シグナルチェーンのセキュリティリスクとその対策技術に関する研究

園田，大樹

(Degree)
博士（科学技術イノベーション）
(Date of Degree)
2023-09-25
(Date of Publication)
2024-09-01
(Resource Type)
doctoral thesis
(Report Number)
甲第8751号
(URL)
https://hdl.handle.net/20.500.14094/0100485935

博　　士　　論　　文

シグナルチェーンのセキュリティリスク とその対策技術に関する研究

令和5年7月

神戸大学大学院 科学技術イノベーション研究科

園 田　　大 樹

目次

第1章

緒論

1.1 研究背景

現在、CPS (Cyber Physical System) や IoT (Internet of Things) のような、現実のフィジカル空間と計算機上のサイバー空間をつなぐシステムが普及している。このようなシステムでは、フィジカル空間において計測した物理量を収集し、サイバー空間において AI (Artificial Intelligence) 技術やクラウド上の計算機資源を用いて分析した後、再度、フィジカル空間に制御情報をフィードバックすることで価値を創出している。2000 年代後半以後、IoT デバイスの普及は、製造業、防災、医療、介護、農林水産業などの様々な分野で急速に進んでおり [1]、総務省が発行する令和 4 年度の情報通信白書 [2] では、2024 年時点で世界には 398.5 億台の IoT デバイスが存在すると予測されている。

CPS や IoT のようなシステムが期待される動作を行い、価値を創出するためには、サイバー空間に入力されるセンサーの情報が信頼できる事が必要である。仮に正確な情報がサイバー空間に与えられない場合、システムは期待される動作をしないばかりか、誤動作によって利用者に損害を与えかねない。特に、近年実現が期待される完全自動運転の自動車やドローンのような自律移動体、あるいは、インフラ設備や製造設備を制御するシステムにおいては、誤動作が引き起こされた際に人命や環境に重大な影響を及ぼす可能性がある。したがって、CPS や IoT システムの安全な運用には、センサー情報の完全性や真正性、可用性を保つこと、即ち、セキュリティを保つことが求められる。

センサーで得られた情報は、図 1.1 に示す通り、複数の変換処理及び信号処理を通して伝達される。まず、フィジカル空間における熱や光のような信号は、物理的、化学的な原理を利用したセンサーによって連続的なアナログ電気信号に変換され、続くアナログ-デジタル変換器 (Analog-to-Digital Converter: ADC) によって、離散的なデジタル信号に変換される。最後に、デジタル信号は CPU のようなデジタル回路に伝送され、後

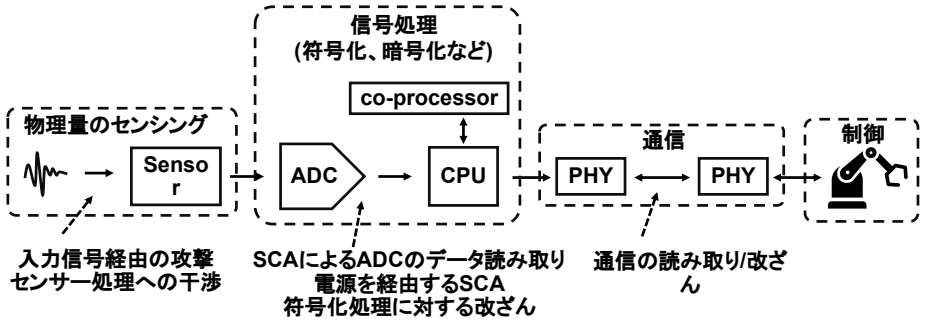

図 1.1: シグナルチェーン上におけるセキュリティ上のリスク

続の処理に利用される。

この一連の処理に対して、悪意ある攻撃者が様々な攻撃を行い、意図的に不具合が引き起こされるリスクの存在が指摘されている [3][4]。例えば、センサの計測過程においては、ドローンの姿勢制御などに使われる MEMS ジャイロスコープに対して、音波を照射することで測定を妨害する攻撃 [5] や、超音波の反射を利用する測距センサに対する攻撃 [6] のように、センサー計測のメカニズムを利用した攻撃が報告されている。ADC の変換過程においても、変換プロセスに介入して変換結果を操作する攻撃 [7] や、変換プロセスからの漏洩情報を用いて変換結果を推測できる脆弱性 [8] が指摘されている。暗号化処理回路に対するハードウェア攻撃は様々な形式のものが報告されており、暗号処理と電磁波や処理タイミングの相関を利用して秘密情報を推測するサイドチャネル攻撃や、レーザーや電磁波によりエラーを注入して解析を行う故障解析攻撃 [9] が議論されている。また、デジタル信号通信には一般的に盗聴、改ざん、なりすまし、悪意あるデータの挿入などのようなサイバー攻撃の可能性が存在する [10]。このような、シグナルチェーンにおけるセキュリティリスクは、IoT/CPS を安全に利用するにあたっての重大な課題である。

本論文では、図 1.2 に示すシグナルチェーンへのセキュリティリスクに対して、センサーが物理量を計測した後、暗号化されるまでの区間におけるハードウェア攻撃への対策技術について論じる。第 2 章では、FOWLP (Fan-Out Wafer Level Packaging) のチップ内部における電源品質・信号品質の観測を通じて、FOWLP におけるプロービング攻撃及びサイドチャネル攻撃への耐性について考察する。第 3 章では、電圧制御オシレータ (Voltage Controlled Oscillator: VCO) ベースの ADC における変換処理へのハードウェア攻撃手法について、実機を用いて実証し、その対策につい

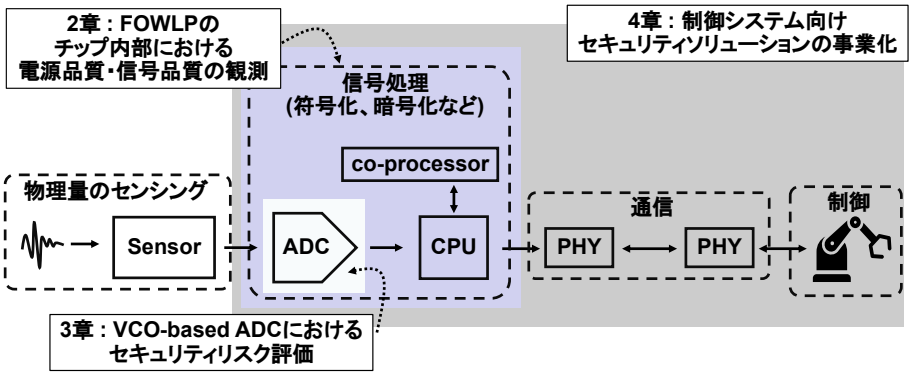

図 1.2: 本論文の研究領域

て論じる。第 4 章では、制御システム向けネットワークセキュリティソリューションであるコネクターシステムの販売事業の実現可能性について説明する。最後に、第 5 章において本論文をまとめる。

1.2 先行研究

1.2.1 ハードウェアに対する物理攻撃の概要

IoT デバイスや IC カードのような、デバイスのサンプルが攻撃者の手元に渡る可能性のあるデバイスにおいて、内部情報の推測や、動作への介入を企図してデバイスの動作を物理的に解析するハードウェア攻撃が行われるリスクがあることが指摘されている [11][12]。

表 1.1 に、ハードウェアに対する攻撃手法と、その分類を示す。ハードウェア攻撃は、攻撃対象のハードウェアに対して加工を行うかどうかにより、パッケージ非加工型と、パッケージ加工型に分類される。

パッケージ非加工型の攻撃では、パッケージから漏洩する入出力や物理的特性を利用した解析を行う事で攻撃を実行する。表 1.1 中のパッシブ型攻撃に分類される、サイドチャネル攻撃は、デバイスによって意図された入出力以外の情報を元にデバイスの解析を行う攻撃であり、電源ノイズと内部情報の相関を利用して攻撃する電力解析攻撃 [13] や、処理タイミングの差を利用するタイミング攻撃 [14] などの攻撃手法が提案されている。これらの攻撃手法は主に暗号アルゴリズムにおいて秘密鍵を解析する目的で適用され、標準的に使われる AES や RSA のような暗号アルゴリズムにおいても攻撃が可能であることが実証されている。また、ア

表 1.1: ハードウェア攻撃の分類 [12]

パッケージ非加工	パッシブ	サイドチャネル攻撃 電力解析攻撃など
	アクティブ	故障注入攻撃 電磁波照射など
パッケージ加工	チップ間	チップ間データ解析 偽装データ挿入など
	チップ開封	マイクロプロービング 配線編集など

クティブ型の攻撃には、電磁波や電源グリッチによって、外部から意図的な故障を注入し、これを解析する故障注入攻撃がある。上記のような方法で回路に故障を注入し、正常な出力との差分を解析する故障解析攻撃は、暗号回路に対する強力な攻撃手段として議論されている [9]。

パッケージ加工型の攻撃では、IC チップが実装されている回路基板や、IC チップのパッケージを有機溶媒や硝酸などの化学薬品やレーザーによって開封、加工し、露出した信号線から内部信号を直接プロービングする攻撃や、チップの発光や発熱を解析する攻撃、レーザー照射による回路改変攻撃が行われる。ただし、このような攻撃を実行するためには、一般的に IC チップの故障解析向けに開発される専用の装置や、高い技術が要求されるため、攻撃者は限定される。

以降では、ハードウェア攻撃の中でも、特に本稿で述べる研究に関連する攻撃である信号線に対するプロービングと ADC に対する攻撃について先行研究を述べる。

1.2.2　プロービングによる攻撃情報の収集

電子回路に対してリバースエンジニアリングや秘密情報の解析を企図する際、攻撃者はオシロスコープやロジックアナライザを用いたプロービングによって、回路の電信信号を直接読み取ることで情報を収集する。収集した電気信号から得られる情報を元に、攻撃者は回路動作の解析を行うことや、ファームウェアのような知的財産、暗号鍵のような秘密情報を得ることが可能である。

一般的に、プロービングは金属配線などの導体に対して物理的に接触することで行われるため、その難易度は攻撃者が目的とする信号線への

アクセスの難易度によって決まる。プロービング攻撃はICチップが実装される基板上でやりとりされるチップ間通信のみならず、ICチップ内部で回路が処理している信号に対しても行われる[15]。前者の配線はPCB基板上におけるミリメートル〜マイクロメートルスケールの配線であるため観測は比較的容易だが、後者の配線はICチップ上のナノメートルスケールにまで配線間隔や幅が縮小するため、攻撃者によるプロービングがより困難になる。ここでは、まず配線スケールが大きくアクセスしやすいボードレベルのプロービング攻撃に関する概要を述べ、続いて、よりスケールの小さいチップレベルのプロービングに関して説明する。

ボードレベルのプロービングを実施する際、まず、攻撃者はICパッケージ上の信号端子や、PCB基板上に露出した金属端子から信号を観測することで、解析する対象の情報を収集することができる。続いて、信号の特性や配置からその役割を推測し、通信内容の解析や、信号を遮断したり、偽装信号を送るなどの手段を用いて介入を行う事で、リバースエンジニアリングや情報の読み出しといった目的が達成される。例えば、文献[16]では、iPhone 5cに実装されているNANDフラッシュメモリの信号をロジックアナライザで読み取り、通信プロトコルを解析することで、内容データを読み出す方法が実証されている。

このようなプロービング攻撃に対しては、製品出荷時にデバッグバスなど攻撃対象となる入出力を無効化することや、バスの高速化による信号観測の困難化、PCB基板表面上への信号露出の削減、あるいは、チップ間通信の暗号化などの対策によって、攻撃者の攻撃コストを上げることで、対策が行われる。また、System on a chip (SoC) や Multi chip module (MCM) のような構造を用いてシステム全体をワンチップ化することで、ICチップのパッケージング内部に信号線を秘匿することが可能である。

ICチップ内部に対するプロービングは、先述のように、ICチップの解析に用いられる専用の機材が必要とされる。まず、プロービング対象のICチップ内のシリコンダイを露出させるため、硝酸や有機溶媒、またはレーザー加工によるパッケージングの開封が行われる。その後、攻撃者は光学的、電子的な観察により回路の構造をリバースエンジニアリングし、観測対象の配線を特定する。最終的に、集束イオンビームによってシリコンや金属配線を切削し、目的の信号線へのバイパスを作成するなどの加工を行うことで、信号の観測が可能となる。上記の手順による回路の改変は高コストかつ専門装置や技術が要求されるが、攻撃の自由度は非常に高く、強力な解析が可能である。

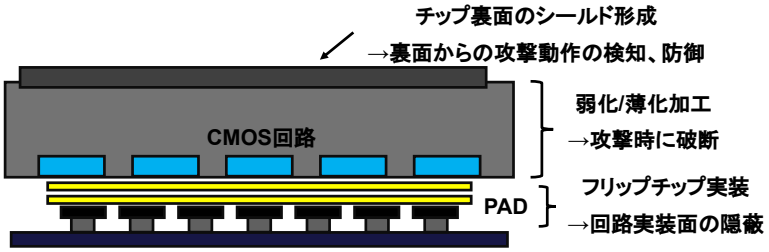

図 1.3: プロービング攻撃に対する対策技術の例

チップレベルのプロービング攻撃への対策として、図 1.3 に示すように、先端パッケージング技術による対策技術が開発されている。例えば、フリップチップ実装されたパッケージでは、シリコンチップの回路形成面が表面に露出しないため、チップが上側から開封されたとしても、回路への直接的なアクセスが困難となる。また、チップに攻撃を企図して圧力が加えられた場合にチップが破損するように意図的に脆く作成する対策や、チップ裏面を経由する回路の切削、研磨のような変更を検知する対策が提案されている [17][18]。

1.2.3 ADC に対するハードウェア攻撃

IoT デバイスの普及とともにハードウェア攻撃の脅威が高くなった 2010 年代以後から、様々な回路に対するハードウェア攻撃技術が提案されている。特に ADC に対する攻撃はセンサーで計測されているデータの改変や、情報の変換結果の盗聴など重大な脅威をもたらしうるため、継続的な研究が必要である。本節では、まず代表的な ADC のアーキテクチャとその特徴について説明し、続いて、先行研究における ADC に対するハードウェア攻撃とその対策手法について述べる。

1.2.3.1 代表的な ADC アーキテクチャ

電子回路において、センサなどによるアナログ信号情報を取り扱う場合、必ず ADC による変換が行われる。ADC は、入力されたアナログ信号を時間方向に離散化する標本化、電圧方向に離散化する量子化及び符号化を行うことで、入力に応じたデジタル信号列を生成する。

ADC はその実装によって、様々な方式のアーキテクチャが存在する。ここでは、代表的な ADC のアーキテクチャとして、逐次比較型 (Successive

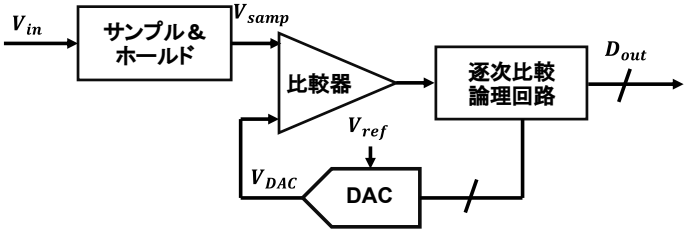

図 1.4: 逐次比較 ADC のブロック図

Approximation Register: SAR) ADC、デルタシグマ型 (ΔΣ) ADC、シングルスロープ型 ADC ついてそれぞれ簡単に説明し、それぞれのアーキテクチャの性能指標について分析する。

図 1.4 に示す SAR-ADC は、入力電圧 V_{in} をサンプリングした電圧 V_{samp} を DAC(Digital to analog comberter) が生成した電圧 V_{DAC} と順次比較し、最も近似する V_{DAC} のデジタルコード D_{out} を出力する方式の ADC である。この時、入力電圧は MSB (Most significant bit) から LSB (Least significant bit) まで二部探索的に比較される。まず最初に、DAC には MSB が 1、残りのビットが 0 に設定されたコードが入力される。このとき、V_{DAC} は参照電圧 V_{ref} の半分の値となる。$V_{samp} > V_{DAC}$ の場合は MSB に 1、$V_{samp} < V_{DAC}$ の場合は MSB に 0 が設定され、この操作が LSB まで順次実行されることで、デジタルコード D_{out} が得られる。このとき、多くの場合、逐次比較型 ADC に用いられる DAC は消費電力を低減するため、電荷を再配分する容量型 DAC が用いられる [19]。

SAR-ADC は、N ビットの出力信号を決めるために N 回の比較が必要であるため、比較毎の DAC、コンパレータ、出力ロジックのセトリング時間が ADC の変換速度を決定する。また、ADC 全体の電圧分解能は内部の DAC によって決定されるため、その性能限界は DAC の回路面積やセトリング時間の設計上の限界に制限される。

上記のように、変換速度及び回路面積にそれぞれトレードオフとなる要因が存在するが、容量の微細化によって DAC は小型化、高速化が進んでおり、小面積実装や低消費電力化が達成されている。また、SAR-ADC を構成する回路には増幅器などの高い消費電力を要する回路が含まれておらず、他方式と比べて低消費電力化が実現可能である。このように、SAR-ADC は中程度の時間分解能、電圧分解能と、低消費電力が両立される構成として、現在最も利用されるアーキテクチャの一つであり、特にモバイルデバイスや IoT のような、電力に制限がある用途に有利である。

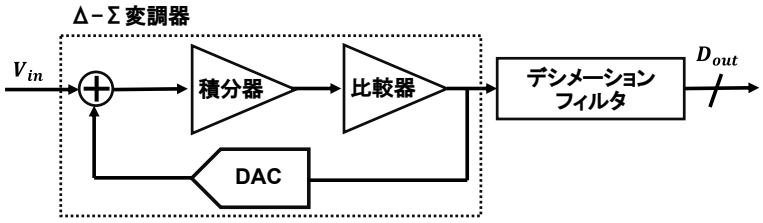

図 1.5: 1 次 ΔΣADC のブロック図

図 1.5 に示す ΔΣ 型 ADC は ΔΣ 変調器とデシメーションフィルタで構成される ADC である。ナイキスト周波数よりも十分高い周波数でのオーバーサンプリングと ΔΣ 変調によるノイズシェーピングによって、高精度の変換が達成される。まず、入力信号は、前段の ΔΣ 変調器でパルス列に変調される。このとき、入力信号 V_{in} はその帯域の数倍から十数倍の周波数でオーバーサンプリングされ、更に、量子化ノイズは DAC を経由して入力にフィードバックされる。また、ΔΣ 変調の過程で、積分器の働きによって量子化ノイズは高周波領域に分布する。この働きをノイズシェーピングと呼ぶ。

後段のデシメーションフィルタでは、ローパスフィルタリングとダウンサプリングを行う事で、高周波領域に分布する量子化ノイズが除去された信号が出力される。その結果、極めてノイズ成分の少ない信号変換が達成される。

ΔΣ 型 ADC では量子化雑音を低減できるため高分解能が達成できるが、積分器にはアンプや容量が必要であり、消費電力や実装面積は他方式と比べて大きくなる。また、変換速度がフィードバックループにある DAC のセトリング時間に制限され低速である。上記の特徴から、低速かつ高精度が求められるセンサデータや、オーディオのサンプリングなどの用途で用いられる。

図 1.6 に示すシングルスロープ型 ADC は、標本化されたアナログ信号と、ランプ信号を比較することで、アナログ信号を量子化する方式の ADC である。標本化されたアナログ信号に対して、ランプ信号を掃引しながらコンパレータで比較を行い、サンプリング時間中にコンパレータが出力したパルスの数をカウントすることで、量子化を実行している。

シングルスロープ型 ADC の量子化器は比較器とカウンタ、ランプ波発生器で構成されるシンプルな回路であることから、小型化に適している。一方で、この方式では、サンプリング時間内にカウント可能なパルス数に

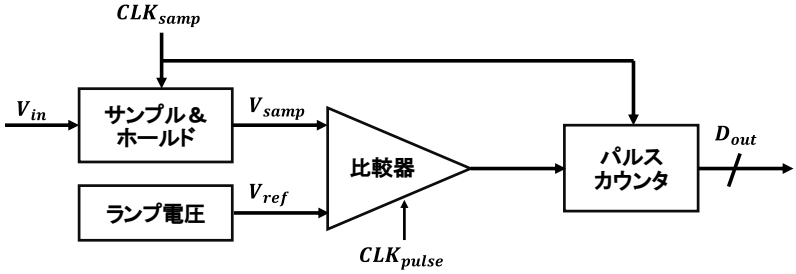

図 1.6: シングルスロープ型 ADC のブロック図

よって電圧分解能が決定されるため、電圧分解能と時間分解能がトレードオフの関係にある。これらを両立するためには、クロック信号の周波数を増加させ、単位時間内の電圧比較回数を増加させる必要があるため、消費電流の増加が課題となる。このような特性から、時間分解能の制約が比較的小さく、電圧分解能と小型化が求められるイメージセンサ向けの ADC として利用されている [20][21]。また、CMOS プロセスの微細化に伴い、電源電圧が小さくなった結果、電圧領域で信号を量子化する方式の ADC では高分解能化が困難となりつつある一方で、シングルスロープ型 ADC や、3 章で議論する VCO-based ADC のような時間領域での量子化を行う ADC は、電源電圧の低下による影響が比較的小さく、微細化と相性の良い方式とされている。

1.2.3.2 各方式の比較

表 1.2 にこれまで述べた ADC の比較表を記載する。一般的に、時間分解能と電圧分解能、消費電力はトレードオフの関係にあり、用途ごとに合わせた方式が採用される。

表 1.2: ADC の各方式の特徴

方式	回路面積	消費電力	時間分解能	ノイズ
SAR-ADC	中	小	中	中
ΔΣ 型	大	大	低	低
シングルスロープ	小	小	低	中

表 1.3: ADC に対するハードウェア攻撃報告例

文献	ハードウェア攻撃の概要
ISCAS2020[8]	SAR-ADC に対する V_{ref} へのサイドチャネル攻撃
A-SSCC2018[22]	シングルスロープ型 ADC へのサイドチャネル攻撃
CICC2022[23]	電源、漏洩電磁波からのサイドチャネル攻撃
IEICE2023[24]	Neural network を用いたサイドチャネル攻撃
S&P2013[25]	電磁波による信号注入攻撃

1.2.3.3 ADC に対するハードウェア攻撃報告

攻撃に対するセキュリティ技術を構築するには、個別の攻撃モデルに対する解析や原理の理解が重要な課題となる。ここでは、ADC に対するハードウェア攻撃に関する先行研究について述べる。

表 1.3 は、ADC に対するハードウェア攻撃の報告例である。先行研究では、ADC の回路コンポーネントにおける EMS (Electro-Magnetic Susceptibility) や、サイドチャネル情報漏洩を利用して、様々なアーキテクチャに対するハードウェア攻撃が報告されている [27]。

