［ハードウェアセキュリティの最新動向］

③ ハードウェアトロージャンの脅威と検出

基般

林　優一 | 奈良先端科学技術大学院大学／産業技術総合研究所
川村信一 | 産業技術総合研究所

ハードウェアに忍び寄る新たな脅威／ハードウェアトロージャンとは何か？

コスト削減などの理由により，ハードウェアメーカは自社で設計したICチップを安価に製造できるサードパーティのファウンドリを利用している．こうした状況下では，IC製造のサプライチェーンにおいて，チップ設計者が意図しない機能が付加され，特定の状況下ではICの破壊やセキュリティの低下を引き起こす可能性がある．

上述のように設計者の意図に反して付加される回路はハードウェアトロージャン（HT：Hardware Trojan）と呼ばれ，新たなセキュリティの脅威と見なされており，対処の必要なセキュリティ課題の1つとなっている．

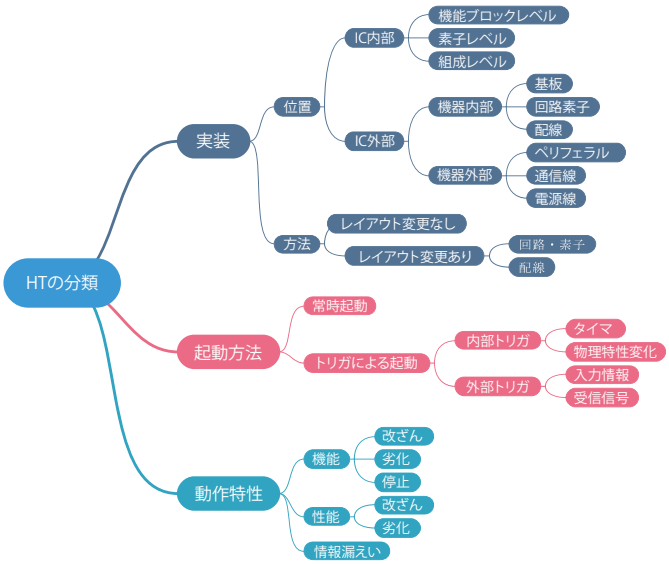

図-1　ハードウェアトロージャンの分類

HTは図-1のように，実装対象，起動方法，動作特性などにより分類され，その組合せは多岐に渡る．本稿ではこうした新たな脅威発見に関する研究動向とHT検知技術について述べる．

HTによる脅威の具体事例と研究動向

HTに関する具体的な脅威事例としては，シリアの核関連と思われる施設の空爆時に用いられたKill SwitchとよばれるHT[1]がある．本例では，シリアのレーダに使用されたICチップに，機能停止を実行できるHTを付加し，軍事作戦を展開する際に遠隔からHTを起動させ，迎撃を阻止したと報じられている．また，民生品では，クラウドサービスを提供する米企業が使用するマザーボードに情報漏えいを引き起こすHTが実装されていた可能性が報じられている[2]．一方，こうした事例において，HTが実際に実装されたと確実に結論付ける報告はなく，また，実装を疑われた側もHTの存在を完全に否定するには至っていない．

今後こうした脅威を抑止するためには，機器設計，製造後のテストでの検出技術や，こうした脅威を疑われた場合に，潔白を証明できる検査技術も求められている．完全な証明ができないまでも，これだけの検証を行ったと説明できることは重要である．

上述した背景の下，HT検出のための研究が近年盛んに行われている．図-2はHTに関する論文の年ごとの出版数とそれらを引用する論文数の推移を表している．2000年を超えたあたりから，論文

数が増加し，2018 年に至るまで増加を続けており，それらの論文を引用する論文も同様の傾向にある．また，図 -2 の論文の国別内訳は図 -3 のようになっており，アメリカ，中国において特に活発に研究が行われている．さらに，出版された論文の助成金は National Science Foundation（NSF）が 114 件，National Natural Science Foundation of China が 66 件，United States Department of Defense が 21 件，Fundamental Research Funds for The Central Universities が 14 件，Semiconductor Research Corporation が 12 件と研究費の面から見てもアメリカと中国におけるサポートが大きく，HT 検出技術や実装困難化技術の開発に力を入れていることが分かる．

