〈ソリューション紹介〉

LSI Solution

早稲田大学との共同研究開発で進める設計工程でのハードウェアトロイ検出

近年、ICチップの一部に悪意のある回路として組み込まれた“ハードウェアトロイ”の脅威が深刻化しています。当社は、本分野の技術研究ではパイオニアである早稲田大学（以下、早大）の戸川研究室と共同で、設計工程で侵入するハードウェアトロイの検出に取り組んでいます。今後、検出ツールの開発と並行してハードウェアトロイ検証サービスなどの展開も図っていきます。

拡がるハードウェアへの脅威

あらゆるデバイスがネットワークに繋がるIoT時代が全盛を迎えています。総務省は2020年にIoTデバイスの数が世界で400億個を超えると予測しており、私たちの生活がどんどん便利になっていく反面、情報通信のセキュリティ対策強化が急務となっています。

ソフトウェアの世界では、ウイルスやワームといったマルウェアによる被害が後を絶ちませんが、ハードウェアの世界でも同様の被害が報告されています。ハードウェアの中に回路として組み込まれ、特定の信号を受け取って外部からのコントロールを可能にする仕組みや、特定のタイミングで本来の機能を誤作動させる仕組みなどをハードウェアトロイと呼びます。このハードウェアトロイの被害が、今後増加していくと予想されているのです。

ICチップやデバイスなどのハードウェアに対して不正な機能を付加し、利用者が想定した以外の動作をさせるのがハードウェアトロイの特徴です。例えばあるハードウェアトロイは暗号化チップにおいてタイマーを使い、特定の時間になるとICチップやデバイスの情報を盗んだり、外部から受信した特定のデータと一致したらパスワードを平文で出力したりするという不正を行います。ほとんどのハードウェアトロイは、特定の信号が入力されたときにのみ動作するよう設計されているので、ICチップの回路動作確認時に検出することはとても困難です。この暗号化チップの場合、ハードウェアトロイが動作する前の暗号化システムに平文を入力すれば暗号化されたデータが正しく出力されるため、回路としては正常と判断されました。その結果、このチップはハードウェアトロイを内蔵したまま市場に出荷され、情報漏えいの被害に発展しました**(図-1)**。

他にも半導体メーカーのファブレス化に伴う外部への設計・製造委託の増加も一因となって、ICチップに悪意のある機能を組み込まれたり、回路を改ざんされたりといったケースが少しずつ話題になり始めています。身近なところでは、多くの人が日々使っているスマートフォンで、個人情報や重要なデータを盗み出す、通信を傍受する、操作を乗っ取るといったことも技術的に可能です。今までウイルスはソフトウェアだけのものと思い込んでいた私たちの常識は、もはや通用しません。IoT時代を迎えている今、ハードウェアにおいてもICチップの誤動作や故障、システムのシャットダウン、大切な情報の流出、ウイルスの拡散など、さまざまな被害が多方面に及ぶ可能性があります**(図-2)**。

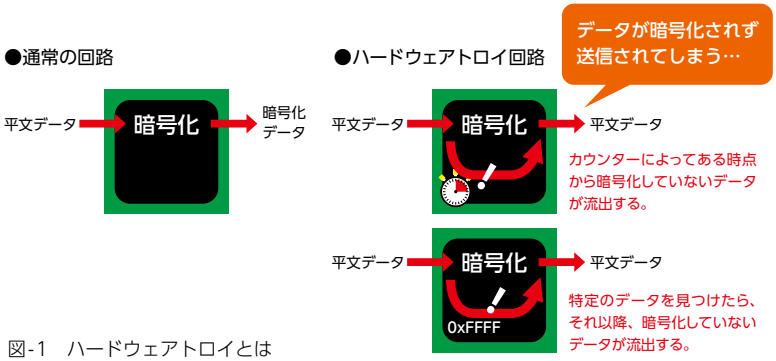

図-1　ハードウェアトロイとは

産学共同で検出技術の精度向上図る

●戸川研究室の紹介

今後、関心が高まっていくであろうハードウェアのセキュリティ技術開発に早くから注力し、耐ハードウェアトロイ設計技術の研究に取り組んでいるのが、早大の戸川研究室(戸川 望　理工学術院教授)です。

総務省は、ハードウェア脆弱性への対策を「戦略的情報通信研究開発推進事業（SCOPE）」などの事業の中で進めていますが、戸川教授は2014年度に「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」を提案し、さらに2017年度には「IoT部品・機器・ネットワークの階層横断セキュリティ技

