NIST サイバーセキュリティ白書

NIST CSWP 46

半導体サプライチェーンにおける共謀脅威の分析

サンジェイ（ジェイ）・レキ コスタス・アンベリアディス

コンピュータセキュリティ

情報技術研究所

アビル・アサン・アキブ

アンクル・スリヴァスタヴァ

電気・コンピュータ工学

メリーランド大学カレッジパーク校

本書は以下から無料で入手できる：

https://doi.org/10.6028/NIST.CSWP.46

2025 年 6 月 30 日

本論文では、実験手順を適切に特定するために、商用、非商用を問わず、特定の装置、機器、ソフトウェア、または材料を識別している。このような識別は、NIST によるいかなる製品またはサービスの推奨または保証を意味するものではなく、また識別された材料または装置が必ずしもその目的に対して利用可能な最良のものであることを意味するものでもない。

NIST テクニカルシリーズの方針

著作権、使用、ライセンスに関する声明

NIST テクニカルシリーズ出版識別子の構文

出版履歴

2025-01-30 に NIST 編集審査委員会によって承認された。

この NIST テクニカルシリーズ出版物の引用方法

Rekhi S, Amberiadis K, Akib AA, Srivastava A (2025) Analyzing Collusion Threats in the Semiconductor Supply Chain.

(National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST。

CSWP 46。https://doi.org/10.6028/NIST.CSWP.46。

認可 ORCID iDs

サンジェイ（ジェイ）・レキ: 0009-0008-8711-4030

Kostas Amberiadis: 0009-0000-7771-5002 Abir Ahsan Akib: 0000-0002-1455-6662

アンクル・スリヴァスタバ 0000-0002-5445-904X

連絡先

hwsec@nist.gov

国立標準技術研究所

担当：情報技術研究所コンピュータセキュリティ部門 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

追加情報

関連する内容、更新の可能性、文書の履歴など、本書に関する追加情報は https://csrc.nist.gov/publications/cswp で入手できる。

すべてのコメントは、情報公開法（FOIA）に基づき公開される。

概要

本研究では、半導体サプライチェーンに関する脅威を分析する枠組みを提案する。この枠組みは、サプライチェーンの様々な段階からの敵対者の共謀を前提とした様々な脅威の重大性を定量化する指標を導入している。フレームワークの実際の適用を説明するために、2 つの異なるケーススタディを提供する。メトリクスと分析は、セキュリティの取り組みを導き、ハードウェアのセキュリティとコストのトレードオフを最適化することを目的としている。

キーワード

共謀、セキュリティメトリクス、サプライチェーンライフサイクル、サプライチェーンセキュリティ

目次

1. 序論 5
2. 半導体サプライチェーンの段階 7
3. サプライチェーン脅威分析の枠組み 8
3.1. 敵の意図を識別する 8
3.2. ハードウェアの脅威を識別 する 8
3.3. 脅威の悪用可能性について、ハードウェア開発ライフサイクルの段階を分析する 8
3.4. 異なる段階における敵対者間の共謀の効果を分析する 8
3.5. 各脅威のセキュリティ上重要な段階を識別する 9
4. ケーススタディ 10
4.1. ハードウェア侵入 10
4.2. 知的財産盗難 10
5. 結論と今後の課題 13
参考文献 14

図一覧

図 1. 半導体サプライチェーンにおけるセキュリティの課題 6
図 2. サプライチェーン脅威分析の方法論 8
図 3. ハードウェア・トロイの木馬挿入の文脈における共謀敵対者の脅威の重大度レベル 9
図 4. 論理難読化の文脈における、共謀する敵対者の脅威の重大度レベル 12

1. 序論

半導体のサプライチェーンには数多くのセキュリティ上の課題がある。ほとんどのチップ設計会社はファブレスとなり、製造はオフショア・ファウンドリーに依存している。これは特に最先端技術ノードに当てはまることであり、2021 年の半導体供給ショックは、こうしたサプライチェーンのセキュリティ問題を顕在化させた。可用性の不確実性に加え、現在の半導体サプライチェーンには、IP の盗難、偽造、トロイの木馬の挿入、リバースエンジニアリングなど、より微妙なセキュリティリスクが数多く存在する。