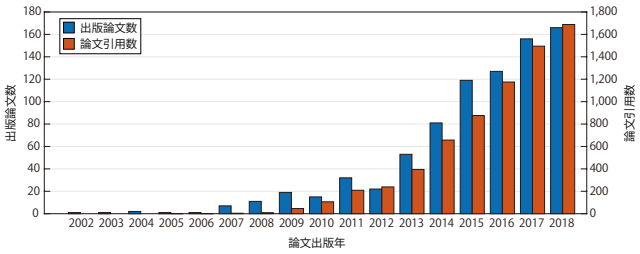

図 -2　HT に関する論文数とその引用件数の推移

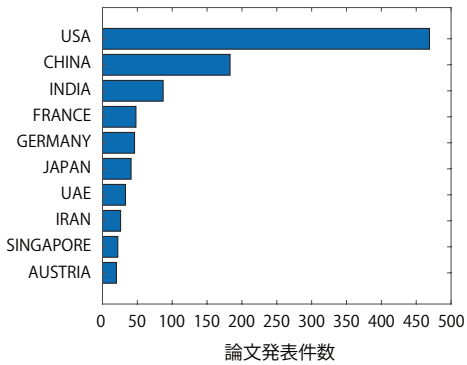

図 -3　HT に関する国別論文出版数（上位 10 カ国）

HT 検出技術の研究動向

図 -2 に挙げた論文のうち，引用件数が多い HT 検出・実装困難化に関連する論文およそ 100 件に着目し，その中で検討されている手法について分類を行った（図 -4）．また，図 -5 は引用数の多い論文をクラスタリングし，クラスタごとの引用関係を示している．

サイドチャネル情報：最も多く提案されている対策手法の 1 つにサイドチャネル情報を用いた HT の検出がある．この手法では HT が実装されていないと仮定されるデバイスの物理特性（消費電力，放射電磁界，実行時間の遅延など）をあらかじめプロファイリングし，これを基準として，HT の実装が疑われるデバイスと比較を行い HT 実装の有無を判断する．

この手法の利点は，対象を非破壊で検査できる点にある．一方，HT が混入していないことが保証されている「ゴールデンサンプル」が必要となり，「これをどこから入手するのか？」という問題が付きまとう．また，製造バラツキによってもサイドチャネル情報は変化する可能性がある．さらに，検出手法の多くは計測量としてサイドチャネル情報を利用することが多く，図 -5 に示す通り，検出および実装困難化技術の多くはサイドチャネル情報のクラスタと接

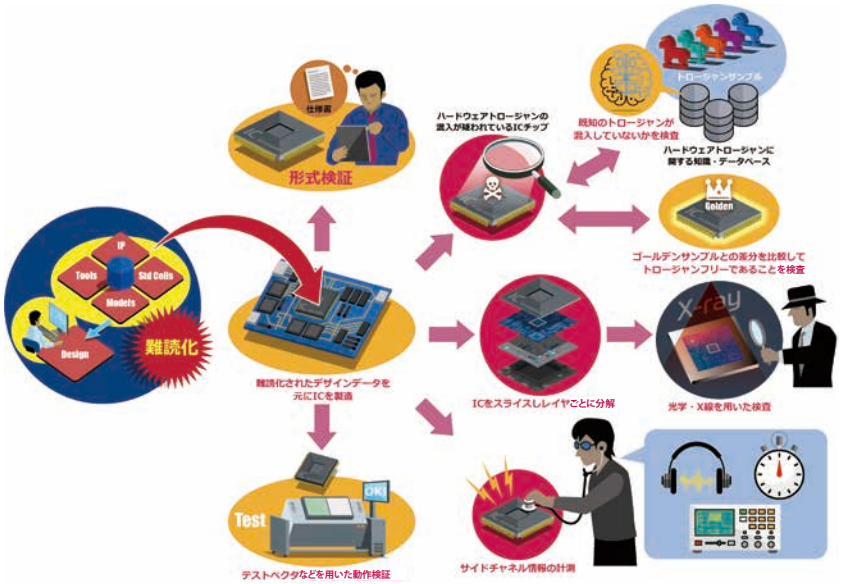

図 -4　ハードウェアトロージャンの検出および挿入困難化手法 [3)]

