

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2008-516310

(P2008-516310A)

(43) 公表日 平成20年5月15日(2008.5.15)

(51) Int.Cl.	F I	テーマコード (参考)
<b>G06F 17/50 (2006.01)</b>	G06F 17/50 654K	5B017
<b>G06F 21/24 (2006.01)</b>	G06F 12/14 520D	5B046
<b>H04L 9/32 (2006.01)</b>	G06F 12/14 530C	5J104
	G06F 12/14 540A	
	G06F 12/14 520F	
審査請求 未請求 予備審査請求 未請求 (全 30 頁) 最終頁に続く		

(21) 出願番号 特願2007-534713 (P2007-534713)  
 (86) (22) 出願日 平成17年9月28日 (2005. 9. 28)  
 (85) 翻訳文提出日 平成19年5月25日 (2007. 5. 25)  
 (86) 国際出願番号 PCT/US2005/034637  
 (87) 国際公開番号 W02006/039286  
 (87) 国際公開日 平成18年4月13日 (2006. 4. 13)  
 (31) 優先権主張番号 10/956, 327  
 (32) 優先日 平成16年9月30日 (2004. 9. 30)  
 (33) 優先権主張国 米国 (US)

(71) 出願人 507103503  
 シンプリシティ インコーポレイテッド  
 アメリカ合衆国 カリフォルニア州 94  
 086 サニーヴェイル ウェスト カリ  
 フォルニア ストリート 600  
 (74) 代理人 100082005  
 弁理士 熊倉 禎男  
 (74) 代理人 100067013  
 弁理士 大塚 文昭  
 (74) 代理人 100086771  
 弁理士 西島 孝喜  
 (74) 代理人 100109070  
 弁理士 須田 洋之

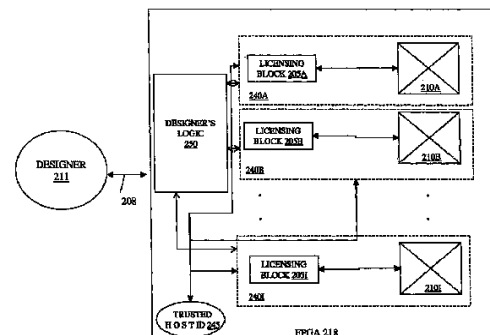
最終頁に続く

(54) 【発明の名称】 ホスト識別子を使用するプログラマブルハードウェアサブデザインのライセンス交付のための機器及び方法

## (57) 【要約】

【課題】 特定のハードウェア設計に関わる複数の当事者間のライセンス交付契約の条項を実行するためのハードウェア技術を提供する。

【解決手段】 ハードウェア技術の使用による特定のハードウェアデザインに関わる複数の当事者間のライセンス交付契約の条項を実行する方法及び機器。一実施形態によれば、ハードウェアサブデザインは、暗号化によってユーザによる修正から保護されたライセンス検証サブデザインを含む。一実施形態では、ライセンスは、外部ハードウェア装置内の信頼できるホスト識別子に基づいて発生される。一実施形態では、各信頼できるホスト識別子は固有であり、同じ信頼できるホスト識別子を共有する集積回路は2つとない。別の実施形態では、集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路である。一実施形態では、ライセンスは、ハードウェアサブデザインが信頼できるホスト識別子を有する集積回路内で実施された時に、ハードウェアサブデザインがどのくらい長く作動することになるかを判断する。



**【特許請求の範囲】****【請求項 1】**

暗号化されたハードウェアサブデザインを発生させる方法であって、  
第 1 の設計者側で第 1 のハードウェアサブデザインを発生させる段階と、  
第 2 の設計者側で第 2 のハードウェアサブデザインを発生させる段階と、  
信頼できるホスト識別子を有する集積回路に前記第 1 のハードウェアサブデザイン及び  
前記第 2 のハードウェアサブデザインをアップロードする段階と、  
前記信頼できるホスト識別子に基づくライセンスを適用することによって前記第 2 のハ  
ードウェアサブデザインを使用可能にする段階と、  
を含むことを特徴とする方法。

10

**【請求項 2】**

前記第 2 のハードウェアサブデザインを発生させながら該第 2 のハードウェアサブデザ  
イン内でライセンス検証サブデザインを暗号化する段階を更に含むことを特徴とする請求  
項 1 に記載の方法。

**【請求項 3】**

前記ライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求  
項 1 に記載の方法。

**【請求項 4】**

前記ライセンスは、前記第 2 のハードウェアサブデザインがどのくらい長く作動するこ  
とになるかを判断することを特徴とする請求項 1 に記載の方法。

20

**【請求項 5】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とす  
る請求項 1 に記載の方法。

**【請求項 6】**

外部ハードウェア装置が、前記信頼できるホスト識別子を提供することを特徴とする請  
求項 1 に記載の方法。

**【請求項 7】**

デジタル処理システム上で実行された時に、  
第 1 の設計者側で第 1 のハードウェアサブデザインを発生させる段階と、  
第 2 の設計者側で第 2 のハードウェアサブデザインを発生させる段階と、  
信頼できるホスト識別子を有する集積回路に前記第 1 のハードウェアサブデザイン及び  
前記第 2 のハードウェアサブデザインをアップロードする段階と、  
前記信頼できるホスト識別子に基づくライセンスを適用することによって前記第 2 のハ  
ードウェアサブデザインを使用可能にする段階と、  
を含む暗号化されたハードウェアサブデザインを発生する方法を前記デジタル処理シス  
テムに実行させる複数の実行可能な命令を収容した機械可読媒体。

30

**【請求項 8】**

前記第 2 のハードウェアサブデザインを発生させる段階の間に該第 2 のハードウェアサ  
ブデザイン内でライセンス検証サブデザインを暗号化する段階を更に含むことを特徴とす  
る請求項 7 に記載の機械可読媒体。

40

**【請求項 9】**

前記ライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求  
項 7 に記載の機械可読媒体。

**【請求項 10】**

前記ライセンスは、前記第 2 のハードウェアサブデザインがどのくらい長く作動するこ  
とになるかを判断することを特徴とする請求項 7 に記載の機械可読媒体。

**【請求項 11】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とす  
る請求項 7 に記載の機械可読媒体。

**【請求項 12】**

50

外部ハードウェア装置が、前記信頼できるホスト識別子を提供することを特徴とする請求項 7 に記載の機械可読媒体。

【請求項 13】

暗号化されたハードウェアサブデザインを発生させるシステムであって、  
第 1 の設計者側で第 1 のハードウェアサブデザインを発生させるための手段と、  
第 2 の設計者側で第 2 のハードウェアサブデザインを発生させるための手段と、  
信頼できるホスト識別子を有する集積回路に前記第 1 のハードウェアサブデザイン及び  
前記第 2 のハードウェアサブデザインをアップロードするための手段と、  
前記信頼できるホスト識別子に基づくライセンスを適用することによって前記第 2 のハードウェアサブデザインを使用可能にするための手段と、  
を含むことを特徴とするシステム。

10

【請求項 14】

前記第 2 のハードウェアサブデザインを発生させながら該第 2 のハードウェアサブデザイン内でライセンス検証サブデザインを暗号化するための手段、  
を更に含むことを特徴とする請求項 13 に記載のシステム。

【請求項 15】

前記ライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 13 に記載のシステム。

【請求項 16】

前記ライセンスは、前記第 2 のハードウェアサブデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 13 に記載のシステム。

20

【請求項 17】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 13 に記載のシステム。

【請求項 18】

外部ハードウェア装置が、前記信頼できるホスト識別子を提供することを特徴とする請求項 13 に記載のシステム。

【請求項 19】

信頼できるホスト識別子を有する集積回路に暗号化された回路デザインをアップロードする段階と、  
信頼できるホスト識別子特定のライセンスに基づいて前記暗号化された回路デザインを使用可能にする段階と、  
を含むことを特徴とする方法。

30

【請求項 20】

前記信頼できるホスト識別子を有する前記集積回路に、暗号化されていない回路デザインをアップロードする段階、  
を更に含むことを特徴とする請求項 19 に記載の方法。

【請求項 21】

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 19 に記載の方法。

40

【請求項 22】

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 19 に記載の方法。

【請求項 23】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 19 に記載の方法。

【請求項 24】

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 19 に記載の方法。

50

**【請求項 25】**

デジタル処理システム上で実行された時に、  
暗号化された回路デザインを信頼できるホスト識別子を有する集積回路にアップロードする段階と、

信頼できるホスト識別子特定のライセンスに基づいて前記暗号化された回路デザインを使用可能にする段階と、

を含む方法を前記デジタル処理システムに実行させる複数の実行可能な命令を収容した機械可読媒体。

**【請求項 26】**

前記方法は、

暗号化されていない回路デザインを前記信頼できるホスト識別子を有する前記集積回路にアップロードする段階、

を更に含む、

ことを特徴とする請求項 25 に記載の機械可読媒体。

10

**【請求項 27】**

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 25 に記載の機械可読媒体。

**【請求項 28】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 25 に記載の機械可読媒体。

20

**【請求項 29】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 25 に記載の機械可読媒体。

**【請求項 30】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 25 に記載の機械可読媒体。

**【請求項 31】**

信頼できるホスト識別子を有する集積回路に暗号化された回路デザインをアップロードするための手段と、

30

信頼できるホスト識別子特定のライセンスに基づいて前記暗号化された回路デザインを使用可能にするための手段と、

を含むことを特徴とするシステム。

**【請求項 32】**

暗号化されていない回路デザインを前記信頼できるホスト識別子を有する前記集積回路にアップロードするための手段、

を更に含むことを特徴とする請求項 31 に記載のシステム。

**【請求項 33】**

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 31 に記載のシステム。

40

**【請求項 34】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 31 に記載のシステム。

**【請求項 35】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 31 に記載のシステム。

**【請求項 36】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 31 に記載のシステム。

50

## 【請求項 37】

信頼できるホスト識別子に基づいて集積回路内の知的財産に制約を加える方法であって

、

信頼できるホスト識別子を有する集積回路上で特定の量の時間に対してのみ実行することができるハードウェアサブデザインを使用可能にする該信頼できるホスト識別子特定のライセンスを発生させる段階、

を含むことを特徴とする方法。

## 【請求項 38】

前記信頼できるホスト識別子を有する前記集積回路に、前記ハードウェアサブデザインをライセンスを必要としない別のハードウェアサブデザインと共にアップロードする段階

10

、

を更に含むことを特徴とする請求項 37 に記載の方法。

## 【請求項 39】

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 37 に記載の方法。

## 【請求項 40】

前記信頼できるホスト識別子特定のライセンスは、前記ハードウェアサブデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 37 に記載の方法。

。

## 【請求項 41】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 37 に記載の方法。

20

## 【請求項 42】

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 37 に記載の方法。

## 【請求項 43】

デジタル処理システム上で実行された時に、

信頼できるホスト識別子を有する集積回路上で特定の量の時間に対してのみ実行することができるハードウェアサブデザインを使用可能にする該信頼できるホスト識別子特定のライセンスを発生させる段階、

30

を含む、信頼できるホスト識別子に基づいて集積回路内の知的財産に制約を加える方法を前記デジタル処理システムに実行させる複数の実行可能な命令を収容した機械可読媒体。

## 【請求項 44】

前記方法は、

前記信頼できるホスト識別子を有する前記集積回路に、前記ハードウェアサブデザインをライセンスを必要としない別のハードウェアサブデザインと共にアップロードする段階

、

を更に含む、

ことを特徴とする請求項 43 に記載の機械可読媒体。

40

## 【請求項 45】

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 43 に記載の機械可読媒体。

## 【請求項 46】

前記信頼できるホスト識別子特定のライセンスは、前記ハードウェアサブデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 43 に記載の機械可読媒体。

## 【請求項 47】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 43 に記載の機械可読媒体。

50

**【請求項 48】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 43 に記載の機械可読媒体。

**【請求項 49】**

信頼できるホスト識別子に基づいて集積回路内の知的財産に制約を加えるシステムであって、

信頼できるホスト識別子を有する集積回路上で特定の量の時間に対してのみ実行することが出来るハードウェアサブデザインを使用可能にする該信頼できるホスト識別子特定のライセンスを発生させるための手段、

