を、ＲＦＩＤタグ１１４からセキュアなデータベース１２４への通信によりシステム内のいずれかの、または、全ての他のコンポーネントの再構成を行うセキュアなリソースとして利用する。例えば、固体ドライブは、ハードウェアリソース１１０を利用して、再構成、あるいは、アップビンまたはダウンビンされる（up- or down-binned）。一例では、メモリ利用を、ハードウェアリソース１１０を利用して、再構成、あるいは、アップビンまたはダウンビンする。一例では、ソフトウェアに対して、ハードウェアリソース１１０を利用して、アップビンまたはダウンビン等の再構成を行う。一例では、ファームウェアを、ハードウェアリソース１１０を利用して、再構成、あるいは、アップビンまたはダウンビンする。

【００１４】

ハードウェアリソース１１０、搭載基板１１２、およびタグ１１４に関するユニットレベルのトレーサビリティ（ＵＬＴ）データをタグ１１４にキャッシュして、さらにはセキュアなデータベース１２４に格納する。ＵＬＴデータは、セキュアなデータベース１２４に、コピーとして、ハードウェアリソース１１０の製造系譜に関連付けられた企業実体とともに格納される。一部の実施形態では、セキュアなデータベース１２４は、ハードウェアリソース１１０から遠隔の位置にある。いずれの場合においても、本明細書における「遠隔データベース」という呼称は、任意のハードウェアリソースから遠隔の位置にあってもなくてもよいセキュアなデータベースのことである。

【００１５】

製造系譜には、ハードウェアリソース１１０および搭載基板１１２の処理および組み立て条件の一部が含まれるが、これらは各々が別の実体により製造されたものであってもよい。

【００１６】

ＵＬＴデータは、ハードウェアリソース１１０、搭載基板１１２、およびＲＦＩＤタグ１１４各々に関していてよい。一実施形態では、ＵＬＴデータは、製造日を含む。一実施形態では、ＵＬＴデータは製造場所（「ｆａｂ」とも称される）を含み、ｆａｂ内で利用されるサブプロセスを含みうる。一実施形態では、ＵＬＴデータは、エッチングツール、スピンオンツール、および熱処理ツールを始めとするデータの追跡等の製造で利用される処理機器を含む。一実施形態では、ＵＬＴデータは特定の処理フローを含む。この理由は、処理フローが複雑になり数十のサブプロセスフローからなる場合もあるからである。一実施形態では、ＵＬＴデータは、複数のハードウェアリソースにウェハを分割するシンギュレーション前の単一のウェハ上に処理のばらつきが起こる可能性のあるハードウェアリソース１１０のウェハサイトの起点を含む。例えばウェハサイトの起点データは特に、処理で利用されるステッパの一部に関するウェハの高歩留まりの部分を追跡することができる。他の製造データを暗号化して、ＲＦＩＤタグ１１４に、そして同時にセキュアなデータベース１２４にキャッシュすることができる。

【００１７】

一実施形態では、ハードウェアリソース１１０のクロック速度を、ビン分割テスト位置等に記録する。クロック速度は、市場で定められているダウンビン要件により可変であってよく、ハードウェアリソース１１０は、最大クロック速度の１００パーセント未満で動作するよう設定されてよい。この結果、ハードウェアリソース１１０は、特定のハードウェアリソース１１０による市場および販売条件による最大機能よりも遅いクロック速度で指定されるビンにビン分割される。

【００１８】

電力消費も、暗号化されてＲＦＩＤタグ１１４にキャッシュされ、ひいてはセキュアなデータベース１２４に格納されうる性能パラメータである。任意のハードウェアリソース１１０が他よりも低い電力を消費するような同様のビン分割法を実行することもできるが、市場条件では最低電力構成は必須ではない。

【００１９】
キャッシュサイズもまた、暗号化されてＲＦＩＤタグ１１４にキャッシュされ、ひいてはセキュアなデータベース１２４に格納されうる性能パラメータである。任意のハードウェアリソース１１０が既に製造および検証されているものよりも少ないキャッシュを要するような同様のビン分割法を実行することもできるが、ある用途では行われた全てのキャッシュは必須ではない。
【００２０】
最大効率命令セットも、暗号化されてＲＦＩＤタグ１１４にキャッシュされ、ひいてはセキュアなデータベース１２４に格納されうる性能パラメータである。任意のハードウェアリソース１１０が最大効率命令セットよりも少なくてもよいような、あるいは全命令セットの全ての特徴を必要としない１つの命令セットよりも少なくてもよいような、同様のビン分割法を実行することもできる。
【００２１】
搭載基板１１２にも、任意の搭載基板１１２と対とさせられた任意のハードウェアリソース１１０を整合させる助けとなるＵＬＴデータが関連付けられていてよい。搭載基板１１２に対する同様のビン分割データを記録してもよい。セキュアに格納可能な他のＵＬＴデータには、搭載基板１１２とハードウェアリソース１１０との間で層間剥離が生じるようなフィールド収集されるデータが含まれる。
【００２２】
任意の搭載基板１１２と対とさせられた任意のハードウェアリソース１１０との間の正および負の相乗作用効果により、搭載基板１１２のＵＬＴデータが、本明細書が開示する複数の方法の実施形態に一定の役割を担うことができる。例えば、任意のハードウェアリソースと対にさせられることで、第１のサプライヤから供給される第１の搭載基板は、第２のサプライヤが供給する第２の搭載基板では生成されないような性能特性上の相乗作用を生じることができる。いずれの場合にも、ＵＬＴデータは、任意の搭載基板１１２と対の任意のハードウェアリソース１１０ごとに、セキュアなデータベース１２４に記録される。
【００２３】
概略図１００は、システムがハードウェアリソース１１０の特定のアップグレードと互換性を有するか否かについての判断を行う方法を示す。システムは、ハードウェアリソース１１０を単体で含んでも、搭載基板１１２を含んでもよく、さらにはハードウェアリソース１１０および搭載基板１１２に連結されうる他のコンポーネントを含んでもよい。ハードウェアリソースは、ＲＦによって、１２１に信号を与えるアンテナ１２０と通信を行い、ハードウェアリソース１１０は、ＲＦＩＤタグ１１４を通じて１１５に応答する。
【００２４】
一実施形態では、ＲＦＩＤタグ１１４は、完全にパッシブであるが、ＲＦＩＤアンテナ１１８とともに、ハードウェアリソース１１０と通信し、クロック速度等の性能特性を再構成する機能を有する。一実施形態では、ＲＦＩＤタグ１１４がハードウェアリソース１１０をプログラミングしなおすのには外部からの援助が必要となり、つまり、ＲＦＩＤタグは、外部電池を利用するが、ハードウェアリソース１１０をプログラミングしなおすのに必要な全てのロジック駆動命令についてはＲＦ通信で十分である。ハードウェアリソース１１０がシステムに設けられる一実施形態では、システムを再構成する電力は、２ピンＤＣ電力等のシリアルバス１１６を通じてシステムから取り出される。
【００２５】
一実施形態では、アップグレードは、ハードウェアリソース１１０による利用が意図されていた現在のソフトウェアファームウェアマイクロコードをアップグレードする最新のソフトウェア－ファームウェアに準じるマイクロコードのバージョンである。一実施形態では、アップグレードは、ハードウェアリソース１１０が処理機能を有しているが、ハードウェアリソース１１０の販売時点または販売を提供された時点では商業的に利用可能ではなかったソフトウェアアプリケーションをサポートする新たな構成設定である。一実施

