設計工程に侵入したハードウェアトロイの検出と耐ハードウェアトロイ設計技術の研究開発（141303001）

研究代表者：戸川 望（早稲田大学)

研究期間：平成26年度～平成28年度

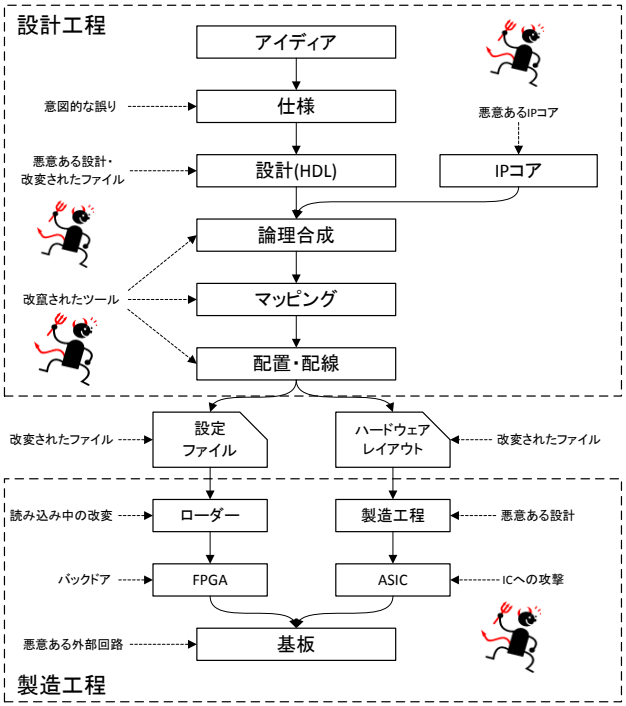
研究背景：ハードウェアトロイとは？

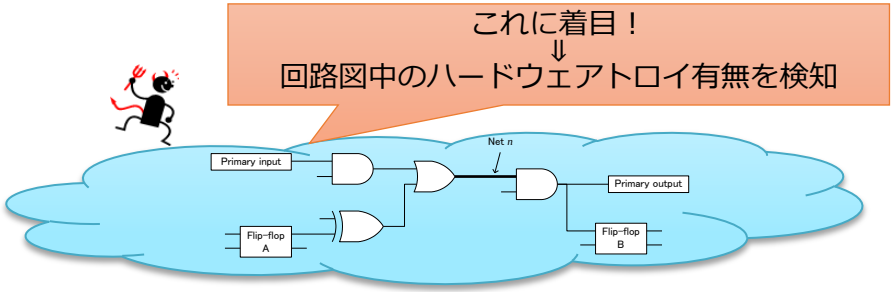
- 集積回路に悪意のある回路（ハードウェアトロイ）が侵入？
  - 背景
    第三者への設計・製造
    外部委託の増加

    意図しない改変のリスク
  - タイミング
    設計工程は危険性が高い

    ネットワークを経由した
    情報の改変で感染

    設計工程に着目した
    ハードウェアトロイ検出





研究開発成果：設計ハードウェアトロイの検出(1/2)

- アプローチ：

HWトロイを構成する信号線

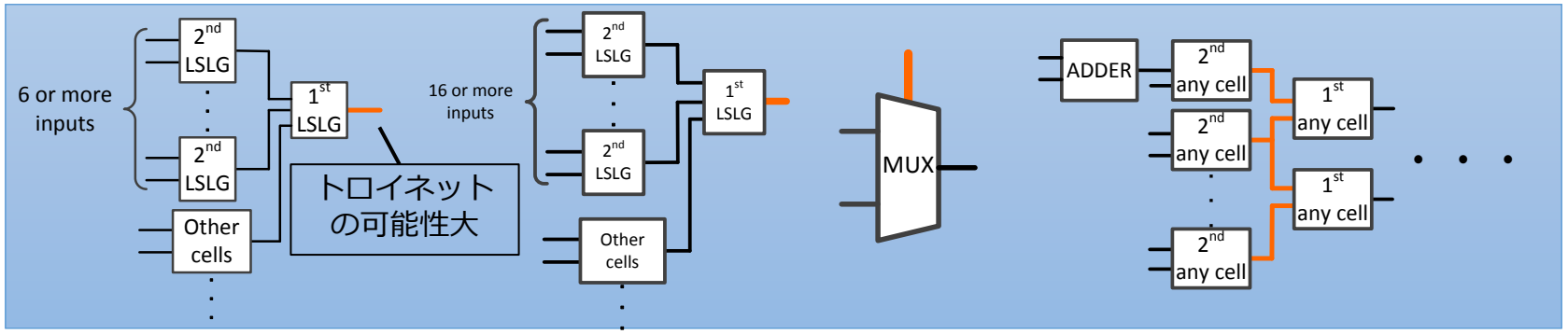
① 設計データ中の全信号線集合の中から，**トロイネット**「**らしい**」ものを見つけ出す（**弱識別ネット**）

② 弱識別ネット集合から「**確実に**」**トロイネット**となるものを見つけ出す（**強識別ネット**）

強識別ネットが1つでも発見されれば，**ハードウェアトロイが侵入**

① **弱識別**：ハードウェアトロイを構成する信号線の9つの特徴

- 特徴にもとづき，各信号線にスコア付けする



研究開発成果：設計ハードウェアトロイの検出(2/2)