これらのセキュリティリスクに対抗するため、サプライチェーンの設計段階からテスト段階に至るまで、さまざまなソリューションが提案されている。対策の開発のために、国防高等研究計画局（DARPA）の「セキュアシリコンの自動実装（AISS）プログラム」[1]、DARPA の「自動実現アプリケーション用構造化アレイハードウェア（SAHARA）プログラム」[2]、海軍水上戦センター （NSWC）クレーン最先端異種統合プロトタイプ（SHIP）プログラム[3]、空軍研究実験所（AFRL）の「保証された設計のためのロックドエレクトロニクス（LEAD）」プログラム[4]、および AFRL の「エーテルスパイ」プログラム[5]など、これらセキュリティ問題に対処することは国家安全保障上極めて重要であるため、数多くの政府資金による研究プログラムが設立されている。このような深刻な課題に対処するためには、脅威の深刻度を最も効果的に軽減できる段階で、セキュリティ対策の取り組みを段階的に進めることが不可欠である。

サプライチェーンの脅威分析は、セキュリティ研究に不可欠な要素である。このような分析の目的は、1）集積回路に関連するさまざまな脅威と関連する脆弱性を識別すること、2）サプライチェーンのさまざまな段階で脅威がどの程度深刻化するかを分析すること、3）敵対者間の共謀による脅威の深刻度を定量化することである。このような分析を始める前にまず認識しておくべきことは、多くの脅威と関連する脆弱性が存在する一方で、半導体のサプライチェーンのすべての段階でそのすべてが悪用されるわけではないということである。脅威の深刻度はサプライチェーンの段階によって異なる。

例えば、サイドチャンネル解析のリスクはチップの使用シナリオにおいてより一般的であるのに対し、ハードウェアのトロイの木馬のリスクは、図 1 に示すように、設計と製造の初期段階においてより一般的である。

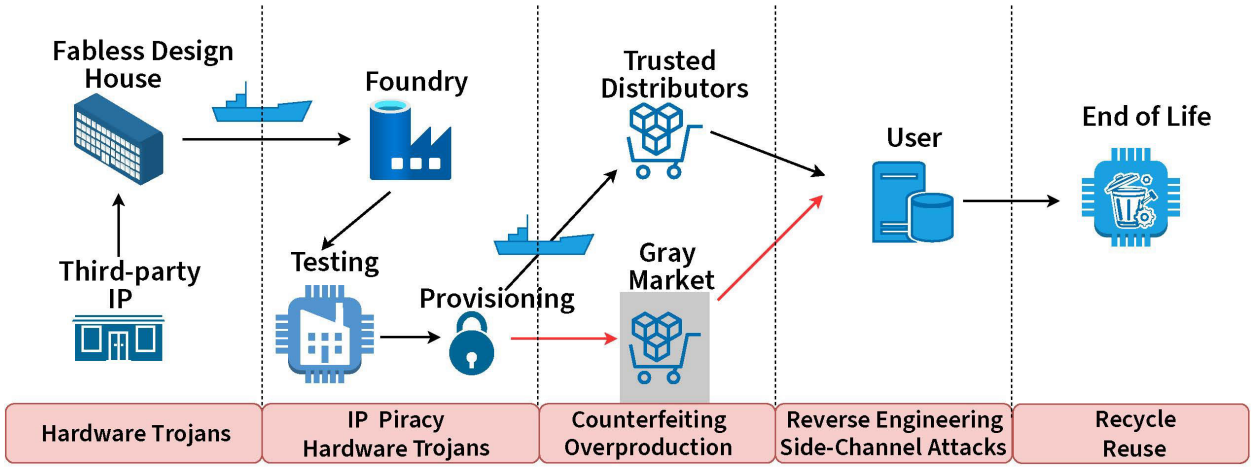

図 1. 半導体サプライチェーンにおけるセキュリティの課題

このことは、脅威分析が、脅威の種類と、脅威が最も効果的に作用するサプライチェーンの様々な段階の両方を考慮しなければならないことを意味している。さらに、サプライチェーンの異なる段階から 1 人以上の敵対者が協力してハードウェアを侵害することもあり、脅威の深刻度が増す。このような内部脅威は共謀の脅威と呼ばれる[6]。

本文書は、ハードウェアのサプライチェーンにおける潜在的な共謀リスクに焦点を当て、以下のように構成する：

- セクション 2 では、半導体サプライチェーンの様々なフェーズについて概説する。
- セクション 3 では、サプライチェーンの脅威を分析する枠組みを説明する。
- セクション 4 では、提案する枠組みを包括的に説明するために、ハードウェアのセキュリティ脅威の 2 つの実例を示す。
- セクション 5 では、議論を締めくくり、今後の研究の方向性を示す。