形態では、アップグレードは、ハードウェアリソース１１０が処理機能を有するが、ハードウェア１１０の販売時点または販売を提供された時点ではまだハードウェアリソース１１０に組み込まれていなかった新たなソフトウェアアプリケーションである。

【００２６】

一実施形態では、ＲＦプログラミングにより、セキュアなデータベース１２４との通信前のハードウェアリソース１１０の第１の機能と比較して向上しているハードウェアリソース１１０の第２の機能のリリース（unleash）を行う。

【００２７】

一実施形態では、ハードウェアリソース１１０のＲＦプログラミングは、ＲＦＩＤタグ１１４によって、アンテナ１２０以外のいかなる外部電力要件をも必要とせずに行われる。この結果、ＲＦプログラミングは、ハードウェアリソース１１０が、出荷用のパッケージング後等に、統括可能なデータ（line-of sight data）が曖昧になってしまった場合であっても、ＲＦＩＤタグ１１４により行うことができるようになる。この結果、ハードウェアリソース１１０のＵＬＴデータおよび性能データに対する識別、および、ハードウェアリソース１１０のプログラミングの両方が、プラグインシステムからのような外部電力ピンを必要とせずに実行可能となる。

【００２８】

一実施形態では、ハードウェアリソース１１０を含むようなシステムは、ＲＦＩＤタグ１１４が固有の適格な識別子を有することを識別および検証することにより、アップグレードと互換性があるか否かを決定することができる。システムが互換性を有する場合には、方法の実施形態は、ＲＦＩＤタグ１１４と通信することにより、ハードウェアリソース１１０を、遠隔データベース１２４に対して認証することを含む。ハードウェアリソース１１０が商品としてパッケージングされた場合、ＲＦＩＤタグ１１４によりシステムがハードウェアリソース１１０にアップグレード可能か否かを確認することができるので、統括可能な識別子は不要である。この結果、ＲＦ命令は、ＲＦＩＤタグ１１４において、コンピューティングシステム１２２等の遠隔システムから受信され、２次元（２Ｄ）レーザ印（laser inscription）等の統括可能な識別子は不要である。

【００２９】

一実施形態では、ハードウェアリソース１１０はダウンビンされて潜在的なベンダへ試供品サンプルとして送信されている。ハードウェアリソース１１０は、送信される前に、任意の回数起動を追跡するトライアルカウンタとともにプログラミングされ、この任意の回数を過ぎると、任意のビンレベルにおいてロックされ、それ以後は、セキュアなデータベース１２４からの更新ライセンスを受信しなければ利用または計測ができないようになる（つまり、特定のｎ分間隔で再起動するということである）。追跡への利用の別の方法は、ハードウェアリソースが動作モードにある全時間であり、この後にハードウェアリソースのアップビン、ダウンビン、またはロックを行うものである。一実施形態では、同意された試供品サンプルの利用量に達した後、ハードウェアリソースは元の構成に戻る。一実施形態においては、同意された利用量の後のアップビンまたはダウンビン等のプログラミングは、ハードウェアリソース１１０によりタグ１１４でライセンスの制御ロジック認証後（control logic post authentication of the license）でヒューズを焼き切る（permanently burning a fuse）ことにより行うことができる。

【００３０】

一実施形態では、任意の回数の起動をした後には、ハードウェアは自動的にアップビンまたはダウンビンを行い、潜在的なベンダに通知する。この実施形態の結果、潜在的なベンダは、ハードウェアリソースがアップビンおよびダウンビンのいずれか１つを行い、複数ではなくて単一の試供品サンプルを利用する機能しかないことから、より少ない数のサンプルを受け取ることになる。一実施形態では、アップビンまたはダウンビンおよび通知の結果、潜在的なベンダはハードウェアリソースのサンプルの継続または購入のライセンスを受け取ることとなる。

【００３１】

ハードウェアリソース１１０のプログラミングおよび再構成は、複数の場所で、複数の製造段階、組み立て、テスト、出荷、プレセールス、ポストセールスを始めとする複数の段階において行うことができる。

【００３２】

＜Ｆａｂ段階におけるプログラミング＞　Ｆａｂ段階におけるプログラミングは、さらに、組み立ておよびテスト段階のプログラミングを含むことができる。一実施形態では、出荷ロットをパッケージングして、組み立て、テスト段階へと移す。組み立て、テスト段階に到達すると、出荷を各ＲＦＩＤタグによりＲＦ調査する。

【００３３】

一実施形態では、組み立ておよびテスト段階で、ハードウェアリソース１１０の性能が期待より大幅に下回ることが明らかとなることもある。この結果、このハードウェアリソース１１０を封じ込めるために回収する。一実施形態では、組み立ておよびテスト段階で、ハードウェアリソース１１０の性能が期待より大幅に上回ることが明らかとなることもある。この結果、このハードウェアリソース１１０を、製造プロセスを微調整するために共通性分析調査をする目的から回収する。

【００３４】

ハードウェアリソース１１０がひとたび任意の搭載基板１１２と対にされてテストされると、ハードウェアリソース１１０のＵＬＴデータを、ハードウェアリソース１１０、搭載基板１１２、およびタグ１１４の固有ＩＤ間の相乗作用を含むように書き直す。ＵＬＴ－２データはセキュアなデータベース１２４に記録される。ハードウェアリソース１１０のソケット付けおよびプログラミングといった時間のかかる動作を避けるべく、ＲＦプログラミングは、必要に応じて一括して、または、個々に行われる。一例では、あるハードウェアリソース１１０は２．０ＧＨｚのクロック速度を必要とするが、このハードウェアリソース１１０がある搭載基板１１２と対になった場合には、２．４ＧＨｚで動作する。ハードウェアリソースは、ＲＦによって、１２１に信号を与えるアンテナ１２０と通信を行い、ハードウェアリソース１１０は１１５に応答する。本実施形態におけるＲＦプログラミングは、ハードウェアリソース１１０を再ヒューズして、２．４ＧＨｚから販売契約を満たす目的から必要となる２．０ＧＨｚにダウンビンすることを含む。ダウンビンは、セキュアなデータベース１２４に対して、ＲＦＩＤタグ１１４を通じて記録される。

