(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2016/080380

発行日　平成29年8月31日(2017.8.31)

(43)国際公開日　平成28年5月26日(2016.5.26)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/56 (2013.01)	G06F 21/56	

審査請求 未請求　予備審査請求 未請求　（全 35 頁）

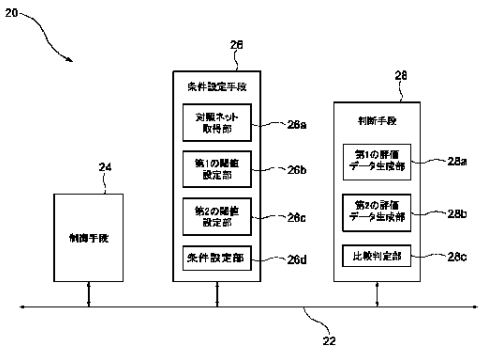
出願番号	特願2016-560230 (P2016-560230)
(21)国際出願番号	PCT/JP2015/082223
(22)国際出願日	平成27年11月17日(2015.11.17)
(31)優先権主張番号	特願2014-233953 (P2014-233953)
(32)優先日	平成26年11月18日(2014.11.18)
(33)優先権主張国	日本国(JP)

(71)出願人　899000068
学校法人早稲田大学
東京都新宿区戸塚町１丁目１０４番地
(74)代理人　100137800
弁理士　吉田　正義
(74)代理人　100148253
弁理士　今枝　弘充
(74)代理人　100148079
弁理士　梅村　裕明
(74)代理人　100158241
弁理士　吉田　安子
(72)発明者　戸川　望
日本国東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内

最終頁に続く

(54)【発明の名称】ハードウェアトロイの検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置

(57)【要約】
ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを備えることを特徴とする。
【選択図】なし



24 Control means
25 Condition setting means
25a Comparison net acquiring unit
25b First threshold setting unit
25c Second threshold setting unit
25d Condition setting unit
28 Determining means
28a First evaluation data generating unit
28b Second evaluation data generating unit
28c Comparing and assessing unit

【特許請求の範囲】
【請求項１】
集積回路のネットリスト中のハードウェアトロイを検出する検出方法であって、
前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、
前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを備えることを特徴とする検出方法。
【請求項２】
前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、
前記判断工程は、
前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断する
ことを特徴とする請求項１記載の検出方法。
【請求項３】
前記スコアは、
前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、
前記判断工程は、
前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断する
ことを特徴とする請求項２記載の検出方法。
【請求項４】
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、
前記判断工程は、
前記最大スコアが前記最大スコア閾値未満の場合、
前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネ

ット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断する
ことを特徴とする請求項３記載の検出方法。
【請求項５】
前記条件設定工程は、
前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、
前記判断工程は、
前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断する
ことを特徴とする請求項４記載の検出方法。
【請求項６】
集積回路のネットリスト中のハードウェアトロイを検出する処理をコンピュータに実行させるための検出プログラムであって、
前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、
前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを含む処理をコンピュータに実行させることを特徴とする検出プログラム。
【請求項７】
前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、
前記判断工程は、
前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断する
ことを特徴とする請求項６記載の検出プログラム。
【請求項８】
前記スコアは、
前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト

中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、
前記判断工程は、
前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断する
ことを特徴とする請求項７記載の検出プログラム。
【請求項９】
前記条件設定工程は、
前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、
前記判断工程は、
前記最大スコアが前記最大スコア閾値未満の場合、
前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断する
ことを特徴とする請求項８記載の検出プログラム。
【請求項１０】
前記条件設定工程は、
前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、
前記判断工程は、
前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断する
ことを特徴とする請求項９記載の検出プログラム。
【請求項１１】
集積回路のネットリスト中のハードウェアトロイを検出する検出装置であって、
前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定手段と、
前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断手段とを備えることを特徴とする検出装置。
【請求項１２】
前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、
前記条件設定手段は、
前記複数の既知ネットリストのそれぞれについて、前記集合ネットに含まれる前記構成ネ

ットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、
前記判断手段は、
前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断する
ことを特徴とする請求項１１記載の検出装置。
【請求項１３】
前記スコアは、
前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、
前記条件設定手段は、
前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、
前記判断手段は、
前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断する
ことを特徴とする請求項１２記載の検出装置。
【請求項１４】
前記条件設定手段は、
前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、
前記判断手段は、
前記最大スコアが前記最大スコア閾値未満の場合、
前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断する
ことを特徴とする請求項１３記載の検出装置。
【請求項１５】
前記条件設定手段は、
前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアトロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、
前記判断手段は、
前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在すると判断する
ことを特徴とする請求項１４記載の検出装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ハードウェアトロイの検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置に関する。
【背景技術】
【０００２】
近年、半導体業界においては、外部業者が情報処理装置に用いられる集積回路の製造に関わるようになったことから、集積回路の安全性が問題視されるようになっている。本来意図されていない機能（ハードウェアトロイ、以下「ＨＴ」とも記す。）を集積回路に挿入することが、第三者である外部業者において容易になったためであり、こうしたハードウェアトロイを検出することが求められている。
【０００３】
一般的には、ハードウェアトロイを検出するには、対象となる情報処理装置のハードウェアトロイに関する情報が必要とされてきた。ハードウェアトロイを含まない健全な設計データを利用して、ハードウェアトロイを検出する方法が提案されている（例えば、非特許文献１参照）。例えば、製造段階において挿入されたトロイの有無は、トロイが挿入されていない健全なチップと、トロイが挿入されたチップとの間で、物理的な重さや電力量、あるいは電磁波などについての差分をとることによって判断することができる。
【０００４】
しかしながら、ハードウェアトロイは、集積回路の製造段階のみならず設計段階においても挿入される可能性がある。設計段階では、製造段階の場合のような差分をとることができず、ハードウェアトロイに関する情報なしにトロイを検出する技術は未だ得られていないのが現状である。
【０００５】
図１４に示すように、ハードウェアトロイ（ＨＴ）回路４６が存在する回路４０においては、例えば通常回路４２を接続する通常ネット４４の一部４８にトリガー回路４６ｂが接続され、通常ネット４４の他の一部４９にペイロード回路４６ａが接続されている。ペイロード回路４６ａは、本来意図されていない機能を有し、トリガー回路４６ｂはペイロード回路４６ａを起動する。こうしたペイロード回路４６ａとトリガー回路４６ｂとによって、ＨＴ回路４６が構成される。
【０００６】
回路４０からＨＴ回路４６を完全に取り除くことができれば、ハードウェアトロイの危険性を完全に取り除くことが可能となる。
【先行技術文献】
【非特許文献】
【０００７】
【非特許文献１】B. Cha and S. K. Gupta, “Trojan detection via delay measurements: a new approach to select paths and vectors to maximize effectiveness and minimize cost,” in Proc. Design, Automation and Test in Europe (DATE), 2013, pp. 1265-1270
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、ＨＴ回路４６は必ずしも明確に存在せずに通常ネット４４に融合していることもあり、ＨＴ回路４６を区別して回路４０から完全に区別することは極めて困難である。
【０００９】
本発明は以上の点を考慮してなされたもので、集積回路のハードウェアトロイに関する

情報を用いずに、ハードウェアトロイを検出する検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置を提供することを目的とする。

【課題を解決するための手段】

【００１０】

本発明に係るハードウェアトロイの検出方法は、集積回路のネットリスト中のハードウェアトロイを検出する検出方法であって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを備えることを特徴とする。

【００１１】

上記検出方法においては、前記複数の既知ネットリストのそれぞれは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記被検ネットリストは、端子間ネットによって接続された一群の回路によって構成される構成ネットを少なくとも一つ含む集合ネットを、少なくとも一つ有し、前記条件設定工程は、前記複数の既知ネットリスト中のそれぞれについて、前記集合ネットに含まれる前記構成ネットの形態を基に、前記トロイネットを含む可能性がある構成ネットを対照ネットとして、前記複数の既知ネットリストから選択し、前記対照ネットにそれぞれ付与されるスコアに基づく条件設定を含み、前記判断工程は、前記被検ネットリストの中から前記対照ネットを検索し、前記検索された対照ネットのスコアを基に前記被検ネットリストの評価データを生成し、前記評価データと、前記設定された条件とを比較して、前記被検ネットリスト中のトロイネットの有無を判断することができる。

【００１２】

前記スコアは、前記複数の既知ネットリストの中で、ハードウェアトロイを含む前記既知ネットリストにのみ含まれる前記対照ネットの方が、ハードウェアトロイを含まない前記既知ネットリストにも含まれる前記対照ネットより大きく設定され、前記条件設定工程は、前記複数の既知ネットリストのそれぞれについて、含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記複数の既知ネットリスト中で最も大きいスコアを前記複数の既知ネットリストの最大スコアとし、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアを基に最大スコア閾値を設定する条件設定を含み、前記判断工程は、前記被検ネットリストに含まれる集合ネット毎に対照ネットのスコアを加算して合計スコアを得、前記合計スコアのうち、前記被検ネットリスト中で最も大きいスコアを前記被検ネットリストの最大スコアとし、前記被検ネットリストの前記最大スコアが前記最大スコア閾値以上のとき、前記被検ネットリストにトロイネットが存在すると判断することができる。