2. 半導体サプライチェーンの段階

半導体サプライチェーンにおけるセキュリティ上の懸念を分析するための最初のステップは、サプライチェーンの様々なステージを概説し、それぞれに関連する潜在的な脅威を特定することである。ステージの標準セットは存在しない。しかし、本分析では、アレノ（Areno）[7]が定義した 7 つのステージを使用する。ユーザーステージは、攻撃対象が類似しているため、展開ステージと統合した。また、Areno [7]によって元々定義されていた 7 つのステージに、使用終了ステージが追加された。ステージの簡単な説明を以下に示す。

1. **コンセプト：**コンセプト段階は、集積回路（IC）の誕生段階である。この段階では、集積回路（IC）の目標と目的が策定され、ハードウェア部品の範囲と目標が議論される。顧客、設計、企画、財務チーム、その他の主要な利害関係者がこの段階に関与する。
2. **設計：**設計段階では、コンセプト段階で生成されたアイデアを形にする。この段階では、さまざまなコンピュータ支援設計（CAD）ツールの助けを借りてコンセプトのプロトタイプを作成し、コンセプト段階で特定された目標が達成されているかどうかを分析する。この段階には、サードパーティ製ソフトウェアやハードウェアのプロトタイプの使用も含まれる。
3. **統合：**統合とは、設計者やサードパーティによるさまざまな設計要素を統合する段階である。多くのデザイン要素にはすでにテスト済みのソリューションがあるため、すべてを一から作成する必要がないため、この段階は極めて重要である。サードパーティからこれらのソリューションを購入し、デザインに統合する方が現実的である。
4. **製造：**IC の設計が終わると、製造段階に入る。この段階には、製造やパッケージングなどいくつかの工程が含まれる。製造施設の建設と維持には高いコストがかかるため、多くのデザイン・ハウスはファブレスを採用し、設計を他所のメーカーに委託している。
5. **テスト：**テストとは、製造事業者が製造した集積回路（IC）が正常に動作することを確認するためにテストする段階である。製造完了後、各 IC はテストを受ける。IC の機能はここでテストされ、設計仕様に準拠していることが確認される。
6. **プロビジョニング：**プロビジョニングは、製造された IC に標準データと機密データをロードする段階である。標準データは一般的なもので、ほとんどがオープンソースで入手可能だが、機密データとは、開示することで IP やセキュリティが損なわれるようなものを指す。例えば、暗号モジュールのキーやロジックロックのキーは機密データである。
7. **展開と使用：**このステージには、顧客に IC を提供し、IC を使用することが含まれる。多くのハードウェア脆弱性はこの段階で悪用される。
8. **使用終了：**IC の製造終了とは、製造事業者が IC を販売または製造しなくなる段階である[8]。これは多くの場合、技術の進歩により、より優れた性能を示す新しい IC が発売されたためである。チップが耐用年数を迎えると、展開されたチップは徐々に交換され、廃棄される。これらの廃棄チップは再利用されたり、新しいハードウェアにリサイクルされたりして、その品質と性能が損なわれることが多い。

3. サプライチェーン脅威分析の枠組み

この研究では、さまざまな脅威を分析する枠組みを提案し、敵対者間の共謀が脅威の深刻さにどのような影響を与えるかを分析する。この分析は、敵対者の意図、アクセス、リソース、そしてそれらの共謀が異なる脅威の重大性にどのように影響するかを議論する 5 つの明確な段階に分かれている。枠組みを図 2 に示す。この枠組みは、内部脅威を含むサプライチェーンの全段階にわたる脅威を組み込んでいる。

図 2. サプライチェーン脅威分析の方法論

3.1. 敵の意図を識別する

サプライチェーンのセキュリティ分析は、敵対者の目的を識別することから始まる。例えば、敵対者はハードウェアの機能を妨害したり、設計者の知的財産（IP）を盗んだりすることを望むかもしれない。この分析では、潜在的な攻撃者、防御すべき資源、緩和が最も適用される半導体サプライチェーンの段階を説明する。

3.2. ハードウェアの脅威を識別する

第二のステップは、敵の意図に関連する脅威を特定することである。例えば、その意図が IP の窃盗であれば、保護すべき IP を特定しなければならない。この文脈では、ロジックの難読化に対する攻撃が脅威として特徴づけられる。同様に、敵がハードウェアへの侵入を意図している場合、ハードウェアのトロイの木馬の挿入を検討する必要があるかもしれない。

