令和４年度重要技術管理体制強化事業
安全保障上重要となる機微技術の流出防止に係る調査

調査報告書

2023年2月

一般財団法人 防衛技術協会

報告書の概要

我が国の機微技術の流出を防止するための方策について、ハード、ソフトの両面に関するリバース・エンジニアリング（以下、REと称する。）対策技術に係る調査を行い、最新の国内外のリバース・エンジニアリングの脅威、対策状況等を調査した結果についてまとめた資料である。

２．１　REの脅威

２．１．１　REとRE対策の概要

２．１．２　ハードウェアのRE技術

２．１．３　ソフトウェアのRE技術

２．１．１　REとRE対策の概要

REは、装備品等の複製や模造品の製造、対象装備品等と同等以上の能力を有する装備品等の開発又は対象装備品等の能力の推定や弱点の把握を行うため、**対象となる装備品等及び関連技術に関する重要技術情報を窃取**することである。REで窃取する情報は、ハードウェアとソフトウェアに分類整理する。

REの対象	REで窃取する情報
ハードウェア	形状、成分（濃度分布等）、材質（素材の配合比、結晶粒度、剛性、硬さ、温度特性等）、加工精度、構成機器の配置
	電気的特性（周波数応答、抵抗率、透磁率等）、光学的特性（分光感度、透過率、吸収率、反射率、焦点距離、検知器サイズ、フィルファクター等）
	電子回路パターン等模造のための設計データ及び加工や製造プロセスのためのパラメータ
ソフトウェア	プログラムのオブジェクトコード、各種データ（運用データ、周波数テーブル、制御則のデータ等）

2．1．1　REとRE対策の概要

RE対策は、防護対策の他に攻撃の検知及び攻撃への対処のセットで総合的に備える必要がある。標準的なRE対策は、構成レベル別に取られる。

RE対策は、対象の装備品によって異なるが、ここでは電子機器の例で説明する。

RE

- 非破壊の高精度計測（外部・内部）
- 筐体の破壊、及び内部への物理的侵入による構造解析
- サイドチャネルによる信号解析
- 外部I/Fからの攻撃 信号改竄、プロトコル攻撃、悪意SW挿入による故障/誤動作の誘導
- ソフトウェア解析ツールによる解読等のソフトウェア攻撃
- 内部信号のプロービングによる特性解析

RE対策

レベル	防護	検知、対処
筐体、装置	**開封困難化**（堅牢な素材、ラッピング素材、シールド化）	**開封痕跡**（タンパ検知センサ、攻撃検知履歴）
基板モジュール	**開封困難化**（封印による防護、カプセル化、及び、埋め込み型相互接続） **形状欺瞞**	**開封痕跡**（タンパ検知センサ、IP消去）
部品及び ソフトウェア	**X線透過防止** プログラム変換による**難読化、暗号化**	**開封時破壊**（脅威検知時に重要部品の自己破壊、重要データ消去、IF回路切断、暗号鍵の消去、及び、回路の溶断等）