【００１３】

また、前記条件設定工程は、前記複数の既知ネットリストのそれぞれについて、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記ハードウェアトロイを含む前記既知ネットリストの最大スコアネット数を基に最大スコアネット数閾値を設定する条件設定を含み、前記判断工程は、前記最大スコアが前記最大スコア閾値未満の場合、前記被検ネットリスト中で、前記最大スコアを有する集合ネットの数である最大スコアネット数を求め、前記被検ネットリストの前記最大スコアが前記最大スコア閾値未満であって、前記被検ネットリストの最大スコアネット数が、前記最大スコアネット数閾値より大きいとき、前記被検ネットリストにトロイネットが存在しないと判断することができる。

【００１４】

さらに、前記条件設定工程は、前記複数の既知ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数を求め、前記ハードウェアト

ロイを含む既知ネットリストのクロック数と前記ハードウェアトロイを含まない既知ネットリストのクロック数とを基に最大一定サイクル数閾値を設定する条件設定をさらに含み、前記判断工程は、前記被検ネットリスト中、前記最大スコアを有する集合ネットが、所定時間内に一定値を出力するクロック数をさらに求め、前記被検ネットリストの最大スコアが前記最大スコア閾値未満であって、前記被検ネットリスト最大スコアネット数が、前記最大スコアネット数閾値以下であり、かつ、前記被検ネットリストについてのクロック数が前記最大一定サイクル数閾値以上の場合に、前記ハードウェアトロイが存在する判断することができる。

【００１５】

本発明に係るハードウェアトロイの検出プログラムは、集積回路のネットリスト中のハードウェアトロイを検出する処理をコンピュータに実行させるための検出プログラムであって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定工程と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断工程とを含む処理をコンピュータに実行させることを特徴とする。

【００１６】

本発明に係るハードウェアトロイの検出装置は、集積回路のネットリスト中のハードウェアトロイを検出する検出装置であって、前記ハードウェアトロイの存在を示すトロイネットを含む既知ネットリストと、前記トロイネットを含まない既知ネットリストとの両方を含む複数の既知ネットリストに基づき、前記トロイネットの有無を判断するための条件を設定する条件設定手段と、前記条件に基づき、被検ネットリストとしての前記集積回路のネットリストを評価し、得られた評価結果から前記被検ネットリスト中のトロイネットの有無を判断する判断手段とを備えることを特徴とする。

【発明の効果】

【００１７】

本発明によれば、公知ネットリストの既知情報に基づいて得られた条件に基づき、被検ネットリスト中のトロイネットの有無を判断することにより、公知ネットリストと種類が異なるネットリストを有する集積回路にハードウェアトロイが含まれるか否かを判断することができる。したがって本発明によれば、対象となる集積回路の、ハードウェアトロイが挿入されていない健全なネットリストやハードウェアトロイに関する公知情報を用いずに、上記集積回路にハードウェアトロイが含まれるか否かを判断することができる。

【図面の簡単な説明】

【００１８】

【図１】本実施形態のハードウェアトロイ検出装置の使用状態を示す図である。

【図２】本実施形態のハードウェアトロイ検出装置の構成を示すブロック図である。

【図３】Case 1の対照ネットを示す説明図である。

【図４】Case 2の対照ネットを示す説明図である。

【図５】Case 3の対照ネットを示す説明図である。

【図６】Case 4の対照ネットを示す説明図である。

【図７】Case 5の対照ネットを示す説明図である。

【図８】Case 6の対照ネットを示す説明図である。

【図９】Case 7の対照ネットを示す説明図である。

【図１０】Case 8の対照ネットを示す説明図である。

【図１１】Case 9の対照ネットを示す説明図である。

【図１２】最大一定サイクル数を説明する図である。

【図１３】ネットリスト中のハードウェアトロイの有無を判断する比較判定の処理手順を示すフローチャートである。

【図１４】ハードウェアトロイ（ＨＴ）回路を模式的に説明する図である。

【発明を実施するための形態】
【００１９】
１．全体構成
以下、図面を参照して本発明の実施の形態を詳述する。図１に示すように情報処理装置１０は、ハードウェアトロイ検出装置（以下、「検出装置」という。）２０に接続される。これにより、情報処理装置１０が備えるネットリスト（以下、「被検ネットリスト」という。）が検出装置２０に入力され得る。被検ネットリストは、情報処理装置１０に含まれる各種回路同士を接続する配線の一覧を記述した設計データである。被検ネットリストは、情報処理装置を構成する回路の階層に合わせて構築された階層を有し、最上位層である集合ネットと、当該集合ネットの下位層である構成ネットを備える。集合ネット及び構成ネットは、情報処理装置の規模に応じて１つ以上設けられる。構成ネットは、回路の端子間を繋ぐ配線（以下、「端子間ネット」という。）によって接続された一群の回路によって構成される。
【００２０】
本図に示す情報処理装置１０は、端子間ネットである通常ネット４４で接続された通常回路４２で構成される。情報処理装置１０がハードウェアトロイを含む場合、さらにＨＴ回路４６が挿入される。ＨＴ回路４６は、ペイロード回路４６ａ、トリガー回路４６ｂを含む。ＨＴ回路４６は、ハードウェアトロイに含まれている特定の端子間ネットであるトロイネットが、ペイロード回路４６ａ、トリガー回路４６ｂ、またはこれら２つの回路の間に存在する。情報処理装置１０の被検ネットリストには、端子間ネットとして、通常ネット４４と、トロイネットとが含まれる。
【００２１】
図２に示すように、検出装置２０は、検出装置２０の各種機能を統括的に制御する制御手段２４、条件設定手段２６、および判断手段２８が、制御バス２２を介して接続されている。
【００２２】
制御手段２４は、予め格納されている基本プログラムなどの各種プログラムを読み出して、これら各種プログラムに従って、検出装置２０全体を制御するようになされている。
【００２３】
条件設定手段２６は、対照ネット取得部２６ａと、第１の閾値設定部２６ｂと、第２の閾値設定部２６ｃと、条件設定部２６ｄとから構成される。条件設定手段２６は、被検ネットリスト中におけるトロイネットの有無を判断するための基準を、トロイネットの有無が既知である公知のネットリスト（以下、「公知ネットリスト」という。）から取得し、得られた基準に基づいてトロイネットの有無を判断するための閾値および条件を設定する。なお、実施の形態では、既知ネットリストとして公知ネットリストを使用しているが、必ずしも既知ネットリストが公知である必要はない。トロイネットの有無が既知であれば、公知でなくても構わない。
【００２４】
判断手段２８は、第１の評価データ生成部２８ａと第２の評価データ生成部２８ｂと比較判定部２８ｃとから構成される。判断手段２８は、情報処理装置１０の被検ネットリストを、条件設定手段２６で設定された基準で評価して、得られた評価結果（評価データ）を条件設定手段２６で設定された閾値を含む条件で判定する。こうして、情報処理装置１０の被検ネットリスト中のトロイネットの有無を判断することによってハードウェアトロイを検出する。
【００２５】
（１）条件設定手段
次に、条件設定手段２６の各部について説明する。
【００２６】
（対照ネット取得部）
対照ネット取得部２６ａは、端子間ネットに関する情報が公開されているゲートレベル

の公知ネットリストに基づき、トロイネットの特徴を抽出する。対照ネット取得部２６ａは、例えばネットワークを介して情報記録サーバーに接続し、公知ネットリストを、情報記録サーバーからランダムに複数個ダウンロードして、これらを図示しない記憶部に記憶する。

【００２７】

公知ネットリストは、例えば米国のサイト（Trust-HUB）に公開されているベンチマークのネットリストを利用することができる。すなわち、公開されているベンチマークの中から、ランダムに複数、例えば１０個選択してもよい。ベンチマークには、トロイネットを含むとされているベンチマーク（HT-inserted）とトロイネットを含まないとされているベンチマーク（HT-free）とが含まれる。

【００２８】

Trust-HUBにおけるベンチマークは、ゲートレベルのネットリストが公開されている。ベンチマークは、端子間ネットで接続されたゲート、フリップフロップ、加算器などのセルを含むいくつかのサブモジュールからなる。

【００２９】

下記表１に示されるように、これらのベンチマークは、ハードウェアトロイの有無（HT-inserted／HT-free）および端子間ネット数が既知である。下記表１に示す１０個のベンチマークのうちでは、７個が“HT-inserted”であり、３個が“HT-free”である。ベンチマークには、ハードウェアトロイに含まれているトロイネット（以下、「公知トロイネット」という。）の名称、種類およびその存在箇所といった情報も、ネットリスト中に明らかにされている。

【００３０】

【表１】

ベンチマーク	タイプ	ネット数
b19	HT-free	108,332
EthernetMAC10GE	HT-free	103,206
s35932	HT-free	6,423
EthernetMAC10GE-T700	HT-inserted	103,220
RS232-T1000	HT-inserted	311
s15850-T100	HT-inserted	2,456
s38417-T100	HT-inserted	5,819
s38584-T200	HT-inserted	7,580
vga_lcd-T100	HT-inserted	70,162
wb_conmax-T100	HT-inserted	22,197