3.3. 脅威の悪用可能性について、ハードウェア開発ライフサイクルの段階を分析する

この時点で、1 つ以上の重大なハードウェア脅威が識別された。次の段階では、その脅威が半導体サプライチェーンのどの段階で悪用できるかを判断する。製造事業者の敵対者がロジックの難読化にどれだけの脅威を与えるか、あるいはプロビジョニングの敵対者がハードウェアのトロイの木馬挿入に脅威を与えるか、といった疑問が提起される。脅威を考慮して、このステップでは、半導体サプライチェーンのセキュリティ上重要な段階を決定する。さらに、このステップでは、サプライチェーン内の特定の時点で脅威が悪用できないかどうかを判断する。

3.4. 異なる段階における敵対者間の共謀の効果を分析する

半導体サプライチェーンの各段階はそれぞれ異なるため、敵対者は半導体サプライチェーンの各段階において、システムへのアクセスやシステムに関する知識の程度は様々である。攻撃の有効性は、敵対者のシステムに関する知識とアクセスレベルに大きく依存する。敵対者が持っている両者の程度は様々である。例えば、製造事業者は詳細な設計知識を持っているかもしれないが、エンドユーザーは通常、システムの内部機能へのアクセスが制限され、ほとんど洞察することができない。その結果、両者の能力は大きく異なる。

このように、ライフサイクルの異なる段階にある敵対者同士が結託することで、脅威はより深刻なものとなる。

分析のこの時点で、サプライチェーンの異なるステージの敵対者が結託した場合の脅威の深刻度を決定するために、線形スケールを適用する。このスケールは 0 から 10 の範囲で、共謀する敵対者グループの相対的な脅威レベルを表す。図 3 は、ハードウェアトロイの木馬挿入の脅威の文脈で開発されたスケールの例である。スケールは 10 から始まり、最も高い脅威の重大度レベルを表している。このシナリオでは、関連するすべての敵対者が共謀していると仮定している。この時点から、一度に 1 人の敵対者を共謀から徐々に排除し、残りの敵対者の可能な組み合わせごとに、結果として生じる脅威の深刻度をアセスメントする。敵対者が削除されるにつれて、脅威の深刻度は、敵対者の数とその特定の役割に応じて減少する。例えば、図 3 に示すように、製造事業者が結託から外された場合、脅威の深刻度は 8 に低下する。しかし、設計者が排除されると、脅威の深刻度は 6 に低下する。これは、悪意のある設計者は、悪意のある製造者に比べて、ハードウェアのトロイの木馬を挿入されるリスクが高いことを示唆している。

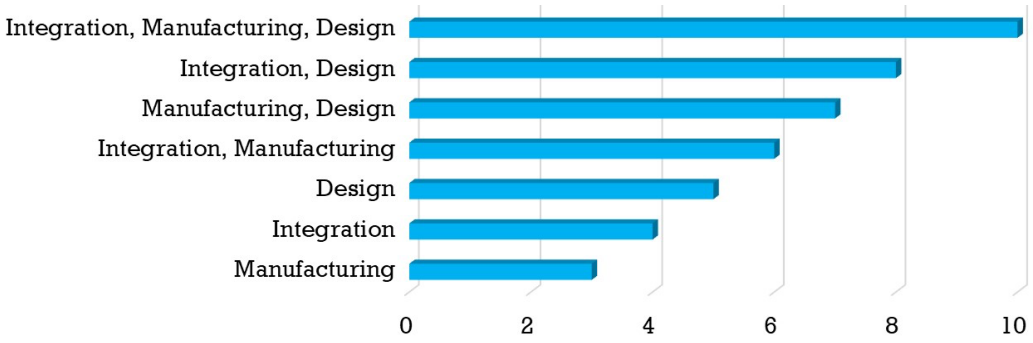

図 3. ハードウェア・トロイの木馬挿入の文脈における共謀敵対者の脅威の重大度レベル

この尺度は相対的なものであり、共謀における異なる敵対者によってもたらされる脅威の深刻度に関するコンテクストを提供するが、深刻度の正確な違いを定量化するものではないことを意味する。例えば、図 3 は、インテグレーターと設計者の結託が、製造事業者と設計者の結託よりも深刻な脅威をもたらすことを示している。この相対的なアプローチは意図的なものであり、利害関係者によって脅威の深刻度を評価する際の優先順位が異なる可能性があるためである。あるアナリストは攻撃完了までの時間を優先するかもしれないし、別のアナリストは攻撃成功の可能性を重視するかもしれない。このような柔軟性により、アナリストは最も重要であると考える評価基準に基づいて、独自にカスタマイズした非線形の尺度を開発することができる。このような尺度により、設計者の脅威と製造事業者の脅威の深刻度を定量的に比較するなど、より詳細な理解が可能となる。