を含むことを特徴とするシステム。

10

**【請求項 50】**

前記信頼できるホスト識別子を有する前記集積回路に、前記ハードウェアサブデザインをライセンスを必要としない別のハードウェアサブデザインと共にアップロードするための手段、

を更に含むことを特徴とする請求項 49 に記載のシステム。

**【請求項 51】**

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 49 に記載のシステム。

**【請求項 52】**

前記信頼できるホスト識別子特定のライセンスは、前記ハードウェアサブデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 49 に記載のシステム。

20

**【請求項 53】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 49 に記載のシステム。

**【請求項 54】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 49 に記載のシステム。

**【請求項 55】**

ユーザによって修正することができない信頼できるホスト識別子を有する集積回路を製造する段階、

30

を含むことを特徴とする方法。

**【請求項 56】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 55 に記載の方法。

**【請求項 57】**

前記集積回路は、暗号化されたライセンス検証サブデザインをハードウェアサブデザイン内に含むことを特徴とする請求項 55 に記載の方法。

**【請求項 58】**

デジタル処理システム上で実行された時に、

40

ユーザによって修正することができない信頼できるホスト識別子を有する集積回路を製造する段階、

を含む方法を前記デジタル処理システムに実行させる複数の実行可能な命令を収容した機械可読媒体。

**【請求項 59】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 58 に記載の機械可読媒体。

**【請求項 60】**

前記集積回路は、暗号化されたライセンス検証サブデザインをハードウェアサブデザイン内に含むことを特徴とする請求項 58 に記載の機械可読媒体。

50

**【請求項 6 1】**

ユーザによって修正することができない信頼できるホスト識別子を有する集積回路を製造するための手段、  
を含むことを特徴とするシステム。

**【請求項 6 2】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 6 1 に記載のシステム。

**【請求項 6 3】**

前記集積回路は、暗号化されたライセンス検証サブデザインをハードウェアサブデザイン内に含むことを特徴とする請求項 6 1 に記載のシステム。

10

**【請求項 6 4】**

信頼できるホスト識別子を有する集積回路であって、

第 1 の設計者によって信頼できるホスト識別子とは独立に使用可能にされた第 1 のハードウェアサブデザインと、

第 2 の設計者によって前記信頼できるホスト識別子に基づいて使用可能にされた第 2 のハードウェアサブデザインと、

を含むことを特徴とする集積回路。

**【請求項 6 5】**

前記第 2 のハードウェアサブデザインは、信頼できるホスト識別子の群に基づいて使用可能にされることを特徴とする請求項 6 4 に記載の集積回路。

20

**【請求項 6 6】**

前記第 2 のハードウェアサブデザイン内のライセンス検証サブデザインは、修正を防止するために暗号化されることを特徴とする請求項 6 4 に記載の集積回路。

**【請求項 6 7】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 6 4 に記載の集積回路。

**【請求項 6 8】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 6 4 に記載の集積回路。

**【請求項 6 9】**

信頼できるホスト識別子を有する集積回路内のロケーションであって、  
集積回路内の暗号化された回路デザインを使用可能にするライセンス交付ブロックと、  
前記暗号化された回路デザインがどのくらい長く作動することになるかを判断するクロック回路と、  
を含むことを特徴とするロケーション。

30

**【請求項 7 0】**

前記ライセンス交付ブロックは、信頼できるホスト識別子の群に基づいて前記暗号化された回路デザインの少なくとも一部分を使用可能にすることを特徴とする請求項 6 9 に記載のロケーション。

**【請求項 7 1】**

前記ライセンス交付ブロックは、前記暗号化された回路がどのくらい長く作動することになるかを判断することを特徴とする請求項 6 9 に記載のロケーション。

40

**【請求項 7 2】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 6 9 に記載のロケーション。

**【請求項 7 3】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 6 9 に記載のロケーション。

**【請求項 7 4】**

複数の集積回路 (IC) を設計する際に使用されるデジタル処理システムであって、

50

表示装置と、  
メモリと、

信頼できるホスト識別子を有する集積回路上でハードウェアサブデザインが特定の量の時間に対して作動することを可能にする信頼できるホスト識別子特定のライセンスを発生させる、前記メモリ及び前記表示装置に結合したプロセッサと、

を含むことを特徴とするシステム。

【請求項 75】

前記プロセッサは、前記信頼できるホスト識別子を有する前記集積回路に、前記ハードウェアサブデザインをライセンスを必要としない別のハードウェアサブデザインと共にアップロードするためのものであることを特徴とする請求項 74 に記載のデジタル処理システム。

10

【請求項 76】

前記信頼できるホスト識別子特定のライセンスは、信頼できるホスト識別子の群に基づいていることを特徴とする請求項 74 に記載のデジタル処理システム。

【請求項 77】

前記信頼できるホスト識別子特定のライセンスは、前記ハードウェアサブデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 74 に記載のデジタル処理システム。

【請求項 78】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 74 に記載のデジタル処理システム。

20

【請求項 79】

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 74 に記載のデジタル処理システム。

【請求項 80】

設計者側の方法であって、

第 1 のハードウェアデザインと、信頼できるホスト識別子を通じて第 2 のハードウェアデザインを使用可能にする第 2 の暗号化されたデザインとを合併する段階、

を含むことを特徴とする方法。

【請求項 81】

前記第 2 の暗号化されたデザインは、信頼できるホスト識別子の群に基づく信頼できるホスト識別子特定のライセンスを通じて使用可能にされることを特徴とする請求項 80 に記載の方法。

30

【請求項 82】

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 81 に記載の方法。

【請求項 83】

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 80 に記載の方法。

40

【請求項 84】

前記第 1 のハードウェアデザイン及び前記第 2 の暗号化されたデザインは、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路内に組み込まれていることを特徴とする請求項 80 に記載の方法。

【請求項 85】

IP ブロック所有者側の方法であって、

別の設計者によって集積回路内に組み込むための暗号化されたデザインを発生させる段階と、

前記集積回路の信頼できるホスト識別子部分に対するデータを許可する段階と、

を含むことを特徴とする方法。

50



**【請求項 8 6】**

前記暗号化されたデザインは、信頼できるホスト識別子の群に基づく信頼できるホスト識別子特定のライセンスを通じて使用可能にされることを特徴とする請求項 8 5 に記載の方法。

**【請求項 8 7】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化されたデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 8 6 に記載の方法。

**【請求項 8 8】**

前記集積回路は、該集積回路に対する固有の値である信頼できるホスト識別子を含むことを特徴とする請求項 8 5 に記載の方法。

**【請求項 8 9】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 8 5 に記載の方法。

**【請求項 9 0】**

信頼できるホスト識別子プロバイダ側の方法であって、  
設計者によって構成することができるプログラマブル・ゲート・アレイ又は特定用途向け集積回路を生成する段階と、  
信頼できるホスト識別子部分を前記プログラマブル・ゲート・アレイ又は前記特定用途向け集積回路に組み込む段階と、  
を含むことを特徴とする方法。

**【請求項 9 1】**

前記信頼できるホスト識別子部分は、暗号化されたライセンス検証サブデザインをハードウェアサブデザイン内に含むことを特徴とする請求項 9 0 に記載の方法。

**【請求項 9 2】**

前記信頼できるホスト識別子部分は、信頼できるホスト識別子の群に基づく信頼できるホスト識別子特定のライセンスを通じて使用可能にされることを特徴とする請求項 9 0 に記載の方法。

**【請求項 9 3】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化されたデザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 9 2 に記載の方法。

**【請求項 9 4】**

前記プログラマブル・ゲート・アレイ又は前記特定用途向け集積回路は、該プログラマブル・ゲート・アレイ又は該特定用途向け集積回路に対する固有の値である信頼できるホスト識別子を含むことを特徴とする請求項 9 0 に記載の方法。

**【請求項 9 5】**

設計者側の方法であって、  
IP ブロックの暗号化された部分によって使用されて該 IP ブロックの残りの部分を使用可能にする信頼できるホスト識別子を発生させる段階、  
を含み、  
前記信頼できるホスト識別子は、集積回路をプログラムするか又は製造する時にソフトウェアによって提供される、  
ことを特徴とする方法。

**【請求項 9 6】**

前記暗号化された部分は、信頼できるホスト識別子の群に基づく信頼できるホスト識別子特定のライセンスを通じて使用可能にされることを特徴とする請求項 9 5 に記載の方法。

**【請求項 9 7】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 9 6 に記載の方法。

10

20

30

40

50

**【請求項 98】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 95 に記載の方法。

**【請求項 99】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 95 に記載の方法。

**【請求項 100】**

IP ブロック所有者側の方法であって、

別の設計者によって集積回路内に組み込むために IP ブロックに関連した暗号化された回路デザインを発生させる段階と、

前記 IP ブロックを使用可能にするために、集積回路をプログラムするか又は製造する時にソフトウェアを通じて信頼できるホスト識別子を前記別の設計者に提供する段階と、を含むことを特徴とする方法。

**【請求項 101】**

前記暗号化された回路デザインは、信頼できるホスト識別子の群に基づく信頼できるホスト識別子特定のライセンスを通じて使用可能にされることを特徴とする請求項 100 に記載の方法。

**【請求項 102】**

前記信頼できるホスト識別子特定のライセンスは、前記暗号化された回路デザインがどのくらい長く作動することになるかを判断することを特徴とする請求項 101 に記載の方法。

**【請求項 103】**

前記信頼できるホスト識別子は、前記集積回路に対する固有の値であることを特徴とする請求項 100 に記載の方法。

**【請求項 104】**

前記集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路であることを特徴とする請求項 100 に記載の方法。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、一般的に、集積回路の設計の分野に関するものであり、より具体的には、特定のハードウェア設計に関わる複数の当事者間のライセンス交付契約の条項を実行するためのハードウェア技術に関する。

**【背景技術】****【0002】**

複合ハードウェアシステムの設計は、ゼロからの新しいハードウェアサブデザインの作成（例えば、専有ハードウェアデザインコード及びサポート文書の各部分）及び IP ブロック所有者によって準備されたハードウェアサブデザインの購入の組合せを伴っている。多くの場合、設計者は、社内的に特定のハードウェアサブデザインを開発するのではなく、ハードウェアサブデザインを IP ブロック所有者（例えば、ハードウェアサブデザインに対して知的財産権を有する組織／個人）から購入する。IP ブロック所有者は、彼の知的財産権のライセンス交付及び管理維持においていくつかの問題に直面している。最大の問題の 1 つは、使用毎ベースのハードウェアサブデザインの無断使用及びそれをライセンス交付する有効な方法の欠如である。残念ながら、FPGA（フィールド・プログラマブル・ゲート・アレイ）及び ASIC（特定用途向け集積回路）には、信頼されかつ固定した固有の識別子はなく、その結果、使用毎のベースでハードウェアサブデザインをライセンス交付することが容易にはできない（例えば、使用毎のライセンスには、特定のハードウェアサブデザインが実施されている全ての装置の課金が必要になり、信頼される固有の識別子がないために、特定のライセンスを特定の FPGA に固定することが困難になると考えられる）。代わりに、IP ブロック所有者は、多くの場合に、設計者がハードウェア

10

20

30

40

50

サブデザインの各使用に対して適正に計上してその支払いを行うと信頼しない限り（例えば、長期的に続くビジネス関係を通して）、グローバルな１回限りのライセンス（例えば、設計者側のいずれか及び全てのＦＰＧＡ上で特定のハードウェアサブデザインを使用するグローバルな１回限りのライセンス）を販売する必要がある。更に、ハードウェアサブデザインがどこでコピーされて適用されているかを追跡する方法がないために、業界内に窃盗が広がり蔓延している（例えば、ハードウェアサブデザインが販売された状態で、ＩＰブロック所有者は、特定のハードウェアサブデザインがＦＰＧＡ上で何回検索されたかをモニタかつ判断することができない）。従って、ＩＰブロック所有者は、ハードウェアサブデザインにおいて知的財産権を最大限利用することができず、かつ彼らのハードウェアサブデザインが最終的にどこで利用されているのかを管理することができない。

