JTAG のセキュリティ脅威

―攻撃の現状とその対策―

王　森レイ*，亀山　修一*，高橋　寛*

JTAG Security Threats: Current Attacks and Countermeasures

Senling WANG*，Shuichi KAMEYAMA*，Hiroshi TAKAHASHI*

*愛媛大学大学院理工学研究科(〒790-8577 愛媛県松山市文京町 3 番)

*Graduate School of Science and Engineering, Ehime University (3 Bunkyo-cho, Matsuyama, Ehime 790-8577)

1. 背景

近年の IoT(Internet of Things)・人工知能・自動運転・ロボティクスなどの情報通信技術（ICT）の急速な進展に伴い，高性能・多機能化される集積回路（IC）が民生機器からミッションクリティカルな機器までに組込まれ，社会の基盤を成している。一方，半導体産業の分業化とグローバル化に伴い，現在の IC は設計から製造，テスト，パッケージング，出荷まで世界中の様々なメーカが参画しているため，信頼できない第三者や悪意のある者による攻撃を受けることが懸念されている。IC のハードウェア・セキュリティが確保されていなければ，外部・内部からの攻撃によって，IC に保存・処理されている機密情報（個人情報や IC の設計情報）が漏洩したり，IC が含まれるシステムの機能安全が脅かされたりする恐れがある。

近年，IC のハードウェア・セキュリティ問題では，一つの可能性として JTAG に起因する脆弱性が着目されている。JTAG とは，バウンダリスキャンアーキテクチャとそれにアクセスするためのシリアルアクセスポートの標準規格（IEEE 1149.1）である [1]。JTAG では，IC の内部コア（ロジック回路）と外部入出力ピンの境界にレジスタを配置し，これらをチェーン状に接続し，僅か 4～5 本の外部端子（TAP:テストアクセスポート）を操作することで，外部からロジック回路を容易にアクセス（制御と観測）できる。JTAG は本来，高密度実装基板での IC 間の電気的導通を容易に検査することが主目的であったが，少数ピンの手軽なインタフェースで IC の内部回路にアクセスできるため，FPGA/CPLD などの論理再構成可能デバイスの書き込みや CPU/MCU などのデバッグでも広く用いられている [1]。さらに，近年の半導体製造プロセスの微細化により複雑になりつつある IC 回路に対するテストを容易かつ効率的に行うために，JTAG は IC 内部に組込まれるテスト機構（例えば：組込み自己テスト BIST，温度電圧モニターなど）のインタフェースとして適用されている。また，近年の SoC（System on Chip）に搭載される多種多様な IP コア†に対するテストおよびデバッグを行うために，JTAG に基づいたラッパーバウンダリースキャン（IEEE 1500）や IJTAG(IEEE 1687)が開発された [1]。

出荷後の電子機器の故障解析や FPGA の回路変更等の目的で，JTAG を IC へのアクセス機構として残しておくことがある。後述する JTAG セキュリティ対策がないと，JTAG インタフェースを介して電子機器を構成する IC の内部コアを直接制御と観測することができる場合もあるので，回路に格納される機密情報を盗んだり，システムの動作を妨害したり，リバースエンジニアリングなどの攻撃行為の「バックドア」として悪用される可能性として指摘されている [2]。特に，近年の IoT 技術の急速な普及に伴い，膨大な数の電子機器がインターネットに接続されるため，悪意のある者が JTAG を悪用してネットワークを介して IoT システムに対して攻撃を行う可能性もある。

本稿では，まず，JTAG におけるセキュリティ脆弱性とそれに伴う脅威の可能性に関して紹介する。次に，対応策としてのセキュリティ強化法を紹介する。

本稿の構成は以下の通りになる。第2章では，テスト容易化設計の観点から，JTAG と IJTAG の構造と動作について解説する。第3章では，JTAG に関わるセキュリティ脅威と攻撃方法について紹介する。第 4 章では，JTAG セキュリティ強化対策を紹介する。第 5 章では，産業界での JTAG セキュリティ対策の導入事例について紹介する。第 6 章では，考察と今後の課題について述べる。第 7 章は本稿をまとめる。

2. JTAG の構造と動作

ここでは，テスト容易化設計の観点から，JTAG の構造と動作について解説する。IEEE 1149.1 規格では，テストアクセスポート(TAP)とバウンダリスキャンアーキテクチャが定義されている。図 1 はそのアーキテクチャを示している。バウンダリスキャンアーキテクチャは通常，チップの内部回路と入出力ピンの間にバウンダリスキャン