文献 [22] では、シングルスロープ型 ADC において、攻撃者が一定以上の精度で ADC が発する電磁界を取得することができる場合、コンパレータの比較結果が遷移するタイミングでのスイッチングに起因する電磁界の変動を観測することで、ADC の出力が推定可能である可能性があること、また、コンパレータに対して擾乱の導入を行い、スロープの変動に影響を与えることで ADC の変換値に影響を与えることができる可能性が指摘されている。

また、逐次比較型 ADC に対しては、DAC による電荷再分配中の参照電圧 V_{ref} や [8]、ADC の電源電位、漏洩電磁波 [23][28]、グラウンド、基板電位 [24] を観測することで、ADC の変換結果を推測するサイドチャネル攻撃が実行可能であることが実験的に示されている。

文献 [25] は ADC の入力段に EMI によって直接信号を注入する攻撃を示している。この時、サンプリング周波数の定数倍の信号をベース信号として用いることで、エイリアシングによって信号を ADC に出力させることもできる。ナイキスト周波数よりも高い周波数の信号を ADC に与えることによって、注入信号はエイリアスとして折り返され、変換結果に現れる。

このように、ADC に対するハードウェア攻撃モデルは ADC のアーキ

テクチャや、攻撃原理、実装によって様々なものが提案されている。セキュリティを考慮したADCを設計するためには、これらのハードウェア攻撃の原理や動作について理解し、対策を施さなければならない。

1.3 本研究の概要と論文の構成

1.3.1 FOWLPのチップ内部における電源品質・信号品質の観測

マルチチップモジュール (MCM) により回路システムを1つのパッケージに実装することで、システム中の信号のプロービングの難易度を向上させることが可能である。一方で、電源からのサイドチャネル漏洩や、パッケージ開封後のマイクロプロービングなど、更に高度な攻撃のリスクは残るため、セキュリティを向上させるためには回路中から漏洩しうる情報に関して分析する必要がある。

第2章では、MCM中の電源品質及び信号品質をオンチップモニタを用いてその場測定することにより、MCMにおける電源設計技術と、そのハードウェア攻撃対策応用について考察する。AESやECDSAのような暗号プロセッサやADCのような回路において、サイドチャネル漏洩が起こることは重大な課題である。MCMを用いたとしても必ず外部に露出する電源ノードを介したサイドチャネル攻撃には電力解析や、電磁波解析が提案されており、このような攻撃が用いる電源ノイズ成分の外部への伝達について実測し、解析を行う。

研究では、MCMを構築するパッケージング技術にはFan-out wafer level packaging (FO-WLP) 技術を選定し、パッケージ底面に搭載されたキャパシタの容量、構造、配置がチップ内の電源品質に与える影響を測定した。パッケージ内部の信号を評価することで、パッケージ内部に秘匿できる情報と、漏出しうる情報の別について考察する。

評価の過程において、パッケージ近傍に配置したランドサイドキャパシタ (LSC) による電源ノイズの抑制効果が、LSCのインピーダンスの特性を強く反映することを実測により明らかにした。この知見をFOWLP中の電源設計に応用することで、暗号回路やADCにおけるサイドチャネル漏洩を減衰させ、セキュリティ対策技術として応用することを考察する。

1.3.2　VCO-based ADC におけるセキュリティリスク評価

第 3 章では、VCO-based ADC におけるセキュリティリスクと、その対策技術について述べる。VCO-based ADC はデジタルスタンダードセルをベースに構成でき、小型、低消費電力かつ高解像度の ADC として構成され、組み込み機器のようなリソースの小さい機器において利用される方式の回路である。この VCO-Based ADC は内部に発振器を持つために、外部から発振信号を注入することで、インジェクションロックと呼ばれる現象を起こし、意図的に変換処理を操作できる可能性が考えられる。本研究においては、電磁波を用いて VCO-based ADC に攻撃信号を導入し、信号変換処理への攻撃モデルとメカニズムを実証する。

シグナルチェーン全体のセキュリティを保つためには、アナログ信号をデジタル信号に変換する境界におけるセキュリティを担保する必要があり、ADC の信号改ざんが可能なことは、深刻なセキュリティリスクとなる可能性がある。研究では、先行研究における類似の攻撃方法への対策から、本研究で提案する攻撃モデル対策への応用可能性を考察する。

1.3.3　制御システム向けセキュリティソリューションの事業化

製造業やインフラ施設においても、IoT や CPS が導入が進められているが、これまで外部に接続されていなかったシステム環境にこれらの技術を導入することによって、サイバー攻撃を受けるリスクも新たに発生している。一方で、製造業やインフラ施設において利用される制御システムは、「安定しているシステムを変更しない」という要求から、システムのセキュリティ更新が困難である課題が発生している。

第４章では、製造業やインフラ設備における制御システムにおけるセキュリティ上の課題について考察し、その課題を解決する「コネクターシステム」の提案と、コネクターシステムのシステムインテグレータ事業について述べる。

本章で述べたように、IoT や CPS が社会実装されている昨今の社会において、デジタル化されたデータのみならず、アナログ信号処理を含むシグナルチェーン全体においてサイバー攻撃リスクが指摘されており、それに対応するためのセキュリティ対策技術が必要となる。提案するコネクターシステムでも同様に、シグナルチェーンにおけるセキュリティリスクに対応しなければならない。本稿第 2 章と第 3 章における研究成果を応用した IC チップをコネクターシステムに適用することで、シグナル

チェーンにおけるセキュリティリスクを低減したシステムを構築可能であることを示す。

第2章

FOWLPのチップ内部における電源品質・信号品質の観測

2.1 はじめに

第1章で述べたように、IoTデバイスのようなユーザーの手元で運用される機材においては、リバースエンジニアリングや機密情報の解析を企図したハードウェア攻撃が脅威となる。特に、プロービングによる情報収集は、ハードウェア攻撃を実施する際の最も基本的な操作であるため、ファームウェアやデバッグバスのような、秘匿すべき情報が伝送されるバスのプロービングを困難にすることはハードウェア攻撃への対策上重要である。このとき、プロービングから取得しうる情報はIC設計者の意図する入出力情報だけでなく、サイドチャネルからの漏洩情報を含むことも注意すべきである。

プロービングの難易度は信号線へのアクセスの難易度によって決まるため、システムに必要な回路全てを1つのASIC上に実装するSoC (System on a chip) や、複数のASICを1つのパッケージ上に搭載し、複数のASICの機能を1つのモジュールとして構築するMCM (Multi chip module) を用いてシステムを構築することで、攻撃者によるプロービングを困難化することができる。特に、MCMは異種混載 (Heterogeneous Ingtegration) が実現できることから、高性能化、高機能化、歩留まりの最適化の観点から注目されており [29][30][31]、縦方向にASICを積み上げて、貫通シリコンビアによって接続する3-D IC chip (3DIC) stacking [32][33][34] や、平面上に複数のASICを並べて構築するFan-out wafer level packaging(FO-WLP)のような平面にチップを並べる2.5次元実装方式によって実現されている。

本章では、FOWLPパッケージ上に実装されたASICのオンチップ測定と、等価回路のシミュレーションを用いて、MCMデバイスにおける電源品質、信号品質を評価し、MCM内部に秘匿される情報の性質について考察する。2.2節では、本研究で用いるテストデバイスと評価環境について

説明し、2.3 節では、測定で得られた結果と知見について述べる。2.4 節では、測定結果から、MCM パッケージ上に秘匿しうる情報について考察する。最後に 2.5 節で本章をまとめる。

2.2 本研究の評価環境

本節では、本研究で用いるテストデバイスの構造について説明する。まず、MCM 全体の構造及び内部の ASIC に搭載された回路の構造、実験に用いたテストデバイスのパラメータを説明し、続いて実験のセットアップについて述べる。

2.2.1 MCM テストデバイス全体の構造

本章で測定対象とする MCM テストデバイスは、図 2.1 に示すように、2 つの同種の ASIC が FOWLP に組み込まれた構造である。この構造は典型的な構造の MCM を模擬しており、それぞれの信号品質及び電源品質 (SI/PI) を評価できるように設計されている。このとき、評価対象である ASIC の電源及び信号は、ASIC に各々搭載された電圧レギュレータモジュール (VRM) の出力 V_{DDL} 及び、ASIC 間で通信される LVDS (Low-voltage differential signaling) による通信信号である。

ASIC は回路実装面を FO インターポーザに向けて配置され、チップ表面の入出力パッドはインターポーザ上に形成されたパターンとバンプを通して接続されている。さらに、パッケージ全体は BGA (Ball-grid array) によって PCB 基板であるマザーボードに接続される。

テストデバイスのパッケージ上には ASIC に電荷を供給するためのランドサイドキャパシタ (Land-side capacitor: LSC) が搭載されており、回路に対して短距離で電荷を供給することができる。更に、マザーボード上にはの複数の位置にシステムレベルでのデカップリングのため、マザーボードキャパシタ (Mother board capacitor: MBC) が配置されている。

2.2.2 ASIC の回路構造

ASIC 上に構築された回路のブロック図を図 2.2 に示す。ASIC 上には、LVDS の送受信 (Tx/Rx) 回路と SRAM (static random access memory) ベースの BIST (Built in self test) ロジックコアで構築された回路が 24 チャネル並べられており、それぞれのチャネルはオンチップの VRM によって給電

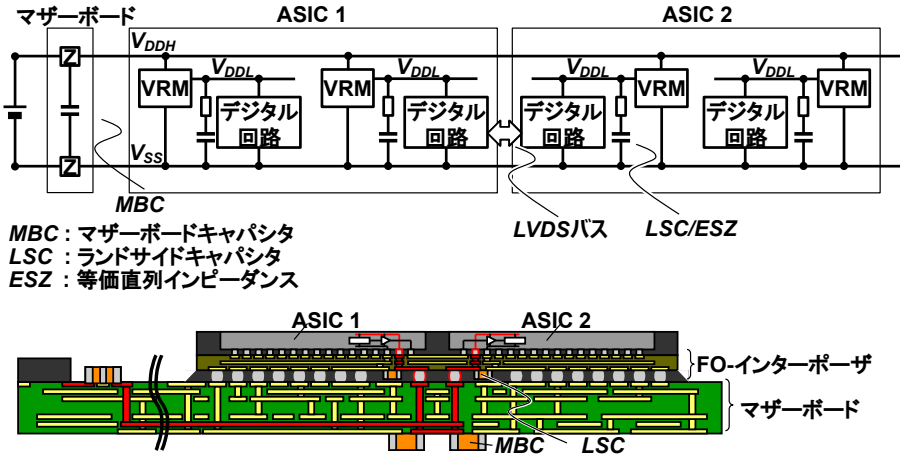

図 2.1: テストデバイスのブロック図 (上), キャパシタの配置 (下)

される。LVDS モジュールの一部は後述するオンチップモニタ回路によるプロービングが可能であり、モジュールの電源品質、信号品質をその場評価することができる。

ASIC 上の VRM は、外部から給電される V_{DDH}(3.3V) から、内部で使用される V_{DDL}(1.8V) の内部電源に変換する。このとき、V_{DDL} の電源ノードは LSC によって安定化される。

Tx 及び Rx、BIST 回路はそれぞれ以下のように動作する。LVDS 回路が Tx モードで動作するとき、16bit のデータを SRAM から受け取り、作動信号としてデータバスに送出する。Rx モードで動作する場合、Tx モードの作動信号を入力として受信し、ビットストリームに変換する。図 2.3 に示される BIST コア回路は、ビットストリームである *RXDATA* を SRAM に記録された期待値データと照合し、*RXDATA* が期待値と異なる場合にそのビット数をカウントし、ビットエラーレート (*BER*) を算出する。

以上の回路を含むデジタルコアの構造を、図 2.4 に示す。チップ上の左右にそれぞれ 12 チャネルの LVDS データチャネルが搭載されており、それらは中央に配置されている制御回路によって制御される。中央に配置される LVDS クロックチャネルはそれ以外の LVDS データチャネルのクロック信号として利用される。ASIC は 0.18μm CMOS プロセスで製造され、サイズは 5.4 mm × 5.4 mm である。

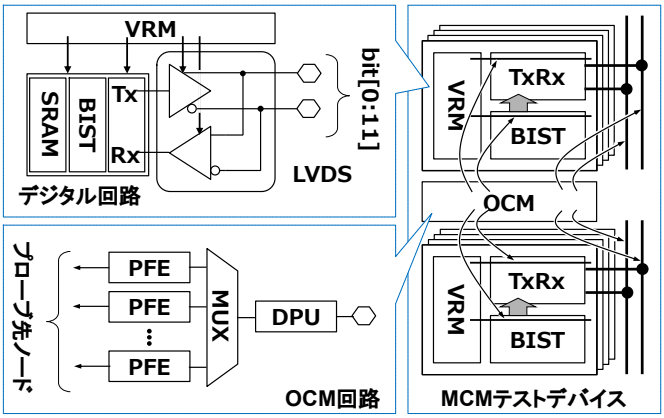

図 2.2: FOWLP テストデバイス回路のブロック図

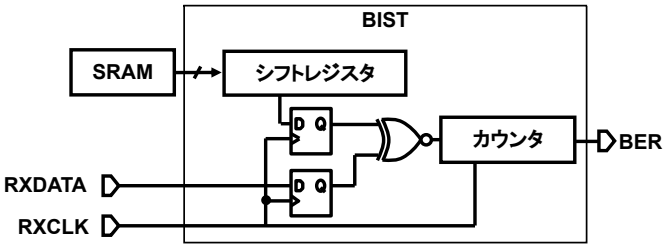

図 2.3: BIST 回路のブロック図

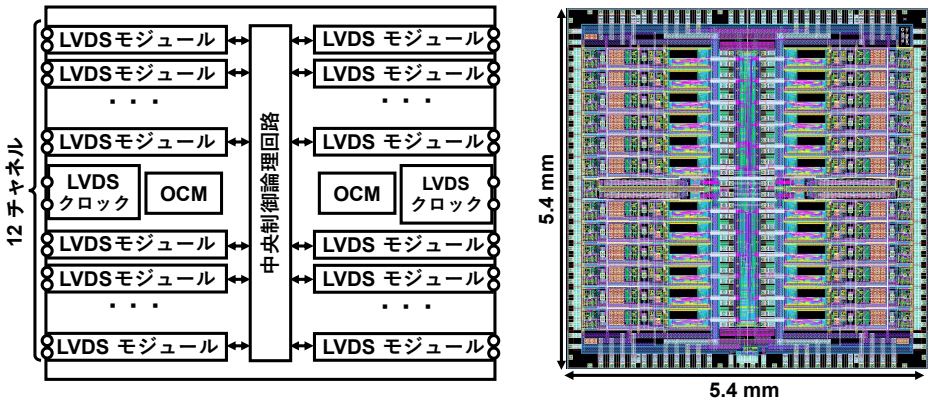

図 2.4: ASIC の構造とブロック図

2.2.3 オンチップモニタリング技術

図 2.5 に示すオンチップモニタ (On-chip Monitor: OCM) 回路は、チップ内部の電位をその場評価するための小型の計測回路である [35][36]。

OCM はアナログ電圧を取得するプロービングフロントエンド (Probing front end: PFE) と、PFE で取得したデータを処理する DPU (Data Processing Unit) で構成される。PFE と DPU では、以下のように電圧計測が行われる。まず、測定対象の信号 V_{SIG} は PFE の内部にあるソースフォロワに入力される。このとき、ソースフォロワは V_{SIG} に対してオフセット電圧を付与し、ラッチコンパレータで比較可能な電圧範囲にシフトして出力する。このことによって、OCM は電源電位からグラウンド電位までの広範な電圧範囲を測定することができる。ソースフォロワによってバイアスされた V_{SIG} は、ラッチコンパレータに入力され、タイミング信号 T_{STRB} の立ち上がりタイミングでリファレンス電圧 V_{REF} と比較される。比較結果は V_{REF} を掃引しながら DPU によって統計的に処理され、T_{STRB} における V_{REF} が測定信号と一致したと判定されたとき、その電圧を T_{STRB} における V_{SIG} と確定する。上記の動作を T_{STRB} を掃引しながら行うことで、所望の時間波形を取得することができる。上記の波形測定プロセスは外部の PC 上のソフトウェアによって制御されることで実施される。

OCM によるプローブ先は図 2.6 に示す PAD 付近と SRAM,BIST モジュール付近の V_{DD} 及び V_{SS}、更に、LVDS モジュールの信号入出力 V_{SIGP} 及び V_{SIGN}、に接続されており、外部から OCM の制御レジスタを操作することで、選択した位置の電位を測定することができる。

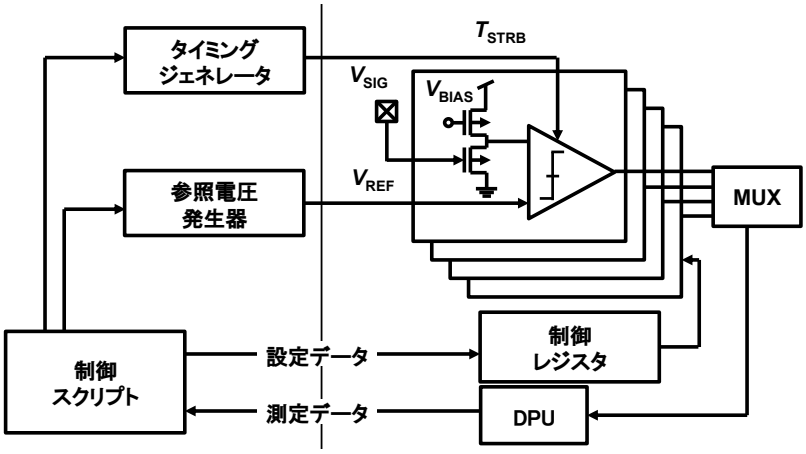

図 2.5: オンチップモニタのブロック図

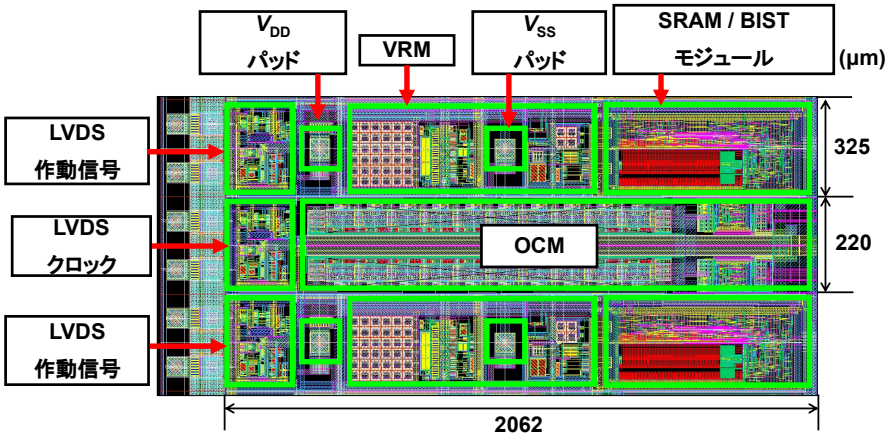

図 2.6: オンチップモニタのプローブ先

2.2.4 テストデバイスのパラメータ

テストデバイスのブロック図を図 2.7 及び図 2.8 に示す。テストデバイス上では、個別の ASIC が対向して配置されており、24 チャネルのうち、片側に配置された 12 チャネルのデータバスと、LVDS クロックチャネルが互いに接続される。

LSC 及び MBC が電源に与える影響の効果を検証するため、図 2.7 に示すオンボード給電方式と、図 2.8 のオンチップ給電方式の 2 種類の給電方式のテストデバイスを用意した。オンボード給電方式では、オンチップの VRM による給電ラインは物理的に切断されており、ボード上の電源コンバータがテストデバイス上のすべての回路に電源を給電する方式である。このとき、電源ラインには、MBC およびパッケージ上の LSC が全て接続される。対して、オンチップ給電方式では、LVDS モジュールに対して個別に配置されたオンチップ VRM と LSC が給電を行う。尚、どちらの給電方式でも、OCM 回路はこれらの電源とは独立に外部から電源が供給され、LVDS と VRM の PDN (Power Delivery Network) からは隔絶される。

本研究では、表 2.1 に示すように、給電方式、LSC の構造、容量のパラメータが異なる 9 種類の評価環境を作成している。#1、#2 は、オンボード VRM による給電を受け、回路を駆動する方式である。#1 には LSC がなく、#2 には 1nF の LSC が実装される。#3 から#9 のオンチップ給電方式の場合、複数の LVDS モジュールの電源ラインをバンドルし、バンドルのうちの 1 つの VRM から電源を供給する。#3,#4 では 6 チャネル、#8 では 3 チャネルをまとめて給電し、それ以外の#5,#6,#7,#9 では、1 つのモジュールに対して 1 つの VRM で給電している。

LSC の構造としては、MLCC (Multilayer ceramic capacitor) と Si Cap (Silicone capacitor) の 2 種類を実装した。表 2.2 は、#3,#4 に実装した容量が 10nF の MLCC と Si Cap における直列等価抵抗 (ESR) と直列等価インダクタンス (ESL) である。尚、この ESR と ESL は、実測されたキャパシタのインピーダンスから、それぞれ共振周波数 F_{res} と、1 GHz 時の値を用いて計算した。

FO インターポーザの誘電率 D_k は 4.4、誘電正接 D_f は 0.02 と仮定する。これらの数値は、次節におけるインピーダンスのシミュレーションで利用される。