【００３５】

＜倉庫格納段階のプログラミング＞　倉庫格納段階のプログラミングは、倉庫に到着したとき以降に実行されるものであってよい。一実施形態では、各々がＲＦＩＤタグをセキュアなデータベースへのアクセスを有するものとして含むハードウェアリソースの出荷ロットが受信され、ＲＦベースの出荷の調査を実行して、意図された出荷が到達したときに各ユニットを認証する。

【００３６】

図２ａは、一実施形態における方法の概略図２００である。ハードウェアリソースのアレイを、搭載基板上に設けられたものとして示しており、そのうち１つのハードウェアリソースを参照番号２１０で示している。このアレイは、１２個のハードウェアリソースとして示され、２ｘ６個のテーブルがアレイに隣接して設けられ、それぞれＵＬＴと性能レジスタを表し、その１つがハードウェアリソース２１０に対応しており参照番号２１１で示されている。示されているハードウェアリソース２１０は、非制限的な実施形態において２．４ＧＨｚクロック速度にビン分割される。ビン分割は、デバイスの結果に相関する有用な履歴を有する処理系譜パラメータに基づいて行うこともできる。

【００３７】

図２ａでは、アンテナ２２０を利用して１２個全てのハードウェアリソース２１０と同時通信が行われる。一実施形態では、１２個のハードウェアリソース２１０を製造後の倉庫に配置し、処理し、それぞれ搭載基板と組み立て、テストし、ビン分割し、出荷ロットとして構成する。セキュアなデータベースと全ハードウェアリソースとの間の、ＲＦＩＤタグそれぞれを介した通信は、マルチプレックス（ＭＵＸ）通信により行われる。一実施

形態では、ＭＵＸ通信により、通信は任意のハードウェアリソースにフォーカスしてバッチ通信を行う。

【００３８】

最初の最良性能データは、性能パラメータをクエリして、それらをセキュアなデータベースに記録することにより構築された。第１のサブアレイ２２６ａは、２．４ＧＨｚのクロック速度を有するよう（８ユニットに）ビン分割され、第２のサブアレイ２２８ａは、２．０ＧＨｚのクロック速度を有するよう（２ユニットに）ビン分割され、第３のサブアレイは、１．８ＧＨｚのクロック速度を有するよう（２ユニットに）ビン分割された。他の性能パラメータも、別のビン分割に利用することができ、複雑なビン分割がクロック速度の第１のビン分割と、電力消費または処理条件等の一部の他のパラメータについては第１のビン分割より低いクロック速度を含むことができる。

【００３９】

アンテナ２２０は、図１に示すコンピューティングシステム１２２等のコンピューティングシステムに接続され、コンピューティングシステムはさらに、これも図１に示されているセキュアなデータベース１２４等の遠隔データベースとも通信状態にある。ＲＦＩＤタグ２１４は、ハードウェアリソース２１０とは別個のコンポーネントとして示されているが、一実施形態においてはハードウェアリソースと一体的に設けられてもよい。

【００４０】

一実施形態では、ハードウェアリソース２１０の１２個のユニットアレイが、セキュアなデータベースから遠隔の倉庫にあり、ハードウェアリソース２１０からセキュアなデータベースへの遠隔通信を利用して、各コンポーネントの認証が行われ、システムのいずれか１つがアップグレードに互換性を有しているか否かを判断する。

【００４１】

一実施形態では、現存している（extant）２．４ＧＨｚのハードウェアリソースのＲＦ調査を、各ＲＦＩＤタグと通信することにより行う。サブアレイ２２６ａの各ハードウェアリソースは、これに対して肯定的な応答を返すが、サブアレイ２２６ａおよび２２６ｃの各ハードウェアリソースは否定的な応答を返す。この方法の実施形態は、特定の量のハードウェアリソースが必要であり、倉庫のロットをＲＦ調査して、適格なハードウェアリソースを任意のソフトウェアまたはアプリケーションに整合させるときに実行されてよい。これら実施形態では、図２ａに示す第１のプログラミングを第１のプログラミングと称し、図２ｂおよび図２ｃに示す反復プログラミングを、「第２のプログラミング」、「後続のプログラミング」等と称する場合がある。

【００４２】

＜出荷段階のプログラミング＞　図２ｂは、一つの方法実施形態におけるさらなるイベントの後の図２ａに示す方法の概略図２０１である。一つの方法実施形態においては、購入者が１２個のユニットを注文したが、市場パラメータは、１２個のユニットのアレイ（図２ａ）のシステムのうち２つのみが２．４ＧＨｚクロック速度を有する必要があると定めている。この結果、最大２．４ＧＨｚの第１のサブアレイ２２６ａのハードウェアリソースのうち６つが、それらの最大クロック速度が購入者にとっては不要ということであるから、それぞれのＲＦＩＤタグによる通信によりダウンビンされた。この結果、ハードウェアリソース２１０は２．４ＧＨｚクロック速度２１１と評価されたにも関わらず（図２ａ）、ＲＦＩＤタグそれぞれによる通信により２．０ＧＨｚにダウンビンされた（図２ｂ）。同様にして、購入者の注文では、クロック速度１．８ＧＨｚのユニットが４つ含まれ、つまり、図２ａでクロック速度が２．０ＧＨｚのユニットのうち２つがクロック速度１．８ＧＨｚにダウンビンされている。

【００４３】

ダウンビン処理では、ダウンビンイベントをＲＦプログラミングにより行うが、ＲＦプログラミングでは、１２個のユニットのアレイを、統括可能な識別子を必要とせずに、それぞれのＲＦＩＤタグによる通信によりプログラミングすることができる。このようなシナリオは、アレイが既にパッケージングされており、各システムが視覚的に曖昧になって

いる場合に生じうる。同様にダウンビン処理におけるダウンビンイベントは、物理的に各ユニットをプログラミングソケットにプラグインする、という、はるかに遅い連続処理ではなくて、ＲＦプログラミングにより同時に（または少なくとも並行処理で）行われる。