3.5. 各脅威のセキュリティ上重要な段階を識別する

最後のステップでは、各脅威が半導体のサプライチェーンのどの段階に位置するかに関連して、各脅威の種類と深刻度を決定する。半導体サプライチェーンのどの段階でセキュリティを確保するか、また確保すべきかの選択は、すべての脅威マトリックスを考慮に入れて、この段階で行わなければならない。これは必然的に、コストとセキュリティのトレードオフを天秤にかけることになる。

4. ケーススタディ

このサプライチェーン脅威分析の枠組みは、様々な脅威タイプに適応することを意図している。以下のシナリオ例では、IP 盗難とハードウェアの侵入を検討している。

4.1. ハードウェア侵入

- ステップ 1：セキュリティ分析は、チップに侵入する敵の意図を識別する。そのために、敵対者はハードウェアを使用不能にする、チップから機密情報を送信する、チップを異常動作させる信号を受信する、などの手段を講じるかもしれない。
- ステップ 2：ハードウェアに侵入する方法の 1 つに、ハードウェアトロイの木馬を挿入する方法がある。ハードウェアのトロイの木馬は、チップ内部のシリコン、プリント回路基板、ファームウェアなどに挿入される可能性がある。この例では、ハードウェアのトロイの木馬回路がチップに挿入されることを脅威と考える。
- ステップ 3：IC ライフサイクルの中でトロイの木馬が挿入される可能性があるのは、プリパッケージング段階だけであるため、設計、統合、製造が関心のある段階となる。ハードウェアのトロイの木馬は、Yu らや Cruz ら[10]、[11]によって、設計と統合の段階でネットリストに挿入されている。ハードウェア・トロイの木馬は、Perez らによって、最終的なレイアウトにも挿入されている。ハードウェアトロイの木馬は、プロビジョニング中、展開中、または使用終了時に挿入することはできないため、分析から除外することができる。この文脈で重要な段階はテストである。これは、チップの機能とトロイの木馬がテストされる段階である。この段階が損なわれると、未テストの IC が市場に出回り、機能や標準への不適合、トロイの木馬の侵入のリスクが高まる。このように、テストはセキュリティ上重要な段階であり、安全を確保しなければならない。
- ステップ 4：ハードウェアにトロイの木馬を挿入する鍵は、検知を困難にすることである。このような意図から、敵はトロイの木馬を設計し、非常にまれな入力の組み合わせとハードウェアへの最小限の変更のみで起動するようにする。このため、設計者は、設計の内部に関する知識により、トロイの木馬を起動させるための稀な入力ベクトルを選択することができるため、最強の敵対者となる。一方、製造事業者は、トロイの木馬を検知しやすくするために、レイアウトに余分なハードウェアを挿入しなければならない。インテグレーターの脅威は、これら 2 つの敵対者の中間に位置する。図 3 は、トロイの木馬を挿入する敵対者の重大度レベルを示している。この場合、敵対者間の共謀が増加すると、挿入されるトロイの木馬の数が増加する。これにより、1 つ以上のトロイの木馬が検出されずに残る可能性が高まる。
- ステップ 5：このステップでは、3 つのステージ（統合、製造、設計）のうち 1 つ以上を保護するオプションがある。サプライチェーンの段階を保護することにはコストがかかるため、保護すべき段階を選択するために、コスト対セキュリティ分析を実施する必要がある。

4.2. 知的財産盗難

- ステップ 1：この例では、敵対的サンプルの意図を知的財産の窃盗と仮定する。IP には、IC 内部で動作する設計やプログラムなど、さまざまな形態がある。例えば、ライバル企業が IP を手に入れ、不当な優位に立つこともある[13]。また、偽造 IC が製造され、品質が劣り、ビジネス、生命、財産に計り知れない損害を与える可能性もある[14]。この場合、保護に値する知的財産は設計秘密であると仮定する。