† IP コア（Intellectual Property Core）とは，FPGA，IC などの半導体デバイスを構成する再利用可能な回路部の設計情報である。

レジスタを配置し，これらをチェーン状に接続してシフトレジスタを構成する。このシフトレジスタを利用して，テストデータ入力（TDI）とテストデータ出力（TDO）を介してチップ内に埋め込まれる回路にデータを印加したり，レスポンスを観測したりすることができる [3]。バウンダリスキャンチェーンの他に，必須のバイパスレジスタ（1ビットのフリップフロップ）とオプションの ID レジスタ（メーカが付与した部品番号，部品バージョンコードなど）が定義されている。

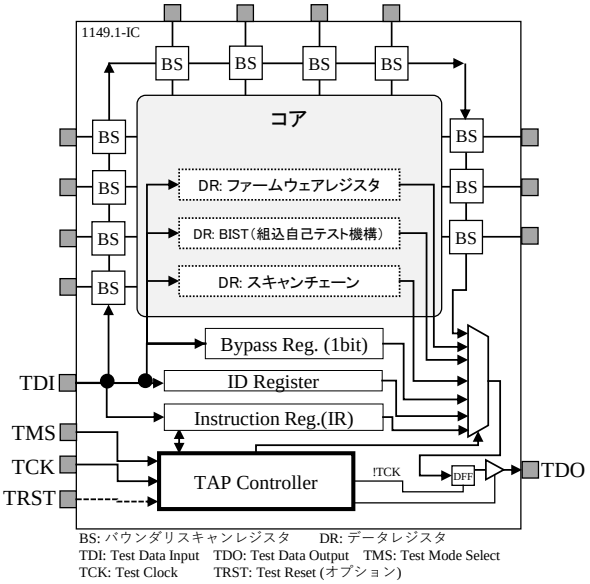

図 1 IEEE1149.1（JTAG）アーキテクチャ

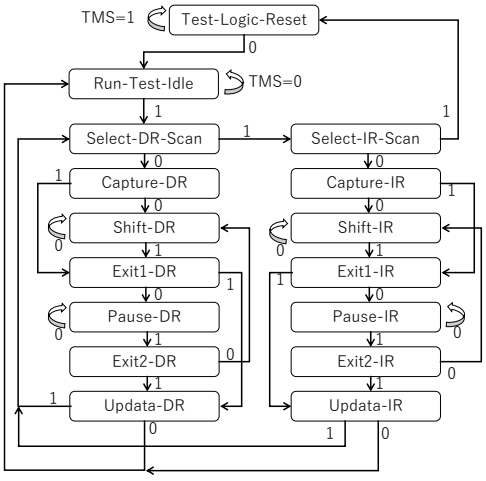

図2 TAP コントローラの状態遷移図

JTAG 標準で定義されたコア回路外部に配置する上記のレジスタ以外にも，設計者がコア回路内部に各種のデータレジスタ(DR)を追加することができる。例えば，IC のコア回路にフィールドテスト機能を持たせるには，対象コア（回路）にスキャンチェーンや BIST のテスト機構を設け，これらのテスト機構に含まれる DR を TDI ポートと TDO ポートを介してアクセスできる。DR へのアクセスは，図2に示すようなステートマシンを実装した TAP コントローラで行う。ユーザは，適切な命令コードを命令レジスタ（IR）にロードすることで対象 DR に対して「キャプチャ」「シフト」「アップデート」という 3 つの基本操作を行う [3]。

大量かつ多様な機能回路（IP コア，メモリ，プロセッサなど）が統合される SoC を容易かつ効率的にテストするために，JTAG を拡張した IEEE 1687 規格（IJTAG）が開発された。図3は IJTAG の構成例を示している。IJTAG では，SIB（Segment Insertion Bit）や SCB（Scan mux Control Bit）を用いて，特定の機能回路に内蔵されるテスト機構（BIST エンジン，スキャンチェーン，温度電圧モニターなど）のみにアクセスできる再構成可能スキャンネットワーク（RSN）を形成できる [1]。