② **強識別**：2つの基準により強識別する

- **基準1**：スコアの合計≧3の信号線 → 「確実に」トロイネット
- **基準2**：基準1を満たさなくても，最大スコア信号線の数が5以下であり，一定値を出力するクロックサイクルが99.999%以上の信号線 → 「確実に」トロイネット

強識別された信号線が1つでもあれば，**ハードウェアトロイ侵入**と判定

識別結果（一部）：

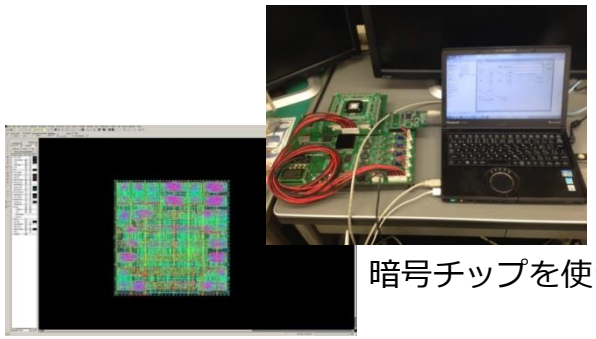
Benchmark	トロイ有無	開発技術による検出/非検出の結果
b19-T100	有	検出
b19-T200	有	検出
EthernetMAC10GE-T700	有	検出
EthernetMAC10GE-T710	有	検出
EthernetMAC10GE-T720	有	検出
EthernetMAC10GE-T730	有	検出
RS232-T1000	有	検出
RS232-T1100	有	検出
RS232-T1200	有	検出
RS232-T1300	有	検出
RS232-T1400	有	検出
RS232-T1500	有	検出
RS232-T1600	有	検出
s15850-T100	有	検出
s35932-T100	有	検出
s35932-T200	有	検出
s35932-T300	有	検出
s38417-T100	有	検出
s38417-T200	有	検出
s38417-T300	有	検出
s38584-T100	有	検出
s38584-T200	有	検出
s38584-T300	有	検出
vga_lcd-T100	有	検出
wb_conmax-T100	有	検出
AES-T1	有	検出
AES-T2	有	検出

Benchmark	トロイ有無	開発技術による検出/非検出の結果
b19	無	非検出
EthernetMAC10GE	無	非検出
RS232	無	非検出
s15850	無	非検出
s35932	無	非検出
s38417	無	非検出
s38584	無	非検出
vga_lcd	無	非検出
wb_conmax	無	非検出
AES	無	非検出
c17	無	非検出
c432	無	非検出
c499	無	非検出
c880	無	非検出
c1355	無	非検出
c1908	無	非検出
c2670	無	非検出
c3540	無	非検出
c5315	無	非検出
c6288	無	非検出
c7552	無	非検出

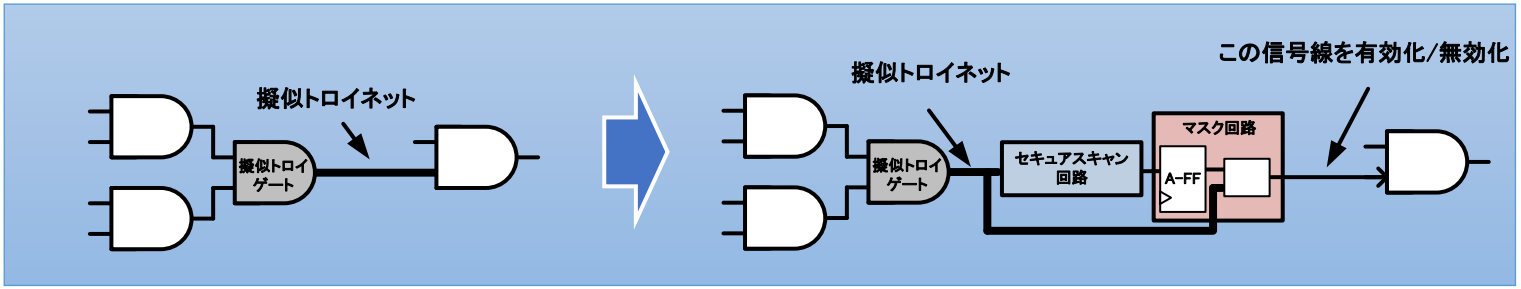
世界で初めて，標準ベンチマークTrust-HUB中の全ゲートレベル回路に対して，誤りなくハードウェアトロイの有無を識別

研究開発成果：耐ハードウェアトロイ回路設計

- アプローチ：
  - ① 擬似トロイネットに「認証回路」を埋め込む
  - ② 認証されると，その信号線は有効化
  - ③ 認証されないと，その信号線は無効化



暗号チップを使って検証



今後の研究開発成果の展開・波及効果創出

- 本研究開発成果は，設計工程ハードウェアトロイ検出基準を見い出すと共に擬似トロイネットに対するセキュアスキャン回路を開発する等，集積回路部品の信頼性に対して世界的に大きな成果を得た
- これらの成果は，直接，IoTの高信頼化に大きく寄与するものと考えられ，今後，産業界と協力し社会実装されることを期待