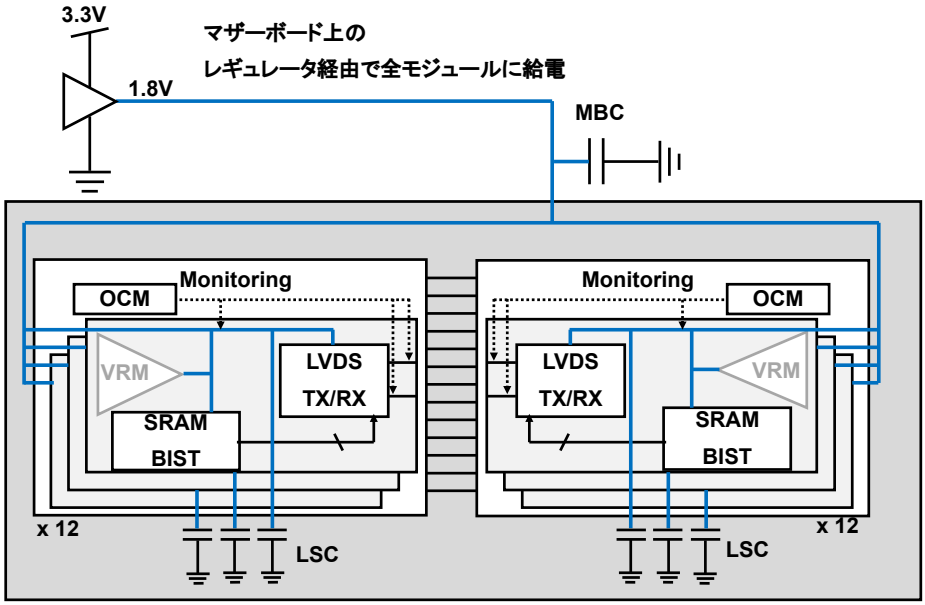

図 2.7: オンボード給電方式のテストデバイス

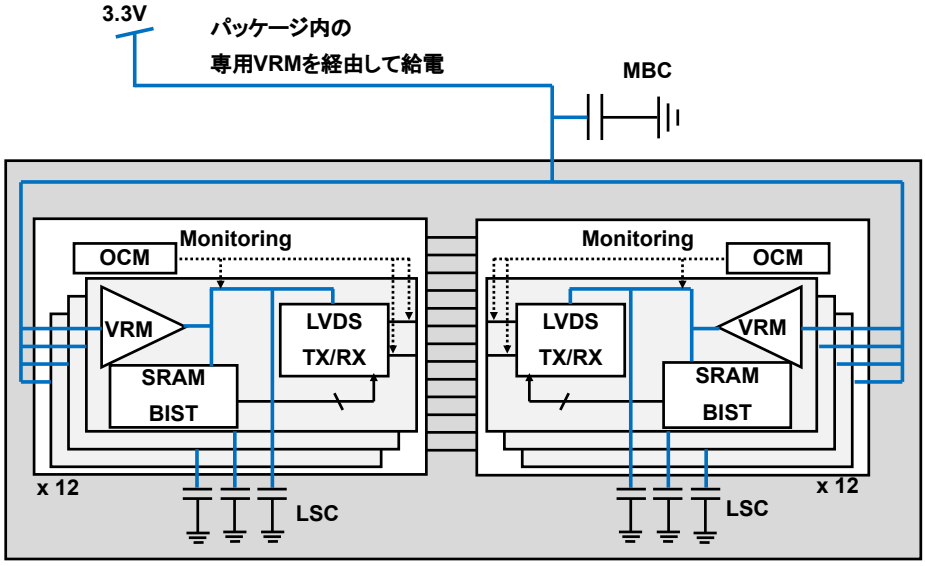

図 2.8: オンチップ給電方式のテストデバイス

表 2.1: 本研究のテストデバイスの条件

番号	VRM あたり モジュール数	LSC 構造	LSC 容量 (nF)	給電方式
#1	–	なし	なし	オンボード (図 2.7)
#2	–	MLCC	1	オンボード (図 2.7)
#3	6	MLCC	10	オンチップ (図 2.8)
#4	6	SiCap	10	オンチップ (図 2.8)
#5	1	なし	なし	オンチップ (図 2.8)
#6	1	MLCC	3.9	オンチップ (図 2.8)
#7	1	MLCC	10	オンチップ (図 2.8)
#8	3	MLCC	3.9	オンチップ (図 2.8)
#9	1	MLCC	1	オンチップ (図 2.8)

表 2.2: LSC の諸元

番号	LSC 構造	LSC 容量 (nF)	ESR(Ω)	ESL(nH)
#3	MLCC	10	0.12	0.37
#4	SiCap	10	0.28	0.16

図 2.9 は評価環境の外観および構造である。ASIC は FO インターポーザに接続されており、図 2.9(a) に示すようにアルミナの支持材がチップの背面に取り付けられている。テストデバイスの縦横の幅は 12.0 mm × 6.0 mm、高さは 1.45 mm である。この高さには、はんだボールの高さは含まない。尚、ASIC どうしの間はおよそ 0.2mm である。FO インターポーザは図 2.9(b) に示すように 3 層で構成され、各層の厚さは 4 μm、全体の厚さはおよそ 20 μm である。各層には金属配線パターンが構築されており、第一層は ASIC の電源、信号を含む入出力と FO インターポーザを接続するバンプのためのパッド、第二層はグラウンドプレーン、第三層は LSC の接続及び、マザーボードと接続するためのはんだボールのためのパッドがそれぞれ形成されている。図 2.9(c) に示す LSC のフットプリントは #3 及び#4 に対応しており、そのサイズは 1.0 mm × 0.5 mm である。LSC は図 2.9(b) の断面写真に示すように、はんだボールの直径以下の高さであり、PCB 基板とは電気的に接続されない。この構造によって、LSC と VRM のダイパッドの距離は最小化され、電源トレースははんだボール、パターン長を含み 0.83 mm 程度となる。また、LSC のグラウンド側のラ

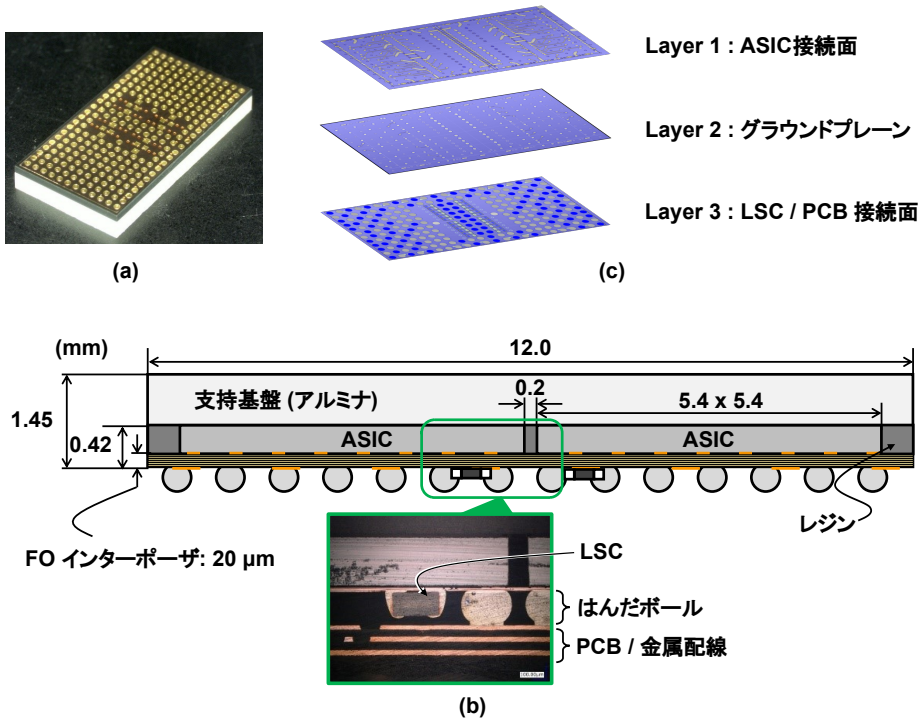

図 2.9: パッケージと LSC の構造

ンドはインターポーザ上のグラウンドプレーンに接続されており、外部のグラウンドのパッドとの距離は 0.95 mm である。これに対して、#1, #2 (図 2.7 の構造を取る) における PCB 基板上に配置された MBC と IC チップの距離は PCB 基板上の配線のため、3.39 mm 程度となる。尚、この距離のうち、1.57 mm は PCB 基板の厚みである。

2.2.5　測定フローのセットアップ

本環境における実験のシーケンスを図 2.10、実験のセットアップを図 2.11 に示す。FPGA には、テストデバイス上の制御回路の操作と、OCM の測定シーケンスの制御機能が実装されている。

FPGA とテストデバイス上の制御回路は、SPI 通信によってテストデバイス上のレジスタ及び SRAM の読み書きを行う事が出来る。まず、図 2.10 上の 1,2 に示すように、テストデバイス上の ASIC に対して、LVDS 及び VRM の動作設定情報を送信した後、Tx 側の SRAM には送信データ、Rx 側の SRAM には期待値データを書き込む。通常、送信データと期待値

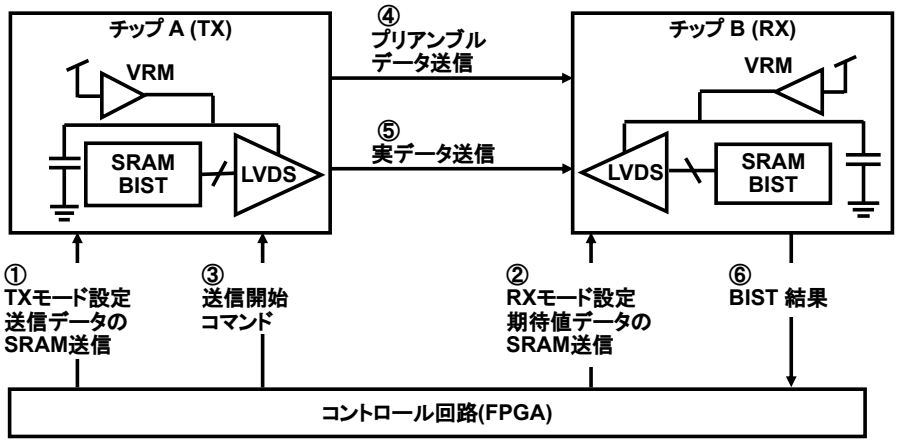

図 2.10: 実験シーケンス

データは同一のデータである。その後、Tx 側の送信開始レジスタを制御することで、通信が開始される。通信シーケンスが実行されたとき、テストデバイス上の ASIC は外部のクロック入力に応じて、まずプリアンブルの送出が開始され、続いて、SRAM 上のデータの送信が開始する。受信側では、受け取ったクロックとデータに応じて BIST 回路が動作する。

OCM の測定シーケンスの制御は、上記の制御回路とは独立に実施される。まず、PFE 回路上のレジスタを操作することで、OCM が測定するプローブ先を選択する。FPGA デバイスでは、DPU から得たプローブ先電圧と参照電圧 V_{ref} の比較結果に応じて、タイミングジェネレータや電圧ジェネレータを操作することで、OCM へのタイミング信号 T_{STRB} と参照電圧 V_{ref} を生成する。このとき、所望の電圧波形をサンプリングする T_{STRB} は、測定の反復ごとに ΔT の時間ステップで漸進的に進む。一方で、T_{STRB} ごとに、V_{ref} は ΔV 変動し、測定対象と最も近い電圧を探索する。ΔT と ΔV は OCM の時間分解能と電圧分解能に相当し、このセットアップではそれぞれ 100 ps と 100μV に設定されている。OCM 回路による波形取得アルゴリズムは先行研究により検討されており [35][36]、車載用チップにおいてのノイズ結合のその場評価にも評価実績がある [37][38]。本研究では、LSC を備えた FOWLP チップ環境上の電源、信号品質評価に利用する。

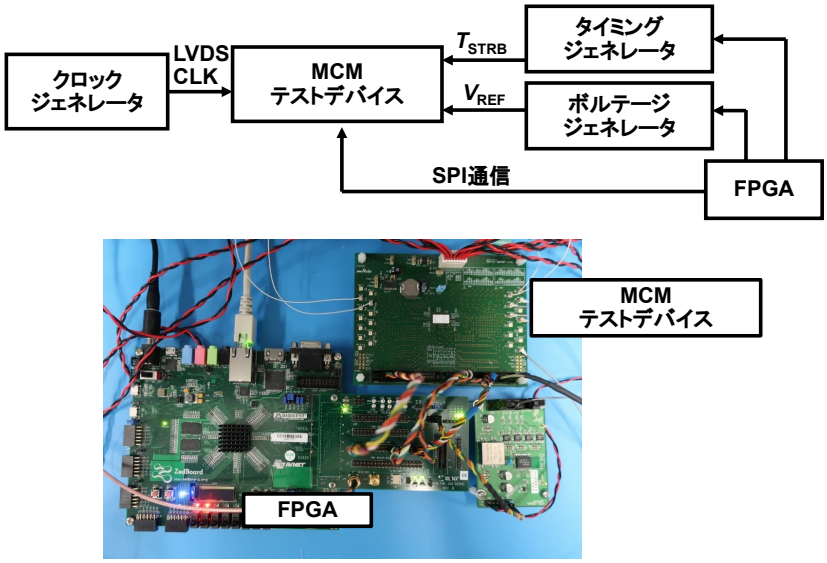

図 2.11: 実験のセットアップとブロック図

2.3 実験評価結果

本節では、前節で示した測定環境の下に観測された測定結果を示す。まず、取得する電源波形、信号波形の特徴について説明し、その後、搭載する LSC の容量が電源品質、信号品質に与える影響について示す。最後に、LSC のキャパシタの選択が電源設計に及ぼす影響を示す。

2.3.1 オンチップ測定波形の特徴

前節で示した測定環境によって測定された電源波形 (V_{DDL}), 作動信号 ($Vsigp$, $Vsign$), グラウンド (V_{SS}) の波形を図 2.12 に示す。このとき、12 対のすべての LVDS モジュールには 400MHz のクロック信号が入力されており、”1010110011001100”のデータパターンを繰り返し送受信している。尚、この測定結果は、オフセット電圧と利得はあらかじめ校正されている。

電源ノードでは、クロックに対応する、1.25ns 間隔の周期的な電圧変動、即ちクロック周波数に対応するスイッチングノイズが、V_{DDL} においておよそ 40mV, V_{SS} でおよそ 10mV 程度観測される。さらに、16 クロックサイクルごとに SRAM から 2 バイトのデータ読み込みが発生し、これに伴い電力が消費されるため、電源ノード、グラウンドノードともに、LVDS 動作のスイッチングノイズに比べて大きな電圧変動が観測されている。信号ノードでは、LVDS の作動信号が観測されており、ビット列の変動に伴う電位の推移が明確に観測されている。

図 2.13 は、デモ回路#3 において、LVDS モジュールを TX モードで動作させた場合と、RX モードで動作させた場合における電源波形の特性の比較である。このとき、LVDS は回路の最高動作速度である 750MHz で動作しており、”0101010101010101”を繰り返すデータパターンを送信している。Tx 回路は、FOWLP 中の配線を介してチップ間の信号線を駆動するため、Rx 動作時よりも高いレベルの電圧変動がみられる。一方で、Rx モード中では、Tx から受信したデータを BIST で比較するため、SRAM から期待値データを読み出すタイミング以外では Tx モードに比べて電圧変動は小さい。Tx のノイズ波形は送信データパターンに大きく依存するため、以後、電源品質を評価するためにはデータ依存性が小さい Rx モードの電源ノイズ波形を解析の対象とする。

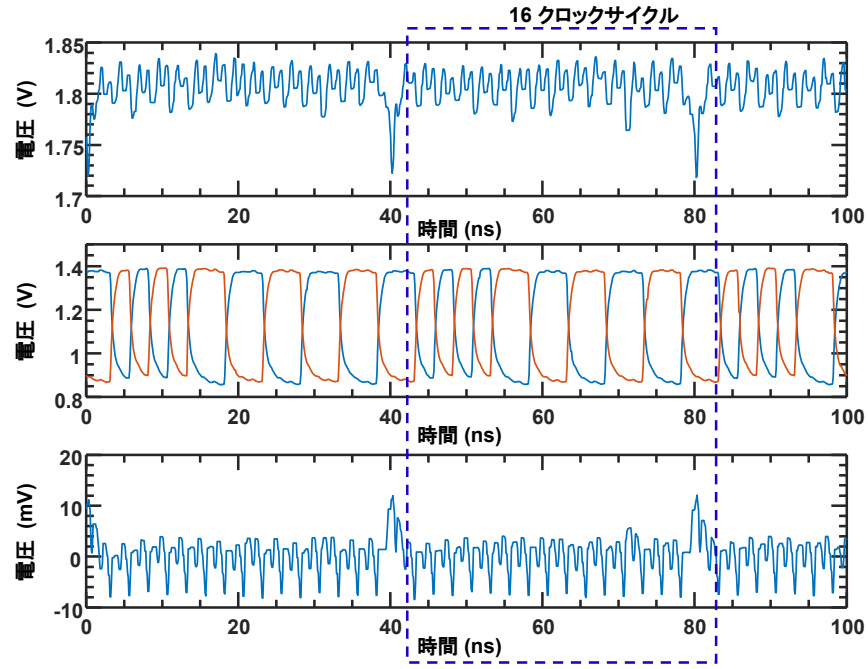

図 2.12: OCM による内部波形の計測結果

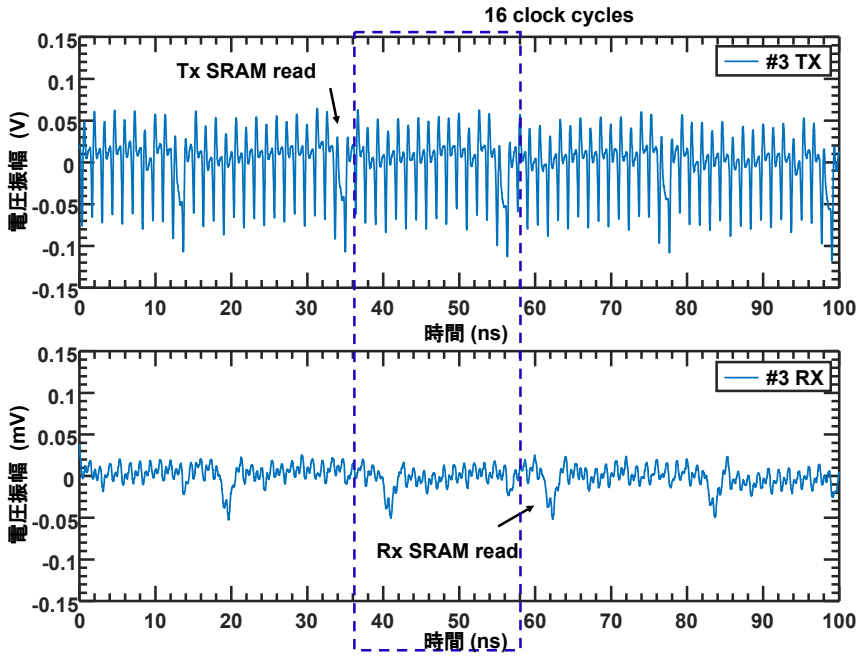

図 2.13: 送信側 (上) と受信側 (下) のノイズ波形比較

2.3.2 電源品質と信号品質の計測

モジュールの電源品質に対して、MBC 及び LSC が与える影響を測定するため、表 2.1 に示す#1,#2 を用いて、(a)MBC, LSC 配置無しの場合、(b) MBC のみ配置の場合、(c) MBC,LSC を両方配置した場合の 3 つの場合について、LVDS モジュールを 750MHz のクロックで駆動したときの電源品質を測定した。図 2.14 は、(a),(b),(c) における電源波形と、それを高速フーリエ変換 (Fast Fourier transform : FFT) によって周波数領域に展開した図を示している。電源波形の周波数特性の特徴として、クロック信号の 750MHz の第一高調波、第二高調波成分が顕著に表れている。

PDN にコンデンサが実装されない (a) の場合、およそ 40mV 程度のノイズ振幅がみられるが、(b),(c) において、MBC, LSC を搭載することで、ノイズが減衰している。(b) の場合、PCB 基板上に総合で 1.2μF の MBC が実装されており、(a) の通り MBC を実装しない場合に比べて 500MHz 以下の成分が減衰しているが、750MHz, 1.5GHz の高周波成分の減衰は見られない。(c) では、容量のスケールとしては MBC の 100 分の 1 程度の 12nF の容量が LSC によって実装されている。この場合、750MHz, 1.5GHz の高調波の減衰が確認された。このことは、LSC が MBC よりも消費電流の発生源に近接して配置されているため、寄生インピーダンスが少なく、高速な電荷供給が可能であることの効果を示している。

更に、LSC が電源、信号品質に与える影響を図 2.15 に示す。この測定では表 2.1 の#5,#6,#7 を用いて、電源波形は VRM の出力である内部 V_{DD} パッド付近の電圧を測定し、信号波形は V_{SIGP} 及び V_{SIGN} の信号パッドで測定している。#5,#6,#7 は、オンチップのレギュレータが各 LVDS モジュールに電源を供給するデバイスであり、MBC はいずれも PDN に接続されていない。#5 は PDN に LSC が接続されない水準、#6 は 3.9nF の LSC が実装されている水準、#7 は 10.0nF の LSC が搭載されている水準である。

このとき、電源ノイズの振幅は LSC 容量に応じて減衰し、これに応じて信号のアイ開口が明瞭になる。表 2.3 には、アイ開口の大きさとジッターの大きさについてまとめている。#5 に対して#6,#7 はアイ幅は 0.2ns 程度、アイ長は 80mV 程度向上した。

以上の結果は、チップ内部に実装された VRM と LSC によって、安定な電源供給が可能であることを示し、そのことによる通信信号品質の改善が実現された事を示している。

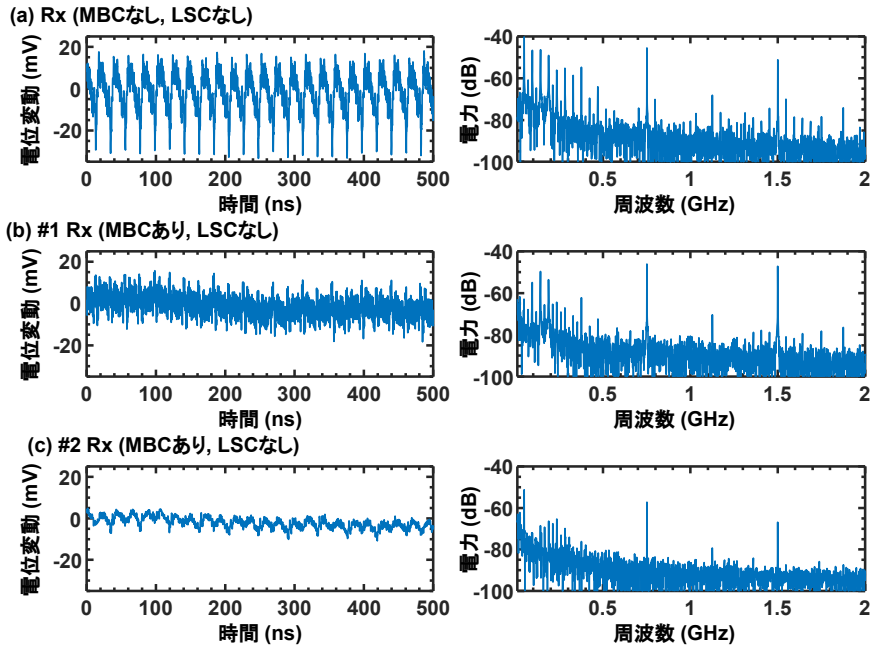

図 2.14: (a)MBC, LSC 配置無しの場合、(b) MBC のみ配置の場合、(c) MBC,LSC を両方配置した場合の電源ノイズ波形

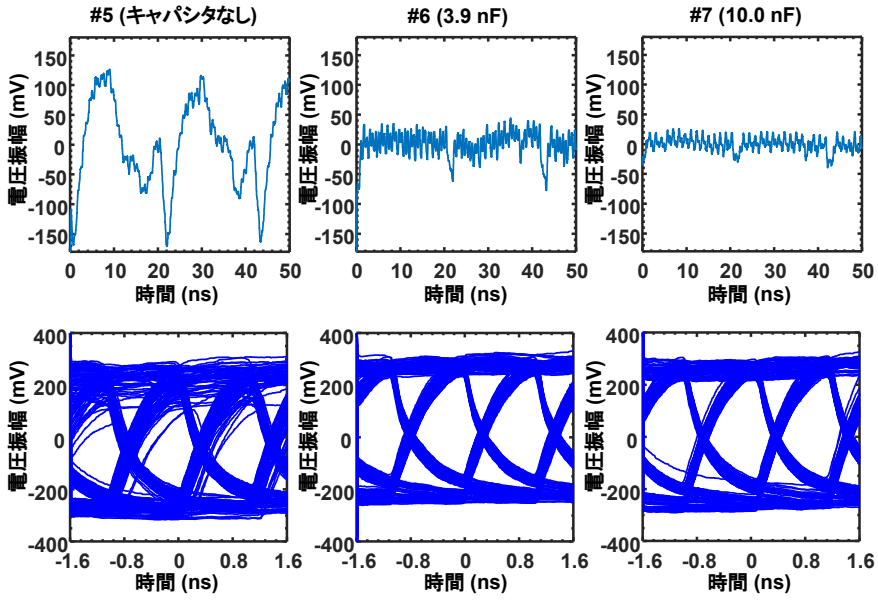

図 2.15: FOWLP 内部の信号品質、電源品質の計測結果

表 2.3: 信号品質の計測結果 (図 2.15)