10

#### 【０００３】

図１Ａは、複数のＩＰブロック１１０Ａ～１１０Ｉを有するＦＰＧＡ１１８を示している。ＦＰＧＡ１１８は、バス１０８を通じて設計者１１１と結合される。設計者１１１（例えば、ハードウェアシステムを作成している個人又は会社）は、ハードウェアサブデザインをバス１０８を通じてＦＰＧＡ１１８に転送する（例えば、設計者１１１は、設計者１１１が以前作成した特定のハードウェアサブデザインを再利用することができ、特注デザインを開発することができ、パブリックドメインのデザインを使用することができ、又は第三者ＩＰブロック所有者から購入したか又はそれによって作成されたデザインを使用することができる）（例えば、設計者１１１は、デザインの表示をＦＰＧＡ１１８に転送し、１つ又はそれよりも多くのＩＰブロック１１０Ａ～１１０Ｉ及び／又は設計者の論理１５０をプログラムすることができる）。

20

#### 【０００４】

ＦＰＧＡ１１８は、設計者の論理１５０と複数のＩＰブロック１１０Ａ～１１０Ｉを含む。設計者の論理１５０は、設計者１１１が既に作成したハードウェアサブデザインを含む。ＦＰＧＡ１１８内の各ＩＰブロック１１０Ａ～１１０Ｉは、第三者から購入したハードウェアサブデザインを含む（例えば、特定のＩＰブロック１１０Ａ内のハードウェアサブデザインは、例えば、図１Ｂに示すように第三者ＩＰブロック所有者１００から購入することができる）。

#### 【０００５】

図１Ｂは、デザインを実施するための設計者１１１と、ＩＰブロック所有者１００と、ＦＰＧＡプロバイダ１２０との間の従来技術のトランザクション流れ図を示している。図１Ｂにおいて、設計者１１１は、最初に、丸で囲んだ１に示すようにＦＰＧＡプロバイダ１２０と通信する。丸で囲んだ１の通信は、ＦＰＧＡ装置１１８をＦＰＧＡプロバイダ１２０から購入する要求とすることができる（例えば、ＦＰＧＡプロバイダは、代理店、小売業者、製造業者、及び／又は卸売業者のようなあらゆる商業レベルのＦＰＧＡ納入業者とすることができる）。次に、ＦＰＧＡプロバイダ１２０は、丸で囲んだ２でＦＰＧＡ１１８を設計者１１１に出荷する（例えば、ＦＰＧＡプロバイダ１２０は、信用調査を行い、送り状を作成し、設計者１１１とＦＰＧＡプロバイダ１２０間の商取引の一部としてオフターを受諾することができる）。

30

#### 【０００６】

設計者１１１が、丸で囲んだ２で、ＦＰＧＡ１１８をＦＰＧＡプロバイダ１２０から受領した後に、設計者１１１は、丸で囲んだ３で、設計者１１１が彼のハードウェアシステムを完了するために必要とする専有ハードウェアサブデザインを購入する要求をＩＰブロック所有者１００に送る（例えば、ＩＰブロック所有者１００は、設計者１１１が彼に与えられた時間及び経費上の制約の範囲内で彼のハードウェアシステムを完了するために必要とする専有ハードウェアサブデザインの所有権を有する場合がある）。設計者１１１が、丸で囲んだ３で、要求をＩＰブロック所有者１００に提供した後に（例えば、設計者１１１は、発注書の形で専有ハードウェアサブデザインを購入するオファーをＩＰブロック所有者１００に電子メールで送ることができ、又はＩＰブロック所有者１００に電話して専有ハードウェアサブデザインを購入することができる）、ＩＰブロック所有者１００は

40

50

、丸で囲んだ4で、専有ハードウェアサブデザインを設計者111に供給する（例えば、IPブロック所有者100は、グローバルライセンスに関する契約を締結して、IPブロック所有者100が有する専有ハードウェアサブデザインのグローバル知的財産ライセンスを購入する設計者111のオファーを受諾した後に、HDL及び/又はRTL実施デザイン詳細及び専有ハードウェアサブデザインの実施に必要な対応する文書を設計者111に提供することができる）。

#### 【0007】

次に、設計者111は、IPブロック所有者100から受領した専有ハードウェアサブデザインをFPGA装置118に組み込む（例えば、設計者111は、図1Aで上述したように、バス108を通じてFPGAプロバイダ120から設計者111が購入したFPGA118をプログラムすることができる）。残念ながら、IPブロック所有者100は、専有ハードウェアサブデザインの詳細が設計者111に送られた後は、彼の知的財産を管理することができなくなる。IPブロック所有者100が彼らの専有ハードウェアサブデザインの一部を暗号化したとしても、設計者111は、彼/彼女が所望する多くのFPGA118にそれを自由に複製して利用することができる（例えば、暗号化された回路の他に、ライセンスコードを複製することにより）。更に、IPブロック所有者100は、設計者111がIPブロック所有者100の提供した専有ハードウェアサブデザインを悪用したか否かを判断することができない上に、設計者111が専有ハードウェアサブデザインを他人に再販したか否かをモニタすることができない（例えば、IPブロック所有者100は、彼の専有ハードウェアサブデザインの最初の設計に何百万ドルも投資したかもしれない、かつIPブロック所有者100は、彼の知的財産を他人にライセンス交付することができないので、設計者111による専有ハードウェアサブデザインの悪用及び/又は窃盗に対する以外は、投資額を取り戻すのは困難であろう）。従って、IPブロック所有者によって作成された専有ハードウェアサブデザインを保護するための改良型の機器及び方法を提供することが望ましいことが分る。

#### 【発明の開示】

#### 【0008】

本発明は、ハードウェア技術の使用による特定のハードウェアデザインに関わる複数の当事者間のライセンス交付契約の条項を実行する方法及び機器を開示する。本発明の1つの態様によれば、ハードウェアサブデザインは、暗号化によってユーザによる修正から保護されたライセンス検証サブデザインを含む。1つの態様では、ライセンス交付検証サブデザインと、IPブロックを使用不可にするハードウェアサブデザイン内の論理コードの一部との接続も、修正を防止するために暗号化される。1つの態様では、ライセンスは、外部ハードウェア装置内の信頼できるホスト識別子に基づいて発生される。別の態様では、ユーザは、信頼できるホスト識別子を修正することはできない。本発明の1つの態様では、各信頼できるホスト識別子は固有であり、同じ信頼できるホスト識別子を共有する集積回路は2つとない。本発明の別の態様では、集積回路は、フィールド・プログラマブル・ゲート・アレイ又は特定用途向け集積回路である。

#### 【0009】

本発明の別の態様によれば、例示的な方法は、設計者によって設計された第1のハードウェアサブデザインを信頼できるホスト識別子を有するプログラマブル・ゲート・アレイ上にアップロードし、並びに第三者によって提供され、かつ特定の信頼できるホスト識別子を有するプログラマブル・ゲート・アレイ上でのみ機能することができる第2のハードウェアサブデザインをアップロードする。本発明の別の態様では、ライセンスは、信頼できるホスト識別子の群に基づいて発生される。1つの態様では、ライセンスは、ハードウェアサブデザインが信頼できるホスト識別子を有する集積回路内で実施された時に、ハードウェアサブデザインがどのくらい長く作動することになるかを判断する。本発明はまた、集積回路の設計に使用することができるソフトウェア媒体を含む機器を開示する。例えば、本発明は、本発明により集積回路を設計することができるデジタル処理システムを含み、本発明はまた、コンピュータシステムのようなデジタル処理システム上で実行された

時にデジタル処理システムに集積回路を設計する方法を実行させる機械可読媒体を提供する。

【 0 0 1 0 】

本発明の他の特徴は、添付の図面及び以下の詳細説明から明らかになるであろう。

【 0 0 1 1 】

本発明は、一例として示すものであり、同じ参照番号が類似の要素を示す添付図面の図に制限するものではない。

【 発明を実施するための最良の形態 】

【 0 0 1 2 】

特定のハードウェアデザインに関わる複数の当事者間のライセンス交付契約の条項を実行するのに使用されるハードウェア技術の方法及び機器を本明細書で説明する。以下の説明においては、説明を目的として、本発明を完全に理解できるように多くの特定の詳細事項に対して説明する。しかし、これらの特定の詳細事項がなくとも本発明を実施することができることは、当業者には明らかであろう。他の事例においては、公知の構造、処理、及び装置をブロック図の形で示し、又は必要以上の詳細事項なく説明を行うために要約して参照する。本発明の方法の多くは、従来の汎用コンピュータシステムのようなデジタル処理システムと共に実施することができる。

【 0 0 1 3 】

図 2 A は、本発明の一例示的实施形態による信頼できるホスト識別子 2 4 5 と、複数のライセンス交付ブロック 2 0 5 A ~ 2 0 5 I と、各ライセンス交付ブロック 2 0 5 A ~ 2 0 5 I に関連した複数の IP ブロック 2 1 0 A ~ 2 1 0 I とを有する F P G A 2 1 8 を示している。設計者 2 1 1 は、バス 2 0 8 を通じて F P G A 2 1 8 と通信する（例えば、設計者 2 1 1 は、バス 2 0 8 を通じて F P G A にダウンロードする前にビットストリームを合成、配置、経路指定、及び発生させることにより、ハードウェアサブデザインの全ての部分を編集することができる）。設計者 2 1 1 は、一実施形態によると、社内で作成されたハードウェアサブデザイン並びに第三者から購入したハードウェアサブデザインを使用するハードウェアシステム設計者とすることができる（例えば、設計者 2 1 1 は、特定のハードウェアサブデザインを IP ブロック所有者 2 0 0 から購入して、設計者の論理 2 5 0 と組み合わせてバス 2 0 8 を通じて F P G A 2 1 8 内で完全なデザインを作ることができる）。バス 2 0 8 は、直接接続ローカルバス（例えば、シリアル及び / 又はパラレルポートを通じて F P G A に直接に接続したコンピュータ）とすることができる。代替的に、バス 2 0 8 は、別の実施形態によると、設計者 2 1 1 が F P G A 2 1 8 と通信するローカル又はワイドエリアネットワークとすることができる。

【 0 0 1 4 】

F P G A 2 1 8 は、設計者の論理 2 5 0 と、信頼できるホスト ID 2 4 5 と、1 つ又はそれよりも多くの IP ロケーション 2 4 0 A ~ 2 4 0 I とを含む。設計者の論理 2 5 0 は、設計者 2 1 1 によって単独に作成されたハードウェアサブデザインを含む（例えば、設計者の論理 2 5 0 は、検証された上に既に試験済みであるハードウェアサブデザインを含むこともあり、また、他のデザインにおいて過去に使用されたハードウェアサブデザインを含む場合がある）。設計者の論理 2 5 0 は、IP ロケーション 2 4 0 A ~ 2 4 0 I から分離され、これは、IP ロケーション 2 4 0 A ~ 2 4 0 I が一実施形態では第三者によって設計されたハードウェアサブデザインのために使用される場合があるからである。

【 0 0 1 5 】

F P G A 2 1 8 内の信頼できるホスト ID 2 4 5（信頼できるホスト識別子）は、F P G A 2 1 8 に対する固有の信頼できるホスト識別子を維持する。信頼できるホスト ID 2 4 5 の実施は、一実施形態では、内蔵連続番号（例えば、F P G A は、内蔵連続番号として製造することができ、又は内蔵連続番号は、1 回限りのプログラマブル連続番号とすることができる）及びライセンス検証サブデザインにおいて使用することができる設計構成要素（例えば、ハードウェアサブデザイン内でのライセンス検証サブデザイン）を用いて、ユーザが目視可能な接続部なしにその連続番号にアクセスすることで（例えば、ユーザ