【００３１】

対照ネット取得部２６ａは、公知ネットリストに基づき、トロイネットである可能性がある端子間ネット（以下、「疑トロイネット」という。）を見出す。すなわち、疑トロイネットは、公知ネットリストの集合ネットに含まれる構成ネットの形態、すなわち各種回路の組み合わせや個数等から見出すことができる。疑トロイネットを含む構成ネットを対照ネットと呼ぶ。例えば、上記表１に示した１０個のベンチマークから、図３～１１に示す９個の対照ネットを見出すことができる。図３～１１中、LSLG(little switching logic gate)は、AND回路，NAND回路，OR回路，NORゲート回路を意味する。図中の太線が疑ト

ロイネットである。ハードウェアトロイは動作し難く制御性が高いため、特定の条件でのみ動作する。すなわち、ハードウェアトロイは、スイッチング確率が低い。図３～１１に示したCase 1～9の対照ネットはいずれも、こうした特徴を含むものである。Case 1～9の各対照ネットについて以下に説明する。

【００３２】

Case 1（図３）においては、1st LSLGの入力として2nd LSLGの出力が含まれている。2nd LSLGの入力の数が６以上であれば、1st LSLGの出力の端子間ネットが疑トロイネットである。2nd LSLGは、入力の数が２つの２入力のものに限定されず、３入力または４入力のものでもよい。

【００３３】

Case 2（図４）は、Case 1の特別な場合であり、Case 1より動作し難い。1st LSLGの入力として2nd LSLGの出力を含み、この2nd LSLGの入力の数が１６個以上の場合、または2nd LSLGの入力として3rd LSLGの出力を含み、この3rd LSLGの入力の数が１６個以上の場合、2nd LSLGの出力を入力として含む1st LSLGの出力の端子間ネットが疑トロイネットである。

【００３４】

Case 3（図５）は、MUX (multiplexer)の選択信号の端子間ネットが疑トロイネットである。

【００３５】

Case 4（図６）においては、ADDER（半加算器または全加算器）の出力を入力としてもつセルを2nd any cellとし、2nd any cellの出力を入力としてもつセルを1st any cellとする。この場合、1st any cellの入力および出力の端子間ネットは、全て疑トロイネットである。全ての2nd any cellにADDERが接続されている必要はなく、図示するように１つの2nd any cellにADDERが接続されていれば、このCase 4に該当する。

【００３６】

Case 5（図７）は、FF（フリップフロップ）を含むサブモジュールの主出力の端子間ネットが疑トロイネットである。

【００３７】

Case 6（図８）においては、他のネットを介さずに、“０”または“１”がFFに直接入力されており、特殊なケースである。このようなFFの出力およびクロックの端子間ネットは、疑トロイネットである。

【００３８】

Case 7（図９）においては、FFのクロックがCase 2の端子間ネット（疑トロイネット）である。Case 2のネットは極めて動き難いので、このようなFFの入力、出力、およびクロックの端子間ネットの全ては、疑トロイネットである。

【００３９】

Case 8（図１０）においては、構成ネットより下位のサブモジュールネットの数が22000以上のサブモジュールにおいて、任意セルの入力の端子間ネットの一つが主入力であり、もう一つはCase 2の端子間ネット（疑トロイネット）である。この場合、Case 2の疑トロイネットは、真のトロイネット（以下「真トロイネット」という。）である可能性がより高い。

【００４０】

Case 9（図１１）においては、スキャンモードとノーマルモードとを制御するTEST-SE信号の否定信号がセルに入力されている。こうしたセルの入力および出力の端子間ネットは、疑トロイネットである。

【００４１】

上記対照ネットには、疑トロイネットが真トロイネットである可能性の高さに適応したスコアが付与される。スコアは、疑トロイネットが真トロイネットである可能性の高さを反映できるように設定する。すなわち、“HT-inserted”の公知ネットリストのみに含まれている対照ネットは、“HT-inserted”および“HT-free”の両方の公知ネットリストに

含まれている対照ネットよりも、真トロイネットを含む可能性が高いので、大きなスコアが与えられる。

【００４２】

例えば、上記表１に示した１０個のベンチマークのネットリストと前述の９個の対照ネット（Case 1～9）とを比較したところ、Case 6～9の対照ネットは、７個の“HT-inserted”のベンチマークのみに存在することが確認された。残りのCase 1～5の対照ネットは、７個の“HT-inserted”のベンチマークおよび３個の“HT-free”のベンチマークの全てに確認された。Case 1～5の対照ネットは、疑トロイネットを有しているにもかかわらず、Case 1～5の対照ネットが含まれている公知ネットリストのうちの３個は“HT-free”である。すなわち、Case 6～9の対照ネットのほうが、Case 1～5の対照ネットよりも真トロイネットを含む可能性が高いといえる。このような真トロイネットを含む可能性の高さを反映して、Case 1～5の対照ネットのスコアを１と設定し、Case 6～9の対照ネットのスコアを２と設定する。真トロイネットを含む可能性の高さを反映した所定の大きさのスコアを付与することにより、対照ネットは、被検ネットリスト中のトロイネットの有無を判断するための基準となる。

【００４３】

以上のとおり、対照ネット取得部２６ａは、公知ネットリストから対照ネットを取得し、真トロイネットを含む可能性の高さを反映した所定の大きさのスコアを対照ネットに付与し、これを図示しない記憶部に記憶する。

【００４４】

（第１の閾値設定部）

第１の閾値設定部２６ｂは、第１の閾値としての最大スコア閾値（T_{score}）（T_{score}は正数）および最大スコアネット数閾値（T_{number}）（T_{number}は正数）を選択する。

【００４５】

最大スコア閾値（T_{score}）は、最大スコア（X_{score}）中から選択される。最大スコア（X_{score}）は、集合ネットに含まれる対照ネットのスコアを加算した合計スコアのうち、公知ネットリスト中で最も大きいスコアとする。

【００４６】

最大スコアネット数閾値（T_{number}）は、最大スコアネット数（X_{number}）の中から選択される。最大スコアネット数（X_{number}）は、公知ネットリスト中の最大スコア（X_{score}）を有する集合ネット（以下、「最大スコアネット」という。）の数とする。

【００４７】

具体的には、第１の閾値設定部２６ｂは、記憶部から受け取った“HT-inserted”の公知ネットリストおよび“HT-free”の公知ネットリスト中の各集合ネットに含まれる構成ネットのそれぞれを、対照ネットと比較する。第１の閾値設定部２６ｂは、構成ネットが対照ネットと一致する場合、当該対照ネットのスコアを集合ネット毎に加算する。この集合ネット毎に加算されたスコアを合計スコアと呼ぶ。合計スコアのうち、公知ネットリスト中、最も大きいスコアを最大スコア（X_{score}）、最大スコア（X_{score}）を有する集合ネットを最大スコアネットとする。また、第１の閾値設定部２６ｂは、公知ネットリスト中の最大スコアネットの数を最大スコアネット数（X_{number}）とする。

【００４８】

第１の閾値設定部２６ｂは、最大スコアネットと、記憶部に記憶された公知トロイネットの情報を比較して、最大スコアネット中に公知トロイネットが含まれる公知ネットリストを抽出する。第１の閾値設定部２６ｂは、公知トロイネットが含まれる公知ネットリストのうち、最大スコア（X_{number}）の最も小さい値を選択して１を加えた値を最大スコア閾値（T_{score}）として図示しない記憶部に記憶する。

【００４９】

例えば、上記表１に示した１０個のベンチマークを前述の９個の対照ネット（Case 1～9）と比較し、各ベンチマークのネットリストについて確認された対照ネットの数を下記表２にまとめる。

【００５０】
【表２】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9
b19	598	38	1108	16586	130	0	0	0	0
EthernetMAC10GE	344	55	2595	417	193	0	0	0	0
s35932	0	0	0	0	420	0	0	0	0
Ethernet MAC10GE-T700	347	56	2595	417	193	3	3	0	0
RS232-T1000	11	2	2	0	12	0	0	0	0
s15850-T100	80	11	1	0	160	2	4	0	3
s38417-T100	206	4	0	0	206	0	0	0	0
s38584-T200	112	4	4	87	405	0	0	0	0
vga_lcd-T100	19	0	1954	168	209	0	0	0	0
wb_conmax-T100	466	55	0	0	1516	0	0	1	0

【００５１】
各ベンチマークの集合ネット毎に合計スコアを算出し、その最大値を最大スコア（X_{score}）とし、最大スコア（X_{score}）を有する集合ネットを最大スコアネットとする。上述したとおり、Case 1～5のスコアは１であり、Case 6～9のスコアは２である。例えば、Case 1～9の対照ネットのうちの１つも含まない集合ネットは、合計スコアが０であり、Case 1の対照ネットを１つ含む集合ネットの合計スコアは１である。また、Case 1の対照ネットを１つとCase 6の対照ネットを１つ含む集合ネットの合計スコアは３である。
【００５２】
得られた結果を、最大スコアネットの内容（通常ネット／トロイネット）とともに下記表３にまとめる。ここで、表３中の最大スコアネットの内容は、公知トロイネットの情報に基づくものである。
【００５３】