番号	#5	#6	#7
アイ長 (mV)	295.7	376.2	382.0
アイ幅 (ns)	0.96	1.16	1.15
ジッタ (ns)	0.39	0.19	0.18

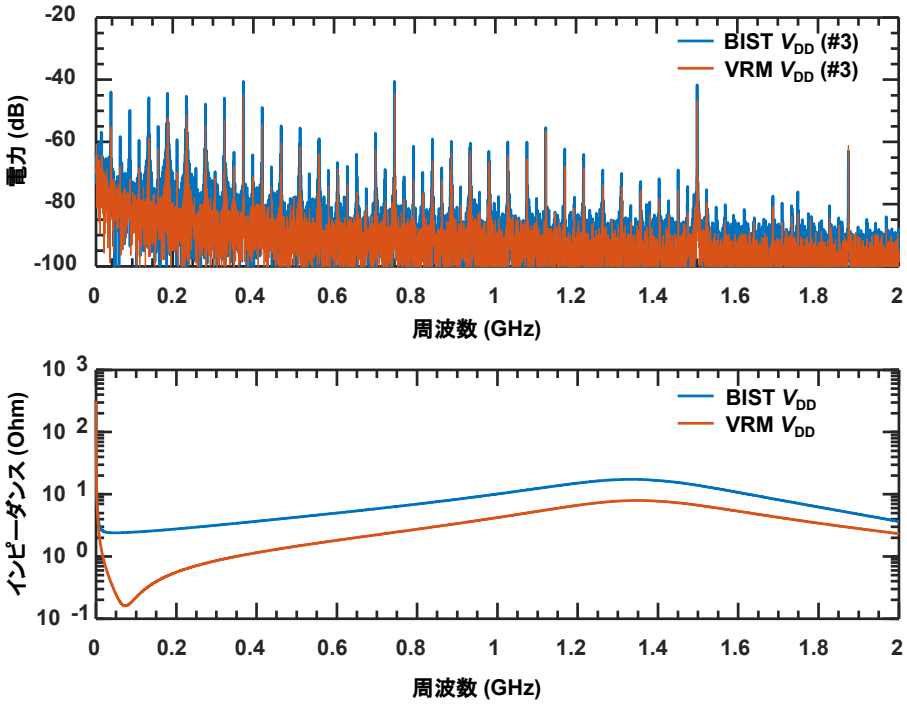

図 2.16: V_{DD}PAD 近辺と BIST モジュール近辺の電源ノイズの比較

図 2.16 は、LVDS モジュールの PDN に対して、LSC が接続されるパッドの近傍 (図 2.6 $V_{DD}pad$) と、遠方 (図 2.6SRAM/BIST) における電源ノイズ測定結果の比較と、両者の電源インピーダンスのシミュレーション結果の比較である。これらの測定点は図 2.6 に示すように、互いにおよそ 900μm の距離にある。

ノイズの周波数成分の大きさは、測定した帯域の全域に渡って、PAD 近辺よりも SRAM 近辺のほうが+3 +6dB 程度大きくなる。また、同様の帯域でそれぞれのインピーダンスをシミュレーションした結果、配線の寄生インピーダンス分、PAD 近辺よりも SRAM 近辺のほうがループイ

ンピーダンスは増加し、このことはノイズの実測結果と整合する。ここで、SRAM の読み込み動作に伴うノイズ成分は特に大きく減衰しており、(750MHz での駆動時、46.875MHz となる) チップ内部の容量成分によって大きく減衰している事が分かる。

2.3.3 キャパシタの種類に応じたノイズの計測

ここでは、LVDS チャネルが 100MHz で動作するときの VRM のノイズを比較することによって、コンデンサの物理構造による違いを検討する。2.0GHz の周波数帯域において、容量が 10nF で等しい MLCC と SiCap のテストチップ (#3,#4) における電源ノイズの周波数成分を比較した。また、シミュレーションにより、両水準のチップの PAD 付近のインピーダンスを導出している。

図 2.17 では、2.0GHz までの周波数範囲で MLCC と Si Cap のテストデバイスにおけるノイズ成分とインピーダンスを比較しており、電源ノイズはそれぞれの LSC のインピーダンスの傾向に従う事が示されている。SiCap は ESL が小さいため、高い周波数領域においてノイズを抑制する効果がみられるが、逆に、共振周波数付近では ESR の小さい MLCC のほうがノイズをより減衰させることが確認できる。

インピーダンスと電源ノイズの関係を詳細に確認するため、図 2.18 では、LVDS の動作周波数を 15MHz から 100MHz に掃引したときのノイズの最大の周波数成分、即ち、動作周波数の 2 倍周波数の成分をプロットし、共振編付近のノイズを比較している。測定結果から、共振周波数付近における LSC のインピーダンスとノイズに明らかな相関があることが分かる。

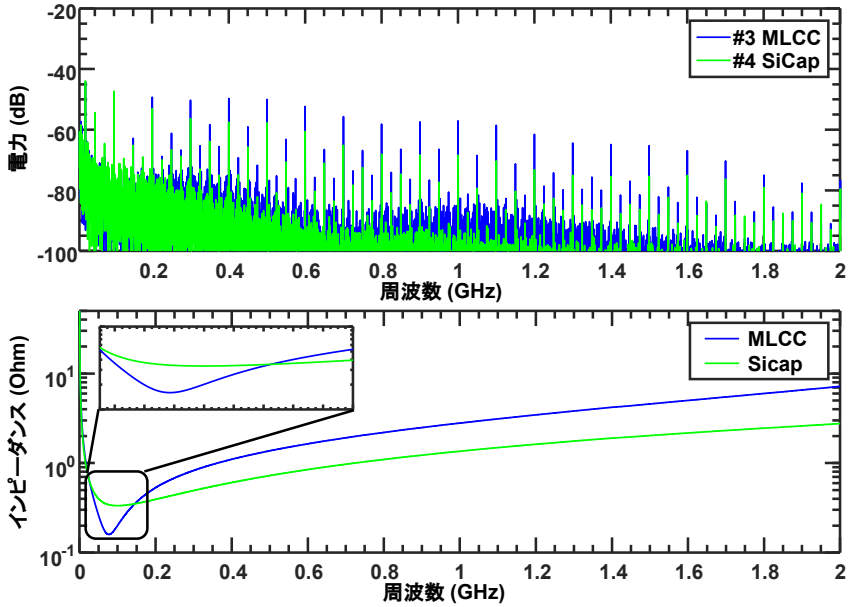

図 2.17: MLCC と SiCap の広域におけるノイズ比較

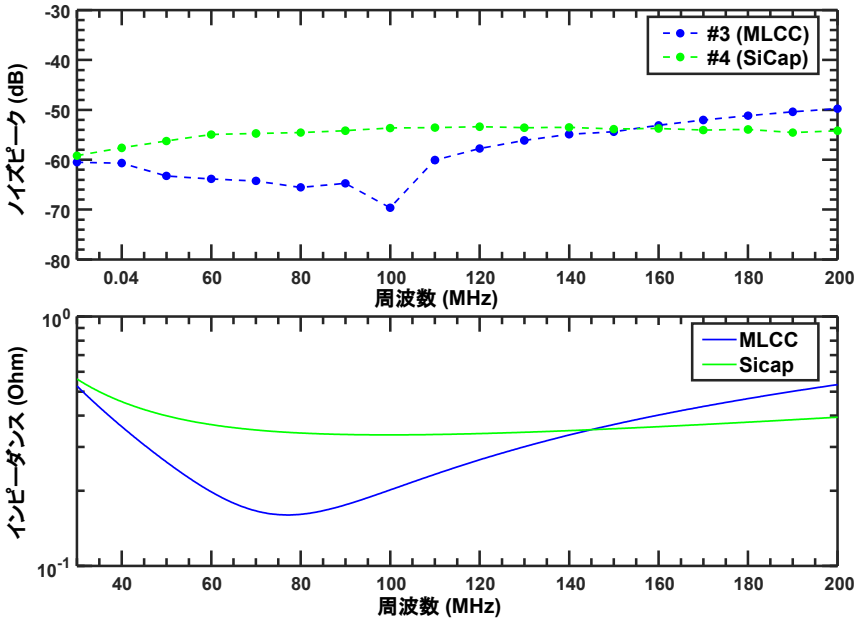

図 2.18: MLCC と SiCap の共振点付近ノイズ比較

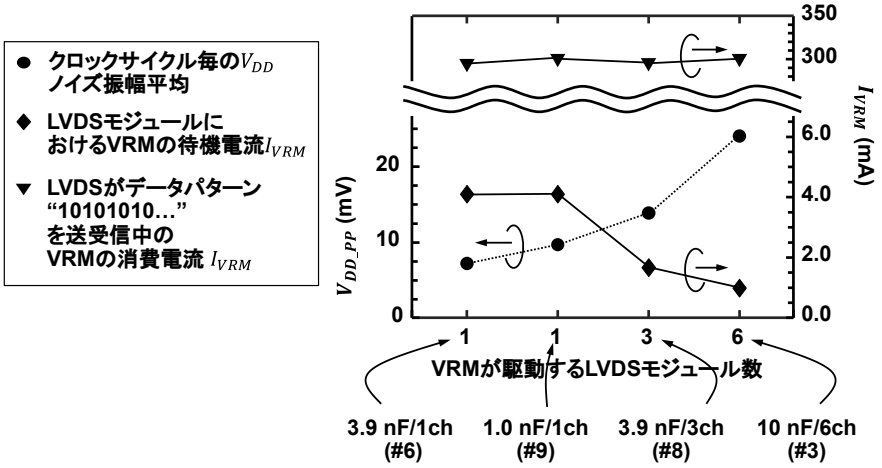

図 2.19: 消費電力と電源品質のトレードオフ

2.3.4　電源品質と消費電流のトレードオフ

図 2.19 は、VRM が駆動する LVDS モジュール数と、電源ノイズ振幅、消費電流をプロットした図である。

テストデバイスの 12 対の LVDS チャネルが、動作周波数 750MHz において、最もデータの遷移が大きいデータである“0101010101010101”を送受信し続ける場合において、クロックサイクル毎のノイズ振幅 VDD_{PP} の平均がプロットされている。モジュールごとの LSC の容量が概ね統一された#3(1.66nF),#8(1.3nF),#9(1.0nF) の比較より、VDD_{PP} は、LVDS チャネルがそれぞれ専用の VRM によって駆動されている場合に最も低くなることが分かる。更に、#6 と#9 の比較から、LSC の容量が大きい場合に VDD_{PP} はより小さくなる。VDD_{PP} は、#3 のとき、#9 の 2.5 倍程度の振幅となり、VDD_{PP} を抑制したい場合は、専用の電源モジュールを設定することが有効である。

ここで、消費電力と電源ノイズ振幅のトレードオフについて考察する。2.19 では、LVDS が動作している場合と、動作していない場合における消費電力 I_{VRM} が示されている。待機電流は明らかに VRM モジュールの増加毎に増えるが、LVDS が動作中であり、消費電流が大きい場合、待機電流の全体への寄与は殆ど無くなる。

この結果から回路のユースケースにおける電源設計の方針として、以下の通り述べられる。まず、消費電力が小さく、あまり頻繁に動作しない回路の場合は、#6 のように、VRM を共用化して給電し、待機電流を抑

制することが合理的である。一方で、サーバーアプリケーション向けなどにおいて、電源品質が求められる場合は、#6,#9 のように専用の VRM 回路と LSC を配置するとよい。

2.4 電源設計への知見とハードウェア攻撃対策への応用

本節では、これまで得られた実験結果を通して、FOWLP におけるハードウェア攻撃対策応用について述べる。

第 1 章においては、ハードウェア攻撃を企図する攻撃者が信号のプロービングによって情報収集を行うことを述べた。プロービングは、露出した、あるいは加工によって露出させた信号線に対して信号を観測する行為であるため、先に述べた通り信号線の微細化や、多層化によって難易度が向上する。従って、MCM のような単体の IC チップで構成されたシステムを用いて重要な信号線をパッケージの内部に秘匿することはプロービングに対する有用な対策と言える。特に、FOWLP はシリコンプロセスで再配線層が形成されるため、FOWLP に対してプロービングを行う場合、IC チップと同等の精度の操作や設備が要求される。また、FOWLP の再配線層は非常に薄膜で脆く、プロービングによる接触により破損しやすいことも、ハードウェア攻撃対策の観点から有用な特徴である。

一方で、電源端子のような外部へ必ず露出してしまう端子からも、サイドチャネル漏洩によるセキュリティ上の脆弱性が存在することが知られている。したがって、電源端子から漏出する信号の特性を分析し、これを抑制する電源設計が必要である。

2.20 はテストデバイスに搭載された VRM における負荷電流の外部伝達の特性の解析環境及びその結果である。シミュレーションにおいて、負荷電流 I_{LOAD} は 1Hz から 1GHz の範囲で掃引され、外部電源の負荷電流 I_{DD} との比をプロットしている。LSC の容量は 10nF を仮定し、オンダイの規制容量は 50pF、ESZ はチップデザインから計算された値を試用している。結果から、テストチップの場合、10MHz 程度のノイズ成分に含まれる情報は外部に線形に漏出することが分かる。一方で、LSC がある場合は、10MHz 以上の負荷ノイズ成分は外部への漏出が抑制され、パッケージの中で消費される。

続いて、このメカニズムによるノイズ減衰が一般的な暗号回路のサイドチャネル漏洩に与える影響について考察する。表 2.4 で示すように、本

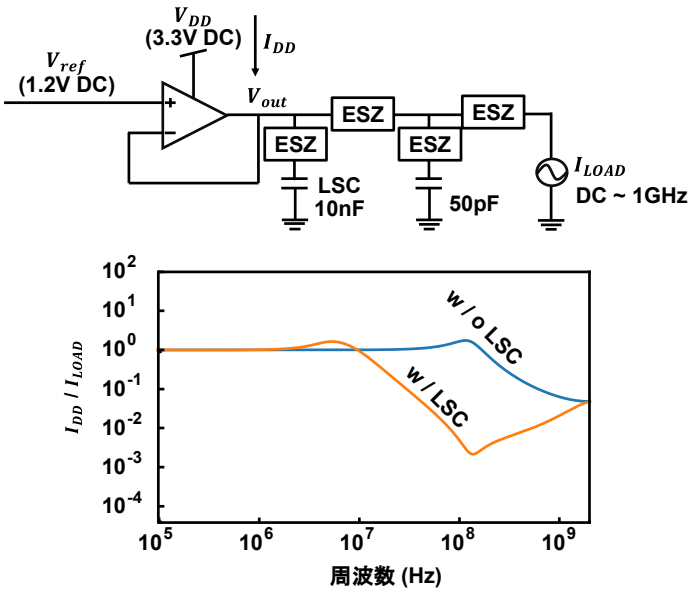

図 2.20: オンチップ VRM の AC 解析環境とその結果

表 2.4: 本研究のテストデバイスと暗号デバイスの要素比較

回路要素	テストデバイス	暗号回路
デジタル回路	BIST	暗号演算エンジン
SRAM	BIST 期待値用 SRAM	暗号文/平文保存用 SRAM
入出力回路	LVDS	外部 IO

章で用いたテストデバイスの回路構成は、スタンダードセルで構成された論理回路 (BIST 回路)、SRAM、IO 回路 (LVDS モジュール) で構成された回路であり、その回路構成は一般的な暗号回路と相似である。したがって、暗号回路と本研究で用いたテストデバイスのノイズ発生メカニズムも相似であり、LSC を暗号回路に適用した場合においても、電源ノイズは減衰するものと考えられる。

また、先行研究では、3 次元積層チップにおいて、オンチップの容量増加によるノイズ減衰効果と、VRM によるローパス特性によるサイドチャネル情報漏洩の減衰の関連が示されており、FOWLP における LSC の配置や、VRM を注意深く設計する事で、チップ外部で観測されるノイズの高周波成分を削減し、先行研究同様同様にサイドチャネル漏洩が減衰する可能性がある [39]。

一方で、サイドチャネル漏洩情報は広い周波数帯に分布することが知られており、低周波成分の情報漏出対策を合わせて行う事が必要である。先行研究では、カレントイコライザを用いたサイドチャネル攻撃対策技術が報告されており、オンチップの容量と併せて利用することで強力なサイドチャネル攻撃対策を実施できると考えられる [40][41]。

2.5 本章のまとめ

本章では、FOWLP における電源品質、信号品質のその場評価を通じて、LSC が電源品質、信号品質に与える影響を測定した。パッケージ内部での電源ノイズのその場測定により、電源ノイズの特性や、遍在が明らかになり、また、MCM デバイスにおける電源デバイスの設計方針について知見を得た。

セキュリティの観点からは、FOWLP でデバイスをパッケージングすることで、デバイス上でのプロービングが困難になることを述べ、その上で漏出しうる情報について考察した。特に、電源ノードは外部からの給電パスを設けることが必須である。電源のシミュレーションと、測定の結果から、電源から漏出しうる情報の特性を明らかにし、MCM の設計を通じてのサイドチャネル漏洩への対策技術としての応用可能性を示した。

第3章

VCO-based ADCにおけるセキュリティリスク評価

3.1 はじめに

第1章では、シグナルチェーン上の脅威として、ADCに対する攻撃手法が近年報告されている事を示した。ADCはCPSやIoTシステムにおいて利用されるセンサー情報の処理に必ず付帯する回路であり、ADCに対する攻撃はシステム全体の制御や動作に致命的な影響を与えうる。このような潜在的なセキュリティ上の脅威に対する対策を考えるために、攻撃モデルやメカニズムの分析が必要である。

本章では、微細化されたCMOS技術に適した構造として近年注目されるVCO-based ADCに対するEMSについて説明し、そのハードウェア攻撃応用の可能性について議論する。研究においては、VCO-based ADCに存在するEMSを用いた出力結果の操作について、実デバイスを用いた実証と測定を行った。測定結果を元に、提案するEMSの影響範囲や性質を明らかにし、その対策について考察する。

3.2 VCO-based ADCの構造

半導体CMOSトランジスタの製造プロセスの微細化はトランジスタの電源電圧の低電圧化や、高速な信号応答、回路の高密度化を実現し、デジタル回路の回路性能を飛躍的に向上させてきた。しかし、微細化が進んだプロセスでは、電源電圧が低く、トランジスタの製造ばらつきが相対的に大きくなるため高い利得や高精度な容量比・抵抗比が求められるアナログ回路では、微細化に応じた性能向上の恩恵は限定的である。したがって、1章で述べた、ΔΣ型ADCやSAR-ADCのようなアーキテクチャのADCは、微細化による性能向上が見込みにくい。

このため、時間領域で量子化を行い、回路構成のほとんどをデジタル回

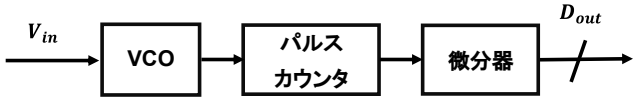

図 3.1: VCO-based ADC のブロック図

路で実現可能な VCO-based ADC が注目されている [42][43][44][45]。図 3.1 に VCO-based ADC の構造を示す。

回路の入力を受け付ける VCO では、式 3.1 に従い、入力信号 V_{in} に応じた周波数 F_{VCO} のパルス信号が生成される。ここで、K_{VCO} は、変換係数である。

$$F_{VCO} = K_{VCO}V_{in} \tag{3.1}$$

このパルス信号は、後段のパルスカウンタによってカウントされ、最後段の微分器を通過することで、ADC の出力 D_{out} が得られる。初段の VCO における位相 P_{VCO} の変化量は発振周波数 F_{VCO} の時間積分であり、パルスカウンタによって量子化される。このとき、量子化誤差は VCO の初期位相として次回のサンプリングにフィードバックされ、これによってノイズシェーピングが働く。この量子化信号を微分器に通過させることで、1 次 ΔΣ 変調が行われる。即ち、ΔΣ 方式の ADC と同様に量子化ノイズが抑制されるため、狭帯域信号を高い SNR でデジタル信号に変換できる。

3.3　VCO-based ADC の EMS

注入同期現象とは、ある発振器の発振周波数に対して、別の外部発振信号を何らかの形で結合すると、発振器が外部信号に同期する現象である [46][47]。この現象は集積回路内の電気信号に対しても発生し、回路性能の向上にも利用される [48][49] が、ここでは電磁界結合による EMS、あるいはハードウェア攻撃可能性の原因として考える [50][51]。

VCO-based ADC は図 3.2 に示すように、注入同期現象による EMS を示す。VCO が周波数 F_{VCO} で発振しているときその近傍の周波数 F_{EMI} で、十分大きな振幅の電磁波を照射したとき、電磁界結合を経由して注入同期現象が発生し、F_{VCO} は F_{EMI} に引き寄せられる。この結果、VCO-based ADC は周波数 F_{EMI} 対応したデジタルコードを出力してしまう。