による修正からサブデザインのライセンス検証部分を保護する)、フィールド・プログラマブル・ゲート・アレイ内で行うことができる。信頼できるホストID 245は、一実施形態では、FPGA 218に永久的に関連付けられた固有番号とすることができる(例えば、信頼できるホストIDは、製造中にFPGA製造業者のような信頼できるホストIDプロバイダによって予め設定された番号とすることができる)。一実施形態では、信頼できるホストID 245の一部は、図2Bに示すように、信頼できるホストIDプロバイダ220によって設計者211に販売されたFPGAの群に関して共通とすることができる(例えば、固定の上位の組のビットを有するマスキングと信頼できるホストIDとを組み合わせることができる)(例えば、FPGA 218の製造時期及び/又は製造場所を示すように、信頼できるホストIDプロバイダ220が設計者211に数値ホストIDの一部を販売したFPGAの特定のバッチと関連付けることができる)。信頼できるホストID 245のアイデンティティは、一実施形態では、FPGA 218に問い合わせすることでバス208を通じて設計者211が検索することができる(例えば、設計者211が有するソフトウェアプログラム又はソフトウェアプログラムは、設計者211が信頼できるホストID 245のコンテンツを読むことを可能にすることができる)。信頼できるホストID 245は、FPGA 218を完全に使用不可にすることなしに変えることはできないことに注意すべきである(例えば、誰かが信頼できるホストID 245のアイデンティティを変えようとした場合、FPGA 218を使用不可にする回路遮断器を通じた改ざんに対して信頼できるホストID 245を保護することができる)。一実施形態では、信頼できるホストID 245は、フィールド・プログラマブル・ゲート・アレイの外部にあり、セキュアではないチャンネル(例えば、仮想専用ネットワークプロトコル)によるセキュアな通信に様々な公知の方法を使用することができる。

#### 【0016】

一実施形態では、設計者211は、FPGA 218にダウンロードする前にビットストリームを合成、配置、経路指定、及び発生させることで、ハードウェアサブデザインの全ての部分を編集することができる。代替的に、部分的再構成を目的とした別の実施形態では、各IPブロック205A~205IをFPGA 218上の異なるロケーションに個別にダウンロードすることができる。各IPロケーション240A~240Iは、ライセンス交付ブロック205A~205IとIPハードウェアデザインブロック210A~210I(例えば、又はIPブロック210A~210I)とを含む。各IPロケーション240A~240Iを設計者の論理250に接続することができる(例えば、特定のIPロケーション240Aが設計者の論理250と通信してハードウェアサブデザイン命令を共有することを可能にするために)。一実施形態では、新しいハードウェアサブデザインが追加及び/又はIPブロック210A~210Iの範囲内から削除された時、IPロケーション240A~240Iを使用可能及び使用不可にすることができる(例えば、IPロケーション240Aは、物理的IPロケーションに対して、図2Bに示すようにIPブロック所有者から購入された専有ハードウェアサブデザインがFPGA 218内で追加及び/又は削除された時に作成されるIPブロック210Aに対して、特定のライセンス交付ブロック205Aの論理的関連付けとすることができる)。一実施形態では、ライセンス交付ブロック205A~205Iを使用して、IPブロック210A~210Iを使用可能にすることができる(例えば、特定のライセンス交付ブロック205Aは、図2Bの丸で囲んだ4で示すように、IPブロック210Aのコンテンツをアンロックして、IPブロック所有者200によって提供されるハードウェアサブデザインを明らかにすることができる)。

#### 【0017】

ライセンス交付ブロック205Aは、ライセンスを受信し、信頼できるホスト識別子245を分析してIPブロックのどの特徴を使用可能にすべきであるかを判断することができる。一実施形態では、ライセンス交付ブロック205A~205Iは、ハードウェアサブデザインの作動を使用可能にするために信頼できるホストID 245と共に(図2Bに示すように)IPブロック所有者200から受信したライセンスコードの整合性を検証す

るライセンス検証ハードウェア（例えば、ハードウェアサブデザインを発生させる間に暗号化されるハードウェアサブデザイン内のライセンス検証サブデザイン）を含む。従って、ライセンス交付ブロック205A～205Iは、IPブロック所有者（図2Bに示すようなIPブロック所有者200など）から受信したライセンスコードを信頼できるホストID245に依存するライセンス交付ブロック205A～205I内の内部暗号化手法と比較することで、知的財産を有するライセンス交付されていない設計者がIPブロック210A～210I内のハードウェアサブデザインにアクセスするのを防止する電子ロックとして作動することができる（例えば、一実施形態では、ライセンスコードは、信頼できるホストID245を有するFPGA上でしか機能することはできない）。一実施形態では、ライセンス交付ブロック205Aは、（図2Bで丸で囲んだ4で示すように）IPブロック所有者200からライセンスコードを受信した設計者211から、バス208を通じてそのライセンスコード（例えば、バイナリデータのストリング）を受信することができる。別の実施形態では、ライセンス交付ブロック205Aは、ライセンスコードを信頼できるホストID245及びライセンス交付ブロック205A内の暗号化手法と比較することができる。一実施形態では、ライセンスコードは、IPブロック210A～210I内に組み込むことができ、及び/又は設計者の論理250内に組み込むことができる。

#### 【0018】

IPブロック210A～210Iは、一実施形態によれば、第三者IPブロック所有者によって提供されたハードウェアサブデザインとすることができる（例えば、図2Bで後述するようなIPブロック所有者200）。別の実施形態では、異なるIPブロック所有者が、IPブロック210A～210Iを形成するように設計者211に自社のハードウェアサブデザインを販売又はライセンス交付していたかもしれない（例えば、第1のIPブロック所有者が、ハードウェアサブデザインをIPブロック210A内に供給する場合があり、一方、異なるIPブロック所有者が、ハードウェアサブデザインをIPブロック210B内に供給する場合もある）。IPブロック210A～210Iのうちの複数のIPブロックは、別の実施形態では、共通のライセンス交付ブロック205A～205Iを共有することができる、及び/又は共通のライセンスコードがコンテンツを使用可能にすることを可能にすることができる（例えば、同じライセンスコードは、ライセンス交付ブロック205A並びにライセンス交付ブロック205Bをアンロックするように作動することができる）。ライセンス交付ブロック205A～205Iは、修正を防止するために暗号化されたライセンス検証サブデザインを含むことができる。一実施形態では、IPブロック210A～210Iは、特定の信頼できるホストID245値を有するFPGA218上でしか機能することはできず、異なるホストID値を有する異なるFPGA上では機能しない。ライセンス交付ブロック205A～205Iは、一実施形態では、IPブロック所有者200によって提供された信頼できるホストID245及びライセンスの組合せに基づいて作動の意思決定を行うことができる。ライセンスが有効でなく、かつ検証が失敗した場合、一実施形態では、ハードウェアサブデザインの論理を妨害する（状態機械をリセットさせ、かつメモリを決して書き込みさせない）信号をアサートすることで、ハードウェアサブデザインの作動を防止することができる。ライセンス検証サブデザインを暗号化して、ユーザがライセンス検証サブデザインのいずれの部分も修正することができないようにすることができる（例えば、このデザインツールフローは、ハードウェアサブデザインのこの部分の編集を防止することができる）。一実施形態では、ハードウェアサブデザインの暗号化は、ハードウェアサブデザイン内のライセンス検証サブデザインを修正から保護する目的だけに行われる。一実施形態では、ライセンス検証サブデザインと、IPブロックを使用不可にするハードウェアサブデザイン内の論理コードの部分との接続を暗号化して修正を防止することができる。

#### 【0019】

図2Bは、本発明の一例示的实施形態による信頼できるホストID245とライセンスコードとを用いたハードウェアデザインの実施に関する設計者211と、IPブロック所有者200と、信頼できるホストIDプロバイダ220との間のトランザクション流れ図

10

20

30

40

50

を示している。図2Bにおいては、設計者211は、ホストID付きFPGA218を購入する要求を信頼できるホストIDプロバイダ220に送る。一実施形態では、信頼できるホストIDプロバイダ220は、IPブロック所有者200が、信頼される製造業者によって製造された各FPGAが固有かつ編集不能なホストID218を有すると信じるように、十分な信頼に足る企業の評判を築いてきたFPGA製造業者のような信頼される製造業者とすることができる。

#### 【0020】

代替的に、別の実施形態では、信頼できるホストIDプロバイダ220は、コンピュータ（例えば、図3のコンピュータ311など）に接続した時に信頼できるホスト識別子を供給する外部ハードウェア装置（例えば、dongle及び/又はマイクロチップ）を製造する企業とすることができる。丸で囲んだ1では、設計者211は、信頼できるホストID（又は信頼できるホスト識別子を有するFPGA218）を信頼できるホストIDプロバイダ220に注文する（例えば、設計者211は、特注集積回路の設計で使用される内蔵の信頼できるホストID245を有するFPGA218の購入の注文書を信頼できるホストIDプロバイダ220に送ることで注文することができる）。また、設計者211は、丸で囲んだ1で、信頼できるホストIDプロバイダ220に、設計者211がどのIPブロック所有者200のハードウェアサブデザインをハードウェアシステムで使用するつもりであるかを連絡することができる（例えば、設計者211は、例えば、IPブロック所有者200が作成したハードウェアサブデザインを使用するつもりであることを信頼できるホストIDプロバイダに連絡することができる）。 10

#### 【0021】

丸で囲んだ2で、信頼できるホストIDプロバイダ220は、FPGA218を有するFPGAを設計者211に出荷するか、又は信頼できるホスト識別子を有する外部ハードウェア装置を供給する（例えば、信頼できるホストIDプロバイダ220は、設計者211と拘束力のある契約を締結して、例えば、設計者211が注文した各FPGA218に対して固有のホストIDを発生させることができる）。一実施形態では、外部ハードウェア装置を直接にFPGAに接続することができるので、外部ハードウェア装置をコンピュータに接続するという点が不要になると考えられる。一例示の実施形態では、信頼できるホストIDプロバイダ220が外部ハードウェア装置を供給した場合、設計者211は、IPブロック所有者200が所有するハードウェアサブデザインが使用されるASIC及び/又はFPGAに接続したコンピュータに外部ハードウェア装置を接続する必要があると考えられる（例えば、設計者211は、IPブロック所有者200が所有するハードウェアサブデザインを使用するASIC及び/又はFPGAへの書込みに設計者211が使用することができるコンピュータ上のUSBポートに信頼できるホスト識別子を有する周辺装置を接続するであろう）。代替的に、一実施形態では、コンピュータの製造番号をホスト識別子として用いることができる。IPブロック所有者200は、外部ハードウェア装置によって発生されたホスト識別子が固有かつ修正不可能であると確信すべきである（例えば、信じる）ことに注意すべきである。従って、IPブロック所有者200は、一実施形態では、信頼できるホスト識別子を発生させたいと考えている各信頼できるホストIDプロバイダ220を事前に資格審査する必要があると考えられる。別の実施形態では、独立した業界団体が、信頼できるホストIDプロバイダの指針及び資格を提供することができる。 30

#### 【0022】

次に、丸で囲んだ3では、設計者211は、IPブロック所有者200に、設計者211がホストID付きFPGA218（又は、信頼できるホスト識別子を有する外部装置）を購入したことを知らせ、設計者211は、IPブロック所有者200が所有するハードウェアサブデザインを発注する（例えば、設計者211は、複合集積回路の一部をIPブロック所有者200から購入して、例えば、設計者211がゼロから設計するのではなく時間を節約することができるようにすることができる）。また、設計者211は、IPブロック所有者200に信頼できるホストIDを知らせることができる（例えば、設計者2 40

10

20

30

40

50



11は、ホストIDを有するFPGA218及び/又は外部ハードウェア装置内で固定レジスタを読み取ることで、信頼できるホスト識別子のIDを判断するソフトウェアプログラムを実施することができる)。

#### 【0023】

次に、IPブロック所有者200は、丸で囲んだ3で、設計者211から受信する信頼できるホストID情報を組み合わせて、設計者211が購入したいと考えているハードウェアサブデザイン向けにカスタマイズされている設計者211のための信頼できるホスト識別子特定のライセンスを発生させる(例えば、IPブロック所有者200は、図2Aに示すように、信頼できるホストID245を使用してハードウェアサブデザイン内のライセンス検証サブデザインを暗号化し、特定のホスト識別子218のみを使用してIPブロック所有者200が供給したハードウェアサブデザイン内の1つ又はそれよりも多くの特徴を検証して使用可能にすることを要件とするライセンスコードを発生させることができる)。一実施形態では、ライセンス検証サブデザインは、IPブロック所有者200によって提供された信頼できるホストID245とライセンスの組合せに基づいて、作動の意思決定を行うことができる。ライセンスが有効でなく、かつ検証が失敗した場合、一実施形態では、ハードウェアサブデザインの論理を妨害する信号をアサートすることで、ハードウェアサブデザインの作動を防止することができる。