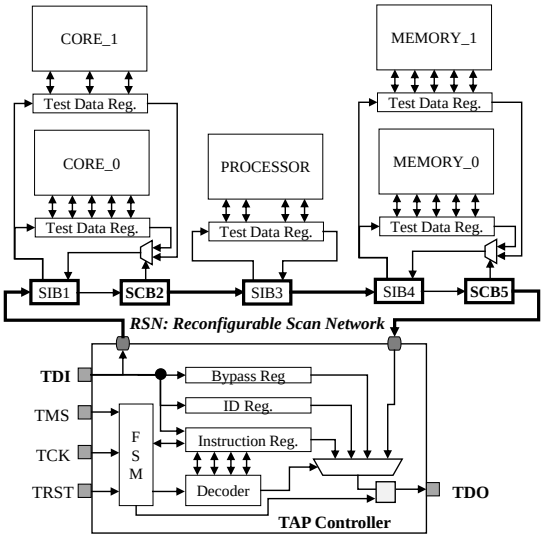

図3　IEEE 1687(IJTAG)構造

図3に示すように，SIB を機能回路（プロセッサやメモリなど）のテスト機構にアクセスするためのゲートとして，SIB が開く場合のみアクセスが可能となり，そうでなければ，テスト機構がバイパスされる。SCB は，同じ階層（SIB を共有する）に属する機構回路のテスト機構のテストデータレジスタ(TDR)を選択するマルチプレクサを制御する。ユーザは TAP コントローラを操作して，TDI を介して SIB と SCB に適切な値を設定することで，ターゲットのテスト機構を RSN に含めることができる [1]。

3. JTAG に関わるセキュリティ脆弱性

JTAG は，僅か4～5本の外部端子で IC 内の回路を容易にアクセスできるため，標準化されたテスト規格として幅広い電子機器に採用されている。さらに，バウンダリスキャン本来の目的である IC 間の電気的導通を検査するためにコア回路の外部に配置されるバウンダリスキャンレジスタだけでなく，コア回路を直接制御と観測する強力なデバッグ機能を追加することができるので，電子機器の出荷後に，悪意のある攻撃者から「バックドア」として悪用されてしまうセキュリティ脆弱性がある。

3.1 JTAG のセキュリティ脅威

JTAG に関わるセキュリティ脅威は主に外部からの脅威と内部からの脅威に分類できる [2]。外部からの脅威は，権

限のないユーザがターゲット IC の JTAG 機構に対してリバースエンジニアリングを行うことで，JTAG 機構へのアクセス権限を取得し，機能回路に内蔵されるテストインフラ（スキャンチェーン），デバッグインフラ（メモリやファームウェアレジスタ）などを悪用する攻撃である。一方，内部からの脅威は，IC 製造の参加者または関与者による悪質なハードウェア（トロイの木馬など）を IC や機能回路（IP コアなど）に埋め込むことが主な原因である。例えば，ユーザがバイパスレジスタを経由して他の機能回路と通信する際に，JTAG インフラに埋め込まれた悪質な回路がバイパスレジスタを通るデータを覗き見るスニッフィング攻撃が可能である [2]。内部からの攻撃は一般的に IC の製造に関わる組織的な行為であり，個人の攻撃者にとっては現実的ではない。そのため，本稿は外部からの脅威のみに着目する。

3.1.1 テストインフラに対する外部攻撃

JTAG を用いて IC の機能回路内に組込まれるテストインフラに対する外部攻撃については，オンチップ暗号回路（DES†, AES†, ECC†）に内蔵されるスキャンチェーンに対する攻撃事例が報告されている [4]。この攻撃は，暗号化処理の実行中に回路を強制的にテストモードに切り替え，暗号レジスタ（スキャンチェーンの一部）に格納されている暗号の中間状態をスキャンシフト動作で大量に取得し，それらの差分を解析することで鍵を導き出すこと（差分攻撃とも呼ぶ）である。また，IC が同じ認証鍵を共有している場合は，その認証鍵が一度盗まれると，攻撃者はそれを再利用してその IC を何度も繰り返して攻撃することが可能となる [4]。

3.1.2 デバッグインフラに対する外部攻撃

JTAG のデバックインタフェースを利用する攻撃が近年は主流になっている。システム開発の水平分業化に伴い，ハードウェア・ソフトウェアはそれぞれ異なるメーカが個別に開発することになるため，ソフトウェア開発プロセスを支援するにはハードウェアの設計者が IC にオンチップデバッグ(OCD)機能を付与する必要がある。そこで，悪意のある者は OCD ツール（例えば Open-OCD[5]）を利用して，ハードウェアに近いレベルで実行コードを改ざんすることによってソフトウェアレベルのセキュリティメカニズムを破る特権昇格攻撃を行うことが可能である。Guri らは，CPU の JTAG ポートを介してメモリの制御ビットを変更できるように故障を注入することで Android OS のカーネルへの高いアクセス権限（root）を獲得する攻撃例を報告した [6]。他には，JTAG デバック機能がメモリダンプに悪用されるリスクもある。Willassen らの研究 [7]では，フォレンジック†調査の目的として，CPU の JTAG ポートを介して基板上に実装される外部フラッシュメモリにアクセスし，データを読み出すための詳細な手順を紹介した。

3.2 JTAG 攻撃の手順

ここでは，JTAG に対する外部からの攻撃事例から，攻撃の手順を整理する。

表1 : JTAG 攻撃手順 [8]