特に、VCO の発振周波数が数 GHz 程度に設計されている場合、Wi-Fi

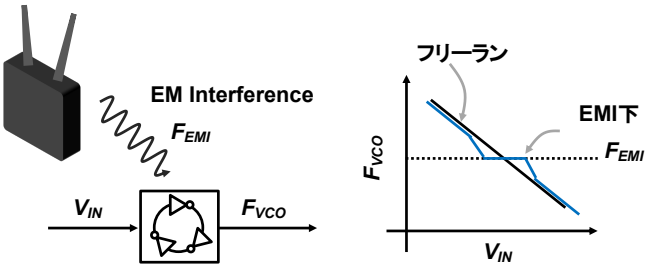

図 3.2: 注入同期現象による VCO の EMS

や LTE などの無線システムの RF キャリア周波数のような環境中の電磁波に電磁干渉を受けうる。一般的に、作動構造は EMS によって発生する外部からのコモンモードノイズの影響を除去する有効な方法として知られているが、この場合は差動チャネルの一方に影響を与えうるため、作動構成によるエラーの補正は行われず、誤ったコードを生成しうる。

3.4 本研究の評価環境

本稿では、リングオシレータ (Ring Oscillator: RO) をベースにした VCO-based ADC を評価の対象とする。本研究で用いる VCO-based ADC のテストデバイスを図 3.3 に示す。テストデバイス 28nm CMOS プロセスで製造されており、チップサイズは 1.0 mm × 1.5 mm、コア電源電圧は 0.9V、IO 電圧は 1.8V である。

テストデバイス上には、シングルエンド型と、差動型の VCO-based ADC が実装されている。図 3.4 にシングルエンド型 ADC の構成図を示す。ADC 回路内のリングオシレータは 7 段のカレントスターブドインバータによって構成される。各段におけるカレントスターブドインバータの伝搬遅延は、入力電圧 V_{in} により制御され、発振周波数 F_{VCO} が変動する。設計上、F_{VCO} は 450mV-850mV の入力電圧 V_{in} に対して、およそ 4.0GHz-2.0GHz の範囲で変動する。

図 3.5 は差動型の VCO-base ADC のブロック図である。VCO-based ADC では、信号が時間領域で変調されるため、直接差動化することが困難である。ここでは、出力段の差分を取ることで、疑似差動構成を取る。疑似差動型 ADC では、変換係数 K_{VCOP} と、K_{VCON} に基づき変換された結果の差分を取ることにより、ADC の出力を決定する。このとき、電圧-周波

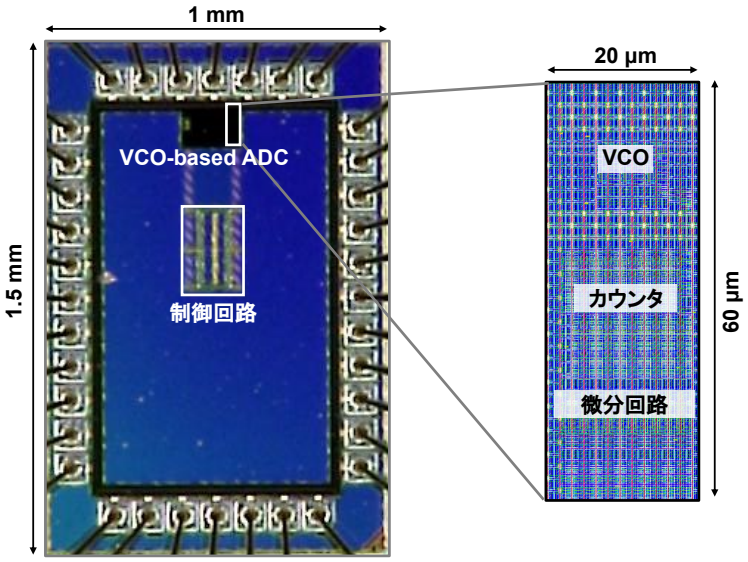

図 3.3: テストデバイスの写真

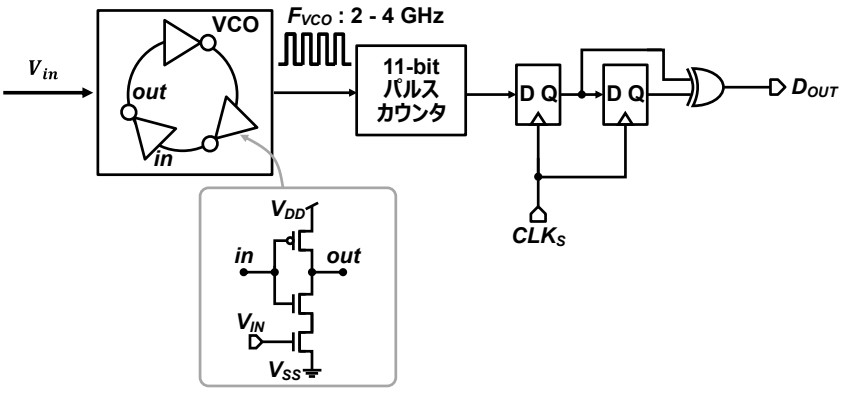

図 3.4: テストデバイス上の VCO-based ADC

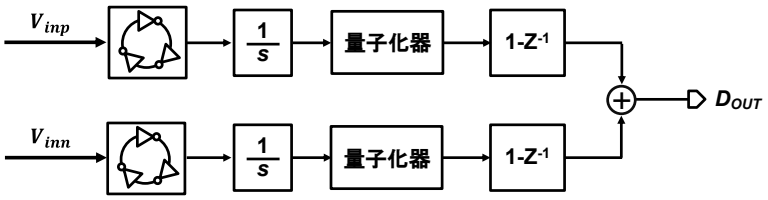

図 3.5: 疑似差動 ADC のブロック図

数変換に伴う偶数次高調波が低減されるため、シングルエンド型 ADC に比べて線形性が高い [52]。

VCO-based ADC はデジタルスタンダードセルでの構築により、20 μm × 60 μm 程度の面積で実装されている。比較のためシングルエンドの実装と、作動構成はどちらもチップ上に実装されており、分解能は 11bit、サンプリングレートは 3MHz である。また、チップ全体の制御回路と差動チャネルの減算回路は論理合成により実装されている。

EMS のテスト環境を図 3.6、に示す。テストチップに対して RF 電磁波は Wi-Fi 用のアンテナから放出される。RF 電磁波は信号発生器 (Signal generator: SG) から、振幅、周波数を設定して生成する方法と、Wi-Fi ルータから放出される電磁波の 2 種類の方法で生成される。このとき、RFSG から放射される信号は単一の周波数を持つ正弦波であり、振幅は 0dBm 15dBm の範囲で設定する。RFSG とアンテナの間には 3dB のアテネータが挿入されているため、アンテナには-3dBm 12dBm の信号が導入される。Wi-Fi ルータからは、IEEE802.11b に基づいた、2.4GHz-2.5GHz の周波数帯域の信号が発振される。

ADC の制御回路の操作は、FPGA 上に実装された通信回路を通じて行う。同様に、ADC の出力コードは FPGA 上の受信回路によって取得され、オシロスコープと PC にストックされる。アンテナとテストチップ間の距離はポジショナーを通じて調整可能であり、テストチップ近傍の電解及び磁界はプローブによって計測されている。テストチップは回路が形成されている面を上側に向けており、ボードに直接ボンディングされている。このため、テストチップ上の回路はアンテナから放射される電磁波に直接曝露する。

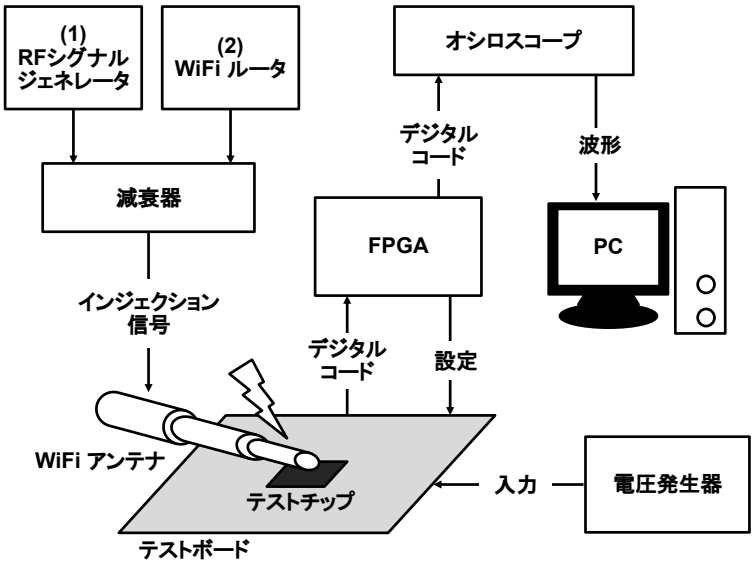

図 3.6: 実験環境のブロック図

3.5　実験評価結果

3.5.1　シングルエンド型 ADC への注入同期

本項では、シングルエンド型 ADC に対して、RF 信号発生器と、Wi-Fi ルータから発生する信号を照射した場合の ADC の出力を示す。3.7 は、EMI 照射なしの場合と、RF 信号発生器で生成した EMI 照射下の場合におけるシングルエンド型 VCO-based ADC の出力コードである。ADC の入力電圧は 0.6V-0.8V の範囲で掃引しており、この時の VCO の発振周波数はおよそ 2.1GHz(0.8V 時) から 3.0GHz(0.6V 時) まで推移する。電磁波照射が無い場合、ADC は VCO の発振周波数に対応したコードを出力するが、十分な大きさの電磁波の照射を受けると、注入同期現象によって、電磁波の周波数 F_{EMI} に対応した一定のコードを出力する様子が確認できる。尚、F_{EMI} が 2.4GHz の場合と、2.5GHz の場合で出力値が影響を受ける範囲が異なるが、これは EMI 照射に利用したアンテナとして Wi-Fi ルータに利用されるダイポールアンテナの特性上、2.4GHz 場合の利得が 2.5GHz の場合よりも大きい事に起因すると考えられる。

図 3.8 は、Wi-Fi ルータからの出力を直接アンテナに入力した場合の ADC の出力である。このとき、信号に対して増幅や減衰などは行っていない。ここで、Wi-Fi ルータの信号の中心周波数は 2.44GHz であり、信

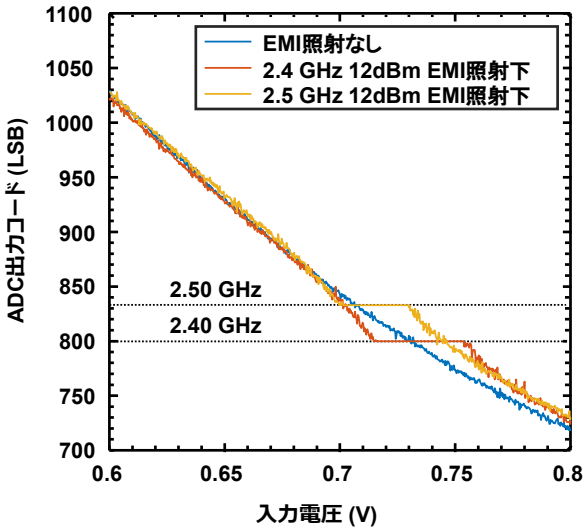

図 3.7: 信号発生器からの信号注入

号は間欠的に生成される。この場合でも、VCO は Wi-Fi ルータの放射に併せて間欠的に誘引されており、ADC の出力に影響を与えている。したがって、Wi-Fi のように環境中に存在する電磁波程度の強度であっても、VCO-based ADC におけるエラーコード出力の原因となりうる。

実験環境において、VCO が影響を受ける入力電圧の範囲とアンテナに与える電力の対応を図 3.9 に示す。灰色の範囲では、周波数が同期することによって、照射した電磁波の周波数 F_{EMI} に応じた値が出力される。また、アンテナに入力する信号の振幅 P_{in} が大きくなるほど ADC 近傍に強い電磁界が発生し、出力コードに影響を与える範囲が広くなることが示されている。

3.5.2 線形性への影響評価

EMS による ADC の線形性への影響を調べるため、ADC の SNDR を測定した。本研究で用いた VCO-based ADC は 0.50V から 0.65V の範囲で線形に応答し、入力がそれより大きくなると線形領域から逸脱する。この線形領域の中心付近である 0.56V 入力時には、VCO はおよそ 3.3GHz で発振する。

図は、この線形領域において、電磁波照射がない場合と、RF 信号発生器から 3.3GHz, 15dBm の信号を照射した際の ADC 出力の周波数スペク

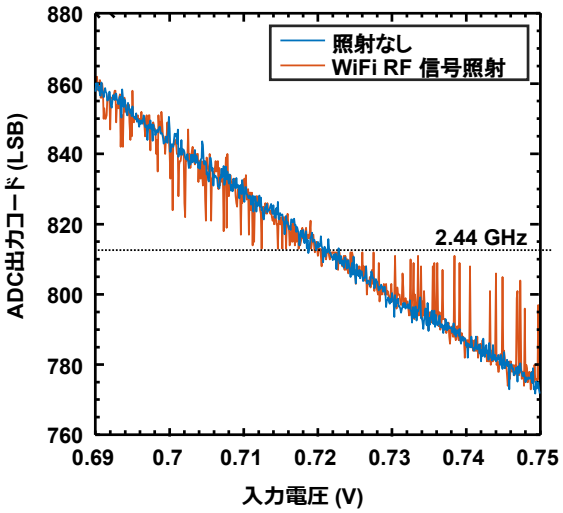

図 3.8: Wi-Fi ルータからの信号注入

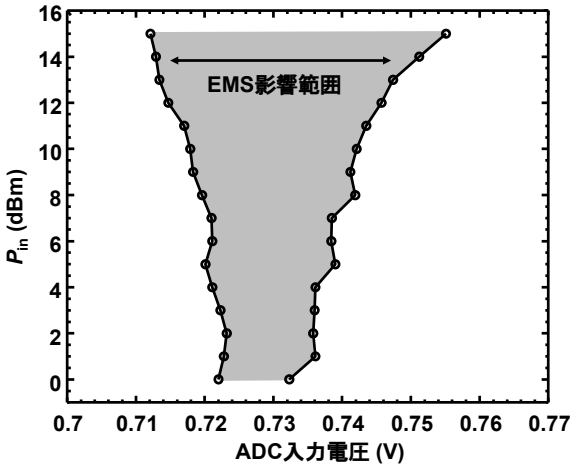

図 3.9: 注入信号強度とロックレンジの範囲

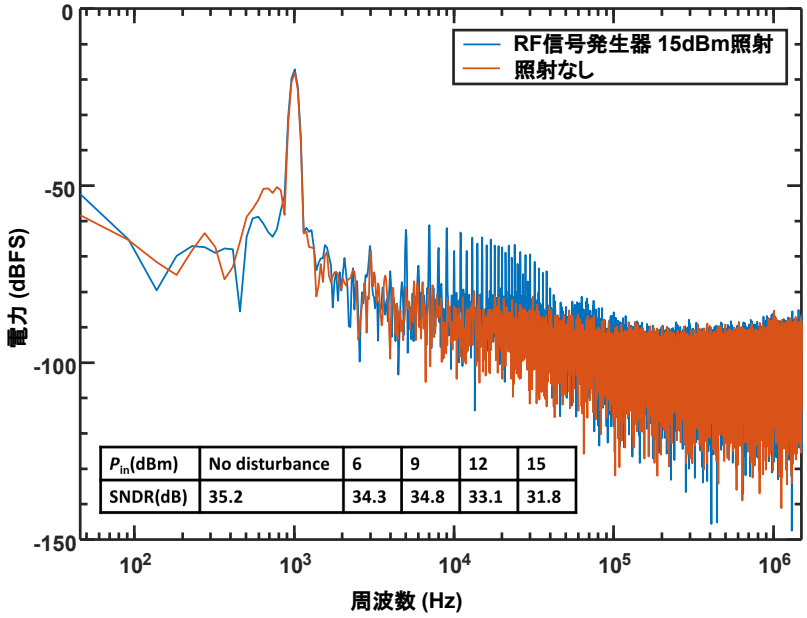

図 3.10: 擾乱環境下での線形性評価

トラムである。このとき、入力信号は線形領域である 0.50V から 0.65V におけるフルスケールの振幅をもつ、1kHz の正弦波であり、ADC 出力の周波数スペクトラムは、広い周波数帯域で入力信号である 1kHz の高調波成分を示している。ADC の SNDR は電磁波照射が無い場合は 35.2dB だが、電磁波照射を与えた場合 31.8dB と、およそ 3dB 減少し、電磁波照射が ADC の性能に大きな影響を与えている。

3.5.3 差動 ADC への影響評価

図 3.11 は疑似差動 ADC における実験結果である。上段の出力コードは下段に示す P-Path と N-path の出力の差分である。P-path と N-path の出力もそれぞれ測定され、図 3.11 下図に示されている。

作動構造に対して、P-path と N-path は (b) 下に示す通り、同じ入力に対して同じ周波数、同じ振幅の RF 照射によって、入力電圧の影響範囲の異なる範囲でそれぞれ個別に周波数が固定される。このため、作動出力も外乱の影響をうけ、(b) 上の図のように、応答にゆがみが生じる。すなわち、作動信号を構成する各経路で EMS の影響範囲が異なるため差動回路構成では完全に EMS の影響を防げないことが示された。

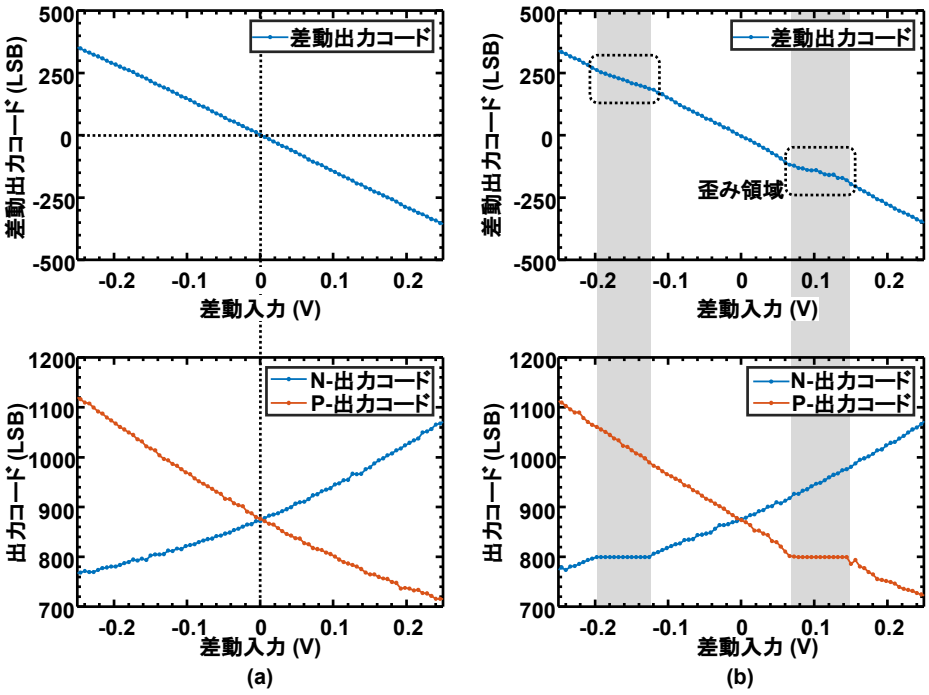

図 3.11: 作動構成 ADC への EMS 影響

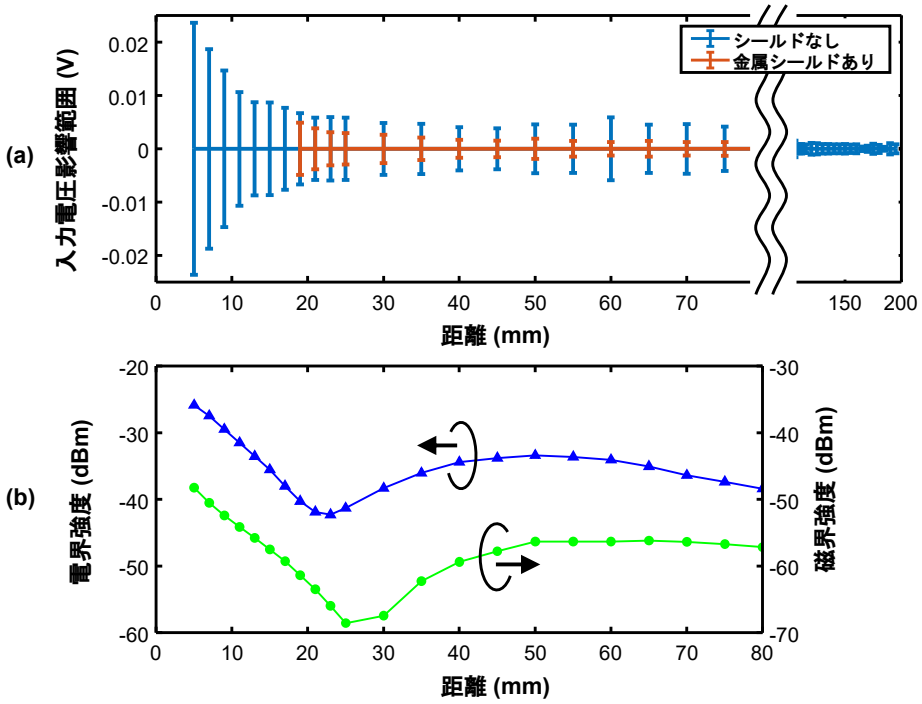

図 3.12: 距離とロックレンジの関係

3.5.4 結合モードの評価

EMI 照射によるテストデバイス上の結合モードを評価するために、アンテナとテストデバイスの距離を変えながら、電磁場の強さ注入同期が起こる範囲の関係を測定した、図 3.12(a) は、横軸のアンテナ-テストデバイスの距離の時に、信号出力が 12dBm、F_{EMI} が 2.4GHz の EMI 信号を照射した際に、信号同期が発生した入力電圧の V_{in} の範囲である。このとき、アンテナとテストデバイスの距離は 20mm 以上離れても VCO ベースの ADC の EMS を示している。

電界と磁界の強度はそれぞれ図 3.12(b) で測定され、電界、磁界の両方がアンテナの近傍界において強く現れていることを示している。尚、波長の 2 倍以上の距離 (125mm) の遠方界での測定により、電界プローバの測定利得は磁界プローバより 20dB 相対的に小さいことが予備的に確認されている。

測定結果より、一般に電磁界強度が強いほど同期する入力電圧範囲が広くなることが分かる。同様の測定はテストチップの領域を除いて テストデバイスボード上の情報 15mm の位置の金属シールドで覆われている

場合にも評価され、図3.12(a)の赤色のバーで示されている。18mm以上の距離で赤のバーと青のバーを比較すると、入力電圧の影響範囲はシールドがあるほど早く減衰していることが確認できる。このことは、テストボード上にもカップリングしている部分があることを示しているが、その寄与はテストチップ上のVCO-based ADC回路への直接的なカップリングよりも弱いことを示している。