#### 【0024】

次に、丸で囲んだ4では、IPブロック所有者200は、固有のホストIDを有する特定のFPGA218向けにカスタマイズされているライセンスコード(例えば、IPブロック所有者200が所有するハードウェアサブデザイン内の1つ又はそれよりも多くの特徴をアンロックするライセンスコード)と共にハードウェアサブデザイン(例えば、IPブロック所有者200が所有するハードウェアサブデザイン)を設計者211に供給する。一実施形態では、IPブロック所有者200は、修正を防止するために暗号化されているハードウェアサブデザイン内にライセンス検証サブデザインを発生させる。一実施形態では、ライセンスは、設計者211がIPブロック所有者200の有するハードウェアサブデザインを使用したいと考えている様々なFPGAのための信頼できるホストIDの群に関して発生される(例えば、IPブロック所有者200は、各々が固有のホストIDを有するFPGAの群上にIPブロック所有者200が所有するハードウェアサブデザインを設置するための注文を設計者211から受注することができ、IPブロック所有者200は、ハードウェアサブデザインの使用を設計者211が購入した全ての資格審査用ホストIDに許可することができる)。

#### 【0025】

信頼できるホストID245を有するFPGA上でのみ機能することができるライセンスを供給することで、IPブロック所有者200は、IPブロック所有者200が所有するハードウェアサブデザインが使用される方法をより有効に規制することができる(例えば、IPブロック所有者200は、信頼できるホストIDの特定の群のみで作業するライセンスを設計者211に供給することで、ハードウェアサブデザインの使用を特定のFPGAにのみ制限することができる)。代替的に、IPブロック所有者200は、一実施形態では、信頼できるホスト識別子を含む外部ハードウェア装置が設計者211側のコンピュータに接続されることを要件とするライセンスコードを供給することができる。例えば、IPブロック所有者200のハードウェアサブデザインは、外部ハードウェア装置が接続されているASIC及び/又はFPGA上でしか作動することはできない。従って、IPブロック所有者200は、グローバルライセンスに対してではなく使用毎のベースで課金することで、知的財産(例えば、ハードウェアサブデザイン)に対して可変の金額を課金することができる(例えば、IPブロック所有者200は、全てのFPGAを対象としてハードウェアサブデザインをライセンス交付する1回限りの料金とは対照的に、ハードウェアサブデザインの全てのインスタンスが既知であるという点で実施機構が存在するので、ハードウェアサブデザインが使用される各FPGAに対して課金することができる)。更に、IPブロック所有者200が所有するハードウェアサブデザインを信頼できるホ

10

20

30

40

50

スト識別子を有するライセンシーだけに制限することで、ＩＰブロック所有者２００は、ＩＰブロック所有者２００が所有するハードウェアサブデザインの無許可サブライセンス交付及び／又は盗難を防止することができる。従って、設計者２１１は、ＩＰブロック所有者２００から事前の許可を得なければ、ＩＰブロック所有者２００からライセンス交付されたハードウェアサブデザインの無許可の複写を発生させることはできない。設計者２１１は、設計者２１１がＩＰブロック所有者２００から受信するハードウェアサブデザインが、特定の信頼できるホスト識別子を用いてのみ機能することになるので、設計者２１１が更に別のコピーを使用することを明示的に許可するライセンスを購入すべきである（例えば、ＩＰブロック所有者２００は、ＩＰブロック所有者２００が付与するライセンスを特定の信頼できるホストＩＤを有するＦＰＧＡだけに制限することができるので、ＩＰ

10

20

30

40

50

#### 【００２６】

図３は、本発明の一例示的实施形態によるデザイン実施に関するコンピュータと、ライセンス発生器と、信頼できるホストＩＤプロバイダとの間の信頼できるホスト識別子及びライセンスコードの使用のハードウェア図を示している。図３は、図３が図２Ｂに示す当事者によって使用される特定のハードウェアを示す点を除き、図２Ｂで発生させる全ての処理が図３に発生させるという点において図２Ｂと類似のものである。コンピュータ３１１は、図２Ｂで上述のように、設計者２１１内にある（コンピュータ３１１は、図２Ａに示すように、バス２０８を通じてホストＩＤ２１８を有するＦＰＧＡと通信することができる）。コンピュータ３１１は、丸で囲んだ１及び丸で囲んだ２に示しかつ図２Ｂで上述のように、通信で信頼できるホストＩＤプロバイダ２２０から信頼できるホストＩＤ２４５を受信する（例えば、ＦＰＧＡ２１８は、当事者が契約を締結した後で、図２Ｂに示すように、コンピュータ３１１で使用されるように、信頼できるホストＩＤプロバイダ２２０が設計者２１１に出荷することができる）。次に、ＩＰブロック所有者２００内のライセンス発生器３００は、丸で囲んだ３及び丸で囲んだ４で、信頼できるホストＩＤ２４５専用のライセンスを発生させる（例えば、ライセンス発生器３００は、ハードウェアサブデザインがアンロックされるように特定の信頼できるホストＩＤ２４５に依存するライセンスを発生させることができる）。一実施形態では、ライセンス発生器３００は、ハードウェアサブデザイン内の暗号化ライセンス検証サブデザインと、特定のＦＰＧＡ２１８内の信頼できるホストＩＤ２４５に依存するカスタマイズホストＩＤ専用ライセンスコードとを発生させるためにＩＰブロック所有者２００が使用するアプリケーションプログラムである。丸で囲んだ４では、信頼できるホストＩＤ専用ライセンスコード並びにハードウェアサブデザインをライセンス発生器３００からコンピュータ３１１（図２Ｂに説明するような設計者２１１側のコンピュータ３１１）に供給する。

#### 【００２７】

図４Ａは、本発明の実施形態の実施に使用することができるコンピュータシステム３１１のブロック図である。コンピュータシステム３１１は、ＨＤＬコードに説明されているデザインの論理合成に使用する。コンピュータシステム３１１は、バス４０１を通じてランダムアクセスメモリ４０４と、読み出し専用メモリ４０６と、大容量記憶装置４０７とに結合されたプロセッサ４０２を含む。大容量記憶装置４０７は、フロッピー（登録商標）ディスクドライブ、固定ディスクドライブ（例えば、磁気ドライブ、光ドライブなど）のような持続性データ記憶装置を表している。プロセッサ４０２は、汎用プロセッサ（「Intel Pentium（登録商標）」プロセッサのような）、専用プロセッサ、及び／又は特殊プログラム論理デバイスにおいて実施することができる。ディスプレイ４２０は、バス４０１を通じてプロセッサ４０２に結合され、コンピュータシステムにグラフィック出力を供給する。このグラフィック出力は、一般的に、コンピュータシステムの作動の制御に使用することができるグラフィカルユーザインタフェースである。キーボード４２１及びカーソル制御装置４２２は、情報及び指令選択をプロセッサ４０２に通信するためにバス４０１に結合される。カーソル制御装置４２２は、一般的に、表示装置４２０

上に表示されるカーソルの制御に使用することができるマウス又は他のカーソル制御装置であることになる。また、プロセッサ 402 には、データの制御及びコンピュータシステム 311 に結合されるプリンタ及び他のコンピュータのような電気装置へ及びそれからの転送に使用することができる入力／出力インタフェース 423 がバス 401 を通じて結合される。また、信頼できるホスト ID 245 をコンピュータシステム 311 に結合することができる。一実施形態では、信頼できるホスト ID 245 は、外部ハードウェア装置である。別の実施形態では、信頼できるホスト識別子は、信頼できるホスト ID 245 を有する FPG A 218 内にある。また、信頼できるホスト ID 245 は、直接にコンピュータシステム 311 にではなく、特定の入力／出力インタフェース 423 に結合することができる。

10

#### 【0028】

図 4 のアーキテクチャは、説明のみを目的として提供するものであり、本発明に関連して使用されるコンピュータシステム又は他のデジタル処理システムは、この特定のアーキテクチャに限定されるものではないことに注意すべきである。

#### 【0029】

ここで、図 4 B を参照して本発明のある一定の実施形態の一般的な例を説明する。図 4 B は、本発明の一例示的实施形態により信頼できるホスト ID 245 を有する FPG A 218 内のハードウェアサブデザインの実施に使用される設計者 211 側のコンピュータシステム 311 内での作動を示す流れ図である。本発明の大部分の実施形態は、HDL デザイン合成ソフトウェアでの使用を意図したものであるが、本発明は、必ずしもこのような使用に限定されるものではない。一実施形態では、ハードウェアサブデザインは、実際には、暗号化によって隠されたこのような部分を有する簡単なネットリストとして簡単に表すことができることに注意すべきである。ハードウェアサブデザインは、HDL 又は動作記述でなくてもよい。コンピュータプログラムにおける他の言語の使用が可能であるが、本発明の実施形態は、HDL 合成システム、特に、販売業者特異の技術／アーキテクチャを有する集積回路と共に使用するために設計された HDL 合成システムにおける使用という関連で以下に説明する。

20

#### 【0030】

公知の通り、プログラマブル IC の納入業者は、一般的に目標のアーキテクチャを判断する。目標アーキテクチャの例は、カリフォルニア州サンホセ所在の「Xilinx、Inc.」製フィールド・プログラマブル・ゲート・アレイのプログラム済みlookupアップテーブル (LUT) 及び関連論理である。目標アーキテクチャ／技術の他の例としては、Altera、「Lucent Technologies」、「Advanced Micro Devices」、及び「Lattice Semiconductor」のような販売業者製の FPG A 及び複合プログラマブル論理デバイスにおける公知のアーキテクチャがある。また、ある一定の実施形態に対しては、本発明は、ASIC と共に採用することもできる。

30

#### 【0031】

図 4 B の方法は、設計者 (図 2 B に示すような設計者 211 など) が、修正から保護されたライセンス検証ハードウェアを含む設計図 (例えば、望ましい回路の動作記述) を作成する作業 411 で始まる。作業 412 においては、隠されている IP ブロックと共にデザインを表示し、編集不能な IP ブロックを除くデザインに対する変更を可能にする (例えば、設計者の論理 250 は、編集可能であるが、IP ブロック所有者 200 によって提供されたハードウェアサブデザイン IP ロケーション 240 A ~ 240 I は、隠すことができる)。次に、作業 413 において、HDL コンパイラで設計図をコンパイルして、技術に無関係の RTL ネットリストを発生させる。このネットリストは、特定の販売業者の技術から独立したものであり、これは、特定の目標アーキテクチャによって使用される構築用ブロック (例えば、lookupアップテーブル、マルチプレクサ、及び AND / OR アレイなど) のライブラリから独立したものであることを意味する。設計図の少なくとも一部は

40

50

、暗号化済みであるために修正に対してセキュアである。

【 0 0 3 2 】

作業 4 1 4 においては、設計図を最適化する（例えば、論理を最適化して論理のタイミングパラメータを改善する）。この作業は、任意的であり、これを使用して最適化ルーチンに従って二重の相互接続及び論理デバイスを除去する。次に、作業 4 1 5 においては、従来の配置及び経路指定ソフトウェアツールを使用して、X i l i n x 又は A l t e r a の F P G A のような目標アーキテクチャにおける回路のデザインを作成する。次に、作業 4 1 6 においては、修正から保護された設計図ライセンス検証ハードウェアを含む I P ブロック（例えば、I P ブロック所有者 2 0 0 から購入したハードウェアサブデザインを有する I P ブロック）を作成するように F P G A の一部をプログラムする構成データを発生させる。

10

【 0 0 3 3 】

図 4 C は、本発明の一例示的实施形態による信頼できるホスト I D 2 4 5 を有する外部ハードウェア装置を使用して A S I C に範囲内でハードウェアサブデザインを実施するのに使用される設計者 2 1 1 側のコンピュータ 3 1 1 内の作業を示す流れ図である。A S I C 内での I P ブロック所有者 2 0 0 が所有するハードウェアサブデザインの実施には、設計者 2 1 1 が図 2 B において上述したような外部ハードウェア装置を購入することが必要である。図 4 C に示す作業 4 1 1 ~ 4 1 5 は、図 4 B に示す作業と同じものである。図 4 C の作業 4 2 6 においては、ハードウェアサブデザインが、F P G A ではなく A S I C での使用のためにライセンス交付されているので、修正から保護された設計図ライセンス検証ハードウェアを含む I P ブロックを A S I C 内で実施するための回路のレイアウトが実行される。