JTAG攻撃手順		詳細手順
Phase 1	JTAGポート特定	Step1: JTAGポート特定 （デバイスのデータシート参照やツール使用）
Phase 2	DRプロパティ特定	Step2:IR長を特定する
		Step3:DR長を特定する
		Step4:DR操作有効な命令コードを特定する
		Step5: DRの構成状態を特定する （キャプチャやアップデート）
		Step6:内部スキャンアーキテクチャ識別
Phase 3	非公開機能リバースエンジニアリング	Step7: 命令と機能を区別する （Step4で取得した命令集合）
		Step8: 各DRの機能を推測する
		Step9: 命令と機能に関連付け

攻撃者は，JTAG を利用して効果的な攻撃を行うためには，ターゲット IC の JTAG 機構をアクセスする命令セットを知ることが必要である。通常，1149.1 の標準命令以外のスキャンチェーン，データレジスタ，オンチップメモリなどのコンポネントに対する操作命令は，権限のないエンドユーザに公開されない。そのため，攻撃者は非公開 JTAG 機能情報（IR と DR の構造情報，命令集合）を特定することが必要である。

表 1 は，JTAG の攻撃手順を示している [8]。

<<Phase 1: JTAG ポートの特定>>

通常，JTAG ポートは IC や基板上のどこかにまとめられているため，IC のデータシートや基板の回路図を参照することで，簡単に特定することができる。JTAG ポートが公開されていない IC に対しては，JTAGulator[9]というオープンソースハードウェアツールを利用すれば，基板や IC から隠蔽されている JTAG ポートの箇所を容易に特定することが可能である。

<<Phase 2: JTAG 機構のプロパティ特定>>

攻撃者が JTAG 機能に関わるレジスタ（IR と各種の DR）のプロパティを特定する。まずは，図2に示す状態遷移に従って TAP を操作しながら，IR および DR の長さを調べる。IR と DR の長さは，十分長い one-cold ベクトル（1 つだけ 0 を含むオール1のビット列）をシフトすることで簡単に特定できる。次は，DR 操作に関わらない未定義（または未使用）の命令コードを探査する。未定義の命令コードは，通常バイパスあるいは切断

†DES: Data Encryption Standard の略で，共通鍵暗号方式によるデータ暗号化のアルゴリズムの一種である。鍵が短いという脆弱性があるため，利用が推奨されない。

†AES: Advanced Encryption Standard の略で，DES に代わる新しい標準暗号となる共通鍵暗号アルゴリズムである。

†ECC: Elliptic Curve Cryptography の略で，楕円曲線を利用した公開鍵暗号方式である。

† フォレンジックとは，犯罪捜査における分析，鑑識を意味することである。

(High-Z)の命令として動作する。未定義の命令コードを特定できれば，ターゲット IC で機能する非公開命令を推測することにつながる。一般的には，異なる JTAG 機能に対する誤操作（あるいは誤動作）を避けるために，有効な命令コードの間に間隔を空けて設計する傾向があるため，未定義の命令コードに挟まれているコードが非公開命令に当たる可能性が高い。さらに，DR の動作特性（キャプチャやアップデート）まで調べると，攻撃者はキャプチャ可能な DR からターゲット IC のデータをダンプしたり，アップデート可能な DR を介してデータを書き込んだりすることが可能になる。

<<Phase 3: JTAG 機能解析>>

攻撃者は Phase 2 で獲得した IR と DR のプロパティ情報を用いて，試行錯誤を重ねることで，ターゲット IC に組込まれる JTAG の非公開機能の詳細（命令コードの区別，機能の区別，DR の動作特性，命令コードと機能の関連付け）を確定する。

例えば，ある DR が更新可能で，隣接する命令コードで特定する別の DR がキャプチャできる場合，攻撃者は 1 つ目の DR がアドレスを送信し，2 つ目の DR が対応するデータをキャプチャしているのを想定でき，この 2 つの DR があるメモリの読み出しに使用されていることを合理的に推測することができる。同様の方法で，隣接する命令コード間の相互作用を調査することにより，攻撃者はより多くの JTAG 機能を発見することができる。

IJTAG 準拠 SoC では，図3に示すように，ユーザが JTAG の TAP ポートを介してスキャンネットワーク上に含まれる機能回路をアクセスする。そのため，攻撃者はまず，表1に示したような JTAG に対するリバースエンジニアリングと同じ方法を利用して，JTAG の非公開機能，命令セットおよび実装される DR を特定する。再構成可能スキャンネットワーク（RSN）の全体構造および構成方法を明らかにするためには，攻撃者は SIB と SCB の各ビットに 1 と 0 を繰り返し設定し，TDI と TDO の間のチェーンの長さの変化を観測することで実現できる。時間をかけて，何度も試行錯誤を繰り返すことで，個々の機能回路(IP コア)に内蔵される TDR やスキャンチェーンへのアクセス方法を特定することも可能である。攻撃者はそれを利用して，オンチップメモリ IP からデータをダンプしたり，ファームウェアを改ざんしたり，機能回路の動作を制御したりすることが可能になる。