3.5.5　実験評価結果のまとめ

本節では、実際にVCO-base ADCテストデバイスを作成し、3.3節において提案したEMSの実機評価を行い、シングルエンド型の場合においては値の直接的な変更及び、変換処理の線形性の減衰が確認された。また、作動構成における影響を確認した。

検証の結果、本章の評価において、VCO-based ADCのEMSを利用してADCの出力コードに影響を与えうることを示した。本章の評価では、無線LANの電波にもVCO-based ADCは感度を示しており、実環境中に普遍的に存在する電磁波に対しても本章で指摘する影響が発生するものと考えられる。

3.6　サイバー攻撃への応用と対策技術の考察

本研究では、特定の周波数において、十分な強度の信号が照射された場合、VCO-based ADCの出力を操作しうることを示した。これを応用して、VCO-based ADCに対して十分な強度でインジェクションロックを発生させられる場合、図3.13のように、所望の出力結果を周波数領域で変調することにより、任意の出力結果をADCに出力させる攻撃が想定される。この攻撃を実行する際に、攻撃装置としてに必要なものは、攻撃周波数に対応するアンテナ、任意信号を周波数変調するVCO回路、攻撃信号を高精度に増幅する増幅器である。攻撃の精度を問題としない場合は専門的な装置など必要なく、どれも比較的容易に入手できるものであり、安価に実行される可能性がある。

電磁界を経由して回路に攻撃を与える手法には、暗号回路に対する故障注入攻撃が挙げられており、この故障注入攻撃への対策は、本節で指摘した脆弱性に対しても有効だと考えられる。先行研究では電磁界攻撃をセンサーにより検知する手法などが提案されている[53]。

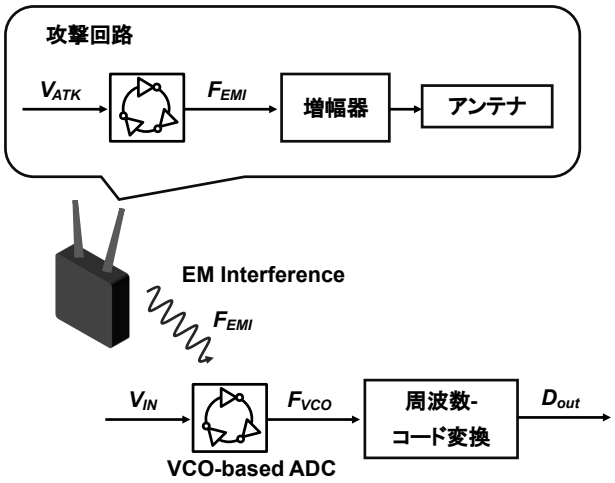

図 3.13: ADC への脅威モデル

一方で、発振器に対して周波数を注入する攻撃は、本章で示した電磁界での結合に限らず、回路に結合する経路すべてにおいて発生しうる。実際に、スマートカードの電源を経由して内部のリングオシレータの周波数を固定することで、スマートカードの IC 内の真正乱数生成器への攻撃が可能であることが先行研究で実証されている。

よって、本節で指摘する脆弱性には、電磁界に限らず、電源、参照電圧、バイアス電圧、アナログ信号の入力などのような攻撃チャネルが想定され、これらの攻撃チャネルを攻撃者に利用させない対策が求められる。具体的には、電源やバイアス電圧 はチップ内部のレギュレータで生成することで直接外部に露出させず、アナログ信号の入力のような外部に露出せざるを得ない端子にはフィルタ回路を搭載するなど、攻撃に利用される信号を遮断することが望ましい。

3.7 まとめ

本章では、VCO-based ADC における EMS の評価を通じて、外界からの電磁波照射によって ADC の出力を固定できることを示した。VCO-Based ADC の発振周波数が既知である場合、本研究で示された脆弱性を利用することで、攻撃者は ADC の出力を任意の値に操作できる他、環境中に存在する Wi-Fi などの電磁波にも影響を受けうるため、セキュリティ上、本脆弱性への対策を考慮した設計は重要である。電磁波照射を利用する他

のハードウェア攻撃の先行研究における知見を適用することで、対策は可能であると考えられるが、一方で、電磁波以外の攻撃チャネルもあり得ることから、VCOへの結合チャネルを慎重に検討する必要がある。

第4章

制御システム向けセキュリティソリューションの事業化

4.1 はじめに

本章では、暗号機能が十分でない既存のシステムにおけるセキュリティを向上させる「コネクターシステム」のシステムインテグレータ事業を提案する。提案事業は製造業やインフラ事業者で利用される制御システムにおいて、IoTやDXの導入に伴い情報化する制御システムにおけるセキュリティ上の課題を解決することを目的としている。

本章で説明するコネクターシステムは、既存の情報/制御システムに暗号通信機能を外付けすることにより、既存システム自体に変更を加えずにセキュリティ機能を向上させるシステムである。コネクターシステムを利用することで、利用期間中にセキュリティ機能が古くなってしまった機材や、性能上の制約によりシステム中の機器が暗号機能に対応できない課題を解決し、既存のシステムの構成を変更することなく、セキュリティを向上させる。

本章で述べる具体的な事業戦略、技術戦略、知財戦略、財務戦略の内容は、神戸大学大学院科学技術イノベーション研究科の取り組みである「イノベーション・ストラテジー研究」において、別紙の「イノベーション・ストラテジー研究成果書」としてまとめた。本書では、別紙記載の詳細には述べず、その概要のみ説明する。

4.2 事業化の背景

1970年代以降、電子工学や情報工学の発展によって様々な情報を電子的に扱うことが可能になり、電子化された情報はコンピュータを使って日常的にやり取りされるようになった。この動きはIT革命あるいは第三次産業革命と呼ばれ、社会に大きな利益を生むと同時に、情報の取り扱

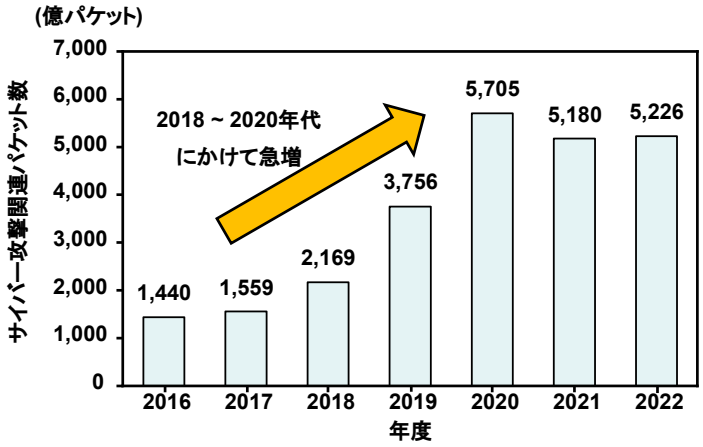

図 4.1: 攻撃関連パケット数の推移 [54]

いの不備による機密情報の流出や、電子情報の不正利用により利益を得るサイバー攻撃のような、新たな社会問題をもたらした。

現在の情報システムのセキュリティを保つ上で、サイバー攻撃への対策を行うことは必要不可欠である。ごく初期のサイバー攻撃はホームページを改ざんするなど、技術力の誇示やいたずらを目的にした被害の小さいものだったが、コンピュータの商用利用の普及や攻撃者の能力の向上に伴い、様々な個人や企業に対して、大きな被害を伴うサイバー攻撃が出現している。例えば、企業や病院などのネットワークに侵入し、情報を利用不能にした上で、元の状態に戻すために身代金を要求するランサムウェアは、情報システムを利用する事業者にとって今日大きな経営リスクである。

また、サイバー攻撃を行う人物、団体による活動は年ごとに活発化している。国立研究開発法人情報通信研究機構 (National Institute of Information and Communications Technology: NICT) では無差別型サイバー攻撃の動向を観測・分析するために NICTER と呼ばれるシステムが運用されている。図 4.1 は NICTER 観測レポート 2022 より作成した、NICTER で 1 年間に観測されたサイバー攻撃関連の通信数である [54]。2018 年から 2020 年にかけてサイバー攻撃関連通信数は急増しており、2020 年に一旦ピークを迎えたものの、2022 年には 5226 億パケットものサイバー攻撃関連の通信が計測された。これは、世界でインターネットに公開されている IP アドレス 1 件あたりに平均して、 年間 183 万回攻撃関連のパケットが送信されている事に相当する。

サイバー攻撃の脅威は、一般的な情報システムのみならず、製造業における生産設備などの機械設備を制御する制御システムにも拡大している。1970 年代以降、制御システムの運用効率の向上や省人化を目的として、制御システムにおいても電子化が進み、マイコンや PLC (Programmable Logic Controller) のような電子的な制御装置が導入された。更に、コンピュータの利用が一般的になると、制御システム中に産業用コンピュータのような情報機器が導入されるようになり、2010 年代以後は IoT 機器や AI による更なる情報化が進みつつある。

制御システムは物理的な設備を制御する性質上、運用面や技術面において一般的な情報システムとは異なる特徴を有する。表 4.1 は、IPA による「制御システム利用者のための脆弱性対応ガイド 第 3 版」[55] より作成した制御システムと一般的な情報システムの技術的特徴比較した表である。例えば、情報システムは不具合や利用状況によってシステム全体を停止することが運用上想定されるが、制御システムの多くは 24 時間 365 日稼働することを前提として作られており、メンテナンス時を除いて基本的に停止することを想定していない。また、情報システムの機材の耐用年数は数年程度に設定されていることがほとんどだが、制御システムに用いられる機材の多くは耐用年数が 10 年から 20 年程度に設定されており、システム全体が 10 年以上に渡って稼働し続ける。通信プロトコルにおいても、情報ネットワークでは高速通信を重視した IP 通信による通信がデファクト・スタンダードとして浸透しているが、制御システムではアナログ通信やシリアル通信ベースの通信プロトコルなど、信頼性を重視したさまざまな通信プロトコルが混在している。このように、制御システムは一般的な情報システムと比べて長期間の安定動作と安全性を求める傾向にあり、情報システムと比べて更新の頻度が低い特徴がある。

従来の制御システムでは、制御系ネットワークに対するサイバー攻撃のリスクは低く、比較的安全だと考えられてきた。しかし、前項で述べたように、情報系ネットワークと制御系ネットワークは混在化しており、制御系ネットワーク上にあるコンピュータであっても、一般的な情報系ネットワークと同様のセキュリティリスクに晒されるようになった。一般的な情報システムがサイバー攻撃を受けた場合、情報の盗難やランサムウェアによるシステムの停止など、情報資産に関する被害が発生するが、特に制御システムにおいては情報システムが受ける被害に加えて、不正操作による生産の停止、情報盗聴による機密情報の漏洩、施設への物理的な被害、製造中に用いる危険な物質の漏洩、周囲の環境への被害、緊急

表 4.1: 制御システムと情報システムの特徴の比較 [55] を元に作成

	制御システム	情報システム
セキュリティの優先順位	システムの継続を優先	情報漏洩の防止を優先
セキュリティの対象	モノ (設備、製品) サービス (連続稼働)	情報
技術のサポート期間	10 年〜20 年	3〜5 年
求められる可用性	24 時間 365 日の安定稼働	再起動は許容範囲
運用管理	現場技術部門	情報システム部門

停止などセーフティ手順の発動、温度や薬品の混合率など製造パラメータの不正変更による製品品質の低下など、様々な形での被害が想定されており、一般的な情報システムに比べてリスクが大きいと言える。

実際に制御システムに対するサイバー攻撃は多大な被害をもたらしている。トレンドマイクロ社が日本と米国、ドイツの製造や電力、石油、ガス業界の法人に行った「産業制御システムのサイバーセキュリティ実態調査」によると、調査対象のいずれの国においても 9 割以上の企業がサイバー攻撃による工場操業停止などの被害経験があり、特に同調査において、産業用制御システムの中断を経験した日本企業においては、平均損害額は年間約 2 億 6906 万円にのぼるとされている [56]。

上記で述べたように近年、サイバー攻撃が活発化しており、セキュリティ対策を確保することは企業にとって経営上の重大な課題となっている。また、情報化が進んだ制御システムにおいてもセキュリティ対策の重要性は増している。制御システムでは一般的な情報システムと比べてシステム上求められる要素に特徴があり、特にサイバー攻撃を受けた場合の被害額や被害の形態において重大な損害を招きやすい。

4.3 イノベーションアイデア

4.3.1 コネクターシステムの事業化アイデアの概要

制御システムにおいては、導入後の時間経過や環境の変化によってセキュリティサポートが無くなった「レガシー機器」や、低性能の IoT デバイスや組み込み機器のように、セキュリティ機能が十分でない機器の利用によって、安全なシステムの運用に求められるセキュリティ要件に対応できない課題が存在する。この課題は、制御システムを運用する事業者に対して、サイバー攻撃を受けるリスクや顧客が要求するセキュリティ水準を満たせないために起こる機会損失などのように、様々な形の損害をもたらす。この課題はレガシー機器などの脆弱なデバイスを新しい機器に入れ替えることで解決されるが、制御システムはシステムの安定稼働が優先される事が多く、機器の更新によるシステムの不安定化への懸念などから、頻繁な機材の更新は避けられる傾向にある。

本書では上記で定義した課題に対し、通信経路上に暗号回路を外挿することで、セキュリティ性能の向上を成立させる「コネクターシステム」を開発し、コネクターシステムを顧客の制御システムに導入するシステムインテグレータ事業について考察する。コネクターシステムを利用することによって、機器自体の更新を行わないままに、セキュリティだけを向上させることが可能である。

本事業における顧客の候補は、保有する制御システムの環境中にレガシー機器や IoT 機器などセキュリティ上脆弱なデバイスを多く含むと考えられる、製造業、病院、研究機関、インフラ分野などの事業者である。それぞれの業界において規模や個別の状況に差異は存在するものの、これらの業界における制御システムは共通して上述したセキュリティ上の課題を有すると考えられる。本事業では、コネクターシステムの導入により、この課題を解決することを提案する。

4.3.2 顧客が持つセキュリティ上の課題

近年、制御システムは「スマート化」やデジタルトランスフォーメーション (Digital Transformation: DX) のような社会的な必要性から、外部環境と接続する機会や必要性が増加しており、これまでより厳格なセキュリティ対策が必要とされている。ここで、図 4.2 に示すように、制御システムにおいてはシステム更新の困難性や、暗号機能が使えないデバイス

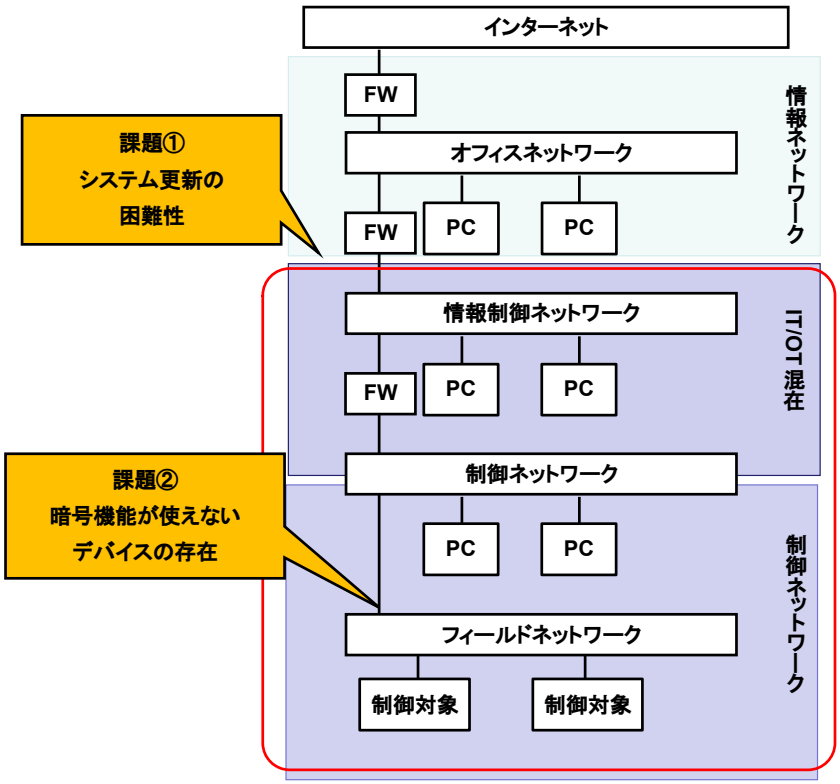

図 4.2: 制御システムにおけるセキュリティ上の課題

の存在が、セキュリティ対策を導入する上での課題となる。

本節では、制御システムが抱えるシステム更新の困難性に関する課題と、システム中に使われる機材の暗号処理能力上の課題についてそれぞれ説明する。

システム更新の困難性に関する課題　情報システムにおいてセキュリティを維持するためには、セキュリティ上の環境に合わせたシステムの更新が必要不可欠である。例えば、個人用コンピュータの基本ソフトウェア (Operating System: OS) として広く利用されている Windows では、セキュリティ上の脆弱性が見つかると、これに対応するために Windows Update と呼ばれるオンラインの更新システムによって修正プログラムを配布している。

しかし、制御システムにおいてはセキュリティ上のリスクに対応するためのシステムの更新、あるいは変更が困難な場合がある。特に主たる要因として、制御システムは可用性を重視し、24 時間 365 日の稼働を求

められることと、セキュリティ更新の方策がそもそも存在しないことの2点が挙げられる。第一に、制御システムは生産ラインやインフラ設備の運用を管理するため、常に稼働していることが求められる。このため、機材やサービスの停止や中断、すなわち、ダウンタイムの発生が許容されない場合が多い。例えば、製造業における生産ラインでダウンタイムが発生し、生産量が計画より大幅に下回ると、後続の生産設備の稼働状況や、サプライチェーン全体に影響を及ぼし、大きな損失が発生する可能性がある。第二に、制御システムに使われる機材は、セキュリティのサポートが既に切れており、更新が不可能な場合がある。このようなセキュリティサポートの切れた機材をレガシー機器という。制御システムに使われる機器は、その機器が運用上価値を持ちうる年数に対して、セキュリティ上のサポート期間が短いことが多い。つまり、セキュリティ上のサポートと、機器本来の有用性自体には直接の関係はなく、セキュリティが切れたとしても、機材をそのまま利用し続けることがある。

このように、制御システムでは、機材の停止及び機材の更新自体が避けられる要因があり、システムの保守や頻繁な更新が困難であるため、新しく発生したセキュリティリスクに対応できないことが課題である。

暗号処理能力上の課題 暗号技術とは、通信や保存中のデータに関するセキュリティリスク対策の基礎的な技術である。例えば、情報の機密性を高める暗号化や、真正性を保証するデジタル署名は暗号技術によって実装される。暗号技術を応用することで、情報の秘匿や、完全性、真正性の保証など、様々なセキュリティ機能を実現できるが、平文を通信する場合に比べて、暗号処理を行う時間のオーバーヘッドや、処理を実行するためのCPU、メモリ性能が要求される。

制御システムに接続される機器の中には、IoTデバイスや、組み込み機器のように、CPUの性能やメモリの容量に制約があり、高度な暗号機能を実行できない課題がある。近年のセキュリティでは、特に計算機資源を要求される公開鍵暗号の実施が求められるため、これらの機能を備えない場合、十分なセキュリティが確保できない可能性がある。

また、制御システムにおいて、末端の機材が接続される制御ネットワークでは、一部に暗号機能を搭載しない専用の通信プロトコルが用いられる。このような通信プロトコルは、通信が決められた時間範囲内に到達するリアルタイム性や、通信内容が欠落しない信頼性などが要件として求められており、これらの要件を満たすRS-232CやRS-422のようなシリアル

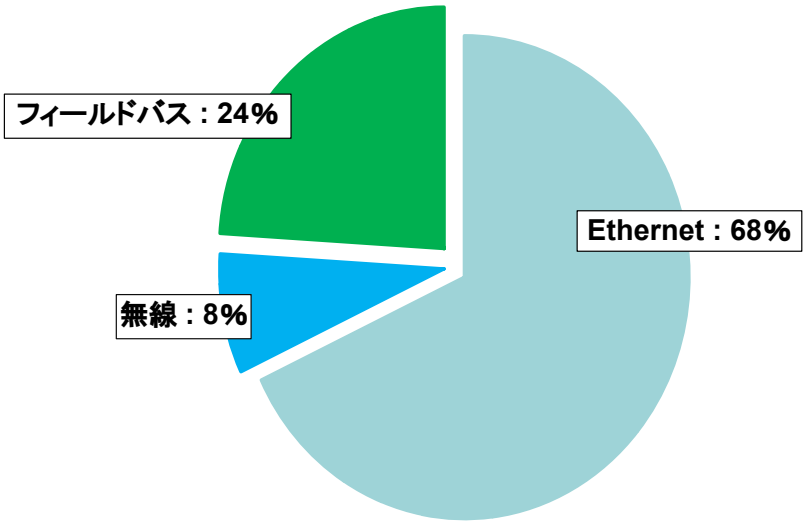

図 4.3: 産業用ネットワークの市場シェア ([57] より作成)

通信規格を物理層に持つフィールドバスが使われてきた。図 4.3 は HMS インダストリアルネットワークス社が毎年公開している「産業用ネットワーク市場シェア動向」[57] の 2022 年版より作成した近年の産業用ネットワークシェアの推移である。同様のレポートは 2016 年から公開されており、全体として、フィールドバスの市場全体におけるシェアは縮小傾向にあり、今後は成長率の高い産業用イーサネットや無線がシェアを拡大すると考えられるものの、耐ノイズ性能など、高信頼性が要求される分野ではフィールドバスプロトコルの利用は今後も長期にわたって続くと考えられる。

このように、制御システムにおいては機材の処理能力やプロトコルの制約上、暗号処理能力に乏しい無防備なネットワークが残存している。従来は閉域網での利用がほとんどであったため、リスクは顕在化しにくかったが、これまでも述べてきたように、スマート化や DX に伴う外部接続の増加によって、今後はセキュリティ上の課題が顕在化すると考えられる。よって、フィールドバスを含む産業用ネットワーク上の通信において、セキュリティの高い通信を行うことが必要である。

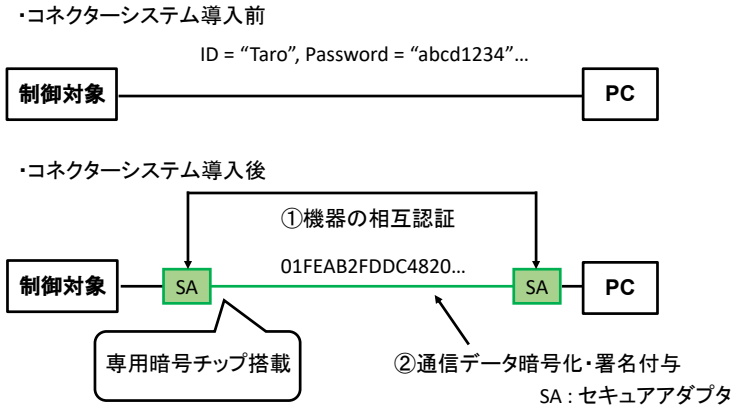

図 4.4: コネクターシステムの構成と機能

4.3.3 コネクターシステムによるセキュリティ課題の解決

コネクターシステムは、制御システムにおけるセキュリティ課題を解決するセキュリティシステムである。図 4.4 に示すように、既存の機器環境に後から「セキュアアダプタ」と呼ばれる機材を接続し、セキュアアダプタ間で暗号通信を行う事で、適用先のセキュリティを向上させることができる。