- ステップ 2： 設計秘密を防御する手法の一つとして、キー入力やキーゲートを導入することにより、設計中の組合せ論理コンや有限状態機械を強化する論理難読化がある[15]。このような技術は、信頼できない製造事業者による攻撃に対する強力な対策となる。ロック・メカニズムの安全性を評価するために、研究者は、デザインのロックを解除しようとする敵対者をエミュレートするために、多くの難読化解除手法を提案してきた。したがって、意図に関連する脅威は論理難読化の脅威である。

- ステップ 3: 脅威が識別されると、サプライチェーンの段階を分析し、どこに脅威が存在するかを特定する。各難読化解除方法は、特定の脅威モデル（すなわち、ロックされた設計へのアクセス及び知識のレベル）を必要とする。ほとんどの難読化解除手法は、入出力（I/O）アクセス、スキャンチェーンアクセス、サイドチャンネル測定へのアクセスなど、何らかのレベルで動作中のチップへのアクセスを想定している。Shamsi らと Massad らは、入力と出力のみが敵にアクセス可能な場合の難読化解除技術を研究している[16][17]。スキャン・チェーンを通じて内部レジスタ値にもアクセスできる場合、ブーリアン充足可能性（SAT）攻撃とその派生技法を用いてロックされたデザインを難読化解除することができる[18]。これらのタイプのアクセスは、プロビジョニング段階が完了した後に利用できる。したがって、これらの技術は、展開・使用ステージや使用終了ステージにおいて、設計の難読化を解除するために使用することができる。現実の世界では、敵対者はチップから秘密を抽出するのに必要なツールやリソースを持つだけでなく、様々な設計を扱う長年の経験を持つ経験豊富なエンジニアや機構である可能性が高い。このような敵対者は、インテグレーター、製造事業者、テスターという形でライフサイクルの初期段階に存在し、そこでは動作するシステムは存在しないが、設計に関する多くの経験と知識が存在する。このシナリオにおける難読化解除技術は、 、ロックされたネットリストを、敵が以前に遭遇したことのあるデザインにマッピングすることに重点を置く。この方向での一つのアプローチは、ロックされたネットリストと以前に遭遇したネットリストの構造的類似性を見つけることである[19]。構造的類似性を利用するもう一つの方法は、Fyrbiak ら[20]が提示したグラフ類似性アルゴリズムを使用することである。このような技術は、統合、製造、テストの各段階において、敵対者が設計上の秘密を抽出するために使用することができる。

  設計ステージには難読化されていない設計が含まれ、プロビジョニングステージには設計の難読化に必要なキーが含まれる。これら 2 つのステージは、設計秘密を抽出するために攻撃を仕掛ける必要はない。このように、ロジック・ロックの文脈では、脅威は設計から製造終了までのサプライチェーンの各段階に存在する。この文脈における IP は設計者のものであり、設計者が侵害された場合、セキュリティは存在しない。繰り返しになるが、プロビジョニングはロジックロックのキーが IC にアップロードされる段階である。キーが知られてしまうと、設計の秘密がすべて明らかになってしまうため、プロビジョニングの段階もセキュリティ上非常に重要である。

- ステップ 4：これまでの分析から、設計秘密に関する情報が限られているステージは、統合、製造、テスト、展開と使用、使用終了である。それらの共謀に関連する脅威を分析するためには、各段階の敵対者がどのような情報や知識を脅威にもたらすことができるかを分析する必要がある。インテグレーターは難読化された設計を階層的に見ることができるかもしれない。一方、製造事業者は、様々な種類の設計を扱った経験を持っている。例えば、オフショア・ファウンドリーは、世界中の様々なファブレス・デザインハウスからのデザインにアクセスできる。テスターはいくつかの入出力ベクトルを持っており、ユーザーは稼働中のシステムを持っている。このように、各段階の敵対者は、それぞれ独自の知識とアクセスのセットを持っている。このことは、より多くの敵対者が結託すればするほど、より多くの情報が利用可能になり、その結果、脅威がより深刻になること

を示している。図 4 は、共謀する敵対者の組み合わせを変えた場合の脅威レベルを示している。ここで、製造事業者は高度な知識を持っているため、彼らだけでも強力な敵になり得る。しかし、稼働中のシステムにアクセスすることで、IP が盗まれる可能性が高まる。このため、生産終了段階やチップ・ユーザー段階の敵対者が強くなる。この文脈では、使用終了ステージと展開・使用ステージの敵対者は、稼働中のシステムに同程度のレベルでアクセスでき、同程度の量の情報を入手できる。このため、図 4 では、使用終了ステージを展開ステージとグループ化している。