4. JTAG のセキュリティ強化技術

ここでは，JTAG の外部からの攻撃に対するセキュリティ強化技術を紹介する。

4.1 認証によるアクセス制限

前章で紹介したように，外部攻撃の端緒は，JTAG ポートに不正にアクセスすることである。そのため，最も古典的な攻撃防止対策は，TAP へのアクセスを制限することである。JTAG インタフェースに暗号技術を用いた認証機構を組込むことで，正しく認証できるユーザのみに対してアクセスを許可するアクセス制限方法が提案されている。

Novak らは，共通鍵暗号方式を用いた JTAG 認証方法を初めて提案した [10]。この方法では，JTAG インフラにロッキング機構を追加し，LOCK と UNLOCK という 2 つの新規命令を用いて，命令デコーダの出力を制御する。TAP コントローラは通常ロックされている状態で，UNLOCK 以外のすべての命令を BYPASS 動作にデコードする。ユーザが UNLOCK 命令を IR に入力し実行すると，パスワードの入力が求められ，入力したパスワードがシステムのロック時に使われたものと一致した場合，TAP コントローラのロックが解除され，アクセスが許可される。共通鍵暗号を用いる認証方式は，パスワードが盗聴やユーザの異動（開発者）など様々なルートで漏洩してしまう恐れがあるため，パスワードの漏洩によるリプレイ攻撃を防ぐために，疑似乱数生成回路 LFSR による製品ごとユーザごとに異なるパスワードを設定できる動的パスワード認証機構も提案された [11]。

セキュリティ向上のために，チャレンジレスポンス認証プロトコルに基づいた JTAG 認証方法がある [12]。この認証方式においては，まず，IC がユーザに対して「チャレンジ」と呼ばれる値（疑似乱数）を送信し，ユーザが保有する秘密鍵をチャレンジに掛け合わせてハッシュ関数や ECC などの暗号アルゴリズムを用いてレスポンスを計算して返信する。IC は，ユーザから返ってきたレスポンスを自ら生成したレスポンスと照合し認証を行う。チャレンジとレスポンスは，認証ごとに異なるため，盗聴されたとしても秘密鍵を導き出すことが困難である。

JTAG インフラの利用者に応じて，異なるアクセス権を付与する階層的認証プロトコルも提案されている。Buskey らの研究 [13]では，マイクロコントローラー内のプログラムを保護するために，ユーザの権限に基づいて，三つの保護レベル（PL0，PL1，PL2）において 4 つのモード（AM0，AM1，AM2，AM3）でアクセスを制御する認証メカニズムを提案している。最も安全な保護レベル PL0 では，JTAG ポートを介したユーザのアクセスを外部機能（例えばバウンダリスキャンの基本機能である相互接続テスト）に限定し，次の保護レベル PL1 では，PL0 と同様の機能に加えて，フラッシュメモリのプログラミングやレジスタへの書き込み/読み出しが許可される。そして，PL2 のユーザはセキュアレジスタやメモリのセキュアセクションを含め，IC へのフルアクセスが可能となる。

4.2 JTAG 構造の複雑化（難読化）

もし，攻撃者がJTAGへのアクセス権限を獲得できた場合，攻撃者は，時間をかけて，何度も試行錯誤を繰り返すことでJTAGの非公開機能を特定することを試みる。この攻撃に対する対策は，JTAG回路の構造を複雑にすることによって，攻撃者がJTAGの非公開機能をリバースエンジニアリングするための時間を大幅に増加させることである。