【表３】

ベンチマーク	最大ｽｺｱ（X_{score}）	最大ｽｺｱﾈｯﾄ数（X_{number}）	最大ｽｺｱﾈｯﾄの内容
b19	2	73	通常ﾈｯﾄのみ
EthernetMAC10GE	2	55	通常ﾈｯﾄのみ
s35932	1	420	通常ﾈｯﾄのみ
EthernetMAC10GE-T700	**6**	1	ﾄﾛｲﾈｯﾄのみ
RS232-T1000	2	2	ﾄﾛｲﾈｯﾄのみ
s15850-T100	**6**	1	ﾄﾛｲﾈｯﾄのみ
s38417-T100	2	**5**	通常ﾈｯﾄとﾄﾛｲﾈｯﾄ
s38584-T200	**3**	1	ﾄﾛｲﾈｯﾄのみ
vga_lcd-T100	2	2	ﾄﾛｲﾈｯﾄのみ
wb_conmax-T100	**4**	1	ﾄﾛｲﾈｯﾄのみ

【００５４】
上記表３に示されるように、最大スコア（X_{score}）が３以上のベンチマーク（Ethernet（登録商標）MAC10GE-T700、s15858-T100、s38584-T200、wb_conmax-T100）において、最大スコアネットに含まれている対照ネットは全てトロイネットである。ベンチマーク（RS232-T1000、s38417-T100、vga_lcd-T100）に示されているように、最大スコア（X_{score}）が２の最大スコアネットにも公知トロイネットが含まれている。公知トロイネットを含む最大スコアネットの最大スコアの値は、２が最小である。最大スコアの最小値に１を加えた値（最小値＋１）を、最大スコア閾値（T_{score}）とする。すなわち、最大スコア（X_{score}）の値が最大スコア閾値（T_{score}）以上であれば、最大スコアネットにトロイネットが含まれる可能性が高いといえる。表３の例では、最大スコア閾値（T_{score}）は３である。
【００５５】
なお、本実施の形態では、上述のような手法で最大スコア閾値（T_{score}）を求めたが、他の手法により最大スコア閾値（T_{score}）を求めることも可能である。例えば、最大スコアネットに含まれている対照ネットが全てトロイネットとなる最小の値を、最大スコア閾値（T_{score}）とするなどの手法が挙げられる。
【００５６】
上記表３によれば、公知トロイネットを含む最大スコアネット数（X_{number}）は比較的小さく、その値は最大でも５である。これに対して、通常ネットのみを含む最大スコアネット数（X_{number}）は大きく、その値は最小でも５５である。最大スコア（X_{score}）が高いほど最大スコアネット数（X_{number}）は減少し、最大スコア（X_{score}）が低いほど最大スコアネット数（X_{number}）は増加する。
【００５７】
したがって、最大スコアネット数（X_{number}）が十分に大きなネットリストは、トロイネットを含まない“HT-free”である可能性が高いと判断する。上記表３によれば、公知トロイネットを含む最大スコアネットのうち、最大スコアネット数（X_{number}）の最も大きな値は、ベンチマーク（s38417-T100）の５である。
【００５８】
この場合、ベンチマーク（s38417-T100）の最大スコアネット数（X_{number}）である５を、最大スコアネット数閾値（T_{number}）とする。すなわち、最大スコアネット数（X_{number}）が最大スコアネット数閾値（T_{number}）以下であれば、最大スコアネットにトロイネッ

トが含まれる可能性が高いといえる。こうして、最大スコアネット数閾値（T_{number}）が選択される。

【００５９】

以上のとおり、第１の閾値設定部２６ｂは、対照ネットと公知トロイネットの情報を比較することにより、最大スコア閾値（T_{score}）と最大スコアネット数閾値（T_{number}）とを選択して第１の閾値として取得し、これを図示しない記憶部に記憶する。

【００６０】

（第２の閾値設定部）

第２の閾値設定部２６ｃは、公知ネットリストにおける最大スコアネットについて最大一定サイクル数（X_{cycle}）を生成し、第２の閾値としての最大一定サイクル数閾値（T_{cycle}）（T_{cycle}は正数）を選択する。具体的には、第２の閾値設定部２６ｃは、最大スコア（X_{score}）が最大スコア閾値（T_{score}）未満の最大スコアネットに対して、論理シミュレータと呼ばれる既存のソフトウェア（例えばＶＣＳ（登録商標））でランダムデータを入力して１Ｍクロック間における値の変化をシミュレートし、一定値を出力する最長のクロック数を最大一定サイクル数（X_{cycle}）として得て、これを図示しない記憶部に記憶する。

【００６１】

第２の閾値設定部２６ｃは、得られた最大一定サイクル数（X_{cycle}）のなかから、最小の値を最大一定サイクル数閾値（T_{cycle}）として選択する。

【００６２】

例えば、図１２に示すように、１Ｍクロック間で一定値を出力する最長のクロック数を、最大一定サイクル数（Max constant cycles）として定義する。最大一定サイクル数が高いほど、最大スコアネットはトロイネットを含む可能性が高くなる。これは、次のように説明される。トロイネットは動作し難く制御性が高いため、トロイネットが存在する場合には、長期間にわたって一定値が出力されることが予測される。この点に着目し、所定のクロック間で一定値が出力されるサイクル数（最大一定サイクル数）によって、最大スコアネットにトロイネットが含まれるか否かを判断する。

【００６３】

下記表４には、ベンチマーク（RS232-T1000、s38417-T100、およびvga_lcd-T100）について、最大一定サイクル数（X_{cycle}）を公知トロイネットの名称とともにまとめる。下記表４に示した３個のベンチマークは、上記表３に示したとおり最大スコア（X_{xvore}）が２で、最大スコアネットにトロイネットが含まれている。

【００６４】

【表４】

ベンチマーク	トロイネット名	最大一定サイクル数（X_{cycle}）
RS232-T1000	iRECEIVER_CTRL	999,999
	iCTRL	999,999
s38417-T100	Tj_Trigger	999,997
	Tj_OUT1234	999,997
	Tj_OUT5678	**999,996**
vga_lcd-T100	Tj_Trigger	999,999
	Tj_OUT1	999,999

【００６５】

上記表４によれば、ベンチマーク（RS232-T1000、s38417-T100、およびvga_lcd-T100）は全て、最大スコアネットの最大一定サイクル数（X_{cycle}）が999,996サイクル以上である。このことから、最大一定サイクル数（X_{cycle}）が999,996サイクル以上の最大スコア

ネットにはトロイネットが含まれていると判断して、999,996サイクルを最大一定サイクル数閾値（T_{cycle}）とする。すなわち最大一定サイクル数閾値（T_{cycle}）（999,996サイクル）は、公知トロイネットを含む最大スコアネットについての最大一定サイクル数（X_{cycle}）の最小値である。

【００６６】

なお、上記表３，４からは、最大一定サイクル数（X_{cycle}）が999,996サイクル以上の場合には、最大スコアネットに公知トロイネットが含まれていることがわかる。その一方、下記表５に示すように、最大一定サイクル数（X_{cycle}）が999,996サイクル以上の最大スコアネットに通常ネットが含まれていることも確認された。

【００６７】

【表５】

ベンチマーク	最大スコア（X_{score}）	最大一定サイクル数が999,996以上の最大スコアネットの数	最大スコアネットの内容
b19	2	59	通常ネットのみ
EthernetMAC10GE	2	10	通常ネットのみ
s35932	1	0	該当せず
RS232-T1000	2	2	トロイネットのみ
s38417-T100	2	3	トロイネットのみ
vga_lcd-T100	2	2	トロイネットのみ

【００６８】

上記表５に示されるとおり、最大スコア（X_{score}）が１のベンチマーク（s35932）には、最大一定サイクル数（X_{cycle}）が999,996サイクル以上の最大スコアネットは存在しない。ベンチマーク（b19およびEthernetMAC10GE）は、いずれも最大スコア（X_{score}）が２で、最大スコアネットに含まれているのは通常ネットのみである。公知トロイネットが含まれていないにもかかわらず、ベンチマーク（b19およびEthernetMAC10GE）には、最大一定サイクル数（X_{cycle}）が999,996サイクル以上の最大スコアネットが存在している。そのような最大スコアネットの数は、それぞれ５９および１０である。

【００６９】

最大スコア（X_{score}）と最大一定サイクル数（X_{cycle}）とを用いても、公知トロイネットの有無は必ずしも正確に判断されていない。これは、回路の規模（端子間ネット数）が関連しているものと推測される。上記表１に示されるように、ベンチマーク（s35932）の端子間ネット数は6,423であり、ベンチマーク（b19およびEthernetMAC10GE）の端子間ネット数は、それぞれ108,332および103,206である。こうした端子間ネット数からわかるように、ベンチマーク（s35932）は小規模回路であり、ベンチマーク（b19およびEthernetMAC10GE）は大規模回路である。最大スコア（X_{score}）および最大一定サイクル数（X_{cycle}）に加えて、最大スコアネット数（X_{number}）を用いることによって、小規模回路のみならず、大規模回路に対しても誤検出なく正確にトロイネットを検出できる。