【００４４】

一実施形態では、１２個のユニットのアレイを図２ｂに示すようにダウンビンして、アレイを商品ロットとして出荷する。一実施形態における出荷の前に、さらに各ユニットをＲＦプログラミングによりロックして、正当な購入者により受信された場合、各ＲＦＩＤタグの各固有の暗号化識別子の認識および認証のみによりアンロックされるようにしておく。一実施形態で、出荷ロットが、紛失、宛先違い、盗難のいずれかの事態に遭遇したとする。このロットの各ハードウェアリソースは、ロックされており、固有暗号化識別子が個々のＲＦＩＤタグによってアクセス可能であるが、各ハードウェアリソースの起動は、無理ではないにしても難しい。これは、セキュアなデータベースからの各ハードウェアリソースの識別および認証が、各ＲＦＩＤタグにより通信されたものであるからである。

【００４５】

購入者が例えば、元の機器製造業者（ＯＥＭ）である場合、このＯＥＭは各ＲＦＩＤタグに記録されており、各ハードウェアリソースは出荷前のロック等によりディセーブルされている。この開示においては、「ＯＥＭ」は、ハードウェアリソースを含むシステム上でも動作するポストセールス実体のことであってもよく、公に向けて販売を行っても行わなくてもよい。ＯＥＭに渡されると、方法の実施形態は、ＯＥＭに、各ハードウェアリソースが該ＯＥＭ向けのものかを判断させる。ハードウェアリソースがこのＯＥＭ宛であった場合、ＯＥＭは、それぞれのＲＦＩＤタグにより各ユニットと通信を行い、さらなる組み立て用のハードウェアリソースをアンロックすることができる。

【００４６】

＜販売時点でのプログラミング＞　図２ｃは、一実施形態におけるさらなるイベントの後の図２ｂに示す実施形態の概略図２０２である。購入者が１２個のユニットのロットを受け取ると、アンテナ２２０（および添付されているコンピューティングシステム）を利用して、ロット内にＯＥＭ向けの任意のハードウェアリソースが存在するか否かをＯＥＭに判断させる。これは、ロット内の複数のＲＦＩＤタグをＲＦポーリングすることによりロットの各ハードウェアリソースをクエリして、添付されているＲＦＩＤタグにキャッシュされている各固有暗号化識別子を認識することにより行われる。

【００４７】

ロットの任意のハードウェアリソースの宛先が間違っていた実施形態では、識別および認証が失敗し、ハードウェアリソースはロックされたままとなり、製造者に戻すしか方策がなくなる。

【００４８】

一実施形態では、市場パラメータに基づいて販売または評価契約がＯＥＭとの間で構築されており、図２ａおよび図２ｂに示したダウンビンイベントが行われている。

【００４９】

ハードウェアリソースロットをさらに処理する前に、少なくとも１つの市場パラメータの変更を観察する。市場パラメータの変更は、一実施形態におけるマーケティング技法であってよく、ここではサプライヤが一定の値引きでシステムの一部または全てをアップビンする申し出を行う。市場パラメータの変更は、例えば以前のマーケティングの見通しとは異なるハードウェアリソース機能のニーズが観察された等のＯＥＭの販売期待の変更であってよい。一実施形態において、市場パラメータの変更は、よりアップビンされたハードウェアリソースを活用することのできるソフトウェアアプリケーションのアップグレードが利用可能になった事であってもよい。一実施形態において、市場パラメータの変更は、よりアップビンされたハードウェアリソースを活用することのできる新たなソフトウェアアプリケーションが利用可能になった事であってもよい。一実施形態において、市場パラメータの変更は、よりアップビンされたハードウェアリソースを活用することのできるアップグレードされたチップセットアプリケーションが利用可能になった事であってもよ

い。一実施形態において、市場パラメータの変更は、よりアップビンされたハードウェアリソースを活用することのできる完全に新しいチップセット構成が利用可能になった事であってもよい。

【００５０】

いずれの場合においても、市場パラメータに１つでも変更が観察された場合には、ＯＥＭは、セキュアなデータベースと通信して、契約を修正する目的でダウンビンまたはアップビンのいずれか１つを申し出る。

【００５１】

図２ｃは、少なくとも１つの市場パラメータの変更に対する応答等の例示的な実施形態を示す。図２ｂの２２６ｂの２つのハードウェアリソースのみが２．４ＧＨｚで構成されていた場合、新たなライセンスを受け取るＯＥＭにより２２６ｃの４つのハードウェアリソースのネットをこのクロック速度でイネーブルした。２２８ｂの６つのハードウェアリソースが２．０ＧＨｚで構成されていた場合、２２８ｃの５つのハードウェアリソースのネットをこのクロック速度でイネーブルした。２３０ｂの４つのハードウェアリソースが１．８ＧＨｚで構成されていた場合、２３０ｃの３つのハードウェアリソースのネットをこのクロック速度でイネーブルした。

【００５２】

再度図１を参照する。第１の例示的な実施形態では、ハードウェアリソース１１０は、商用ベンダから販売時点に取り除かれたシステムの一部である。キャッシュレジスタにおいて、または商用ベンダの制御内の一部の適切な位置において、購入者は、システムが任意の価格で現在の構成よりも向上したハードウェアリソース１１０の第２の機能をリリースすることができる旨を伝えられる。購入者がこの申し出に同意する場合、ＲＦドングル１２０を利用して、ＲＦＩＤタグ１１４によりハードウェアリソース１１０に通信する。システムがアップグレードに互換性を有するか否かを、ＲＦ通信により判断する。これは、遠隔データベースが販売時点の場所とは離れた場所にある場合、電話によって遠隔データベース１２４にアクセスすることで行われる。ハードウェアリソース１１０は遠隔データベース１２４に対して認証され、遠隔データベース１２４のオーナおよび購入者からライセンスが与えられ、ハードウェアリソース１１０はこのライセンスを、電源投入されるとシリアルバス１１６を用いて受信して、ＲＦＩＤタグ１１４に格納されたこのライセンスを認証してハードウェアリソース１１０をアップグレードする。これにより、商品パッケージからハードウェアリソース１１０を取り出す必要もなくＲＦ命令に基づいてプログラミングを行うことができる。この結果一実施形態では、内部バッテリを含むハードラインの電源からハードウェアリソース１１０に電源投入することなく、ＲＦプログラミングを行うことができる。

【００５３】

第２の例示的な実施形態では、システムが内部バッテリを起動してハードウェアリソース１１０に電源投入して第２の機能をリリースする点以外は、第１の例示的な実施形態と同じ方法が利用される。