続されている．

ゲートレベルの特性評価：サイドチャネル情報の次に検討されている検出手法にゲートレベルの特性評価を利用した手法がある．この検出手法ではゲートレベルの物理特性に着目し，それに応じた電力や実行時間遅延などを用いてHTが挿入されたか否かを判断する．しかし，ゲートレベルの物理特性はIC製造過程におけるばらつきの影響を受けることが多いため，HT挿入による特性の変化なのか，製造ばらつきなのかを区別することが難しいため，製造ばらつきを抑える手法に主眼が置かれ検討が進められている．

テストベース：本検出法は，出荷前に通常チップに適用される機能テストのプロセスと同時にHTの検出も行う．たとえば，HTが起動するような入力（テストベクタ）を与えて，その結果起こる異常動作を検出する方法が考えられる．ただし，検出対象となるオブジェクトは不明であり，HTが起動する確率は非常に低いため，効果をあげるには通常の出荷テストとは異なるテストベクタを定義する必要がある．ただし，トロイの木馬を駆動させるテストベクタを必ず定義できるとは限らないため，本手法のみ

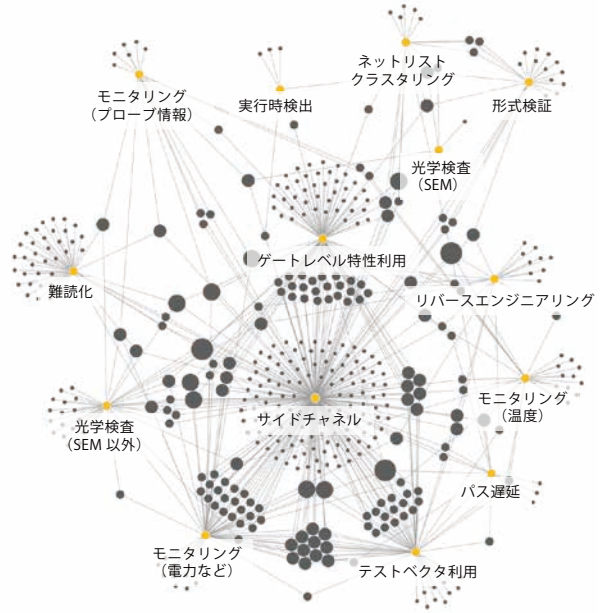

図-5　検出および挿入困難化手法の分類と関係[3)]

での検出は非常に不確実なものとなる．

光学検査：光学検査を用いた方法はIC内部のレイヤ1つずつ除去し，検査対象となるチップを破壊することによって実施される．そのため，光学検査は，リバースエンジニアリング技術に依存した検出手法となっている．光学検査では，走査光学顕微鏡（SOM），走査電子顕微鏡（SEM），およびピコ秒イメージング回路分析（PICA）を使用してレイヤの構造を復元し，収集された画像から最終的なチップのレイアウトを再構築することで，設計者が作成したレイアウトと比較し，HTの実装の有無を判断する．

光学検査は強力な検出手法であるが，コストが高く検出までに多大な時間を要するという問題点がある．

形式検証：ICチップの設計情報にHTが混入していないことを証明するアプローチである．第三者から供給されたICの機能ブロックにHTが含まれないことが証明されれば，チップベンダは安心してこれを使用できる．形式検証の手法を用いて，ICの機能ブロックが与えられた仕様通りに動作し，それ以外の動作をしないことを証明する方法である．たとえば，対象となる機能ブロックに許可されたあらゆる入力パターンに対して，実装物の出力と仕様の出力とが一致することを確認する方法が考えられる．この方法は，回路規模が大きくなると証明に時間がかかるという課題を有する．

電気特性計測：機器の電気計測に基づいてHTを検出手法がある．物理量としては計測しやすいインピーダンスなどに着目し，TDR（Time-Domain Reflectometry）などの手法を用いてHTの有無や実装された位置などを特定する．ただし，本手法もサイドチャネル情報を用いた検出法と同様に多くの場合，ゴールデンサンプルが必要となる．最近では設計データから電磁界シミュレーションにより導出したHTが存在しない電気特性をゴールデンサンプルとして用いる手法も提案されている．また，本手法はIC外部に接続されたHTにも有効である．