【００７０】

以上のとおり、第２の閾値設定部２６ｃは、最大一定サイクル数閾値（T_{cycle}）を第２の閾値として取得して、これを図示しない記憶部に記憶する。

【００７１】

（条件設定部）

条件設定部２６ｄは、最大スコア閾値（T_{score}）、最大スコアネット数閾値（X_{number}

）、および最大一定サイクル数閾値（X_{cycle}）を記憶部から受け取って、これらの閾値を用いて、トロイネットの有無について、記憶されている公知ネットリストのハードウェアトロイの有無（HT-inserted／HT-free）と一致した結果が得られる条件を設定する。トロイネットの有無を判断する条件は、以下の（Ａ），（Ｂ）である。いずれかの条件を満たす場合には、トロイネットが存在する。

（Ａ）最大スコア（X_{score}）が最大スコア閾値（T_{score}）（T_{score}は正数）以上

（Ｂ）最大スコア（X_{score}）が最大スコア閾値（T_{score}）（T_{score}は正数）未満、最大スコアネット数（X_{number}）が最大スコアネット数閾値（T_{number}）（T_{number}は正数）以下、かつ最大一定サイクル数（X_{cycle}）が最大一定サイクル数閾値（T_{cycle}）（T_{cycle}は正数）以上

【００７２】

例えば、上記表１に示した１０個のベンチマークについては、トロイネットが存在するのは、次のいずれかの場合である。

（ａ）最大スコア（X_{score}）が３以上

（ｂ）最大スコア（X_{score}）が３未満、最大スコアネット数（X_{number}）が５以下、かつ最大一定サイクル数（X_{cycle}）が999,996サイクル以上

【００７３】

上記表１に示した１０個のベンチマークについて、条件（ａ），（ｂ）と各ベンチマークについての既知情報のハードウェアトロイの有無（HT-free／HT-inserted）とを、下記表６にまとめる。下記表６においては、条件（ａ）または条件（ｂ）を満たしていれば“○”としている。なお、「条件（ａ）または条件（ｂ）」を、「条件（ａ／ｂ）」と記載する。

【００７４】

【表６】

ベンチマーク	条件		タイプ
	a	b	
b19	―	―	HT-free
EthernetMAC10GE	―	―	HT-free
s35932	―	―	HT-free
EthernetMAC10GE-T700	○		HT-inserted
RS232-T1000		○	HT-inserted
s15850-T100	○		HT-inserted
s38417-T100		○	HT-inserted
s38584-T200	○		HT-inserted
vga_lcd-T100		○	HT-inserted
wb_conmax-T100	○		HT-inserted

【００７５】

“HT-free”である３個のベンチマークは、条件（ａ／ｂ）を満たしていない。一方、“HT-inserted”である７個のベンチマークは、条件（ａ／ｂ）を満たしており、条件（ａ／ｂ）による判定はベンチマークの既知の情報によるハードウェアトロイの有無（HT-free／HT-inserted）と完全に一致している。このように検出装置１０は、最大スコア閾値

（T_{score}）、最大スコアネット数閾値（T_{number}）、および最大一定サイクル数閾値（T_{cycle}）に基づいたトロイネットの有無を決定する条件（ａ／ｂ）を用いて判定することによって、ベンチマークが“HT-free”および“HT-inserted”のいずれであるかを正しく識別できる。

【００７６】

以上のとおり、条件設定部２６ｄは、最大スコア閾値（T_{score}）、最大スコアネット数閾値（T_{number}）、および最大一定サイクル数閾値（T_{cycle}）を用いてトロイネットの有無を判断する条件（Ａ），条件（Ｂ）を設定し、これを図示しない記憶部に記憶する。

【００７７】

こうして、条件設定手段２６は、トロイネットを含む可能性を反映した大きさのスコアが付与された複数の対照ネットを取得するとともに、第１の閾値としての最大スコア閾値（T_{score}）（T_{score}は正数）および最大スコアネット数閾値（T_{number}）（T_{number}は正数）と、第２の閾値としての最大一定サイクル数閾値（T_{cycle}）（T_{cycle}は正数）を設定し、第１および第２の閾値を用いてトロイネットの有無を判断する条件を設定する。

【００７８】

条件設定手段２６は、基準としての対照ネットを、閾値（最大スコア閾値（T_{score}）（T_{score}は正数）、最大スコアネット数閾値（T_{number}）（T_{number}は正数）、最大一定サイクル数閾値（T_{cycle}）（T_{cycle}は正数））およびこれを用いて設定された条件とともに、図示しない記憶部に記憶する。記憶された基準、閾値および条件は、ネットリスト中のトロイネットの有無を判断するために判断手段２８に送出される。

【００７９】

（２）判断手段

次に、判断手段２８について説明する。判断手段２８は、情報処理装置１０から被検ネットリストを取得し、当該被検ネットリストを記憶部から受け取った基準で評価する。判断手段２８は、評価結果を評価データとして得、記憶部から受け取った条件で評価データを判定してハードウェアトロイの有無を判断する。

【００８０】

また、判断手段２８は、公知ネットリストから抽出した基準としての対照ネットを、閾値（最大スコア閾値（T_{score}）（T_{score}は正数）、最大スコアネット数閾値（T_{number}）（T_{number}は正数）、最大一定サイクル数閾値（T_{cycle}）（T_{cycle}は正数））および条件とともに図示しない記憶部から適宜受け取る。

【００８１】

（第１の評価データ生成部）

第１の評価データ生成部２８ａは、被検ネットリストについて、最大スコアネットに関する情報（最大スコア（X_{score}）および最大スコアネット数（X_{number}））を得る。被検ネットリストについての最大スコア（X_{score}）および最大スコアネット数（X_{number}）は、条件設定手段２６における第１の閾値設定部２６ｂについて説明した手順と同様の手順で得られる。

【００８２】

こうして、第１の評価データ生成部２８ａは、被検ネットリストについて最大スコア（X_{score}）と最大スコアネット数（X_{number}）とを得て、これを第１の評価データとして図示しない記憶部に記憶する。記憶された第１の評価データは、比較判定部２８ｃに送出される。第１の評価データは、被検ネットリストの中から対照ネットを検索し、検索された対照ネットのスコアを基に生成される。

【００８３】

（第２の評価データ生成部）

第２の評価データ生成部２８ｂは、被検ネットリストにおける最大スコアネットについて、最大一定サイクル数（X_{cycle}）を生成する。被検ネットリストについての最大一定サイクル数（X_{cycle}）は、条件設定手段２６における第２の閾値設定部２６ｃについて説明した手順と同様の手順で得られる。

【００８４】
こうして、第２のデータ生成部２８ｂは、被検ネットリストについて最大一定サイクル数（X_{cycle}）を得て、これを第２の評価データとして図示しない記憶部に記憶する。記憶された第２の評価データは、比較判定部２８ｃに送出される。
【００８５】
（比較判定部）
比較判定部２８ｃにおいては、比較判定プログラムに従って比較判定処理が行われる。具体的には、比較判定部２８ｃは、被検ネットリストから得た第１の評価データおよび第２の評価データを、第１の閾値および第２の閾値に基づいて得られた条件と比較し、被検ネットリストにトロイネットが含まれるか否かを判定する。以下、比較判定処理手順について図１３を参照して説明する。
【００８６】
比較判定処理にあたっては、図１３に示す比較判定処理手順ＲＴ１の開始ステップから入って、ステップＳＰ１に移る。
【００８７】
比較判定部２８ｃは、ステップＳＰ１において、被検ネットリストの最大スコア（X_{score}）が、最大スコア閾値（T_{score}）以上であるか否かを判断する。ステップＳＰ１において肯定結果が得られると、このことは、被検ネットリストがトロイネットを含み“HT-inserted”であることを表しており、このとき比較判定部２８ｃはステップＳＰ５へ移る。
【００８８】
一方、ステップＳＰ１において否定結果が得られると、比較判定部２８ｃはステップＳＰ２に移る。ステップＳＰ２において比較判定部２８ｃは最大スコアネット数（X_{number}）が最大スコアネット数閾値（T_{number}）以下であるか否かを判断する。ステップＳＰ２において否定結果が得られると、このことは、被検ネットリストにはトロイネットは含まれておらず“HT-free”であることを表しており、このとき比較判定部２８ｃはステップＳＰ６へ移る。
【００８９】
ステップＳＰ２において肯定結果が得られると、比較判定部２８ｃはステップＳＰ３に移る。ステップＳＰ３において比較判定部２８ｃは最大一定サイクル数（X_{cycle}）が最大一定サイクル数閾値（T_{cycle}）以上であるか否かを判断する。ステップＳＰ３において肯定結果が得られると、このことは、被検ネットリストがトロイネットを含み“HT-inserted”であることを表しており、このとき比較判定部２８ｃはステップＳＰ５へ移る。
【００９０】
ステップＳＰ３において否定結果が得られると、比較判定部２８ｃはステップＳＰ４へ移る。ステップＳＰ４において比較判定部２８ｃは、全ての最大スコアネットについて、最大一定サイクル数（X_{cycle}）を最大一定サイクル数閾値（T_{cycle}）と比較したか否かを判断する。
【００９１】
ステップＳＰ４において否定結果が得られると、このことは、最大一定サイクル数（X_{cycle}）が最大一定サイクル数閾値（T_{cycle}）と比較されていない最大スコアネットが残っていることを表しており、このとき比較判定部２８ｃはステップＳＰ３に戻る。
【００９２】
ステップＳＰ４において肯定結果を得ると、このことは被検ネットリストにはトロイネットは含まれておらず“HT-free”であることを表しており、ステップＳＰ６へ移る。
【００９３】
ステップＳＰ５において比較判定部２８ｃは、被検ネットリストがトロイネットを含むことを示す出力信号を生成して出力し、ステップＳＰ７へ移り、比較判定処理手順ＲＴ１を終了する。
【００９４】