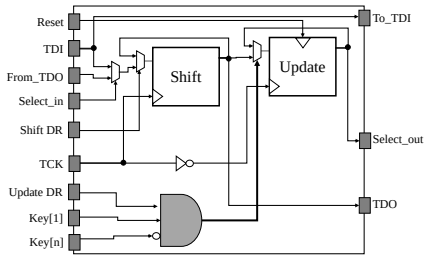

図4 ロッキングSIB

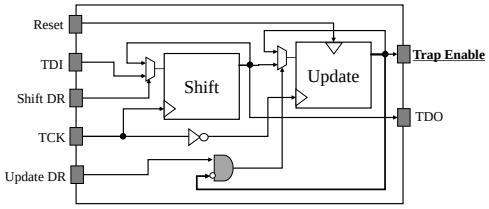

図5 トラップレジスタの構造

Dworakらは，IJTAGの再構成可能スキャンネットワーク(RSN)の構造を難読化するために，スキャンチェーンの構成を制御するSIBにキービットを追加することで図4に示すような認証機能付きのLSIB(Locking SIB)を提案している[14]。さらに，試行錯誤方法によるLSIBキーを探索する総当たり攻撃を防ぐために，不正な値が書き込まれるとLSIBを永久にロックするトラップレジスタ（図5）を導入した。Zygmontowiczらは，このLSIBに基づいて，ダミーLSIB（ハニーポット）やロッキングペアLSIB（同時動作しない）やスイッチングLSIBを提案した[15]。これらの特別なLSIBを組み合わせてIJTAGに導入することで，スキャンネットワークの完全構造を隠ぺいし，攻撃者によるリバースエンジニアリングの難易度が大幅に上がる。

4.3 攻撃検知

ここでは，実行中の攻撃行動をリアルタイムで検出し，攻撃を止める能動的な防御方法を紹介する。このセキュリティ対策は，ユーザの JTAG に対する操作行動をオンチップで監視し，不正な行動パターンを検出することが肝要である。これまでは，ルールに基づく静的検出方法と機械学習を用いた検出方法が提案されている。

静的検出手法 [16][17]**:** JTAG インフラの設計者が正常のアクセス手順とデータシーケンス（命令とデータ）に基づいてアクセスルールを決め，そのルールに従ってユーザのアクセス動作をチェックするハードウェア（検出器）を設計・実装する。攻撃者がルール通りに正当な操作（手順や入力データ）を行うことができなければ，その操作を攻撃行為として検出し，そのアクセス操作を禁止する。

機械学習を利用した攻撃検出技術 [8]**:** 事前に機械学習の代表的な手法であるランダムフォレストやサポートベクターマシン（SVM）を利用して訓練された分類器を用いてユーザの実操作が正常であるか異常であるかを識別する。設計者は JTAG の命令シーケンスに対してあらゆる特徴を抽出し，正常や異常のラベルをつけて，分類器を訓練する。その後，訓練済みの分類器を攻撃検出器として IC に実装し，JTAG ボードの実入力データ（主には命令）に対して自律的にシーケンスを分類することで，攻撃を検出する。

5. JTAG セキュリティ対策の実例

JTAG への攻撃を防ぐために最も簡単な方法は，電子機器をエンドユーザに出荷する前に JTAG のアクセスポートを完全に無効にすることである。例えば，TMS の配線をヒューズで物理的に切断する方法がある。しかしながら，物理的な変更は，出荷後に JTAG を用いてボードテストやオンチップデバッグなどを行うことができなくなるため，柔軟なセキュリティ対策が必要である。

表2 JTAG セキュリティ対策の取り組み製品例

メーカ	製品	セキュリティ強化対策
Intel	インテル® 100 シリーズ・デスクトップ・チップセット	JTAG命令を暗号化する。認証鍵は秘密保持契約(NDA)を締結した者のみに配布する。
NXP	i.MX6 series processors	One Time Programmable (OTP) eFusesを使用し、3つのセキュリティモード（No Debug、Secure Debug、Debug Enable）で動作できる。
Samsung	ARTIK IoT platform	JTAGがロックされている。アクセスするための鍵を入手するには，サムスンへの問い合わせが必要。
Texas Instruments	C2000マイコン MSP430マイコン	物理的ヒューズ、eFuse、JTAGロック機構などの複数のセキュリティ対策を利用する。
Xilinx	Zynq-7000 AP SoC	eFuseを用いてJTAG機能を有効/無効にする。

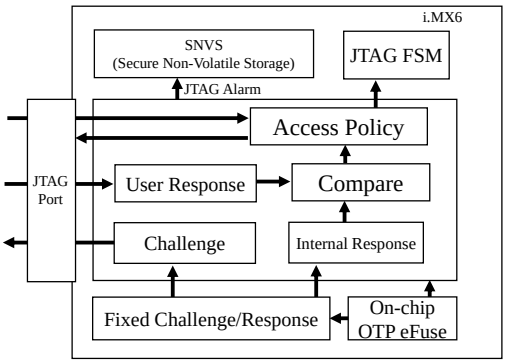

図6 セキュア JTAG コントローラ

近年，デバイスメーカは最新の製品において，JTAG に関わる様々なセキュリティ強化技術を導入している。表2は，JTAG のセキュリティに関するメーカの取り組み事例を示している。その中，NXP®社が自社の i.MX6 シリーズプロセッサ向けに開発したセキュア JTAG コントローラ(SJC)では，One Time Programmable (OTP) eFuse を用いて JTAG へのアクセスを 3 つのセキュリティモード（No Debug, Secure Debug, Debug Enable）に設定することができる。図6に SJC の構造図を示す。ユーザはICを利用する前に，専用ツールを用いてオンチップ OTP eFuse に JTAG の動作モードを指定するプログラムを一度だけ書き込む。No Debug モードでは，実装基板における IC 間の電気的導通テストのためのバウンダリスキャンのみが利用可能である。Secure

