応用

スパイチップはあるのか ハードウェアセキュリティの必要性

長谷川健人 | 早稲田大学　戸川　望 | 早稲田大学

マザーボードにスパイチップ！？

先日，インターネットメディアを中心に，コンピュータのメイン基板であるマザーボードに設計段階で存在しなかったIC チップが挿入されたという報告が話題となった[1]．そのIC チップはネットワークとシステムメモリの両方にアクセス可能であり，まるで不正な情報収集を目的とした“スパイチップ”のような存在であったと報告されている．この情報に対し関係者はスパイチップ挿入の事実を否定しており，真偽は定かでない．しかし，今回の話題から，こうしたハードウェアにおける機密漏洩の脅威は現実となり得るものであり，このような事例に対する世間の関心も高まっていることが伺える．実際，ハードウェアセキュリティの研究分野では以前からこうした可能性が議論されており，近年盛んに研究が進められている[2, 3]．以下では，こうしたハードウェアにおける脅威とその対策方針を解説する．

複雑化するハードウェア設計・製造工程

ハードウェア製品は多くの工程を経て我々の手元に届く．図-1 にハードウェア設計・製造工程の主要な流れを示す．ハードウェア設計・製造工程は大きく分けて設計工程と製造工程に大別され，最後に流通を経て我々の手元に届く．近年では設計・製造工程を効率化するため，それぞれの工程において製品ベンダ以外の複数の第三者がかかわっている．

設計工程では，製品ベンダが示した仕様に従い，製品ベンダ内の設計チームや外部委託された第三者ベンダがハードウェアを設計する．ここではハードウェア記述言語（Hardware Description Language, HDL）と呼ばれる専用の言語を用いて回路が設計される．このとき，プロセッサコアや通信インタフェースなど，汎用的に利用される回路はHDL で記述されたIP（Intellectual Property）コアと呼ばれる単位で第三者ベンダから提供されることもあり，これを利用することで設計を効率的に進めることができる．その後，HDL で記述された回路をチップ

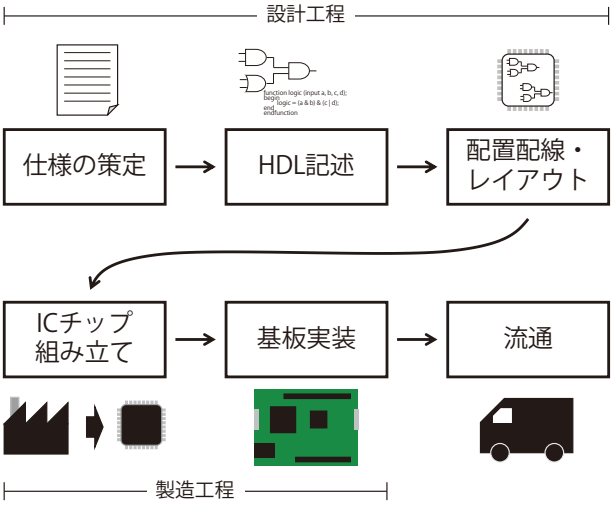


図-1　ハードウェア設計・製造から流通までの流れ

内の物理的な配置・配線に落とし込む作業に移行する．こうして設計工程が完了したのち，製造工程に移る．

IC チップや回路基板は専門業者に委託して製造される．これを受け持つのがファウンドリと呼ばれる業者であり，IC チップや基板の製造装置を持ちさまざまな発注先から製造を請け負っている．その後，製造されたハードウェアが流通経路を経て，製品としてユーザの手元に届く．

ハードウェアトロイの潜在的リスク

ハードウェアの設計・製造工程で悪意のある回路を挿入される危険性は以前から指摘されている．攻撃者は製品ベンダやユーザの利用時にその存在を知られないよう悪意のある回路を挿入する．このことから，悪意のある回路はソフトウェアにおける“トロイの木馬”になぞらえて“ハードウェアトロイ”と呼ばれる．ハードウェアトロイは，ハードウェアの知識さえあれば挿入するのが比較的容易な反面，通常は潜伏状態にあることから検出は困難である．

どうやって IC チップにハードウェアトロイを挿入するのだろう．ハードウェア設計工程では IP コアがしばしば用いられており，攻撃者はこの IP コアにハードウェアトロイを挿入する．このとき，攻撃者はハードウェアトロイの発見を困難にするため，トリガ条件を設定する．トリガ条件には，あるデータ系列が入力された場合やある一定の時間が経過した場合が考えられる．トリガ条件が満たされたとき，悪意のある機能として内部情報の流出や IC チップの耐久性を低下させるための消費電力の増大などが引き起こされる．

ではそうした回路を検出できるだろうか？ 設計情報の正当性を評価するためのテスト工程では，設計情報に基づきその回路の動作をコンピュータ上でシミュレートする手法が用いられる．しかし，このシミュレーションは実機テストに比べ数百倍以上の時間がかかるため，ハードウェアのすべての入出力をテストするのは現実的でない．実際にはあらかじめ生成したいくつかのテストパターンを与えてテストするが，限られたテストパターンに基づくシミュレーションだけではハードウェアトロイが有効化される確率が低いため，ハードウェアトロイを検知するのは困難である．