またステップＳＰ６において比較判定部２８ｃは、被検ネットリストがトロイネットを含まないことを示す出力信号を生成して出力し、ステップＳＰ７へ移り、比較判定処理手順ＲＴ１を終了する。

【００９５】

判断手段２８は、比較判定部から得られた出力信号に基づき、判定結果を図示しない表示手段に出力する。表示手段は、出力信号に基づいた出力結果を表示する。

【００９６】

２．効果

上記構成において、検出装置２０は、公知ネットリストから対照ネットを抽出し、さらに第１の閾値および第２の閾値を選択して、予め条件を設定する。そして検出装置２０は、情報処理装置１０の被検ネットリストを取得すると、当該被検ネットリストに対照ネットが含まれるか否かを判断する。被検ネットリストに対照ネットが含まれている場合、検出装置２０は、当該対照ネットに基づき、第１の評価データおよび第２の評価データを生成する。検出装置２０は、予め設定された条件に基づき、生成された第１の評価データおよび第２の評価データを評価し、これにより被検ネットリストにトロイネットが含まれるか否かを判断する。

【００９７】

以上のとおり、本実施形態に係る検出装置２０は、公知ネットリストの既知情報に基づいて得られた条件に基づき、被検ネットリスト中のトロイネットの有無を判断することにより、公知ネットリストと種類が異なるネットリストを有する情報処理装置１０にハードウェアトロイが含まれるか否かを判断することができる。したがって検出装置２０は、対象となる情報処理装置１０の、ハードウェアトロイが挿入されていない健全なネットリストやハードウェアトロイに関する公知情報を用いずに、情報処理装置１０にハードウェアトロイが含まれるか否かを判断することができる。

【００９８】

一例として、上記表１に示した１０個のベンチマークから、（Case 1～9）の９個の対照ネットが得られること、このときの最大スコア閾値（T_{score}）、最大スコアネット数閾値（T_{number}）、および最大一定サイクル数閾値（T_{cycle}）は、それぞれ３、５、および999,996であること、さらに、閾値を用いてトロイネットの有無を判断する条件が以下のとおり設定されることを示した。

（ａ）最大スコア（X_{score}）が３以上

（ｂ）最大スコア（X_{score}）が３未満、最大スコアネット数（X_{number}）が５以下、かつ最大一定サイクル数（X_{cycle}）が999,996サイクル以上

【００９９】

こうしたハードウェアトロイの検出方法の一例を、被検ネットリストとして他の公知ネットリストに適用してトロイネットの有無を判断し、その結果を既知情報と比較することにより、本実施形態に係るハードウェアトロイの検出方法の正当性を確認した。

【０１００】

他の公知ネットリストとしては、Trust-HUBで公開されている全ベンチマーク３４個を用いた。Trust-HUBで公開されている全ベンチマーク３４個のうち、“HT-inserted”のベンチマークは２５個であり、“HT-free”のベンチマークは９個である。こうした３４個のベンチマークを所定の基準で評価して、評価結果を所定の条件で判定した。

【０１０１】

まず、各ベンチマークに含まれている構成ネットを、上述の９個の対照ネット（Case 1～9）と比較した。各ベンチマークについて、含まれている対照ネットの数を求め、最大スコア（X_{score}）および最大スコアネット数（X_{number}）を得た。その結果を、対照ネットの数とともに下記表７，８にまとめる。下記表７，８には、上記表１に示した１０個のベンチマークについての結果も併せて示した。

【０１０２】

【表７】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9	最大スコア（X_{score}）	最大スコアネット数（X_{number}）
b19−T100	822	43	84	16701	131	0	0	0	0	3	1
b19−T200	822	43	84	16701	131	0	0	0	0	3	1
EthernetMAC10GE−T700	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE−T710	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE−T720	347	56	2595	417	193	3	3	0	0	6	1
EthernetMAC10GE−T730	347	56	2595	417	193	3	3	0	0	6	1
RS232−T1000	11	2	2	0	12	0	0	0	0	2	2
RS232−T1100	11	2	2	0	12	0	0	0	0	2	2
RS232−T1200	10	2	2	0	12	0	0	0	0	2	2
RS232−T1300	9	2	2	0	12	0	0	0	0	2	2
RS232−T1400	12	3	2	0	12	0	0	0	0	2	3
RS232−T1500	11	2	2	0	12	0	0	0	0	2	2
RS232−T1600	9	2	2	0	12	0	0	0	0	2	2
s15850−T100	80	11	1	0	160	2	4	0	3	6	1
s35932−T100	3	3	1	0	420	2	2	0	4	8	1
s35932−T200	3	3	0	0	420	0	0	0	4	4	3
s35932−T300	3	3	1	0	420	0	0	0	4	5	1
s38417−T100	206	4	0	0	206	0	0	0	0	2	5
s38417−T200	203	3	0	0	206	0	0	0	0	2	4
s38417−T300	206	4	0	0	206	4	4	0	0	6	1
s38584−T100	112	3	2	0	404	0	0	0	4	3	2
s38584−T200	112	4	4	87	405	0	0	0	0	3	1
s38584−T300	123	16	3	783	405	0	0	0	0	3	1
vga_lcd−T100	19	0	1954	168	209	0	0	0	0	2	2
wb_conmax−T100	466	55	0	0	1516	0	0	1	0	4	1

【０１０３】

【表８】

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Case 7	Case 8	Case 9	最大スコア（X_{score}）	最大スコアネット数（X_{number}）
b19	598	38	1108	16586	130	0	0	0	0	2	77
EthernetMAC10GE	344	55	2595	417	193	0	0	0	0	2	55
RS232	5	0	2	0	12	0	0	0	0	1	19
s15850	68	5	0	0	160	0	0	0	0	2	5
s35932	0	0	0	0	420	0	0	0	0	1	420
s38417	199	1	0	0	206	0	0	0	0	2	2
s38584	110	3	2	0	404	0	0	0	0	2	9
vga_lcd	16	0	1954	161	209	0	0	0	0	1	2340
wb_conmax	455	52	0	0	1516	0	0	0	0	2	48

【０１０４】

３４個の全てのベンチマークの最大スコア（X_{score}）および最大スコアネット数（X_{number}）について、上述の条件（ａ／ｂ）を満たすか否かを調べ、その結果を既知情報によるハードウェアトロイの有無（HT-free／HT-inserted）とともに下記表９にまとめる。下記表９には、前述の１０個のベンチマークについての結果も併せて示した。下記表９においては、条件（ａ／ｂ）を満たしていれば、“○”としている。

【０１０５】

【表９】

ベンチマーク	条件(a／b)	タイプ
b19-T100	○	HT-inserted
b19-T200	○	HT-inserted
EthernetMAC10GE-T700	○	HT-inserted
EthernetMAC10GE-T710	○	HT-inserted
EthernetMAC10GE-T720	○	HT-inserted
EthernetMAC10GE-T730	○	HT-inserted
RS232-T1000	○	HT-inserted
RS232-T1100	○	HT-inserted
RS232-T1200	○	HT-inserted
RS232-T1300	○	HT-inserted
RS232-T1400	○	HT-inserted
RS232-T1500	○	HT-inserted
RS232-T1600	○	HT-inserted
s15850-T100	○	HT-inserted
s35932-T100	○	HT-inserted
s35932-T200	○	HT-inserted
s35932-T300	○	HT-inserted
s38417-T100	○	HT-inserted
s38417-T200	○	HT-inserted
s38417-T300	○	HT-inserted
s38584-T100	○	HT-inserted
s38584-T200	○	HT-inserted
s38584-T300	○	HT-inserted
vga_lcd-T100	○	HT-inserted
wb_conmax-T100	○	HT-inserted
b19	－	HT-free
EthernetMAC10GE	－	HT-free
RS232	－	HT-free
s15850	－	HT-free
s35932	－	HT-free
s38417	－	HT-free
s38584	－	HT-free
vga_lcd	－	HT-free
wb_conmax	－	HT-free

【０１０６】

上記表９には、３４個のベンチマーク全てについて、既知情報によるハードウェアトロイの有無（HT-free／HT-inserted）と一致する結果が得られたことが示されている。上述のような基準および条件を用いることによって、“HT-inserted”の２５個のベンチマーク全てにおいて、誤検出無しでトロイネットの一部を確実に検出することができた。

【０１０７】

既存手法を用いた場合には、“HT-inserted”の２５個全てのベンチマークについて、ハードウェアトロイを正確に検出することはできない。検出に成功したハードウェアトロイの数は、下記表１０に示すように、既存手法１では４個であり、既存手法２では８個にとどまっている。しかも、既存手法の場合には、ペイロード回路やトリガー回路などの回路におけるハードウェアトロイの情報を、事前に知る必要がある。ここで、既存方法１はＵＣＩによる手法であり、既存方法２はＶｅｒｉ Ｔｒｕｓｔによる方法である。ＵＣＩは、回路検証中に活性化しない信号を特定し、その信号に対してマルチプレクサを挿入することで、ハードウェアトロイを検出する。Ｖｅｒｉ Ｔｒｕｓｔは、回路検証中に活性化しない信号を特定し、その信号に対して観測性を高めることによりハードウェアトロイを検出する。