【００５４】

第３の例示的な実施形態では、限られた時間だけアップグレードを申し出、受け付ける点以外は、第１の例示的な実施形態と同じ方法が利用される。

【００５５】

一実施形態では、任意のハードウェアリソース１１０に性能異常等の問題が生じているとする。例えば性能異常が標準を下回るイベントである場合には、特定のハードウェアリソース１１０を要求して、標準を下回るイベントをこの特定のハードウェアリソース１１０または同様のハードウェアリソース用に修理することが可能であるか否かを判断するべく調査する目的から回収して取り出すことができる。

【００５６】

例えば性能異常が驚くほど良い方向に標準を超えている場合、特定のハードウェアリソース１１０を要求して、標準を超える振る舞いを将来製造する同様のハードウェアリソー

スで再現することが可能であるか否かを判断するべく調査する目的から回収して取り出すことができる。

【００５７】

＜ポストセールスのプログラミング＞　ある例示的な実施形態で、スマートフォンに含まれるハードウェアリソースが販売の後も利用されてきており、このハードウェアリソースでより多くの機能を活用できるソフトウェアがとうとう利用可能となったとする。本実施形態では、スマートフォンのハードウェアリソースはダウンビンされており、それから一定時間が経過してから、アップビンされた再構成におけるハードウェアリソースを活用できるソフトウェアのアップグレード、または、新たなソフトウェアが開発された、とする。倉庫、組み立ておよびテストにおけるダウンビンは、第１のプログラミングと称され、このアップビンの実施形態におけるような反復プログラミングは後続のプログラミングと称される場合がある。

【００５８】

例えば、新たなソフトウェアが開発され、このソフトウェアは前にＯＥＭに販売されたハードウェアリソースの出荷ロットと相関しているとする。ユーザはこのハードウェアリソースを正当なベンダに持参してアップビンを要求することができる。ＲＦＩＤタグ１１４の認証が真である場合、ハードウェアリソースに関するＵＬＴおよび性能データをセキュアなデータベースと共有する。ハードウェアリソース１１０の再構成が許可される場合、ＲＦ命令をＲＦＩＤタグにより送受信することでプログラミングを行う。

【００５９】

プログラミングの結果、ＵＬＴデータが更新され、これは特定のプログラミングがハードウェアリソースおよび搭載基板の間の相乗作用に関するイベントとして記録されるだけではなく、セキュアなデータベースにも記録されることを意味する。

【００６０】

図３は、例示的な実施形態における搭載基板３００の立面断面図である。搭載基板３００は、中間層誘電体材料３３２を含む複数の層に埋め込まれるコア３１２およびＲＦアンテナ３１８を含む。ＲＦアンテナ３１８は、禁止ゾーン（ＫＯＺ）３３４に設けられる。示される実施形態では、ＫＯＺ３３４は２５０マイクロメートル（μｍ）のバッファを端部に含み、この端部と対向しＲＦアンテナ３１８と隣接した箇所に１５０μｍのバッファを含む。一実施形態では、ＲＦアンテナ３１８は図示のように２５０μｍである。一実施形態では、ＲＦアンテナ３１８はＺ方向の厚みが約２００μｍである。

【００６１】

一実施形態における複数の金属化層を３３６、３３８、３４０、３４２、および３４４で示す。さらに、はんだマスク３４６が搭載基板の上面に示されている。

【００６２】

一実施形態では、ＲＦＩＤタグ３１４は、はんだマスク３４６上に設けられ、ＲＦアンテナ３１８への電気的連通が複数の金属化層のいずれかまたは全てを通じて連結されている。同様に、ハードウェアリソース３１０が、はんだマスク３４６の上面の搭載基板３００にも設けられている。

【００６３】

一実施形態では、ＲＦＩＤタグが、コア３１２が占有する空間の一部を占有する等の形態で搭載基板３００内に設けられている。この結果、ＲＦＩＤタグ（コア空間３１２の一部）およびＲＦアンテナが、搭載基板３００の内部構造と一体的に設けられる。同様の構造がコア３１２から負のＺ方向にも反映されている。

【００６４】

図４は、例示的な実施形態における方法４００のフロー図である。方法４００は、対象システムのハードウェアリソースのアップビンまたはダウンビンに利用される。

【００６５】

４０５で、方法４００は対象システムと、システムに含まれるＲＦＩＤタグを利用してＲＦ通信を行うことを含む。例えば、ＯＥＭの遠隔サーバ、再販業者等は、対象システム

と、ハードウェアリソースに連結されたＲＦＩＤタグをクエリすることで通信する。様々な実施形態では、通信はシステムのユーザに対してトランスペアレントであってよい。一実施形態では、遠隔サーバは、対象システムの構成に関する情報を要求して、対象システムのハードウェアリソースがアップビンまたはダウンビン可能であるか否かを判断することができる。

【００６６】

４１０で、対象システムのアップビンまたはダウンビンについて証明を行う。様々な実施形態では、遠隔サーバの要求に応じて、サポートされている構成ＵＬＴテーブルの情報を遠隔サーバに通信する。遠隔サーバと対象システムとの間のこの通信もエンドユーザに対してトランスペアレントであってよい。遠隔サーバは、対象システムのアップビンまたはダウンビンについて証明されていないと判断する。証明されていない場合には、方法４００が終了する。

【００６７】

４１５で、対象システムがアップビンまたはダウンビンについて証明されている場合には、次に、ハードウェアリソースの受信者がシステムのアップビンまたはダウンビンを望んでいるかどうかを判断することができる。システムのアップビンまたはダウンビンを望んでいるかどうかの判断方法には様々なものが存在しうるが、多くの実施形態では、遠隔サーバから対象システムにメッセージを送る方法が採用されうる。メッセージは、例えばポップアップまたは他のメッセージブロックによりアップビンまたはダウンビンの利用可能性を示すことで、対象システムにおける表示が可能である。ハードウェアリソースの受信者がアップビンまたはダウンビンを望まない場合、方法４００を終了する。

【００６８】

４２０で、ハードウェアリソースの保持者がアップビンまたはダウンビンを望む場合、対象システムは遠隔サーバから暗号化ライセンスを取得することができる。様々な実施形態では、暗号鍵は、対象システムおよび／またはシステムの特定のハードウェアリソース（例えばプロセッサまたはチップセット）を識別する固有コードである。暗号鍵を送信するとき、遠隔サーバはこのハードウェアリソースに固有のＵＬＴ記録にアクセスする。