20

【 0 0 3 4 】

図 5 は、本発明の一例示的实施形態による信頼できるホスト識別子 5 4 5 と、設計者の論理 5 5 0 と、複数のライセンス交付ブロック 5 0 5 A ~ 5 0 5 I と、クロック回路 5 2 5 と、各ライセンス交付ブロック 5 0 5 A ~ 5 0 5 I 及びクロック回路 5 2 5 に関連した複数の I P ブロック 5 1 0 A ~ 5 1 0 I とを有する F P G A 5 1 8 を示している。F P G A 5 1 8 は、図 2 A で上述した F P G A 2 1 8 と類似のものである。しかし、図 5 に示す F P G A 5 1 8 は、I P ロケーション 5 4 0 A ~ 5 4 0 I 内の各ライセンス交付ブロック 5 0 5 A ~ 5 0 5 I と通信するクロック回路を含む。クロック回路 5 2 5 は、一実施形態では、前回記憶された値よりも大きい場合に限り新しい値（例えば、特定のハードウェアサブデザインが何回実施されたかのカウンタ又は現在の日付 / 時間など）を記憶することができる。一実施形態では、クロック回路 5 2 5 は、リセットすることができないので、記録された時間が確実に順方向に移動し続けるようにするのに使用される。

30

【 0 0 3 5 】

各 I P ロケーション 5 4 0 A ~ 5 4 0 I は、ライセンス交付ブロック 5 0 5 A ~ 5 0 5 I と I P ブロック 5 1 0 A ~ 5 1 0 I とを含む。クロック回路 5 2 5 は、特定の I P ロケーション 5 4 0 A ~ 5 4 0 I がどのくらい長く作動することになるかを支配する情報を記憶する（例えば、クロック回路 5 2 5 は、図 2 A に示すように、I P ブロック所有者 2 0 0 によってライセンス交付ブロック 5 0 5 A に提供されたライセンスコードに基づいて、I P ロケーション 5 4 0 A がどのくらい長く作動することができるかに関する情報を記憶することができる）。一実施形態では、特定の作動期間の限界に達した時、クロック回路 5 2 5 は、1 つ又はそれよりも多くの I P ブロック 5 1 0 A ~ 5 1 0 I を使用不可にすることができる（例えば、図 2 A で上述したのと同様に、I P ロケーション 5 4 0 A ~ 5 4 0 I は、設計者 2 1 1 が I P ロケーション 5 4 0 A ~ 5 4 0 I に関連した I P ブロック 5 1 0 A ~ 5 1 0 I にアクセス可能である期間にわたって使用可能して、I P ブロック 5 1 0 A ~ 5 1 0 I 内のハードウェアサブデザインにアクセスするライセンスが満了となった時に使用不可にすることができる論理モジュールとすることができる）。

40

【 0 0 3 6 】

一実施形態では、クロック回路 5 2 5 は、クロック回路 5 2 5 に関連した特定の I P ブ

50

ロック 510A ~ 510I が最後に更新された時 (例えば、設計者 211 がバス 508 を通じて特定の第三者ハードウェアサブデザインを IP ブロック 510A ~ 510I に最後に更新した時) を記憶することができる。別の実施形態では、クロック回路 525 は、ライセンス交付ブロック 505A がどのくらい長く作動することができるか (例えば、IP ブロックに関連した IP ロケーションが無効化される前にどのくらいか) を判断するカウンタダウタイマを記憶することができる。本発明の別の実施形態では、クロック回路 525 は、IP ロケーション 540A ~ 540I の最終更新時を含むことができる (例えば、IP ブロック所有者 200 が以前にハードウェアサブデザインの群を設計者 211 にライセンス交付していた場合、クロック回路 525 は、例えば、部分的な再構成計画のために IP ロケーション 540A 及び 540B に関する最終更新時を記憶することができる) 。一実施形態では、ホスト ID 545 を有する外部ハードウェア装置は、バッテリーによって電源が提供されかつ IP ブロック 510A ~ 510I 内のハードウェアサブデザインが所定の時間量にわたって作動することを可能にするクロック回路を含むことができる (例えば、クロック回路 525 と同様の) 。別の実施形態では、信頼できるホスト識別子 545 を有する外部ハードウェア装置の内部のメモリは、上述したようなクロック回路 525 に対して説明した実施形態の全てを含むことができる。

10

20

30

40

50

#### 【0037】

一実施形態では、設計者 211 は、ソフトウェアライセンス交付サブシステム (例えば、カリフォルニア州サンタクララ所在の「Macromedia, Inc.」による「GLOBE TROTTER (登録商標)」) をそれ自体が使用するソフトウェアアプリケーションを使用して、ハードウェアサブデザインに関する評価ライセンスを IP ブロック所有者 200 から受信することができる。評価ライセンスは、ソフトウェアベースの信頼できるホスト識別子を含むことができる (例えば、評価ライセンスは、アプリケーションソフトウェアに関するソフトウェアライセンスと共に送られた追加ビットのデータ内のソフトウェアベースの信頼できるホスト識別子を含むことができる) 。次に、設計者 211 は、ソフトウェアアプリケーションを使用して、図 5 に示すように、ソフトウェアベースの信頼できるホスト識別子と評価ライセンスとを FPGAs 18 内のライセンス交付ブロック 505A に転送し (例えば、JTAG シリアル通信法を通じて) 、その結果、ライセンス交付ブロック 505A は、ソフトウェアベースの信頼できるホスト識別子を使用してハードウェアサブデザイン内の 1 つ又はそれよりも多くの特徴を使用可能にすることができる。一実施形態では、IP ブロック 210A 又はライセンス交付ブロック 205A の暗号化部分 (例えば、ハードウェアサブデザイン内のライセンス検証サブデザイン) によって使用される信頼できるホスト識別子 245 を発生させ、集積回路プログラム又は製造時に信頼できるホスト識別子 245 が提供される時に、IP ブロック 210A (例えば、ハードウェアサブデザイン) の残りの部分を使用可能にすることができる。別の実施形態では、集積回路のプログラム時又は製造時にソフトウェアを通じて信頼できるホスト識別子を IP ブロック所有者 200 が設計者 211 に供給し、例えば、IP ブロック 210A を使用可能にする。このソフトウェアは、集積回路がプログラムされている時に設計者 211 が実施することができ、このソフトウェアは、一般的に、IP ブロック所有者によって提供された許可メッセージ又は信号を通じて使用可能された IP ブロックと共にプログラム又は製造させることになる実施可能なコンピュータプログラムコードを含むと考えられる。この許可メッセージ又は信号は、ソフトウェアによって利用されるソフトウェア又はデータ構造の暗号化部分に供給することができ、又はこの許可メッセージ又は信号は、ネットワーク接続部を通じて、IP ブロック所有者によって制御されるデータ処理システムから供給することができる。

#### 【0038】

図 6 は、本発明の一例示的实施形態による修正を防止するために行われる IP ブロック所有者側の信頼できるホスト識別子 245 を有するハードウェアサブデザイン内のライセンス検証サブデザインの暗号化を示す流れ図である。作業 601 においては、IP ブロック (例えば、図 2A の IP ブロック 210A のような) のためのハードウェアサブデザイ

ンは、図 2 B で上述のように I P ブロック所有者 2 0 0 によって設計される。ハードウェアサブデザインは、一実施形態では、I P ブロック所有者 2 0 0 によって最初に作成されたデザインとすることができる。別の実施形態では、I P ブロック所有者 2 0 0 は、ハードウェアサブデザインを有することができるが、このハードウェアサブデザインは、最初に別の企業によって作成されたものである。作業 6 0 2 においては、I P ブロック内のハードウェアサブデザインを実施するように F P G A をプログラムするデータを発生させる。一実施形態では、図 3 で説明するような I P ブロック所有者 2 0 0 側のライセンス発生器 3 0 0 を使用して、図 2 A に示すように、I P ブロック 2 1 0 A ~ 2 1 0 I の 1 つ又はそれよりも多くの内部でハードウェアサブデザインを実施するように P F G A 2 1 8 をプログラムするデータを発生させることができる。

10

#### 【 0 0 3 9 】

次に、作業 6 0 3 においては、ハードウェアサブデザイン内のライセンス検証サブデザインを H D L 及び / 又は R T L レベルで及び可能性として他のレベルでもホスト I D 情報を用いて暗号化する（例えば、図 2 A で説明するように、I P ブロック所有者 2 0 0 によって提供されたハードウェアサブデザインが、信頼できるホスト識別子 2 4 5 を有する特定の F P G A 上でしか機能しないことを保証するために）。最後に、作業 6 0 4 においては、別々に開発された設計者の論理 2 5 0 （例えば、図 2 A の設計者の論理 2 5 0 のような設計者によって作成されたハードウェアサブデザイン）と共に、図 2 B で説明したように、I P ブロック所有者 2 0 0 によって提供されたハードウェアサブデザインを信頼できるホスト識別子 2 4 5 を有する F P G A 2 1 8 に実施することになる F P G A システムの設計者 2 1 1 にハードウェアサブデザイン情報を提供する。

20

#### 【 0 0 4 0 】

図 7 は、本発明の一例示的实施形態による信頼できるホスト識別子 2 4 5 を設計者 2 1 1 から受信した後に行われる I P ブロック所有者 2 0 0 側のライセンス発生器 3 0 0 によるハードウェアサブデザインライセンスコードの発生を示す流れ図である。作業 7 0 1 においては、ライセンス発生器 3 0 0 は、ハードウェアサブデザインの要求を設計者 2 1 1 側のコンピュータシステム 3 1 1 から受信する（例えば、設計者 2 1 1 は、I P ブロック所有者 2 0 0 が所有するハードウェアサブデザインを供給する契約を I P ブロック所有者 2 0 0 と締結したと考えられる）。作業 7 0 2 においては、I P ブロック所有者 2 0 0 は、信頼できるホスト識別子 2 4 5 の要求を設計者 2 1 1 に送る（例えば、信頼できるホスト識別子 2 4 5 の要求を I P ブロック所有者 2 0 0 が送って特定のライセンスに対して設計者 2 1 1 にどれだけ請求するかを決めることができる）。作業 7 0 3 においては、信頼できるホスト識別子 2 4 5 を設計者 2 1 1 から受信する（例えば、I P ブロック所有者 2 0 0 が、信頼できるホスト識別子 2 4 5 を有する F P G A 2 1 8 上でのみハードウェアサブデザインを使用するライセンスを発生させることができるように）。

30

#### 【 0 0 4 1 】

作業 7 0 4 においては、信頼できるホスト識別子 2 4 5 に基づいて固有の I P ブロックライセンスコードを発生させる（固有の I P ブロックライセンスコードをライセンス発生器 3 0 0 が発生させることができる）。作業 7 0 5 においては、I P ブロック所有者 2 0 0 が所有するハードウェアサブデザイン内のライセンス検証サブデザインを暗号化することができる。作業 7 0 6 においては、I P ブロック所有者 2 0 0 側のライセンス発生器 3 0 0 から固有の I P ブロックライセンスコードとハードウェアサブデザインとを設計者 2 1 1 に供給する（例えば、図 2 B に示すように、例えば、設計者 2 1 1 と I P ブロック所有者 2 0 0 の間の契約に基づく義務を履行するために）。

40

#### 【 0 0 4 2 】

図 8 は、本発明の一例示的实施形態による信頼できるホスト識別子 2 4 5 を設計者 2 1 1 から受信した後に行われる I P ブロック所有者 2 0 0 側のライセンス発生器 8 0 0 による期限を有する固有のハードウェアサブデザインライセンスの発生を示す流れ図である。図 8 は、ライセンス発生器 8 0 0 が、設計者 2 1 1 からの要求に基づいてライセンスの期限を更に発生させる点において図 7 と異なっている（例えば、I P ブロック所有者 2 0 0