【０１０８】

【表１０】

ベンチマーク	本手法	既存手法1	既存手法2
b19-T100	○	×	×
b19-T200	○	×	×
EthernetMAC10GE-T700	○	×	×
EthernetMAC10GE-T710	○	×	×
EthernetMAC10GE-T720	○	×	×
EthernetMAC10GE-T730	○	×	×
RS232-T1000	○	×	×
RS232-T1100	○	×	×
RS232-T1200	○	×	×
RS232-T1300	○	×	×
RS232-T1400	○	×	×
RS232-T1500	○	×	×
RS232-T1600	○	×	×
s15850-T100	○	○	○
s35932-T100	○	×	○
s35932-T200	○	○	○
s35932-T300	○	×	○
s38417-T100	○	○	○
s38417-T200	○	×	○
s38417-T300	○	○	○
s38584-T100	○	×	×
s38584-T200	○	×	○
s38584-T300	○	×	×
vga_lcd-T100	○	×	×
wb_conmax-T100	○	×	×

【０１０９】

以上のように、ハードウェアトロイの挿入されていないネットリストや、ハードウェアトロイに関する情報を用いずに、公知のネットリストから得られた基準および条件を用いることによって、ゲートレベルの被検ネットリストが“HT-free”および“HT-inserted”のいずれであるかを識別することが可能となった。しかも、上述の基準および条件を用いた場合には、既存手法を用いた場合よりも正確な識別結果が得られており、こうした点でも既存手法に対して優位性を有することが確認された。

【０１１０】

３．他の実施の形態

なお、本発明は、本実施の形態に限定されるものではなく、本発明の要旨の範囲内で種

々の変形実施が可能である。例えば、上述の実施形態においては、公知ネットリストとして所定のサイト（Trust-HUB）からダウンロードした所定の１０個のベンチマークを用い、こうした公知ネットリストから９個の対照ネットを選択することを一例として説明したが、公知ネットリストの数および対照ネットの数はこれに限定されない。公知ネットリストの数は任意に設定して、ランダムに選択することができる。また、対照ネットの数や種類は、公知ネットリストの数や種類によって、変わり得るものである。

【０１１１】

また、実施形態においては、対照ネットのスコアとして１または２を例に挙げたが、公知ネットリストの種類や数が変更された場合には、各対照ネットのスコアの大きさも変わり得る。

【０１１２】

さらに、実施形態においては、被検ネットリスト中のハードウェアトロイの有無の判定に用いる最大スコア閾値および最大スコアネット数閾値の値は、それぞれ３および５に設定したが、これらの数値もまた、変わり得るものである。最大スコア閾値および最大スコアネット数閾値は、上述の実施形態に示したように、公知ネットリストとの比較に基づいて適宜設定することができる。必要に応じて、公知ネットリストとの比較に基づいて得られた閾値よりも、厳しい閾値を設定してもよい。

【０１１３】

また、トロイネットを含むか否かを判断する指標の一つとして、最大一定クロック数（１Ｍクロック間で一定値を出力する最長のクロック数）を用いたが、これに限定されるものではない。被検ネットリスト中に潜むトロイネットの可能性を示すものであれば、最大一定サイクル数以外の任意のパラメータを用いてもよい。そのような場合においても、上述した実施形態で説明したように、公知ネットリストとの比較に基づいて適切な閾値を設定することができる。

【０１１４】

公知ネットリストからトロイネットの有無を判断するための基準を得、この基準に基づいてトロイネットの有無を判断するための条件を設定し、得られた基準および条件を用いてゲートレベルの被検ネットリスト中のトロイネットの有無を判断することによってハードウェアトロイを検出することは、本発明の範囲内である。

【０１１５】

情報処理装置１０を検出装置２０に直接接続して、情報処理装置１０の被検ネットリストを入力する場合について説明したが、被検ネットリストを得ることができれば、情報処理装置１０を検出装置２０に接続する形態に限定されない。

【０１１６】

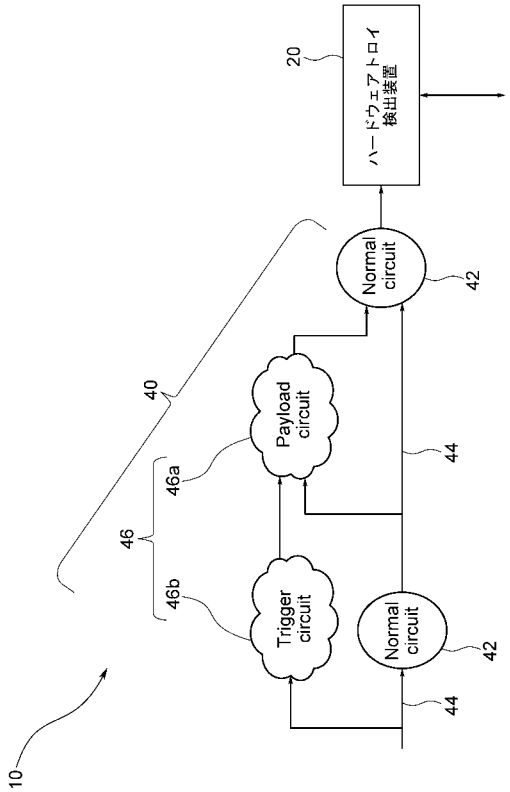
また、上記実施形態の場合、ネットリストは情報処理装置１０に含まれている場合について説明したが本発明はこれに限られない。情報処理装置１０は、必ずしもネットリストを保持している必要はない。この場合、検出装置２０はネットリストを記憶した記憶媒体や、ネットワーク上のサーバーなどからネットリストを取得してもよい。