ここでは6つの代表的な検出手法についてそれぞ

れの概要を述べたが，こうした手法の高精度化を図るために機械学習を適用する研究も増加している．

本稿では紙面の関係上すべての対策を説明することは困難であるが，各対策などの最新動向については表 -1 に示す論文誌，国際会議で活発に議論されている．そのため，本技術に興味のある読者はこれらで発表された論文を参考にされたい．

現状決定打となる HT 検出・実装困難化の技術なく，複数の技術を組み合わせることが望ましい．前述の 6 つの検知手法のいずれも，それが有効に働くためには，これだけは信頼できるという拠りどころ（信頼の起点）が必要である．たとえば，特定の資格を持った従業員は不正を行わないという仮定や国内の特定の工場で製造された IC には HT は混入しないというような仮定もその一例である．そのため，HT の検出対象となるデバイスにおいて，信頼の起点をどこに置くべきかを考慮した上で，使用する検出技術を適用することが重要である．

HT に立ち向かうには

本稿ではハードウェアトロージャンの脅威，その脅威を抑止するための検出技術について解説した．ハードウェアレベルで実装が行われるハードウェアトロージャンはソフトウェアレベルでの脅威とは異なり，製品出荷後にソフトウェアパッチなどをリリースすることでその脅威を完全に取り除くことは困難である．また，サプライチェーンを利用して機器を製造するメーカ，もしくは，その一部で機器の製造を担うメーカはハードウェアトロージャンの検知，実装困難化についてはもちろん，ハードウェアトロージャンの実装を疑われた場合，その可能性を否定できるような技術を知る（所有する）必要がある．

現在のところ，HT を排除するための決定打は与えられていない状況であるが，HT を検出するために利用できる信頼の起点がどのような部分に設けられるのかを検討し，本稿で解説した検出，実装困難化技術を複合的に応用していくことが現状の解と言えよう．

参考文献

1) Adee, S. : The Hunt for the Kill Switch, IEEE Spectrum (May 2006).
2) Bloomberg Businessweek : The Big Hack : How China Used a Tiny Chip to Infiltrate U.S. Companies (2018), https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
3) 情報セキュリティ工学研究室，http://www.iselab.jp/

(2020 年 2 月 4 日受付)

林　優一（正会員）　yu-ichi@is.naist.jp

2009 年東北大学大学院情報科学研究科博士課程修了，奈良先端科学技術大学院大学・先端科学技術研究科教授．情報セキュリティ，環境電磁工学の研究に従事．IEEE EMC Society 電磁情報漏えいに関する分科委員会委員長．博士（情報科学）．

川村信一（正会員）　shinichi.kawamura@aist.go.jp

1985 年東京大学大学院工学系研究科修士課程修了．2020 年 4 月まで（株）東芝勤務．2018 年より産業技術総合研究所 サイバーフィジカルセキュリティ研究センター　副研究センター長，同ハードウェアセキュリティ研究チーム チーム長兼務．工学博士．

表 -1　HT について活発に議論されている論文誌・学会

	論文誌	会議
1	IEEE Design & Test of Computers	HOST : Hardware-Oriented Security and Trust
2	IEEE Trans. on Very Large Scale Integration Systems	S&P : IEEE Symposium on Security and Privacy
3	IEEE Computer	DATE : Design, Automation, and Test in Europe
4	IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems	ICCAD : International Conference on Computer Aided Design
5	IEEE Trans. on Information Forensics and Security	CHES : Cryptographic Hardware and Embedded Systems
6	IEEE Spectrum	DAC : Design Automation Conference
7	IEEE Transactions on Computers	CCS : Computer and Communications Security
8	IACR Cryptology ePrint Archive	IOLTS : International On-Line Testing Symposium
9	Journal of Electronic Testing	DFT : Defect and Fault Tolerance in VLSI and Nanotechnology Systems
10	ACM Trans. on Design Automation of Electronic Systems	HLDVT : High Level Design Validation and Test