Debug モードでは，バウンダリスキャンテストに加え，チャレンジレスポンス認証プロトコルによるデバッグ機能が有効になる。また，Debug Enable モードでは，JTAG すべての機能が認証をせずに使用可能になる。

6. 考察と今後の課題

IC のさらなる複雑化に伴い，JTAG 準拠のテスト・デバッグインフラが必要不可欠になっている。JTAG の導入によってテスト容易性は向上するが，セキュリティの脆弱性が懸念されている。JTAG に対する外部からの攻撃を防ぐためには，これまでに様々なセキュリティ強化技術が提案された。これらの技術を必要に応じて実製品に導入すれば十分なセキュリティを確保することができると考えられる。

一方，本稿で紹介したようなセキュリティ対策を導入するには，暗号回路を含む認証機構や分類器などの専用ハードウェアリソースを追加することが必要である。すなわち，IC 製品のテスト容易性（品質），セキュリティと実装コスト（ハードウェアオーバヘッド）はトレードオフの関係にある。ミッションクリティカルのハイエンド製品では，広範囲の攻撃脅威をカバーするために高コストな対策（二つ以上）を講じることを許容すべきである。一方，IoT 領域においては，低スペックのマイコン，低消費電力の通信モジュール（例えば：LoRaWAN, ZigBee など），大容量かつ低コストメモリがほとんどである。これらのデバイスは，一般的に非常に低いコストで製造される。JTAG インフラにコストのかかるセキュリティハードウェアを設けることはメーカにとって厳しいことである。しかしながら，これらの保護されていないデバイスが，インターネットに接続されることは，IoT システム全体を脅かす「バックドア」を残してしまうこととなる。そのため，電子機器の適用領域に応じてより軽量なセキュリティ対策を開発することが今後の課題となる。例えば，ユーザ側で一方向性変換の関数を使わず，排他的論理和演算 2 回，加算 3 回という簡単な演算のみで認証できる SAS-L[†]という軽量化暗号技術の導入である[18]。

7. まとめ

現在，システム，ボード，IC のテスト・評価用の標準インフラとして，JTAG が広く適用されている。近年の IoT 技術の急速な普及に伴い，インターネットを介して JTAG 準拠の電子機器が連携し，あらゆる産業や社会経済分野を支えている。このような環境においては，JTAG のセキュリティ対策が重要な課題となっている。そこで，本稿では，JTAG のセキュリティ脆弱性とそれに伴う脅威の可能性に関して紹介し，対応策としてのセキュリティ強化法を紹介した。筆者らは，出荷後のフィールドテストやオンチップデバッグを実現することは重要であると考えるので，JTAG のセキュリティに関する状況を正確に理解し，積極的に対策を施すことによって，過度に恐れることなく JTAG を活用することを推奨したい。

謝辞

本研究は一部，科研費(19K11878)の助成を受けたものである。

参考文献

1) 亀山修一，”バウンダリスキャン技術講座 第 9 回 バウンダリスキャン規格の適用拡大と最新動向，”エレクトロニクス実装学会誌,Vol.24, No.1, pp.154-161, 2021.
2) E. Valea, M. Da Silva, G. Di Natale, M. Flottes and B. Rouzeyre, "A Survey on Security Threats and Countermeasures in IEEE Test Standards," in *IEEE Design & Test*, vol. 36, no. 3, pp. 95-116, June 2019, doi: 10.1109/MDAT.2019.2899064.
3) ケネス・P．パーカー(著)，亀山修一(監訳)：“バウンダリスキャンハンドブック，”青山社，2012 年，第 3 版，ISBN978-4-88359-303-3
4) B. Yang, K. Wu, and R. Karri, “Secure Scan: A Design-for-Test Architecture for Crypto Chips,” IEEE Trans. Comput. Des. Integr. Circuits Syst., vol. 25, no. 10, pp. 2287–2293, Oct. 2006, doi: 10.1109/TCAD.2005.862745.
5) Open On-Chip Debugger, http://openocd.org/, accessed on 5 July 2021.
6) M. Guri, Y. Poliak, B. Shapira and Y. Elovici, "JoKER: Trusted Detection of Kernel Rootkits in Android Devices via JTAG Interface," 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 65-73, doi: 10.1109/Trustcom.2015.358.
7) Willassen S. (2006) Forensic Analysis of Mobile Phone Internal Memory. In: Pollitt M., Shenoi S. (eds) Advances in Digital Forensics. DigitalForensics 2005. IFIP — The International Federation for Information Processing, vol 194. Springer, Boston, MA. https://doi.org/10.1007/0-387-31163-7_16
8) X. Ren, F. P. Torres, R. D. Blanton and V. G. Tavares, "IC Protection Against JTAG-Based Attacks," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 1, pp. 149-162, Jan. 2019, doi: 10.1109/TCAD.2018.2802866.
9) JTAGulator by Grand Idea Studio. Available online: http://www.grandideastudio.com/jtagulator/, accessed on 5 July 2021.
10) F. Novak and A. Biasizzo, “Security extension for IEEE Std 1149.1,” J. Electron. Test. Theory Appl., vol. 22, no. 3, pp. 301–303, 2006.