【００６９】

遠隔サーバは暗号鍵を用いて、アップビンまたはダウンビンを可能とさせる暗号化命令を生成する。例えば、遠隔サーバは、マイクロコード命令を生成して、オプションとして命令に対する不正アクセスを防止する命令を暗号化する。マイクロコード命令は、対象システムが１以上のハードウェアコンポーネントを正しくプログラミングして動作を行うフィーチャ（１または複数）をネーブルする用途に利用する。遠隔システムはさらに、アップビンまたはダウンビンが成功したことを確認し、対象システムがコードを実行して所望のフィーチャを実装してよい旨を伝えるために、対象システムへ送信するための確認命令を生成することができる。

【００７０】

４２５で、遠隔サーバはこのように暗号化されたアップビンまたはダウンビン命令を対象システムに送信する。

【００７１】

４３０で、対象システムは、暗号化命令に対応する復号鍵でアップビンまたはダウンビン命令を復号化して、対象システムをプログラミングする。非制限的な例示的実施形態では、復号化マイクロコード命令を利用して、セキュリティ違反にあまり抵触することなくセキュアにアップビンまたはダウンビンを行う。言い換えると、マイクロコード命令を復号化して直接プロセッサコアに送り、ここでマイクロコード命令を内部で実行してプログラミングを開始する。送信された命令はこれら実施形態ではマイクロコードでありうるので、命令の不正抽出能力、または、命令を不正な者に提供するといったことは大幅に低減する。

【００７２】

一部の実施形態では、マイクロコード命令はプロセッサにより実行され、フィーチャを

アップグレードするプログラミングを開始する。例えば一部の実施形態で、マイクロコード命令はプロセッサまたは他のハードウェアコンポーネント内で動的ヒューズプログラミングロジックを開始して、１以上のヒューズを開き、以前利用不可能であった回路への経路をイネーブルする。これら実施形態では、動的ヒューズプログラミングロジックにより、ソース電圧がヒューズバンク等に供給されて、選択されたヒューズをイネーブルにすることができる。ヒューズのイネーブルに成功すると、フィーチャを行う回路への経路を形成する。

【００７３】

４３５で、フィーチャをイネーブルするべくコンポーネントをプログラミングした後で、アップビンまたはダウンビンが成功したか否かを判断する。様々な実施形態では、遠隔サーバが送信したコードを利用して、イネーブルされたフィーチャの動作を検証することができる。例えば一実施形態では、確認コードをマイクロコード命令とともに送信する。プログラミングが完了すると、対象システムは確認コードを実行する。確認コードは新たにイネーブルされた回路を動かして、意図した用途での動作が可能であるかを検証し、より詳しくは、対象システムの特定の構成での動作が可能かを検証する。

【００７４】

４３５で、アップビンまたはダウンビンが不成功であったと判断される場合、制御はブロック４４０へ渡され、ここでエラー処理プロシージャが行われる。様々な実施形態では、エラー処理コードを対象システム上に実装することで、エラーを処理することができる。一部の実施形態では、エラー処理プロシージャを遠隔のソースからダウンロードすることができる。４４５で、エラー処理コードを実行した後で、アップビンまたはダウンビン処理を再試行するか否かを決定する。例えば、エラー処理ルーチンによりエラーが訂正された場合には、アップビンまたはダウンビン処理を再試行することができる。アップビンまたはダウンビンを再試行する場合には、制御はブロック４３０に戻る。

【００７５】

４３５でアップビンまたはダウンビンが成功したと判断される場合、４５０でアップビンまたはダウンビンを遠隔サーバに報告する。詳しくは、サポートされている構成ＵＬＴテーブルからの情報を遠隔サーバに送って、アップビンまたはダウンビンが成功裏に完了したことを示す。サポートされている構成テーブルからの情報に加えて、対象システムを識別する情報も含めることで、遠隔サーバは適切な手段を講じることができる。

【００７６】

４６０で、例示的な実施形態では、遠隔サーバが、アップビンまたはダウンビン分の勘定書を対象システムに請求する。例えば企業のＩＴ部門は、遠隔サーバを実装するＯＥＭの勘定書を維持する。一実施形態では、アップグレードに対する支払いに異なる方法が利用される。例えば一実施形態では、個々のエンドユーザがクレジットカード情報を提供して、エンドユーザが求めたアップビンまたはダウンビンについての請求を認証する。

【００７７】

加えてアップビンまたはダウンビンについての支払いを受け取ると、遠隔サーバは、アップビンまたはダウンビンに関する情報（例えば対象システムの識別に関する情報、有効になったアップグレード、および、プラットフォーム、構成、画像等の対象システムに関する更なる情報等）を格納してよい。さらに図４の４７０で示すように、遠隔サーバは、中央データベースにアップビンまたはダウンビンの情報を通信する。

【００７８】

図５は、例示的な実施形態におけるシステムのブロック図である。示されている電子システム５００は、本開示で述べたセキュリティ暗号化されたＲＦＩＤタグ５８０の実施形態に連結された半導体デバイス等のハードウェアリソースを具体化することができる。一実施形態では、電子システム５００は、電子システム５００の様々なコンポーネントを電気的に連結するシステムバス５２０を含むコンピュータシステムである。システムバス５２０は、様々な実施形態において単一のバスまたは複数のバスの組み合わせいずれであってもよい。電子システム５００は、集積回路５１０に給電する電圧源５３０を含む。一部

の実施形態では、電圧源５３０は、システムバス５２０を介して集積回路５１０に電流を供給する。

【００７９】

一実施形態では、集積回路５１０はシステムバス５２０に電気的に連結されており、任意の１つの回路、または複数の回路の組み合わせを含む。一実施形態では、集積回路５１０は、任意の種類であってよいプロセッサ５１２を含む。本明細書では、プロセッサ５１２は、マイクロプロセッサ、マイクロコントローラ、グラフィックプロセッサ、デジタル信号プロセッサ、または他のプロセッサ等であってよいがこれらに限定はされない、任意の種類の回路であってよい。集積回路５１０に含まれうる他の種類の回路は、携帯電話機、ページャ、ポータブルコンピュータ、双方向ラジオ、および同様の電子システム等のワイヤレスデバイスで利用されるカスタム回路または特定用途向けＩＣ（ＡＳＩＣ）（例えば通信回路５１４）である。一実施形態では、プロセッサ５１０は、ＳＲＡＭ（エスラム）等のオンダイメモリ516を含む。一実施形態では、プロセッサ５１０は、プロセッサのキャッシュメモリであってよいｅＤＲＡＭ（埋め込みＤＲＡＭ）等の埋め込みオンダイメモリ５１６を含む。