コネクターシステムによって、システムには機器のすり替えを防ぐ機器認証機能と、通信データに暗号化とデジタル署名を付与する暗号処理機能が提供される。これらの機能によって、セキュリティに関する性能が低い機材であっても、通信内容の盗聴や、通信内容の改ざん、なりすましによる偽装通信のようなサイバー攻撃のリスクを低減することができる。

コネクターシステムの導入に末端機器の直接的な変更は必要なく、暗号処理もセキュアアダプタ内部で完結するため、導入先の機器の計算リソースを一切必要としない。即ち、計算リソースが足りない IoT 機器や、導入から年月の経ったレガシー機器であっても、十分な暗号通信が可能である。また、セキュアアダプタを通過する通信プロトコルには論理的な制限はなく、制御システムで使われる産業用通信プロトコルにおいても、送受信回路の調整によって対応することが可能である。以上の解決方針を表 4.2 に示す通りまとめる。コネクターシステムによって、前節で定義された 2 つの課題である「システム更新に関する課題」及び「暗号処理能力の課題」を解決可能である。

表 4.2: 課題に対するコネクターシステムによる解決方針

課題の概要	解決策
システム更新の困難性	既存の機器の入れ替えなし
暗号機能に対応できない機器	暗号機能を外付け 接続先性能に非依存

4.3.4　コネクターシステムの想定ユースケース

本節では、産業用制御システムにおける一般的なセキュリティリスクについて考察し、コネクターシステムの想定ユースケースを説明する。これまで述べてきたように、産業用制御システムを利用する製造業においては、既存のシステムをできるだけ変更しないことを求められるため、近年発生したセキュリティリスクに対応できないことが課題である。ここでは具体的に、産業用制御システム中に、セキュリティサポートが切れたレガシー機器が存在しており、かつ、暗号通信機能を備えない場合を想定する。

IPA が発行した「スマート工場のセキュリティリスク分析調査」では、無線ネットワークや外部媒体、保守用 PC など様々な経路から第三者が不正接続し、機器を不正操作するリスクを指摘している [58]。仮に、システム内部に侵入を許した場合、通信の盗聴や改ざんによってシステム全体が乗っ取られるセキュリティリスクが存在する。

このようなケースでは通信相手が正規のものであると認証できれば、攻撃のリスクは低減されるが、先述したように、暗号機能の乏しい環境では十分なセキュリティを持つ認証を実施できない。また、仮に暗号通信が利用可能であったとしても、そのハードウェア、またはソフトウェアの実装に脆弱性があると十分なセキュリティ性能を保証できない可能性がある。例えば、Internet Exploler のような古いブラウザソフトをベースに作られたソフトウェアの場合、セキュリティ機能が危殆化、あるいは既知の脆弱性への未対応によって、十分に機能しない可能性がある。ブラウザベースのソフトウェアであれば、ブラウザを新しいものに更新する事も考えられるが、システムベンダの動作保証範囲は開発中に検証したものに限られるなどの事情から、古いブラウザソフトの利用を続けざるを得ない場合もある。

コネクターシステムを利用することで、このようなリスクに対応することが可能である。図 4.5 のように、コネクターシステムを導入すること

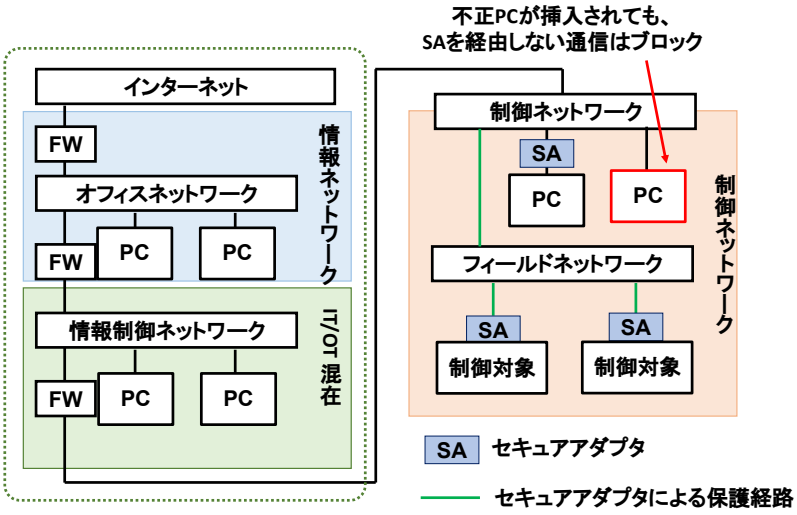

図 4.5: コネクターシステムのユースケース

によって、正当に認められた機器間において、機器認証及び暗号通信を行うことができるようになる。このとき、正当な PC の外からは通信内容は暗号化されて読み取れず、認証されない機器からの通信は廃棄される。よって、仮に制御ネットワーク上や、その上位のシステムに侵入された場合でも、通信内容から機密情報は読み取れず、また、不正な命令の発行の難易度を上げることが可能である。

4.4 事業戦略

4.4.1 事業モデル

図 4.6 に事業モデルの概略を示す。本事業では、顧客である制御システムを管理する事業者に対して、コネクターシステムの導入事業、セキュリティコンサルティング事業、コネクターシステムの保守管理事業の 3 つの事業を行う事により収益を得る。この際、コネクターシステムを構成する機器であるセキュアアダプタや、保守管理やセキュアアダプタの更新に必要な暗号鍵、公開鍵証明書はそれぞれの業務委託先から調達する。セキュアアダプタの製造委託先は、半導体部品を製造する半導体ファウンドリ及び半導体後工程企業と、回路基板や筐体の組み立てを請け負う企業で構成される。暗号鍵と証明書の管理を委託する事業者は、公開鍵

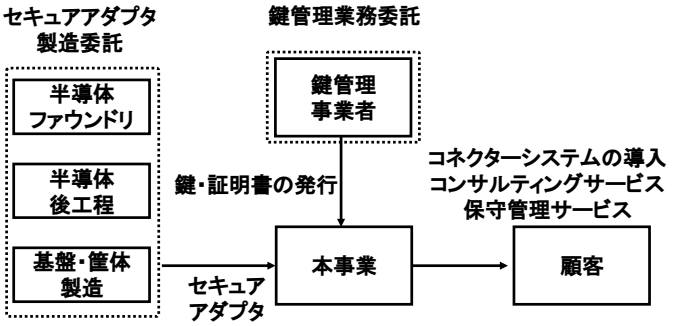

図 4.6: 本事業のモデル

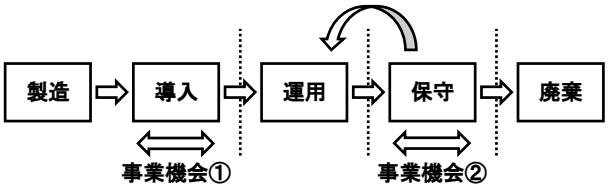

図 4.7: コネクターシステムのライフサイクル

の正当性を担保するプライベート認証局を運営する企業である。

コネクターシステムのライフサイクルは図4.7に示すように、製造、導入、運用、保守、廃棄の5つの段階に分けることができる。本事業では、コネクターシステムのライフサイクルのうち、「導入」と「保守」の段階において事業を実施する。本事業が実施する「導入」の段階は先に挙げたコンサルティング事業とシステムの導入事業に対応し、「保守」の段階は保守管理事業に対応する。「導入」の段階では、本事業は営業活動によって獲得した顧客のシステムに対して、まずセキュリティ上のリスクや脆弱性に関するコンサルティングを行う。この時点で、顧客は自社の脆弱性の情報を知ることができる。コンサルティングの結果、コネクターシステムの導入によって低減できるリスクが発見された場合、コネクターシステム導入の実施計画を顧客に提案し、顧客の環境に導入する。「保守」の段階では、既に顧客環境に導入されたコネクターシステムに必要な保守管理、または顧客システムの更新に合わせたシステムの再構築を実施する。

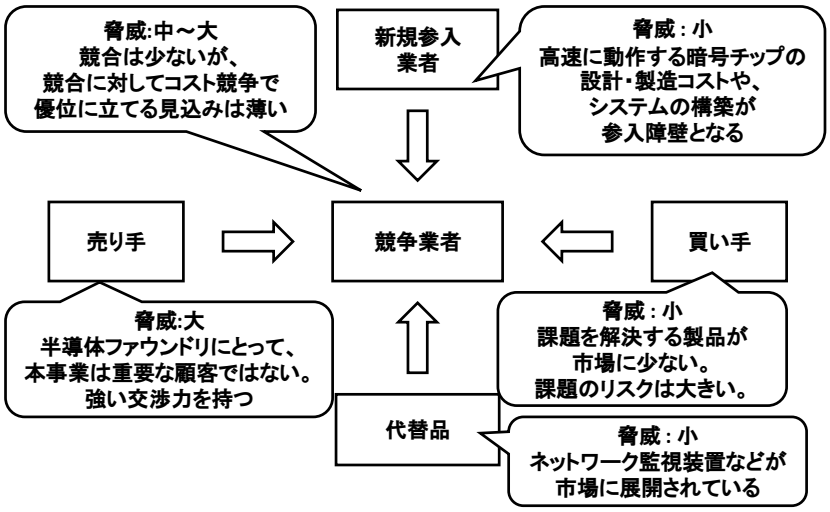

図 4.8: ファイブ・フォース分析の結果

4.4.2 業界環境分析

本事業が取る戦略を決定するため、コネクターシステムが属する業界に関するファイブ・フォース分析による業界環境部分析を行う。分析の結果、業界内の競争、売り手の交渉力が強いことが分かった。

まず、分析の前提として、本事業の競争業者は、「レガシー機器や産業用通信プロトコルに対するセキュリティリスクを低減する」「システム内部の設備の入れ替えを行う必要がない」機能を持つ商品を提供する業者を想定する。社で構成される業界を想定する。尚、制御システム向けのファイアウォールや侵入検知システムなど、その他の制御システム向けセキュリティソリューション製品は上記の性質に合致せず、「レガシー機器をそのまま使用し続けつつ、セキュリティを確保する」という工場のセキュリティ課題を解決しないため、直接の競争業者とはみなさず、代替品を提供する業者として考察する。図 4.8 は本節のファイブ・フォース分析をまとめた図である。以下、それぞれの要素について詳細を記載する。

4.4.2.1 新規参入の脅威

レガシー機器を含む制御システムのセキュリティ業界について、新規参入の脅威を評価する。レガシー機器に対してセキュリティを施す場合、我々が提案するコネクターシステムのようにセキュリティ機能を外挿する必要があり、ハードウェアや鍵管理を伴う事業はセキュリティ標準の

認証試験やセキュアなハードウェア及びソフトウェア開発に数年程度の開発期間と、チップ製造に関する費用として数億円程度の巨額の投資を要する。また、外付けデバイス同士で相互に認証を行う仕組みを構成するには、既に鍵運用の実績のある公開鍵認証局と協業しての技術開発が必要である。以上のように、複数の参入障壁があることから、新規参入の脅威は小さいと評価できる。

4.4.2.2　売り手の交渉力

本事業では、売り手に相当するものが 3 つ挙げられる。それぞれについて記述する。 全体として、売り手の交渉力は中程度から強いと評価される。

半導体前工程/後工程　半導体ファウンドリから本事業への交渉力は強いと考えられる。 半導体ファウンドリの生産能力は現在世界的に逼迫している状況である他、ファウンドリは非常に多様な顧客を持つ。 現在、一部プロセスの需要は緩みつつあるが、依然としてパワー半導体やマイコンなどの一部製品の不足は続き、本事業で利用するプロセスの供給も限られる可能性がある 。一方で、本事業からの発注は小規模であり、ファウンドリから見た顧客としての重要度は高くない。 本事業で使用する半導体プロセスは特に先端である必要はなく、TSMC など最先端装置を有するファウンドリ以外の選択肢も存在するが、TSMC 以外での発注では試作品を製造する段階で、試作の結果にかかわらず量産に移行する条項や、契約後も製造ラインを維持するために１年ごとに一定数の生産ノルマを課されるなど、強い交渉力を背景とした要求が想定される。

回路実装、筐体組み立て　回路実装、箱体組み立て業者から本事業への交渉力は弱いと考えられる。回路実装の発注先は多くの選択肢が存在し、業界内での競争は激しいものと考えられる。筐体組み立ても同様である。

鍵管理　コネクターシステムで扱う暗号鍵は、信頼できる鍵管理システムから発行される鍵を利用しなければならない。鍵、証明書を発行するシステム、すなわち認証局の機能は、本事業が信用できる機関であれば問題ないため、自社で用意することも、他社が提供するシステムを利用することも可能である。自社でシステムを運用する場合、コスト上のメリットが得られる。一方、クラウドベースの認証局を利用することで、認証局

運営に関する信頼性の担保や漏洩時のリスク管理などの面で優位性がある。本事業では信頼面を優先し、クラウドベースの認証局を利用すると仮定する。クラウドベースのプライベート認証局サービスは中程度の競争環境にあり、国際的には DigiCert, Comodo CA, Global Sign, GoDaddy, Asseco Data Systems などが主要なプレーヤーである。国内でもセコム、富士通、東芝、NTT、凸版印刷など、多数の業者がサービスを展開しているものの、提供する機能自体に大きな差は無く、企業の信用や価格によって競争が展開されている。以上のように、自社運用の選択肢が存在することや、プライベート認証局サービス市場の競争環境から、売り手としての認証局の交渉力は弱いと考えられる。

4.4.2.3 買い手の交渉力

買い手はレガシー機器を含む制御システムを運用し、セキュリティ機能に課題意識のある事業者と定義される。具体的には製造業における工場システムや、病院の医療機器、研究に関わる計測システムなどを運用する主体である。以下の要因から、買い手の交渉力は弱いものと考えられる。まず、レガシー機器は実環境に大量に存在し、セキュリティ上の脆弱性になりやすいが、出口対策セキュリティとして、レガシー機器に対応する製品は市場に少ない。また、買い手は工場や医療現場が想定されるが、いずれの環境でも高いセキュリティ要件が求められると想定される。工場ではヒアリングにより、発注元からデータの取り扱いについてセキュリティ対策を行うように要求があり、そのためのガイドラインや規格が公開されている

4.4.2.4 代替品の脅威

代替品としては以下のような運用や製品が想定されるが、いずれもレガシー機器のセキュリティ上の課題を解決しない。よって、代替品の脅威は弱いと考える。

スタンドアロン運用 外部ネットワークから完全に切り離し、単独の機材として運用する方法をスタンドアロン運用という。サイバー攻撃対策としてはネットワークを通じての侵入が不可能であるため、セキュリティ上有効な対策ではあるが、一方で運用上の利便性は極めて低い。運用効率の面で機会損失を発生させ、実質的なコストが発生する機材では取りにくい対策であり、代替品の脅威は小さい。

従来型の境界型セキュリティ　外部ネットワークと内部ネットワークのセキュリティポリシーを厳密かつ強固にすることで、内部ネットワークを安全な領域と見做す、従来から行なわれてきたセキュリティ方式である。“内部”と“外部”を厳密に区別し、厳密かつ適切に運用する限りにおいて、典型的なサイバー攻撃のほとんどは防御できる。一方で、近年の業務システムはクラウドシフトによって外部サービスを多く利用すること、リモートワークなどに代表されるシステムへの正規の外部アクセスの増加、サイバー攻撃の高度化によって境界防御を原則的に運用することが難しくなってきている。また、APT 攻撃のように、高度化したサイバー攻撃への対応が難しいことも指摘されている。よって、本書で指摘する事業課題の解決にはなりえず、代替品としての脅威は小さい。

レガシー機材の入れ替え　レガシー機器の取り扱いをやめ、ゼロトラストアーキテクチャなど、今後デファクト・スタンダードとなるセキュリティ対策を組み込んだネットワークを新規に構築することは、コネクターシステムを導入することの代替となりうる。本来行うべき理想的なセキュリティ対策であるが、イノベーションアイデアの章で述べたようにコストが大きくなるため、本対策を制御システムで行うことは一般的に困難と考えられる。よって、代替品の脅威としては小さい。

4.4.2.5　業界内の競争

競合の数として、定義を満たす製品は少ないが、セキュリティ大手のグループから製品が発売されており、グループ内全体で最適化されたバリューチェーンやブランド力に由来する価格競争力は強力と考えられる。また、システム自体の性能や販売面で優位に立つのは難しい。このため、業界内の競争の力は強く、業界内で優位性を得るための戦略を構築する必要があると考えられる。

4.4.2.6　ファイブ・フォース分析からの洞察

ファイブ・フォース分析から、新規参入の脅威、買い手の交渉力、代替品の脅威は弱いが、売り手の交渉力と業界内での競争は強く、対応が必要であると考えられる。以下では、売り手の交渉力への対応と、業界内での競争への対応について考察する。

売り手の交渉力への対応 半導体チップを製造する半導体ファウンドリはコネクターシステムの重要部品である ASIC の製造を委託する。本事業で想定する ASIC は、性能上の理由から数世代前のプロセスを想定しており、複数の事業者で製造可能である。一般的に半導体の試作を依頼する場合、試作のみではなくその後の量産製造を行うように要求されるほか、量産移行後は年間製造数のノルマが存在し、ノルマが達成されなかった場合製造終了となる。

対応策としては、製造プロセスを下げ、要求に対応できる製造業者の選択肢を増やすことや、代替品として FPGA (Field Programmable Gate Array) を最終製品に継続的に利用し、ファウンドリとの直接的な取引を避けることが考えられる。

業界内の競争への対応 業界内の競争で優位性を持つための戦略として、コストリーダーシップ戦略と、差別化戦略、集中戦略の 3 つの戦略を取りうると言われている。業界内の競合企業に対して、コスト面で優位性を獲得するのは困難である。また、コネクターシステムには、適用先のネットワークのプロトコルに依存しないという特徴がある。従って、対応可能なプロトコルを拡大し、コネクターシステムでのみ対応可能な顧客に注力する差別化集中戦略をとることで、業界内での競争に対応することが可能だと考える。

4.4.3 競争戦略の選択

競合製品のセキュリティ対象となる通信は一般的にオフィス向けネットワークでも利用される、IP 通信 / Ethernet でデータ通信に利用される TCP/UDP 通信ベースの通信に限定されている。一方で、図 4.4 で示したように、制御システムで使われるネットワーク環境は産業用 Ethernet(66 %)、無線 (7 %)、フィールドバス (27 %) に分かれる。図 4.9 は主な制御システム用プロトコルにおける IP フレーム利用の分類である。

Ethernet/IP(シェア 17 %) や PROFINET(シェア 17 %) など、産業用 Ethernet のほとんどは TCP/UDP ベースの通信を行うため、Cythemis による通信の保護が可能である。 一方で、EtherCAT(シェア 11 %)、 CC-Link IE Field(2 %)、またフィールドバス規格全般は TCP/UDP を利用しない通信であり、競合製品の仕様では保護は難しいと考えられる。

よって、コネクターシステムでは非 IP 通信やフィールドバスに対応することによって技術的な差別化を行うことが可能である。まず、初期の事

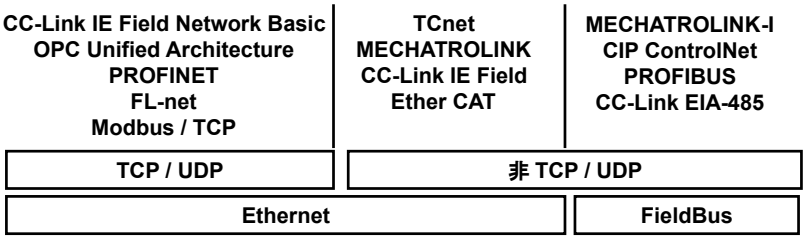

図 4.9: 産業用プロトコルの分類

業ではターゲットとなる市場において、PoC を実施することでレガシー機器に対する効果的なセキュリティソリューションとしてコネクターシステムを認知させることを目指す。特に非 TCP/UDP の通信セグメントで差別化が有効であれば、早期の普及を目指し、市場でのシェアを獲得することによって非 TCP/UDP におけるセキュリティ対策としてのデファクト・スタンダードとなりうる。また、TCP/UDP 通信市場と、非 TCP/UDP 通信市場の境界にある市場として、両通信の混在市場が存在する。混在市場において、セキュリティリスクへの対策を非 TCP/UDP 通信と TCP/UDP 通信において統一的に導入したい場合、コネクターシステムは両方の通信に対応できるため、この市場の顧客も獲得可能である。混在市場において、TCP/UDP 通信におけるコネクターシステム導入のモデルケースを創出することで、より市場の大きい分野の顧客にも営業の拡大が可能になると考えられる。

4.5　コネクターシステムの実装上の課題と技術戦略

本事業における製品であるコネクターシステムのハードウェア筐体であるセキュアアダプタは、顧客環境に配置し、運用することを想定している。このため、IoT 機器と同様に、悪意ある攻撃者がハードウェア攻撃を実施する可能性が想定される。

セキュアアダプタのハードウェア構成は、主として外部通信回路からの信号を受け取る送受信回路及び、専用の ASIC による暗号計算回路である。よって、プロービングによる情報収集や、暗号回路に対するサイドチャネル攻撃、物理信号受信回路における ADC に対するハードウェア攻撃が想定される。

本稿２章で議論したように、プロービングによる情報収集への対策として、システムを単体のICチップに集積実装する方法が有効である。また、サイドチャネル攻撃には暗号回路の論理層や物理層において、先行研究で報告されるサイドチャネル攻撃対策技術を実装することで対応する[59]。ADCにおいても、第1章で議論した攻撃可能性や先行研究や、第4章で提示した攻撃可能性が指摘されており、ADCの実装によって個別に対策が必要である。

4.6 まとめ

本章では、制御システムにおける２つの課題である、システム更新上の課題と、暗号処理能力の課題を解決する「コネクターシステム」を提案し、コネクターシステムのシステムインテグレータ事業について市場分析と、事業戦略の分析を行った。本章の詳細は、別紙の「イノベーション・ストラテジー研究成果書」としてまとめている。

本事業に使用するチップはフィールド上で攻撃者の手に渡る可能性があるため、物理的な解析に対して耐性を持つ必要がある。第二章、第三章で述べたシグナルチェーン上のセキュリティ技術は、攻撃者の解析に対抗するための技術として利用することができ、コネクターシステム上のチップにも有用である。