【符号の説明】

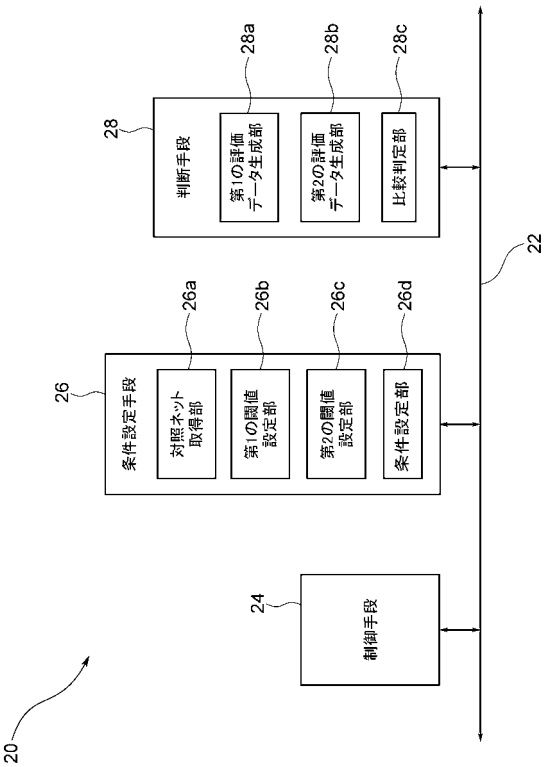
【０１１７】

１０　情報処理装置
２０　ハードウェアトロイ検出装置
２２　制御バス
２４　制御手段
２６　条件設定手段
２８　判断手段

【図１】

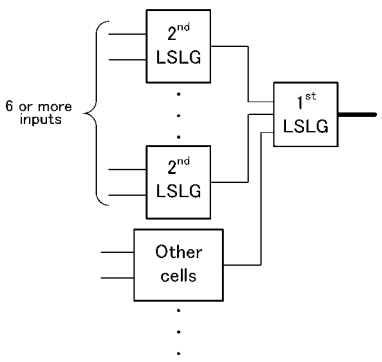


【図２】



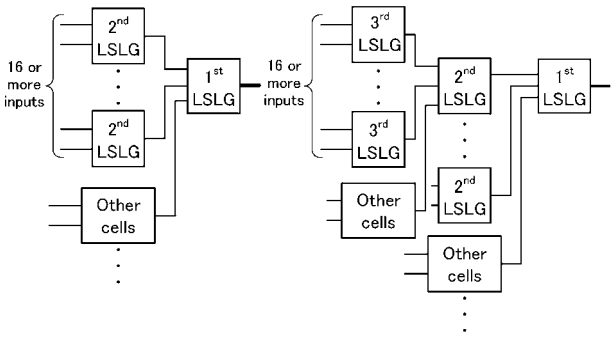
【図３】

Case 1



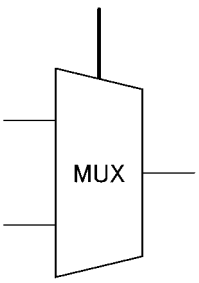
【図４】

Case2



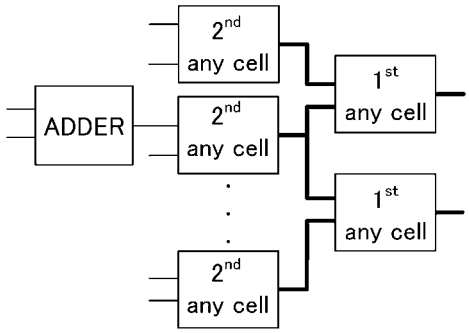
【図５】

Case 3



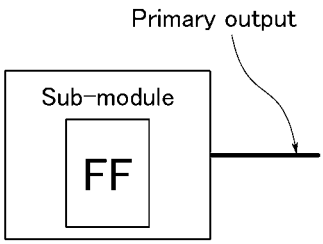
【図６】

Case 4



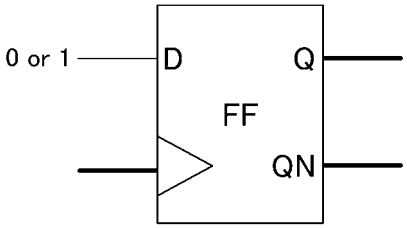
【図７】

Case 5



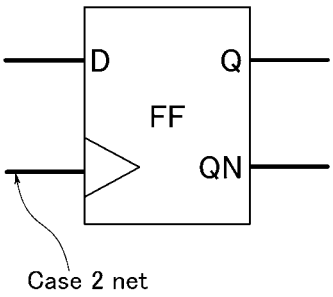
【図８】

Case 6



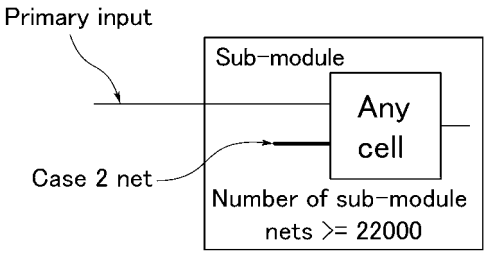
【図９】

Case 7



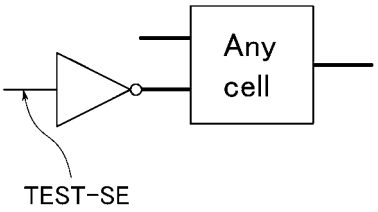
【図１０】

Case 8

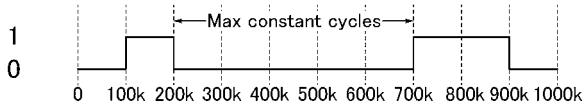


【図１１】

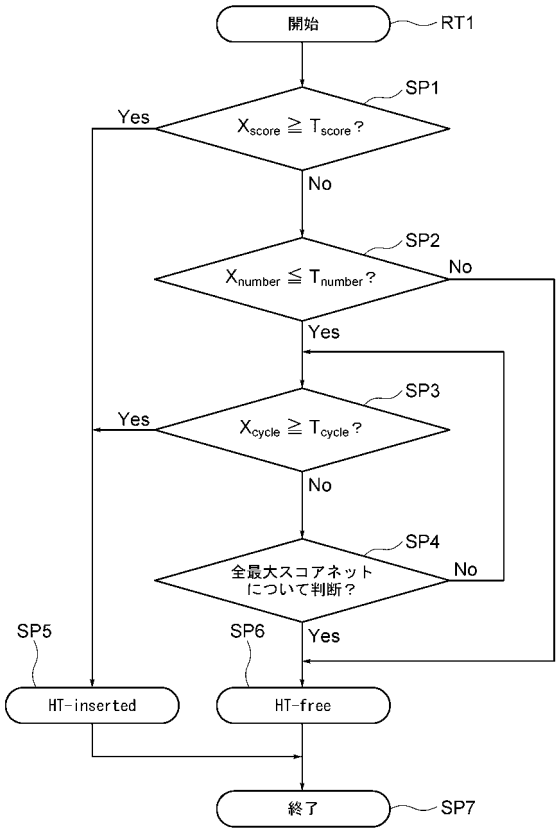
Case 9



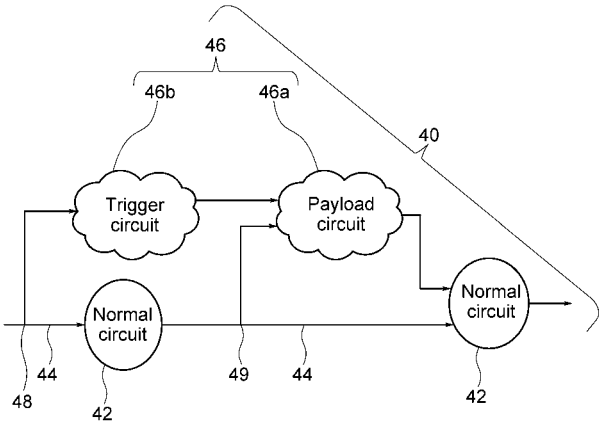
【図１２】


1
0
Max constant cycles
0 100k 200k 300k 400k 500k 600k 700k 800k 900k 1000k

【図１３】


開始
RT1
SP1
Yes
$X_{score} \geqq T_{score}$?
No
SP2
$X_{number} \leqq T_{number}$?
No
Yes
SP3
Yes
$X_{cycle} \geqq T_{cycle}$?
No
SP4
全最大スコアネット
について判断？
No
SP5
SP6
Yes
HT-inserted
HT-free
終了
SP7

【図１４】


46
46b
46a
40
Trigger circuit
Payload circuit
Normal circuit
Normal circuit
48
44
42
49
44
42

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/082223

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/56(2013.01)i, *H01L21/82*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/56, H01L21/82

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2016
Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Mainak Banga and Michael S. Hsiao, Trusted RTL: Trojan Detection Methodology in Pre-Silicon Designs, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010, 2010.06.13, pp.56-59	1-15
A	Emi OGITA, Toshinori HOSOKAWA, Masayoshi YOSHIMURA, "An evaluation of Trojan Circuits on AES Encryption Circuits", IEICE Technical Report, 06 February 2013 (06.02.2013), vol.112, no.429, pages 37 to 42	1-15
A	JP 2012-207993 A (Renesas Electronics Corp.), 25 October 2012 (25.10.2012), abstract; paragraphs [0030] to [0032], [0037], [0046], [0049] to [0050]; fig. 5 to 6 (Family: none)	1-15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family 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 application or patent 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	Date of mailing of the international search report
02 February 2016 (02.02.16)	09 February 2016 (09.02.16)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/082223

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Yier Jin, Kathan Kupp, and Yiorgos Makris, Experiences in Hardware Trojan Dsign and Implementation, IEEE international Workshop on Hardware-Oriented Security and Trust, 2009. HOST'09, 2009.07.27, pp.50-57	1-15
T	Tomohiro BOYASHIKI, Toshinori HOSOKAWA, Masayoshi YOSHIMURA, "A Hardware Trojan Detection Method Based on Information of Nontransitional Lines", College of Industrial Technology, Nihon University Dai 47 Kai Gakujutsu Koenkai Koen Gaiyo [online], 06 December 2014 (06.12.2014), [retrieval date 01 February 2016 (01.02.2016)], Internet: <URL: http://www.cit.nihon-u.ac.jp/laboratorydata/kenkyu/kouennkai/reference/No.47/pdf/2-58.pdf>, 2-58, pages 313 to 316	1-15

国際調査報告	国際出願番号 ＰＣＴ／ＪＰ２０１５／０８２２２３

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. G06F21/56(2013.01)i, H01L21/82(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. G06F21/56, H01L21/82

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Mainak Banga and Michael S. Hsiao, Trusted RTL: Trojan Detection Methodology in Pre-Silicon Designs, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010, 2010.06.13, pp.56-59	1-15
A	荻田　英実、細川　利典、吉村　正義，ＡＥＳ暗号回路におけるトロイ回路設計の影響評価およびその一考察，電子情報通信学会技術研究報告，2013.02.06，Ｖｏｌ．１１２、Ｎｏ．４２９，ｐ．３７－４２	1-15

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０２．０２．２０１６	０９．０２．２０１６

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ	４２２９
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６		

国際調査報告 国際出願番号 ＰＣＴ／ＪＰ２０１５／０８２２２３

Ｃ（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2012-207993 A (ルネサスエレクトロニクス株式会社) 2012.10.25, ［要約］、段落［００３０］－［００３２］、［００３７］、［００４６］、［００４９］－［００５０］、［図５］－［図６］ (ファミリーなし)	1-15
A	Yier Jin, Kathan Kupp, and Yiorgos Makris, Experiences in Hardware Trojan Dsign and Implementation, IEEE international Workshop on Hardware-Oriented Security and Trust, 2009. HOST'09, 2009.07.27, pp.50-57	1-15
T	坊屋敷 知拓、細川 利典、吉村 正義, 信号未遷移情報に基づくトロイ検出法, 日本大学生産工学部第４７回学術講演会講演概要［オンライン］, 2014.12.06, [検索日 2016.02.01], インターネット：＜ＵＲＬ：http://www.cit.nihon-u.ac.jp/laboratorydata/kenkyu/kouennkai/reference/No.47/pdf/2-58.pdf＞, ２－５８, ｐ．３１３－３１６	1-15

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（２０１５年１月）

フロントページの続き

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

（出願人による申告）平成２６年度、総務省、戦略的情報通信研究開発推進事業、産業技術力強化法第１９条の適用を受ける特許出願

(72)発明者　大屋　優
日本国東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。