【００８０】

一実施形態では、電子システム５００は、さらに、ＲＡＭの形態であるメインメモリ５４２、１以上のハードドライブ５４４、および／または、ディスク、ＣＤ，ＤＶＤ，フラッシュメモリ鍵、およびその他の公知の取り外し可能な媒体等の取り外し可能媒体５４６を処理する１以上のドライブ等の、特定のアプリケーションに適切な１以上のメモリ要素を含むことのできる外部メモリ５４０を含む。様々なメモリの機能には、セキュリティ暗号化されたＲＦＩＤタグの実施形態を有する半導体デバイスが含まれてよい。

【００８１】

一実施形態では、電子システム５００はさらに、ディスプレイデバイス５５０、オーディオ出力５６０を含む。一実施形態では、電子システム５００は、キーボード、マウス、トラックボール、ゲームコントローラ、マイクロフォン、音声認識デバイス、または情報を電子システム５００に入力する任意の他のデバイス等のコントローラ５７０を含む。

【００８２】

セキュリティ暗号化されたＲＦＩＤタグ５８０は、システムバス５２０に連結されてよく、ＲＦ通信５８１は、システム５００とセキュアなデータベースとの間で、ハードウェアリソース（１または複数）の識別、認証、アンロック、およびアップビンおよびダウンビンのいずれかといった目的に有効とすることができる。

【００８３】

本明細書では集積回路５１０は、本明細書での様々な実施形態および先行技術で認識されているそれらの均等物で述べられている、セキュリティ暗号化されたＲＦＩＤタグ、電子システム、コンピュータシステム等のハードウェアリソース、１以上の集積回路製造方法、セキュリティ暗号化されたＲＦＩＤタグを有する半導体デバイス等のハードウェアリソースを含む電子組み立ての１以上の製造方法等の、複数の異なる実施形態での実装が可能である。要素、材料、配置、寸法、および動作シーケンスは全て、セキュリティ暗号化されたＲＦＩＤタグの実施形態の特定のトランジスタ装置に適合するよう変更することができる。

【００８４】

これまでの説明から、ＲＦＩＤタグおよび認証をセキュアなデータベースに利用する複数の実施形態のソフトウェアコード命令を、ディスクドライブ等の従来のコンピュータ駆動媒体に記録することができ、これら命令を、コンピュータ駆動媒体からコードを読み出すことで実行可能であることは理解されるであろう。

【００８５】

本開示全体にわたって利用される「一実施形態（"one embodiment"）（"an embodiment"）」といった記載は、実施形態との関連で記載される特定の特徴、構造、または特性が、本発明の少なくとも１つの実施形態に含まれることを示している。「一実施形態では、

（"in one embodiment"）（"in an embodiment"）」といった言い回しが本開示の随所に見られるが、これらは必ずしも全てが同一の実施形態のことを表しているわけではない。さらに、特定の特徴、構造、また特性は、一以上の実施形態において適切に組み合わせることができる。

【００８６】

「上部（upper）」「下部（lower）」といった言い回しは、Ｘ－ＺまたはＹ－Ｚ座標に関する記載であることを理解されたく、「隣接した」といった言い回しは、示されているＸ－Ｙ座標に関する記載であることを理解されたい。例示した実施形態が逆方向または回転させられた方向といった様々な配向で示されても、依然としてこれら言い回しは関連する。

【００８７】

米国特許法施行規則３７Ｃ．Ｆ．Ｒセクション１．７２（ｂ）で要約が必要であると記載されていることから要約セクションを設けるが、これによって読み手は技術的な開示の本質および要点を迅速に理解することができる。しかしこれを請求項の範囲または意味を解釈する、あるいは限定する用途に利用するべきではないことを理解されたい。

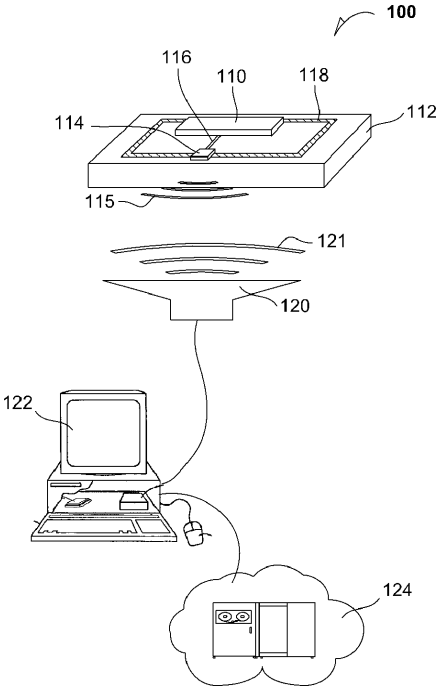
【００８８】

上記した詳細な記載においては、様々な特徴を単一の実施形態に一括りにすることで、開示を合理的に行っている。この開示方法を、本発明の請求されている実施形態が各請求項で明示されているものより多くの特徴を必要とすることを反映していると解釈されるべきではない。そうではなくて、以下の請求項が示すように、発明の主題は開示されている単一の実施形態の全ての特徴より少ないものの中に存在する。従って以下の請求項は詳細な記載に組み込まれ、各請求項は単独で一つの好適な実施形態を構成する。

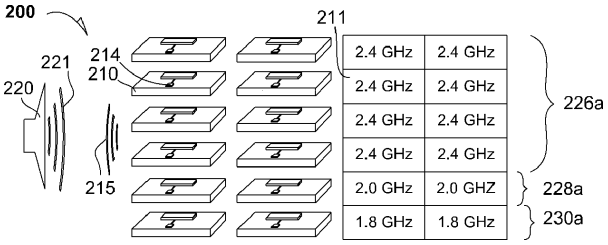
【００８９】

当業者であれば、本発明の本質を説明する目的で記載され図示された部分または方法の段階の詳細、材料および構成に関して、添付請求項が示す本発明の原理および範囲から逸脱せずに様々な他の変更を加えることができることを理解する。