図-2　身近に起こり得るハードウェアトロイの脅威

術の研究開発」を提案して、それぞれ採択されています。

これまで同研究室では、危険性が高い設計工程に着目することで検出技術の研究に取り組んできましたが、2019年からは当社と共同で検証ツールへのアルゴリズム実装や検証実験を行っています。

ハードウェアトロイの検出手法は、回路の構造からいくつかのハードウェアトロイらしい特徴を見つけ出し(弱識別)、それをスコアリングする(強識別)ことで、総合的にハードウェアトロイかどうかの判断をしていきます。

●開発の役割とプログラム設計

当社は、同研究室のアルゴリズムをプログラム化してハードウェアトロイ検出ツールの開発を行っています。ハードウェアトロイの標準ベンチマークである「Trust-HUB」が公開しているデータの調査も行いながら、実際の回路相当のゲートネットで検出できるかどうかを確認することで検出技術の精度向上に取り組んでいます。

検出ツールの開発は、早大の「トロイネットの特徴に基づくハードウェアトロイ検出手法」の内容を基に、実際の設計現場の意見を取り入れながら進めています。プログラム設計においては、製品の作り方に依存しないように解析アルゴリズムを調整して解析結果が従来の検出結果と同等になるよう考慮しています。

また、ハードウェアトロイが組み込まれていない製品を解析したときに、ハードウェアトロイであると誤認識してしまう場合も考慮しておかねばなりません。ハードウェアトロイは現時点では未知な部分が多く、その回路設計データに入っているかどうかの判断が難しいのが実情です。開発中の検出ツールでは、判別のつきにくい回路があった場合、現在既知となっているハードウェアトロイのパターンの見直しを行うなどの精度向上策を講じています。

本検出ツールは2020年に完成予定ですが、ハードウェアトロイの検証サービス開始に備え解析した内容が視覚的に分かりやすいようにするインタフェースの整備なども進めています(図-3)。

ICチップの安全性を高める検証サービスを

ソフトウェアのマルウェア対策は、悪意のあるウイルス作成者とのいたちごっこ化しており、抜本的な解決策は見つかっていません。ハードウェアトロイについても同様のことが言えます。半導体メーカーが安心して委託先に設計を依頼できる環境や、エンドユーザーが安心して製品を使えるよう早急に仕組みを整備しなければなりません。ICチップはもとより、エンドユーザーが使う製品自体の安全性を高めるためにも、当社が開発を進めているハードウェアトロイ検出ツールは極めて重要な存在になっていくものと考えています。

今後は第三者から購入したIP(Intellectual Property)や、外部に設計を委託した回路をお客様に提出していただき、当社が検証してお返しするといったハードウェアトロイ検証サービスの展開を視野に入れています。まずは、現在取り組んでいるハードウェアトロイの検出について早大と協力し、さらに精度を高めていく考えです。

(LSIソリューション事業部　永田 真一)

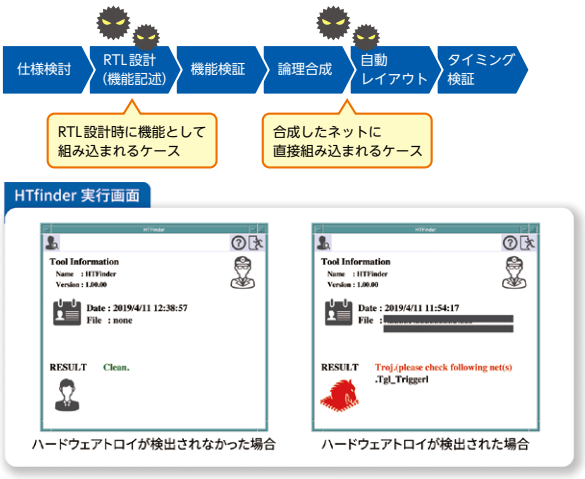

図-3　当社のツールによる検出例

■戸川研究室　大屋 優 氏 (JSPS特別研究員)からのコメント

貴社と商用化に向けて進めている技術の基幹研究は、私が半導体自動設計の最難関国際会議の一つであるDATE[注1]に採択され口頭発表したものになります。

貴社開発の検証ツールは世界が直面している半導体セキュリティの問題に、どこよりも先駆けて実用的な対策を示すことになります。今後は、静観していた数多くの企業が貴社の後を追う形でこの分野に参画し、加速度的に市場が拓けていきます。その中で貴社が重要な役割を果たしていくことを強く期待しております。

注1) DATE (Design, Automation & Test in Europe)：電子設計とテストに関する国際会議