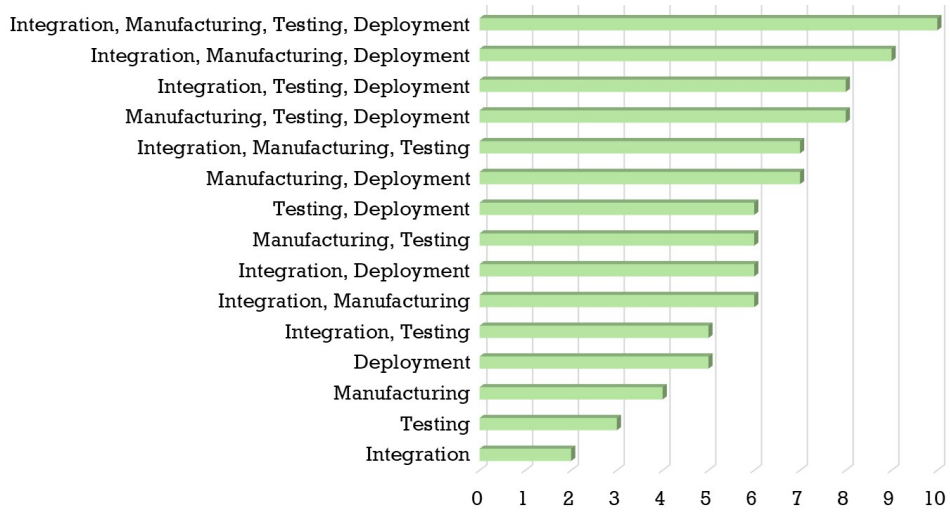

図 4. 論理難読化の文脈における、共謀する敵対者の脅威の重大度レベル

これらの敵対者が製造事業者と結託した場合、稼働中のシステムへのアクセスが豊富な知識と組み合わされ、脅威はより深刻になる。もし完全性攻撃者が彼らと結託すれば、攻撃対象は容易に小さな部分に分割され、その結果、攻撃はより早く収束することができ、論理難読化の脅威の深刻度が増す。統合、製造、テスト、展開の各ステージが連携するシナリオは、脅威の深刻度が最も高い。サプライチェーンのこの時点で、共謀は広範なシステム知識と広範なアクセスの収束をもたらし、重大度レベル 10 に分類される。この共謀シナリオから敵対者を系統的に排除することで、知識とアクセスのレベルがどのように変化し、その結果、脅威の深刻度がどのように影響されるかを観察することができる。

- ステップ 5：コスト対セキュリティ分析を実施し、セキュリティを確保すべきステージ （すなわち、統合、製造、テスト、展開と使用、使用終了）に優先順位をつける。

5. 結論と今後の課題

半導体のサプライチェーンセキュリティを調査すると、レジリエンスと安全性の高いインフラを提供するために対処すべき弱点と機会が複雑に絡み合っていることがわかる。半導体の需要が世界的に増加し続ける中、サプライチェーンの中断がもたらす影響は深刻さを増している。本稿では、半導体のライフサイクル全体におけるセキュリティ上の懸念と談合の影響、そして攻撃の動機を分析する。他の動機もこの方法論で分析できる。本手法は、緩和計画に役立つ相対的なリスクベースのスコアを提供する。将来的には、NIST はこの作業を拡張して、3D ヘテロジニアス統合に関連するサプライチェーンの脅威を分析し、さまざまなハードウェアの脆弱性を枠組みに統合することを計画している。このようなハードウェアとサプライチェーンのセキュリティ問題に対処することは、国益を守り、経済の安定を促進するために不可欠である。

参考文献

[1] DARPA (2020) DARPA Selects Teams to Increase Security of Semiconductor Supply Chain.https://www.darpa.mil/news/2020/semiconductor-supply-chainsecurity で入手可能。

[2] DARPA (2021) 防衛ニーズに対応した安全なカスタムチップの国内製造を拡大する。https://www.darpa.mil/news-events/2021-03-18 で入手可能。

[3] NSWC Crane Corporate Communications (2019) NSWC Crane は OTA を活用し、米国政府が最先端のマイクロエレクトロニクスの安全な設計、組立、パッケージング、テストにアクセスできるようにする。https://www.navsea.navy.mil/Media/News/Article/2005099/nswc-crane-leverages-otato-ensure-that-the-us-government-has-access-to-secure/。