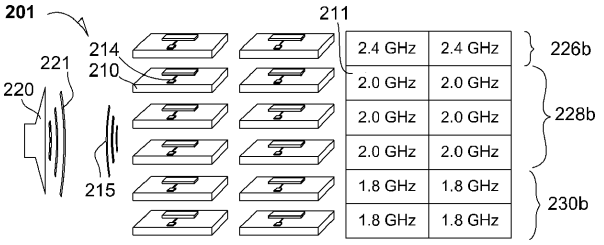
【図１】



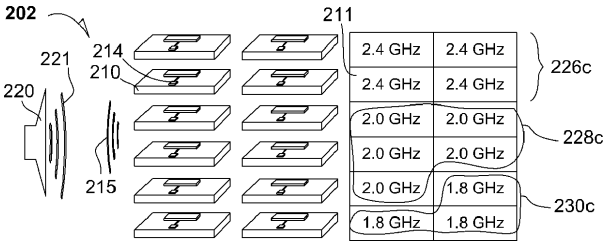
【図２ａ】



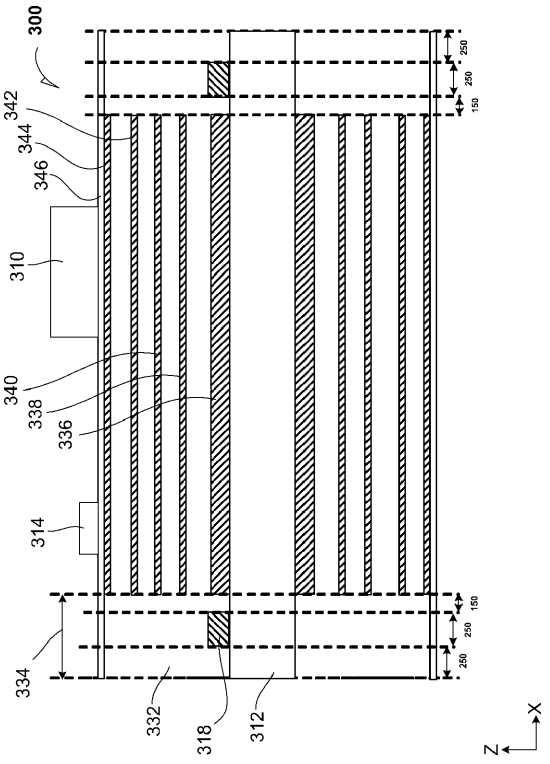
【図２ｂ】



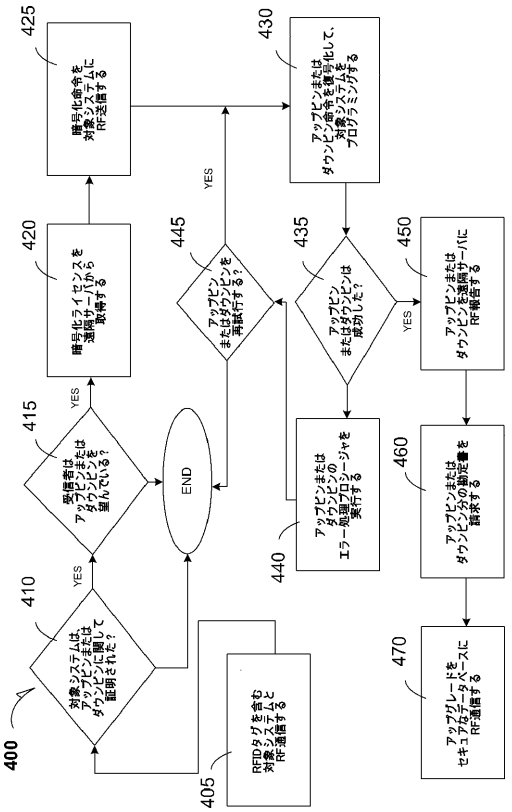
【図２ｃ】



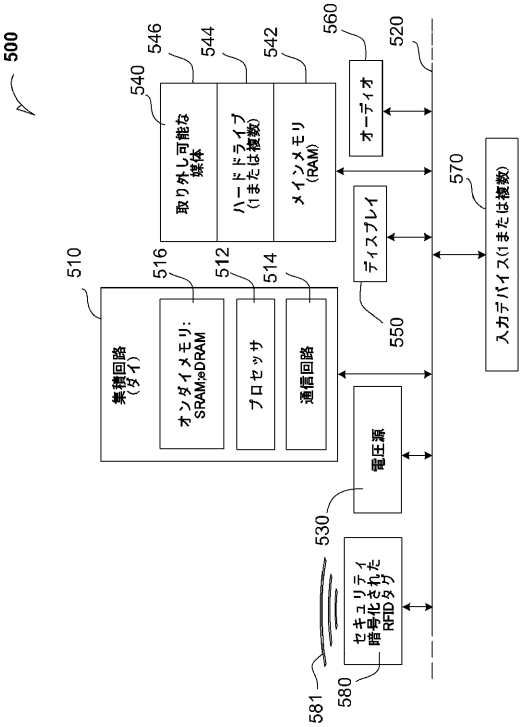
【図３】



【図４】



【図５】


500
540
546
544
542
560
520
取り外し可能な媒体
ハードドライブ（1または複数）
メインメモリ（RAM）
オーディオ
570
510
516
512
514
ディスプレイ
550
集積回路（ダイ）
オンダイメモリ：SRAMまたはDRAM
プロセッサ
通信回路
入力デバイス（1または複数）
電圧源
530
セキュリティ暗号化されたRFIDタグ
581
580

フロントページの続き

(51)Int.Cl. F I
G06F 9/445 (2006.01) G06K 19/00 Q
G06F 9/06 610A

(72)発明者 フィンテル、ジェームス スティーブン
アメリカ合衆国 95052 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・2200 インテル・コーポレーション内
(72)発明者 ダグラス、ジョナサン
アメリカ合衆国 95052 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・2200 インテル・コーポレーション内
(72)発明者 カービー、ウィリアム ジェイ.
アメリカ合衆国 95052 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・2200 インテル・コーポレーション内
(72)発明者 ゲイツ、ティム
アメリカ合衆国 95052 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・2200 インテル・コーポレーション内
(72)発明者 アベルス、ティム
アメリカ合衆国 95052 カリフォルニア州・サンタクララ・ミッション カレッジ ブーレバード・2200 インテル・コーポレーション内

審査官 木村 励

(56)参考文献 特表2008-500600（JP, A）
特開2001-043088（JP, A）
特開2007-025903（JP, A）
特開2008-257486（JP, A）
特開2008-129911（JP, A）
特表2008-535078（JP, A）
国際公開第2008/041978（WO, A1）
特表2004-508780（JP, A）
米国特許出願公開第2006/0035603（US, A1）
特開2005-011008（JP, A）

(58)調査した分野(Int.Cl., DB名)
G06K 17/00
G06K 19/00 - 19/18
G06F 9/445
G06F 11/00
H01L 21/02