次に，IC チップの組み立てや基板実装を行う製造工程におけるハードウェアトロイ挿入の危険性を検討する．製造工程は一般に製造機器が自動化されており，設計情報に基づき自動的に実装される．この工程において，製造機器に設定するパラメータや入力するデータを改変することで，製造されるハードウェアの機能を改変する攻撃も指摘されている．このように挿入されたハードウェアトロイも同様に通常は潜伏状態にあるため，これを検知するのは困難である．

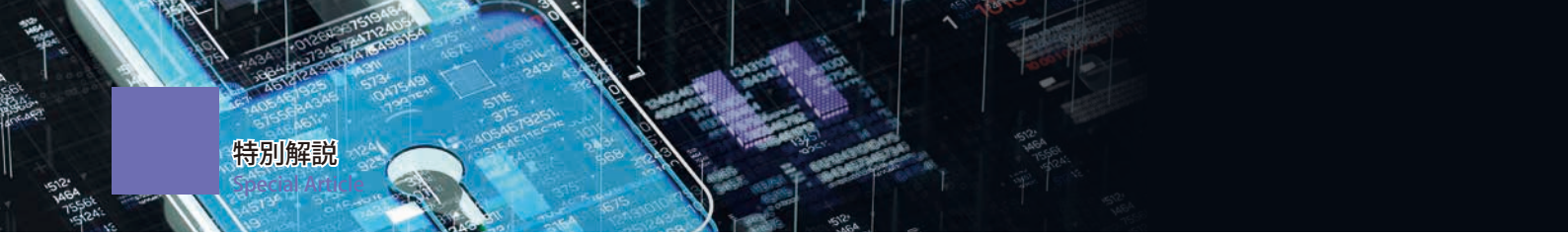
さらに，流通工程においてもハードウェアトロイ挿入のリスクは存在する．ハードウェア製品に対し，基板上に新たな IC チップやパーツを取り付けることは攻撃者にとって可能である．

以上のように，ハードウェアの設計・製造工程においてハードウェアトロイが挿入されるリスクは随所に存在する．

ハードウェアトロイの検知技術

ハードウェアトロイの脅威に対し，我々はいかにして対抗するべきだろうか．現在，ハードウェアトロイを検知するための研究が国内外で進められている[3)]．

ハードウェア設計工程におけるハードウェアトロイ検知では，ハードウェアの設計情報を利用して，ハードウェアトロイを構成する回路の特徴に着目した手法が提案されている．設計情報を構造的に解析し，あらかじめ抽出したハードウェアトロイの特徴と照合することで，ハードウェアトロイの検知が可



能となる．このアプローチに対し，近年では機械学習を組み合わせた手法も提案されている．

ハードウェア製造工程におけるハードウェアトロイ検知手法も提案されており，その代表例としてサイドチャネル情報にもとづく手法が挙げられる．サイドチャネル情報とは，ハードウェアが動作する上で必然的に外部に漏洩する情報のことで，たとえば消費電力や漏洩電磁波などが挙げられる．これらの情報を高精度に計測することで，ハードウェアの動作をある程度推測することができる．サイドチャネル情報に基づく手法では，あらかじめハードウェアトロイが挿入されていないことが保証された“ゴールデン回路”と呼ばれる回路と比較して，テスト対象の回路からハードウェアトロイを検知する．ところが，ゴールデン回路を保証するためにはすべての設計・製造工程が信頼できる必要があるため，現実的でない．この課題を克服するため，近年では同一の IC チップ内でサイドチャネル情報を比較するなど，ゴールデン回路を必要としない手法も提案されている．

ハードウェアセキュリティの今後

かつてコンピュータが一般に普及し始めたころ，アンチウィルスソフトウェアはコンピュータの重荷と見なされていたが，現在ではその必要性が広く認知されている．今，ハードウェアにも同様のことが起こり始めているといえよう．ハードウェアの IP コア化や製造拠点の国際化により，ハードウェアの設計・製造工程はかつてに比べ効率的になり，容易かつ安価になってきている．このような背景のもとでハードウェアの設計・製造工程やその製品の複雑化が進み，さまざまな脅威が顕在化してきている．これらに対し，ハードウェアの側面からセキュリティを考えることが重要な課題となってきている．複雑化するハードウェア設計・製造工程において，ハードウェアセキュリティ技術は今後ますます発展させる必要がある．

参考文献

1) https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
2) Ghosh, S., Basak, A. and Bhunia, B. : How Secure Are Printed Circuit Boards Against Trojan Attacks?, IEEE Desgin & Test, vol.32, No.2, pp.7-16 (2015).
3) Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S. and Tehranipoor, M. : Hardware Trojans : Lessons Learned after One Decade of Research, ACM Transactions on Design Automation of Electronic Systems, vol.22, No.1, pp.1-23 (2016).

(2018 年 11 月 9 日受付)

長谷川健人（学生会員） kento.hasegawa@togawa.cs.waseda.ac.jp
2017 年に早稲田大学大学院基幹理工学研究科情報理工・情報通信専攻修士課程修了．現在，同博士後期課程在籍．

戸川　望（正会員） togawa@togawa.cs.waseda.ac.jp
1997 年に早稲田大学大学院理工学研究科電気工学専攻修了．博士（工学）．現在，同大学基幹理工学部情報通信学科教授．