[4] システム研究所（2020 年） AFRL-ノースロップ・グラマン：Locked Electronics for Assured Design（LEAD）：ASIC IP ブロックを遅延ロックして機能を保護する。https://isr.umd.edu/research-funding/afrl-northrop-grumman-locked-electronicsassured-design-lead-delay-locking-asic-ip で入手可能。

[5] Wolfe F (2020) Aether Spy 次世代多機能レーダーが前進、ノースロップグラマンが発表。*Defense Daily*.https://www.defensedaily.com/aether-spynext-generation-multi-function-radar-advance-northrop-grumman-says/air-force/ で利用可能。

[6] CISA (2020) 内部脅威の定義。https://www.cisa.gov/topics/physicalsecurity/insider-threat-mitigation/defining-insider-threats で入手可能。

[7] Areno M (2020) 集積回路に対するサプライチェーンの脅威。インテルホワイトペーパー。https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-08/supply-chain-threats-against-integrated-circuitswhitepaper-july2020.pdf で入手可能。

[8] Evernex (2024) EOL の意味：ハードウェアの寿命が尽きるとはどういうことか？https://evernex.com/industry-guide/eol-meaning/ で入手可能。

[9] Vincent J (2018) 中国のスパイがアップルやアマゾンなどが使用するサーバーにマイクロチップを挿入したと報じられた。https://www.theverge.com/2018/10/4/17935868/-chinese-spies-microchip-hackservers-apple-amazon-supermicro。

[10] Yu S, Liu W, O'Neill M (2019) An improved automatic hardware trojan generation platform.*IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (IEEE, Miami, Florida), pp 302-307. . https://doi.org/10.1109/ISVLSI.2019.00062

[11] Cruz J, Huang Y, Mishra P, Bhunia S (2018) An automated configurable Trojan insertion framework for dynamic trust benchmarks.*Design, Automation & Test in Europe Conference & Exhibition* (IEEE, Dresden, Germany) pp 1598-1603. . https://doi.org/10.23919/DATE.2018.8342270

[12] Perez TD, Pagliarini S (2023) 確定レイアウトにおけるハードウェアのトロイの木馬挿入：方法論からシリコン実証まで。*IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (IEEE) 42(7)：2094–2107. https://doi.org/10.1109/TCAD.2022.3223846

[13] Astute Electronics (2024) SK Hynix Engineer Jailed for Semiconductor IP Theft Amidst Global Tech Rivalry.https://www.astutegroup.com/news/general/sk-hynixengineer-jailed-for-semiconductor-ip-theft-amidst-global-tech-rivalry/ にて入手可能。

[14] Takahashi D (2011) Feds close huge chip counterfeiting case (exclusive).https://venturebeat.com/business/feds-close-the-books-on-a-huge-chip-counterfeitingscheme/。

[15] Chakraborty A, Jayasankaran N G, Liu Y, Rajendran J, Sinanoglu O, Srivastava A, Xie Y, Yasin M, Zuzak M (2019) Keynote: A disquisition on logic locking.*IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (IEEE) 39(10):1952-1972。https://doi.org/10.1109/TCAD.2019.2944586。

[16] Shamsi K, Li M, Pan D Z, Jin Y (2019) KC2：Key-Condition Crunching for Fast Sequential Circuit Deobfuscation.*Design, Automation & Test in Europe Conference & Exhibition* (IEEE, Florence, Italy) pp 534-539. . https://doi.org/10.23919/DATE.2019.8715053

[17] Massad M E, Garg S, Tripunitara M (2017) Reverse Engineering camouflaged sequential circuits without scan access.*IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (IEEE, Irvine, CA) pp 33-40. https://doi.org/10.1109/ICCAD.2017.8203757

[18] Subramanyan P, Ray S, Malik S (2015) Evaluating the security of logic encryption algorithms.*IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (IEEE, Washington, DC) pp 137-14. . https://doi.org/10.1109/HST.2015.7140252

[19] Cheng Y, Wang Y, Li H, Li X (2015) A similarity-based circuit partitioning and trimming method to defend against hardware trojans.*IEEE Computer Society Annual Symposium on VLSI* (IEEE, Montpellier, France) pp 368-373. . https://doi.org/10.1109/ISVLSI.2015.93

[20] Fyrbiak M, Wallat S, Reinhard S, Bissantz N, Paar C (2020) Graph similarity and its applications to hardware security.*IEEE Transactions on Computers* (IEEE) 69(4):505-519. https://doi.org/10.1109/TC.2019.2953752