[†] SAS-L とは，Simple And Secure password authentication protocol, Light processing version の略で，高知工科大学の清水明宏教授らが開発したワンタイムパスワード認証方式の 1 つである。

11) G. Chiu and J. C. Li, "A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores," in IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, vol. 20, no. 1, pp. 126-134, Jan. 2012, doi: 10.1109/TVLSI.2010.2089071.
12) Amitabh Das, Jean da Rolt, Santosh Ghosh, Stefaan Seys, Sophie Dupuis, et al. “Secure JTAG Implementation Using Schnorr Protocol,” J. Electron. Test. Springer Verlag, 2013, 29 (2), pp.193-209. 10.1007/s10836-013-5369-9.
13) R. F. Buskey and B. B. Frosik, "Protected JTAG," 2006 International Conference on Parallel Processing Workshops (ICPPW'06), 2006, pp. 8 pp.-414, doi: 10.1109/ICPPW.2006.65.
14) J. Dworak et al., “Don’t forget to lock your SIB: Hiding instruments using P1687,” in Proc. 2013 IEEE Int. Test Conf., Anaheim, CA, 2013, pp. 1–10.
15) A. Zygmontowicz et al., “Making it harder to unlock an LSIB: Honeytraps and misdirection in a P1687 network,” in Proc. 2014 Design Autom. Test Eur. Conf. Exhibition, Dresden, 2014, pp. 1–6.
16) R. Baranowski, M. Kochte, and H. J. Wunderlich, “Access port protection for reconfigurable scan networks,” J. Electron. Test. Theory Appl., vol. 30, no. 6, pp. 711–723, 2014.
17) S. Kan, J. Dworak, and J. G. Dunham, “Echeloned IJTAG data protection,” in Proc. 2016 IEEE Asian Hardware-Oriented Security Trust, Yilan, 2016, pp. 1–6.
18) SAS-L2, https://www.kochi-tech.ac.jp/power/research/sas-liot.html, accessed on 5 July 2021.

――――――――――――――――――――――――――――著者紹介

王森レイ（おう　しんれい）

2014 年に九州工業大学大学院情報工学府情報工学専攻博士後期課程修了。同年愛媛大学工学部助教を経て，2017 年から同大学理工学研究科特任講師，現在に至る。論理回路に対するテスト容易化設計，低消費電力テスト，故障診断に関する研究に従事。博士（工学）。IEEE，電子情報通信学会，情報処理学会，エレクトロニクス実装学会の会員。

亀山修一（かめやま　しゅういち）

1972 年富士通㈱に入社以来，生産技術部門で電子回路の試験技術/試験設備の開発に従事。現在，愛媛大学客員研究員，東海大学非常勤講師，亀山技術士事務所代表。 IEEE-CS，エレクトロニクス実装学会，電子情報通信学会，日本技術士会等の会員。エレクトロニクス実装学会バウンダリスキャン研究会主査，博士（工学），技術士（電気電子）。著書：バウンダリスキャンハンドブック（青山社）

高橋寛（たかはし　ひろし）

1996 年に愛媛大学で博士（工学）学位取得，以来，愛媛大学工学部助手，准教授を経て，2010 年から同大学理工学研究科教授，2018 年から愛媛大学工学部長，現在に至る。論理回路の高信頼化，テスト，診断に関する研究に従事。2000 年に米ウィスコンシン大学マディソン校客員研究員（文部科学省在外研究員），2012 年に電子情報通信学会最優秀論文賞，2014 年に IEEE Computer Society Annual Symposium on VLSI 最優秀論文賞，2016 年に日本信頼性学会高木賞，2020 年に IEEE CASS Shikoku Chapter Best Paper Award 受賞。IEEE，電子情報通信学会及び情報処理学会のシニア会員。