50

が所有する特定のハードウェアサブデザインがどのくらい長く作動することになるかに関する、かつ図5に示すようにクロック回路525内に及び/又は外部ハードウェア装置上に記憶される期限)。作業701~704は、図7で上述のものと同じである。作業801においては、設計者211からの要求に基づいてライセンスの期限を発生させる(例えば、期限は、設計者がIPブロック所有者200にいくら支払う意志があるかに基づくものとすることができる)。作業802においては、図7で上述の作業705と同様に、IPブロック所有者200が有するハードウェアサブデザイン内のライセンス検証サブデザインを暗号化して修正を防止する。作業803においては、期限を有する固有のIPブロックライセンス及びハードウェアサブデザインを設計者211に供給する。従って、図8は、設計者からの要求に基づく期限付きライセンスを発生させる点において図7と異なっている。更に、図8においては、期限を含む固有のIPブロックライセンスを設計者211に供給する。

10

#### 【0043】

本発明の様々な方法の作業は、機械可読記憶媒体と考えることができるメモリに記憶されたコンピュータプログラムの命令シーケンスを実行するデジタル処理システム内の処理ユニットによって実施することができる。メモリは、ランダムアクセスメモリ、読み出し専用メモリ、大容量記憶装置のような持続性記憶メモリ、又はこれらの装置の組合せとすることができる。命令のシーケンスの実行により、処理ユニットが本発明による作業を実行する。ネットワーク接続を通して、記憶装置又は1つ又はそれよりも多くの他のデジタル処理システム(例えば、サーバコンピュータシステム)からコンピュータのメモリに命令を取り込むことができる。命令は、いくつかの記憶装置(例えば、DRAM、及びバーチャルメモリのようなハードディスク)に同時に記憶することができる。その結果、これらの命令の実行は、処理ユニットで直接に実行することができる。これ以外の場合、命令は、直接に実行することはできず、又は処理ユニットで直接には実行することができない。これらの状況下では、実行は、命令を解釈する解釈ルーチンをプロセッサに実行させることにより、又は受信した命令を、プロセッサが直接に実行することができる命令に変換する命令をプロセッサに実行させることによって行うことができる。他の実施形態では、ソフトウェア命令の代わりに又はソフトウェア命令と組み合わせて、配線接続回路を使用して本発明を実施することができる。従って、本発明は、ハードウェア回路とソフトウェアのいかなる特定の組合せにも又はコンピュータシステム又はデジタルシステムによって実施される命令のいかなる特定のソースにも限定されない。更に、本文書で使用される時の「暗号化」は、設計者によるライセンス交付に関わるサブデザインの部分の修正の防止に使用することができるあらゆる機構を指すものである。ハードウェアサブデザインは、例えば、逆コンパイルが許可されないバイナリデータベースに予めコンパイルすることができる。

20

30

#### 【0044】

本発明を特定の例示的な実施形態を参照して説明したが、特許請求の範囲で示すような本発明の広範な精神及び範囲から逸脱することなく、これらの実施形態に様々な修正及び変更を行うことができることが明らかであろう。従って、本明細書及び図面は、限定的な意味ではなく例示的に考えるものとする。

40

#### 【図面の簡単な説明】

#### 【0045】

【図1A】複数のIPブロックを有する従来技術のFPGAを示す図である。

【図1B】ハードウェアデザイン実施のための設計者とIPブロック所有者とFPGAプロバイダとの間の従来技術のトランザクション流れ図である。

【図2A】本発明の一例示的な実施形態による信頼できるホスト識別子と複数のライセンス交付ブロックと各ライセンス交付ブロックに関連した複数のIPブロックとを有するFPGAを示す図である。

【図2B】本発明の一例示的な実施形態により信頼できるホスト識別子とライセンスコードとを用いたハードウェアデザイン実施のための設計者とIPブロック所有者と信頼できる

50

ホスト I D プロバイダとの間のトランザクション流れ図である。

【図 3】本発明の一例示的实施形態によるデザイン実施のためのコンピュータとライセンス発生器と信頼できる I D プロバイダとの間での信頼できるホスト識別子及びライセンスコードの使用のハードウェア図である。

【図 4 A】本発明の実施形態の実施に使用することができるコンピュータのブロック図である。

【図 4 B】本発明の一例示的实施形態により信頼できるホスト識別子を有する F P G A 内でハードウェアサブデザインを実施するのに使用される設計者側のコンピュータ内の作動を示す流れ図である。

【図 4 C】本発明の一例示的实施形態により信頼できるホスト識別子を有する外部ハードウェア装置を使用して A S I C 内でハードウェアサブデザインを実施するのに使用される設計者側のコンピュータ内の作動を示す流れ図である。

【図 5】本発明の一例示的实施形態による信頼できるホスト識別子と、複数のライセンス交付ブロックと、複数のクロックメモリと、各ライセンス交付ブロック及びクロックメモリに関連した複数の I P ブロックとを有する F P G A を示す図である。

【図 6】本発明の一例示的实施形態による修正を防止するための I P ブロック所有者側の信頼できるホスト識別子を有するハードウェアサブデザイン内のライセンス検証サブデザインの暗号化を示す流れ図である。

【図 7】本発明の一例示的实施形態により信頼できるホスト識別子を設計者から受信した後の I P ブロック所有者側のライセンス発生器によるハードウェアサブデザインライセンスコードの発生を示す流れ図である。

【図 8】本発明の一例示的实施形態による信頼できるホスト識別子を設計者から受信した後の I P ブロック所有者側のライセンス発生器による期限を有するハードウェアサブデザインライセンスコードの発生を示す流れ図である。

【符号の説明】

【 0 0 4 6 】

2 0 5 A ~ 2 0 5 I    ライセンス交付ブロック

2 0 8    バス

2 1 0 A ~ 2 1 0 I    I P ブロック

2 1 1    設計者

2 4 5    ホスト識別子

10

20

30



【図 1 A】

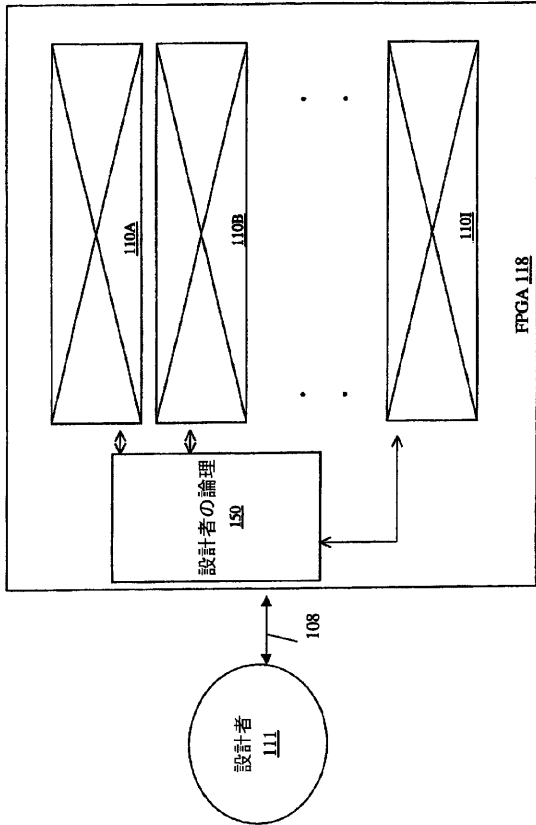


FIGURE 1A (従来技術)

【図 1 B】

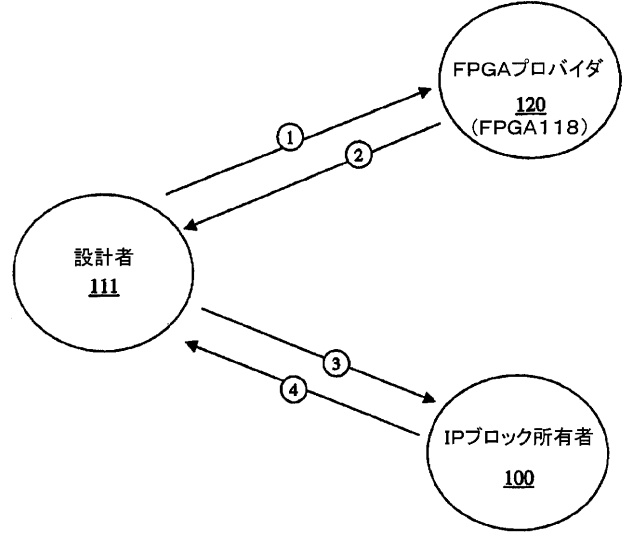


FIGURE 1B (従来技術)