第5章

結論

CPS や IoT のような、フィジカル空間とサイバー空間をつなぐシステムを通して、様々な情報がやり取りされる社会が実現しつつある。このような社会において、安全に情報を利活用するためにセキュリティ技術が活用されているが、サイバー攻撃の手法は日々高度化、複雑化しており、その対策技術の開発は社会にますます求められるようになった。

IoT デバイスが普及するに従い、センサーデバイスが過去に類を見ない速度で社会に浸透していく状況で、従来のデジタルデータに対するセキュリティ対策だけではなく、アナログ信号処理を含む信号処理全体に対するサイバー攻撃リスクが高まりつつあることが指摘されている。CPS や IoT のようなシステムは、自動車やドローンのような自立移動体や、インフラ設備のような重要度の高いシステムにおいても利用されるようになりつつあり、セキュリティ技術によるリスク対応の重要性は高い。

本論文では、IoT デバイスでは、攻撃者がサンプルを手に入れやすいという前提のもと、プロービングと ADC に対する攻撃の 2 種類のハードウェア攻撃リスクに対して議論した。

第二章では、FOWLP のテストデバイスの内部電位を測定し、LSC がパッケージ内部の ASIC の電源品質・信号品質に与える影響の評価を行った。また、評価結果から得られた知見を電源設計を応用し、プロービング攻撃やサイドチャネル攻撃のようなハードウェア攻撃に対して、先端パッケージング技術を用いることで秘匿しうる情報について考察した。FOWLP のような MCM を利用することで、ボードレベルのシステムをチップレベルに集積化し、信号の観測を困難にする一方で、電源のような外部に接続せざるを得ない端子などからのサイドチャネル攻撃から守ることのできる情報の別について考察した。

更に、第三章では、アナログ信号処理系におけるセキュリティリスクについて実機を用いた解析を行い、セキュリティリスクへの対策について考察した。VCO-based ADC においては、VCO に対して電磁波を経由してインジェクションロックを発生させることで、デジタルコードを ADC に出力させることが可能なことを実証した。この攻撃は、与える電磁波

の周波数を変更することで所望の値を出力させることが可能であり、セキュリティ上重大な脆弱性となりうる。先行研究では、暗号回路を対象として、電磁波を用いた故障注入攻撃への対策として、回路やパッケージにセンサを搭載することで攻撃を検知する手法が提案されており、本研究で提案した ADC に対する攻撃に対しても、同様の手法の応用を提案している。

第四章では、これらの技術を適用しうるシステムとして、セキュリティシステムである「コネクターシステム」への信号処理チップに第二章、第三章の技術の適用について議論した。コネクターシステムは製造業などの制御システムで課題となる、セキュリティ更新上の課題と、暗号処理能力上の課題を解決可能なシステムである。本論文の２章、３章で議論した内容は、コネクターシステム上におけるシグナルチェーン上の脆弱性に対応するために適用可能な技術であり、これらの技術は事業計画の一部として活用される。

本論文では、以上で述べたように、シグナルチェーンにおける信号処理と通信のセキュリティを確保する上で考察すべき課題について議論した。本論文で議論された以外にも、様々なハードウェア実装上の脆弱性を利用したハードウェア攻撃は多数報告されており、本論文の内容は、先行研究に対して相補的な内容を提供するものである。本研究を含め、多様な観点からシグナルチェーンのセキュリティリスクを低減することで、より安全なデバイスの構築技術の議論が可能となると考えられる。

謝辞

本研究を遂行するにあたり、多くの方々に御指導、御協力いただきましたことに心より感謝申し上げます。

本研究の機会を与えて頂き，終始適切な御助言を賜りました神戸大学大学院科学技術イノベーション研究科・永田真教授に深く感謝致します. 本研究を通じて、多くの貴重な経験を得ることができましたことを心より感謝いたします。

本研究に関し，熱心に御指導いただきました神戸大学大学院科学技術イノベーション研究科・三木拓司 准教授に深く感謝致します。

本研究を進めるにあたり，終始熱心な御指導を賜りました神戸大学大学院科学技術イノベーション研究科・福家信洋准教授に心より感謝致します。

日頃よりお世話になり、半導体チップの実装技術に関して様々なご助言を頂きました科学技術イノベーション研究科、沖殿貴朗研究員に深く感謝致します。

研究活動の機会を頂いた、株式会社村田製作所の葛西亮氏、田中大介氏、三原恭次氏、牧田和推氏、村上嘉英氏ならびに、産業技術総合研究所の島本晴夫氏、荒賀佑樹氏、渡辺直也氏に感謝いたします。

本研究に関し、適切な御指導、御助言を頂きました大阪大学大学院情報科学研究科・三浦典之教授に深く感謝致します。

本研究室での日々の生活を快適に過ごせるよう、事務・会計処理など細やかな配慮をしていただきました、田中路氏、山崎美喜氏に感謝致します。

日頃よりお世話になり、様々な観点からご意見をいただきました神戸大学大学院科学技術イノベーション研究科・門田和樹氏、同研究科、永田研究室卒業生の渡邊航氏に深く感謝致します。

永田研究室、科学技術イノベーション研究科の皆様ならびに関係者の方々に感謝致します。

最後に、私をここまで育ててくださいました両親に心より感謝致します。

参考文献

[1] 総務省, “Iot 利用環境構築事例集,” 2021, https://www.soumu.go.jp/main_content/000750546.pdf.

[2] 総務省, “令和 4 年版 情報通信白書,” 2022, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/.

[3] 藤本大介, “センサの計測過程におけるセキュリティ,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 13, No. 2, pp. 142–150, 2019.

[4] I. Giechaskiel and K. Rasmussen, “Taxonomy and challenges of out-of-band signal injection attacks and defenses,” *IEEE Communications Surveys and Tutorials*, Vol. 22, No. 1, pp. 645–670, 2020.

[5] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking drones with intentional sound noise on gyroscopic sensors,” in *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC’15, p. 881–896, USA, 2015, USENIX Association.

[6] B.S. Lim, S.L. Keoh, and V.L.L. Thing, “Autonomous vehicle ultrasonic sensor vulnerability and impact assessment,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 231–236, Feb. 2018.

[7] 健人水田, 拓司三木, 典之三浦, 真永田, “センサー mcu の ad 変換器を悪用したアナログ情報漏洩・改竄攻撃,,” 電子情報通信学会総合大会,, No. A-20-1, Mar. 2019.

[8] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, “A random interrupt dithering sar technique for secure adc against reference-charge side-channel attack,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 67, No. 1, pp. 14–18, 2020.

[9] D. Boneh, R.A. DeMillo, and R.J. Lipton, “On the importance of checking cryptographic protocols for faults,” W. Fumy, editor, in *Advances in*

Cryptology — EUROCRYPT '97, pp. 37–51, Berlin, Heidelberg, 1997, Springer Berlin Heidelberg.

[10] E. Levy, A. Shabtai, B. Groza, P.S. Murvay, and Y. Elovici, "Can-loc: Spoofing detection and physical intrusion localization on an in-vehicle can bus based on deep features of voltage signals," July, 2021.

[11] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for ic chip level hardware security," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 30, No. 1, pp. 5–14, 2022.

[12] 松本勉, "実装攻撃に対抗する耐タンパー技術の動向," 情報処理, Vol. 49(7), pp. 799–809, July. 2008.

[13] J.J. P. Kocher and B. Jun, "Differential power analysis," in *Advances in Cryptology - CRYPTO '99*, Vol. 1666, pp. 338–397, Aug. 1999.

[14] P. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology - CRYPTO '96*, Vol. 1109, pp. 104–113, Aug. 1996.

[15] H. Wang, D. Forte, M.M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test*, Vol. 34, No. 5, pp. 63–71, 2017.

[16] S. Skorobogatov, "The bumpy road towards iphone 5c nand mirroring," 2016.

[17] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.C. Souriau, G. Simon, and A. Merle, "A novel structure for backside protection against physical attacks on secure chips or sip," in *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*, pp. 515–520, 2018.

[18] T. Miki, M. Nagata, H. Sonoda, N. Miura, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, and K. Kikuchi, "Si-backside protection circuits against physical security attacks on flip-chip devices," *IEEE Journal of Solid-State Circuits*, Vol. 55, No. 10, pp. 2747–2755, 2020.

[19] S. Thirunakkarasu and B. Bakkaloglu, "Built-in self-calibration and digital-trim technique for 14-bit sar adcs achieving ± 1 lsb inl," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 23, No. 5, pp. 916–925, 2015.

[20] Y. Nitta, Y. Muramatsu, K. Amano, T. Toyama, JunYamamoto, K. Mishina, A. Suzuki, T. Taura, A. Kato, M. Kikuchi, Y. Yasui, H. Nomura, and N. Fukushima, "High-speed digital double sampling with analog cds on column parallel adc architecture for low-noise active pixel sensor," in *2006 IEEE International Solid State Circuits Conference - Digest of Technical Papers*, pp. 2024–2031, 2006.

[21] H. Totsuka, T. Tsuboi, T. Muto, D. Yoshida, Y. Matsuno, M. Ohmura, H. Takahashi, K. Sakurai, T. Ichikawa, H. Yuzurihara, and S. Inoue, "6.4 an aps-h-size 250mpixel cmos image sensor using column single-slope adcs with dual-gain amplifiers," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 116–117, 2016.

[22] V.V. Gadde, H. Awano, and M. Ikeda, "An encryption-authentication unified a/d conversion scheme for iot sensor nodes," in *2018 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, pp. 123–126, 2018.

[23] M. Ashok, E.V. Levine, and A.P. Chandrakasan, "Randomized switching sar (rs-sar) adc protections for power and electromagnetic side channel security," in *2022 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–2, 2022.

[24] R. TAKAHASHI, T. MIKI, and M. NAGATA, "An analog side-channel attack on a high-speed asynchronous sar adc using dual neural network technique," *IEICE Transactions on Electronics*, Vol. advpub, p. 2022CTS0002, 2023.

[25] D.F. Kune, J. Backes, S.S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*, pp. 145–159, 2013.

[26] I. Giechaskiel, Y. Zhang, and K.B. Rasmussen, "A framework for evaluating security in the presence of signal injection attacks," In *Lecture*

Notes in Computer Science, pp. 512–532, Springer International Publishing, 2019.

[27] S. Kennedy, M.R. Yuce, and J.M. Redouté, "Susceptibility of flash adcs to electromagnetic interference," *Microelectronics Reliability*, Vol. 81, pp. 218–225, 2018.

[28] M. Ashok, E.V. Levine, and A.P. Chandrakasan, "Randomized switching sar (rs-sar) adc for power and em side-channel security," *IEEE Solid-State Circuits Letters*, Vol. 5, pp. 247–250, 2022.

[29] I. Savidis, S. Kose, and E.G. Friedman, "Power noise in tsv-based 3-d integrated circuits," *IEEE Journal of Solid-State Circuits*, Vol. 48, No. 2, pp. 587–597, 2013.

[30] J. Roullard, A. Farcy, S. Capraro, T. Lacrevaz, C. Bermond, G. Houzet, J. Charbonnier, C. Fuchs, C. Ferrandon, P. Leduc, and B. Flechet, "Evaluation of 3d interconnect routing and stacking strategy to optimize high speed signal transmission for memory on logic," in *2012 IEEE 62nd Electronic Components and Technology Conference*, pp. 8–13, 2012.

[31] C.T. Wang and D. Yu, "Signal and power integrity analysis on integrated fan-out pop (info_pop) technology for next generation mobile applications," in *2016 IEEE 66th Electronic Components and Technology Conference (ECTC)*, pp. 380–385, 2016.

[32] J. Knickerbocker, C. Patel, P. Andry, C. Tsang, L. Buchwalter, E. Sprogis, H. Gan, R. Horton, R. Polastre, S. Wright, and J. Cotte, "3-d silicon integration and silicon packaging technology using silicon through-vias," *IEEE Journal of Solid-State Circuits*, Vol. 41, No. 8, pp. 1718–1725, 2006.

[33] J. Van Olmen, A. Mercha, G. Katti, C. Huyghebaert, J. Van Aelst, E. Seppala, Z. Chao, S. Armini, J. Vaes, R.C. Teixeira, M. Van Cauwenberghe, P. Verdonck, K. Verhemeldonck, A. Jourdain, W. Ruythooren, M. de Potter de ten Broeck, A. Opdebeeck, T. Chiarella, B. Parvais, I. Debusschere, T. Hoffmann, B. De Wachter, W. Dehaene, M. Stucchi, M. Rakowski, P. Soussan, R. Cartuyvels, E. Beyne, S. Biesemans, and B. Swinnen, "3d stacked ic demonstration using a through silicon via

first approach," in *2008 IEEE International Electron Devices Meeting*, pp. 1–4, 2008.

[34] B. Charlet, L. Di Cioccio, P. Leduc, and D. Henry, "*3D Integration at CEA-LETI*,", chapter 19, pp. 375–392, John Wiley and Sons, Ltd, 2008.

[35] K. Noguchi and M. Nagata, "An on-chip multichannel waveform monitor for diagnosis of systems-on-a-chip integration," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 15, No. 10, pp. 1101–1110, 2007.

[36] T. Hashida and M. Nagata, "An on-chip waveform capturer and application to diagnosis of power delivery in soc integration," *IEEE Journal of Solid-State Circuits*, Vol. 46, No. 4, pp. 789–796, 2011.

[37] A. Murata, S. Agatsuma, D. Ikoma, K. Ichikawa, T. Tsuda, M. Nagata, K. Yoshikawa, Y. Araga, and Y. Harada, "Noise analysis using on-chip waveform monitor in bandgap voltage references," in *2013 9th International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, pp. 226–231, 2013.

[38] K. Taniguchi, M. Nagata, A. Tsukioka, D. Fujimoto, N. Miura, T. Egami, R. Akimoto, K. Niinomi, T. Komatsu, Y. Fukuba, and A. Tomishima, "Susceptibility evaluation of can transceiver circuits with in-place waveform capturing under rf dpi," in *2017 11th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMCCompo)*, pp. 59–63, 2017.

[39] K. Monta, H. Sonoda, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, K. Kikuchi, N. Miura, T. Miki, and M. Nagata, "3-d cmos chip stacking for security ics featuring backside buried metal power delivery networks with distributed capacitance," *IEEE Transactions on Electron Devices*, Vol. 68, No. 4, pp. 2077–2082, 2021.

[40] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda, and M. Nagata, "An intermittent-driven supply-current equalizer for 11x and 4x power-overhead savings in cpa-resistant 128bit aes cryptographic processor," in *2014 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, pp. 225–228, 2014.

[41] C. Tokunaga and D. Blaauw, "Secure aes engine with a local switched-capacitor current equalizer," in *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pp. 64–65,65a, 2009.

[42] M. Hovin, A. Olsen, T. Lande, and C. Toumazou, "Delta-sigma modulators using frequency-modulated intermediate values," *IEEE Journal of Solid-State Circuits*, Vol. 32, No. 1, pp. 13–22, 1997.

[43] R. Muller, S. Gambini, and J.M. Rabaey, "A 0.013mm2 5μw dc-coupled neural signal acquisition ic with 0.5v supply," *2011 IEEE International Solid-State Circuits Conference*, pp. 302–304, 2011.

[44] A. Iwata, N. Sakimura, M. Nagata, and T. Morie, "The architecture of delta sigma analog-to-digital converters using a voltage-controlled oscillator as a multibit quantizer," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 46, No. 7, pp. 941–945, 1999.

[45] J. Huang and P.P. Mercier, "A 112-db sfdr 89-db sndr vco-based sensor front-end enabled by background-calibrated differential pulse code modulation," *IEEE Journal of Solid-State Circuits*, Vol. 56, No. 4, pp. 1046–1057, 2021.

[46] S. Verma, H. Rategh, and T. Lee, "A unified model for injection-locked frequency dividers," *IEEE Journal of Solid-State Circuits*, Vol. 38, No. 6, pp. 1015–1027, 2003.

[47] B. Hong and A. Hajimiri, "A general theory of injection locking and pulling in electrical oscillators—part i: Time-synchronous modeling and injection waveform design," *IEEE Journal of Solid-State Circuits*, Vol. 54, No. 8, pp. 2109–2121, 2019.

[48] J. Lee and H. Wang, "Study of subharmonically injection-locked plls," *IEEE Journal of Solid-State Circuits*, Vol. 44, No. 5, pp. 1539–1553, 2009.

[49] M. Hossain and A.C. Carusone, "Cmos oscillators for clock distribution and injection-locked deskew," *IEEE Journal of Solid-State Circuits*, Vol. 44, No. 8, pp. 2138–2153, 2009.

[50] S. Osuka, D. Fujimoto, Y.i. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Em information security threats against ro-based trngs: The frequency injection attack based on iemi and em information leakage," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 61, No. 4, pp. 1122–1128, 2019.

[51] M. Dumont, M. Lisart, and P. Maurine, "Modeling and simulating electromagnetic fault injection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 40, No. 4, pp. 680–693, 2021.

[52] Y.G. Yoon, M.C. Cho, and S. Cho, "A linearization technique for voltage-controlled oscillator-based adc," in *2009 International SoC Design Conference (ISOCC)*, pp. 317–320, 2009.

[53] N. Homma, Y. ichi Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki, "Em attack is non-invasive? - design methodology and validity verification of em attack sensor," Cryptology ePrint Archive, Paper 2014/541, 2014, https://eprint.iacr.org/2014/541.

[54] 国立研究開発法人情報通信研究機構, "Nicter 観測レポート 2022," 2023, https://csl.nict.go.jp/report/NICTER_report_2022.pdf.

[55] 独立行政法人情報処理推進機構, "制御システム利用者のための脆弱性対応ガイド 第3版," 2017, https://www.ipa.go.jp/security/controlsystem/ssf7ph0000004lud-att/000058489.pdf.

[56] トレンドマイクロ株式会社, "産業向けサイバーセキュリティの実態調査," 2022, https://resources.trendmicro.com/jp-docdownload-form-m484-web-industrial-cybersecurity-survey-report.html.

[57] HMS ネットワークス, "産業用ネットワーク市場シェア動向 2023（hms networks 統計）," 2022, https://www.hms-networks.com/ja/news-and-insights/2023/05/05/industrial-network-market-shares-2023.

[58] 独立行政法人情報処理推進機構, “スマート工場のセキュリティリスク分析調査,” 2022, https://www.ipa.go.jp/security/reports/vuln/ug65p90000019e7c-att/000098863.pdf.

[59] R. Jevtic and M.G. Otero, “Methodology for complete decorrelation of power supply em side-channel signal and sensitive data,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 69, No. 4, pp. 2256–2260, 2022.

発表論文一覧

本研究に関する発表論文

学術雑誌

[1] Hiroki Sonoda, Ryo Kasai, Daisuke Tanaka, Yoshihide Murakami, Kyoshi Mihara, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Takuji Miki, Makoto Nagata, "In-Place Evaluation of Powering and Signaling Within Fan-Out Multiple IC Chip Packaging," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 12, no. 7, pp. 1140-1149, July. 2022.

[2] Hiroki Sonoda, Ryo Kasai, Daisuke Tanaka, Yoshihide Murakami, Kyoshi Mihara, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Takuji Miki, Makoto Nagata, "Measurement of Electromagnetic Field Immunity of Voltage-Controlled Oscillator-Based Analog-to-Digital Converters in 28 nm CMOS Technology," *Japanese Journal of Applied Physics*, Vol. 61, No. SC1045, pp. 1-7, Feb. 2022.

国際会議

[3] Hiroki Sonoda, Makoto Nagata, Daisuke Tanaka, Yoshihide Murakami, Kyoshi Mihara, Kazuo Makida, Katsuya Kikuchi, "In-Place Power Noise and Signal Waveform Measurements on LVDS Channels in Fan-Out Multiple IC Chip Packaging," *International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, pp. 1-3, Oct. 2019.

[4] Hiroki Sonoda, Ryo Kasai, Daisuke Tanaka, Yoshihide Murakami, Kyoshi Mihara, Kazuo Makida, Katsuya Kikuchi, Makoto Nagata, "Power Noise Suppression by Land-Side Capacitors within Fan-Out Multiple IC Chip Packaging," *IEEE International Symposium on Elec-*

tromagnetic Compatibility, Signal & Power Integrity (EMC+SIPI),W3-TU-PM-A1, Aug. 2020. (Virtual conference)

[5] Hiroki Sonoda, Takuji Miki, Makoto Nagata, "Electromagnetic Susceptibility of VCO-based ADC in 28 nm CMOS Technology," *International Conference on Solid State Devices and Materials (SSDM) Extended Abstracts*, L-3-4, pp. 698-699, Sep. 2021.

その他の発表論文

学術雑誌

[6] Yuuki Araga, Ryo Kasai, Daisuke Tanaka, Yoshihide Murakami, Kyoshi Mihara, Kazuo Makida, Hiroki Sonoda, Makoto Nagata, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, "Landside Capacitor Efficacy Among Multi-Chip-Module Using Si-Interposer," *IEICE Electronics Express*, vol.18, no.9, May 2021.

[7] Takuji Miki, Makoto Nagata, Hiroki Sonoda, Noriyuki Miura, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, "Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices," *IEEE Journal of Solid-State Circuits (JSSC)*, vol. 55, no. 10, pp. 2747-2755, Oct. 2020.

[8] Takuji Miki, Noriyuki Miura, Hiroki Sonoda, Kento Mizuta, Makoto Nagata, "A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side-Channel Attack," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp.14-18, Jan. 2020.

国際会議

[9] Takuji Miki, Noriyuki Miura, Hiroki Sonoda, Kento Mizuta, Makoto Nagata, "A Random Interrupt Dithering SAR Technique for Secure ADC against Reference-Charge Side-Channel Attack," *in Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-1, Oct. 2020.

[10] Takuji Miki, Makoto Nagata, Hiroki Sonoda, Noriyuki Miura, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, "A Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices," *in Proceedings of IEEE Asian Solid-State Circuits Conference*, #3-1, pp. 25-28, Nov. 2019.

[11] Hiroki Sonoda, Kazuki Monta, Takaaki Okidono, Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, Katsuya Kikuchi, Noriyuki Miura, Takuji

Miki, Makoto Nagata, "Secure 3D CMOS Chip Stacks with Backside Buried Metal Power Delivery Networks for Distributed Decoupling Capacitance," *in Proceedings of the 66th IEEE International Electron Device Meeting*, #31.5, pp. 1-4, Dec. 2020.

図一覧

表一覧

神戸大学博士論文「シグナルチェーンのセキュリティリスクとその対策技術に関する研究」全91頁
提出日　2023年7月26日
本博士論文が神戸大学機関リポジトリKernelにて掲載される場合、掲載登録日(公開日)はリポジトリの該当ページ上に掲載されます。