【図 2 A】

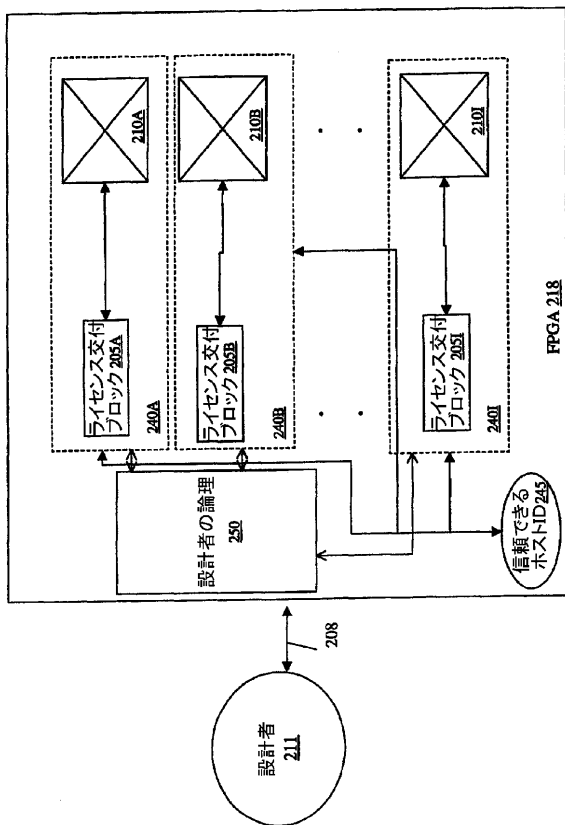


FIGURE 2A

【図 2 B】

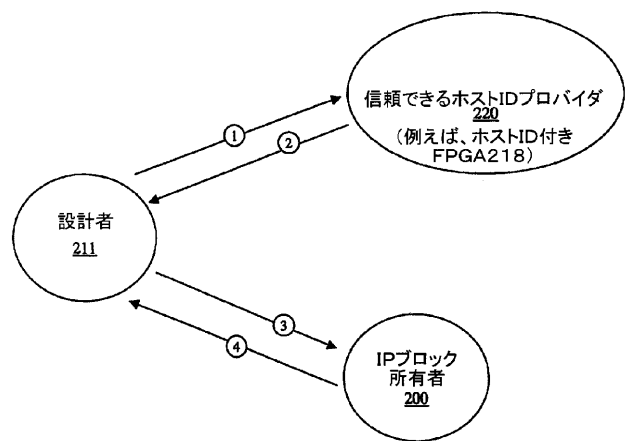


FIGURE 2B

【図 3】

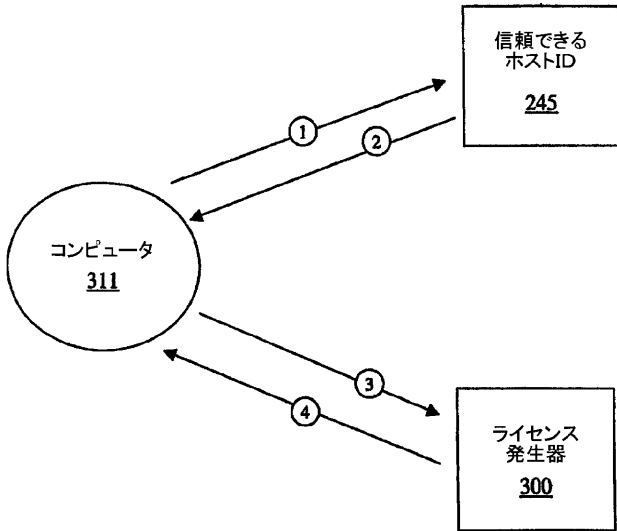


FIGURE 3

【図 4 A】

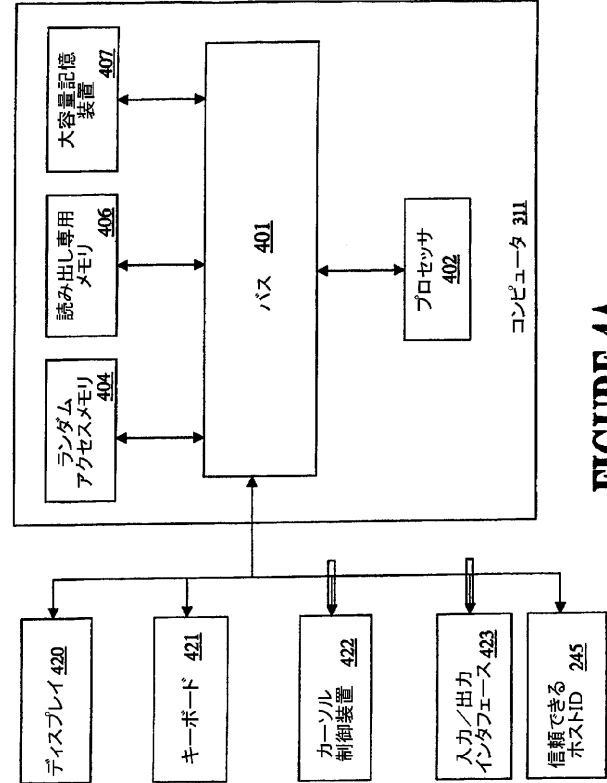


FIGURE 4A

【図 4 B】

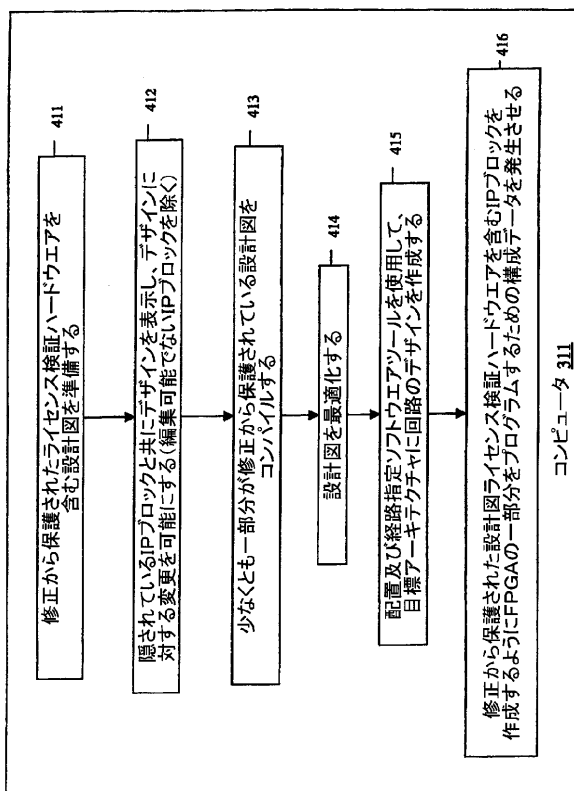


FIGURE 4B

【図 4 C】

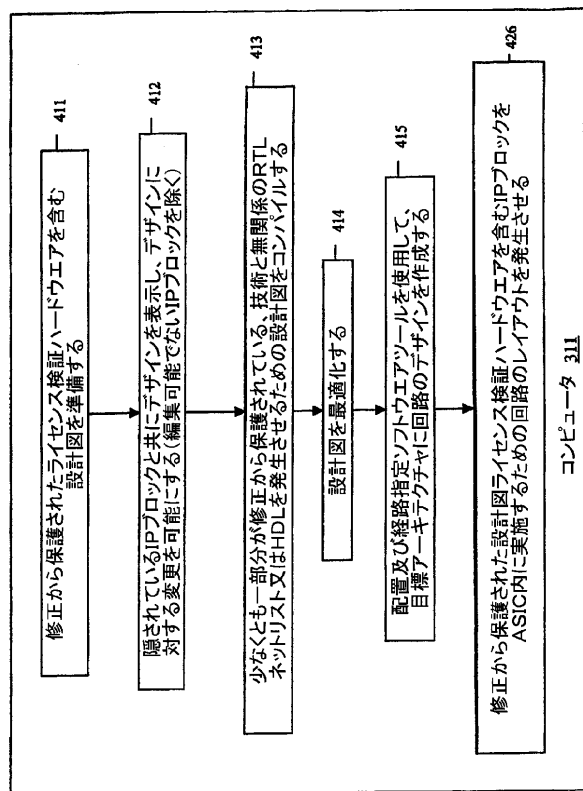


FIGURE 4C

【図 5】

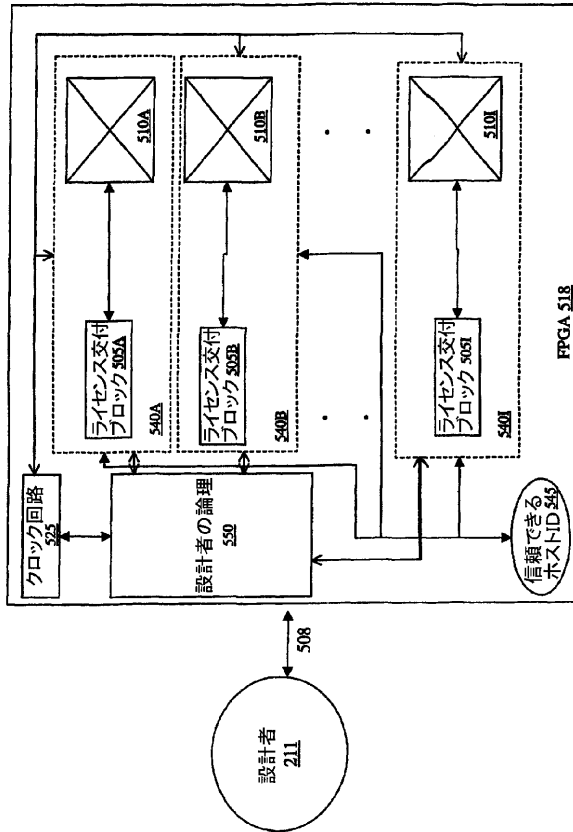


FIGURE 5

【図 6】

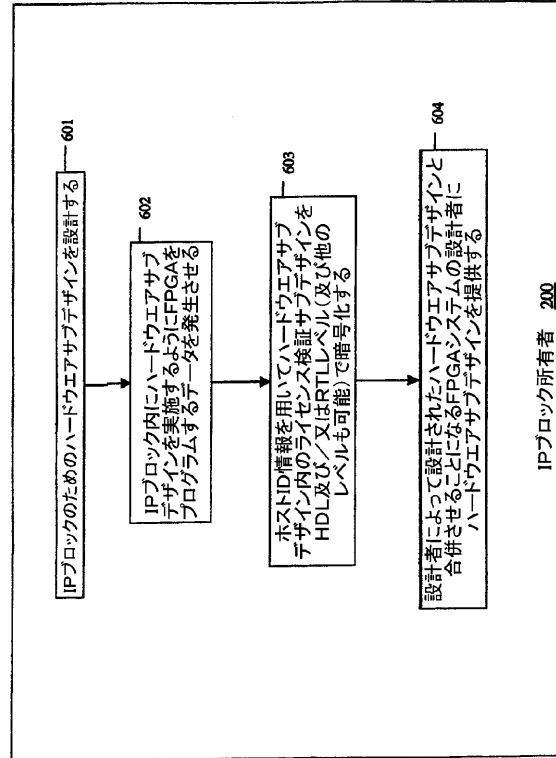


FIGURE 6

【図 7】

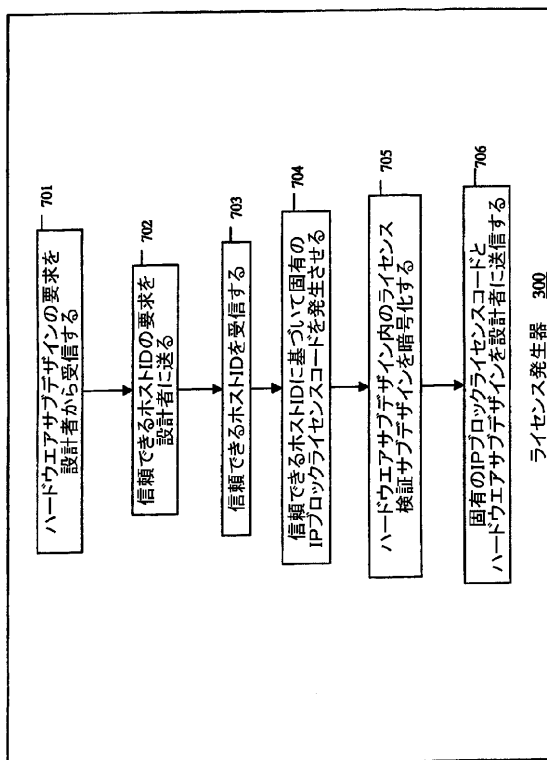


FIGURE 7

【図 8】

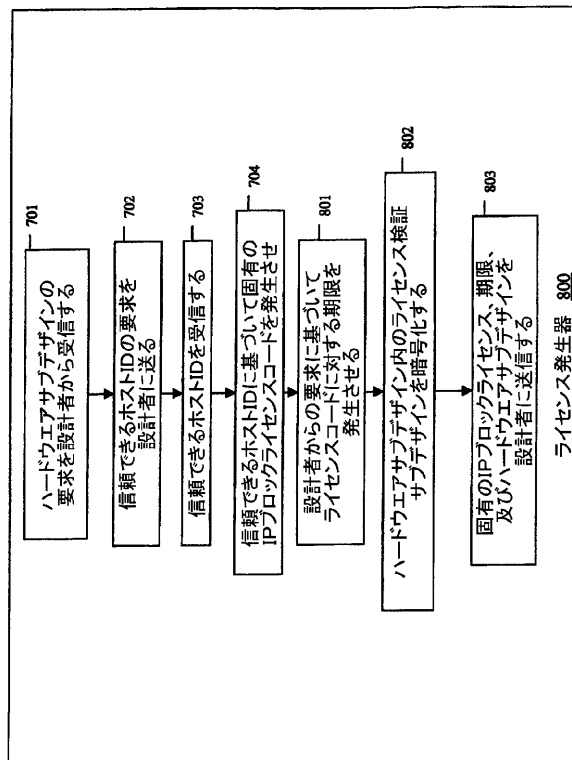


FIGURE 8

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International Application No.  
/US2005/034637

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> G06F17/50		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 357 037 B1 (BURNHAM JAMES L ET AL) 12 March 2002 (2002-03-12) column 1, line 30 - line 33 column 2, line 26 - column 4, line 19	1-104
X	US 2003/126450 A1 (MASTER PAUL L ET AL) 3 July 2003 (2003-07-03) paragraph '0003! paragraph '0010! - paragraph '0015!	1-104
A	US 2003/140255 A1 (RICCHETTI MICHAEL ET AL) 24 July 2003 (2003-07-24) paragraph '0003! - paragraph '0016!	1-104
A	US 2002/199110 A1 (KEAN THOMAS A) 26 December 2002 (2002-12-26) paragraph '0001! paragraph '0005! - paragraph '0016! paragraph '0059! - paragraph '0079!	1-104
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family		
Date of the actual completion of the international search 17 January 2006		Date of mailing of the international search report 30/01/2006
Name and mailing address of the ISA European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016		Authorized officer Anticoll, C

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International Application No

/US2005/034637

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6357037	B1	12-03-2002	NONE	
US 2003126450	A1	03-07-2003	AU 2002361772 A1 WO 03058390 A2	24-07-2003 17-07-2003
US 2003140255	A1	24-07-2003	NONE	
US 2002199110	A1	26-12-2002	NONE	

## フロントページの続き

(51)Int.Cl.

F I

テーマコード(参考)

H 0 4 L 9/00 6 7 5 D

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(72)発明者 マケルヴェイン ケニス エス

アメリカ合衆国 カリフォルニア州 9 4 0 2 4 ロス アルトス ヴィア ウェアタ 1 2 0 9

Fターム(参考) 5B017 AA03 AA07 BA06 BA07 BB10 CA15

5B046 AA08 BA02 BA03

5J104 AA07 AA16 EA03 EA04 EA15 KA02 KA04 KA15 NA02 NA05

NA27 NA37 NA38 NA39

【要約の続き】

【選択図】図2 A