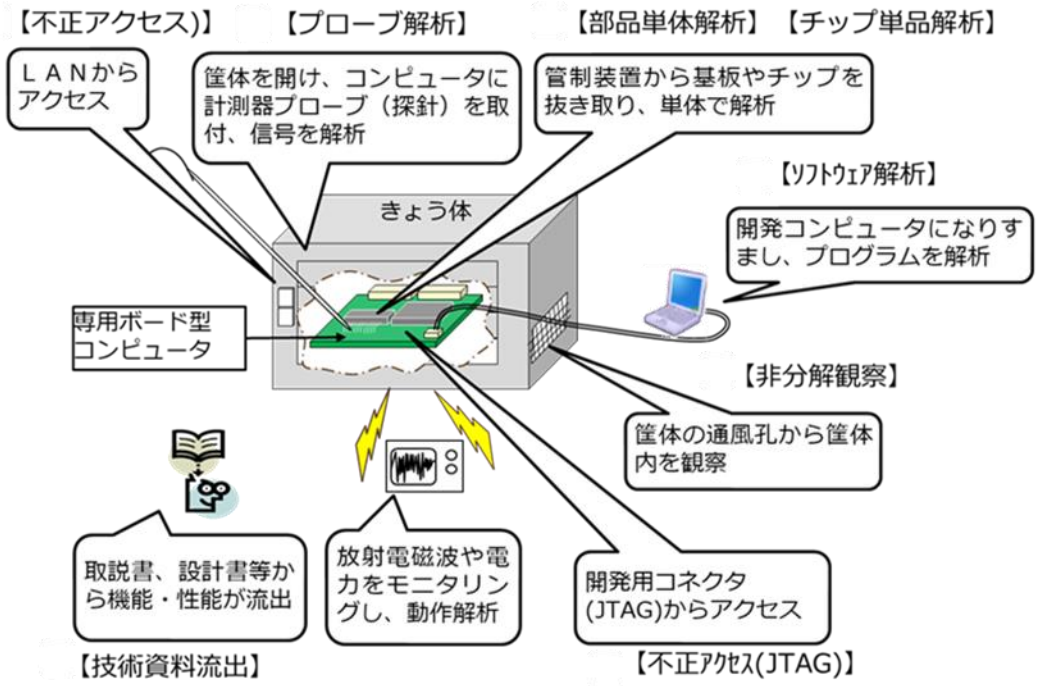
：非破壊
：破壊

２．１．１　REとRE対策の概要

- 装備品等に組み込まれる電子装置等に対するRE例

筐体、基板モジュール、部品・ソフトウェアの順に**外部から内部へ、非破壊高精度計測からプロービング 、分解計測・構造解析等**が行われる。

i. 筐体の分解：制御基板モジュール取り出し等
ii. 制御基板モジュールの非破壊高精度計測：回路配線パターン読み取り等
iii. サイドチャネル攻撃 による信号解析：暗号鍵取得等
iv. ICチップ端子のプロービングによるデータ伝送特性解析：バイナリーデータ取得等
v. ソフトウェア解析ツールによるバイナリーデータ読解：バイナリーデータからソースコード取得



２．１．１　REとRE対策の概要

２．１．２　ハードウェアのRE技術

２．１．３　ソフトウェアのRE技術

２．１．２　ハードウェアのRE技術

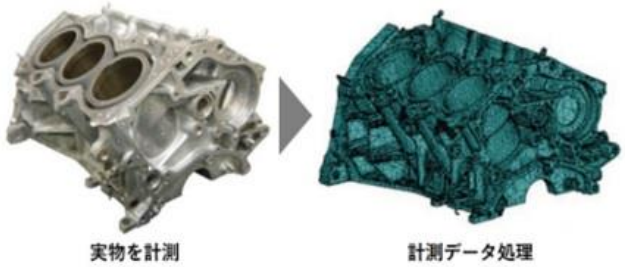
● 技術の概要

- 形状、成分（濃度分布等）、加工精度、材質（素材の配合比、結晶粒度、剛性、硬さ等）、材質の温度特性、電気的特性（周波数応答、抵抗率、透磁率等）、回路パターンなど模造のための設計データ及び加工や製造プロセスのためのパラメータがREのために窃取される。
- 対象となるハードウェアは、装備品等本体及びそれを構成する無線装置や制御用コンピュータ等及び油圧ポンプモータやエンジン等の機械装置、ICチップやトランジスタなどの部品等であり、形状、材質や内部構造などの情報が攻撃の対象となる。
- 形状・構造の分析では、３次元スキャナやX線計測のように**非破壊によるもの**と、研磨や溶解による半導体チップパッケージの開封など**破壊によるもの**とに分けることができる。
- ハードウェアの加工技術・組立て製造のノウハウが反映された精密形状、**構造、素材特性・成分等の技術情報の取得を狙った計測・分析には、汎用製品の設計・製造に使用される各種の計測システムが利用**される。また、**装備品等及び関連技術の能力（機能・性能）や脆弱性の分析にも各種の計測システムが用いられる。**

2．1．2　ハードウェアのRE技術　形状・構造

● 非破壊計測による精密形状・構造の分析（3Dスキャナ）

- 装置表面の形状をタッチセンサーや光の縞模様を投影して精密に計測する技術で、機械部品等を製造している工場で品質管理のため一般的に使用している技術である。



富士テクノリサーチ　リバースエンジニアリングサービス
https://ftr.co.jp/solution/3d-measurement/reverse-engineering/

名称	FARO	EinScan	Inspec
外観			
最適対象サイズ	50~1000mm	30~4000mm	~100mm
精度	0.05mm	0.1mm （ワンショット精度）	0.01mm （ワンショット精度）
光沢面	○	×	×
移動可能	○	○	×
要求設置スペース	150~800mm	無し、ハンディ型	据え置き型

日本3Dプリンタ　3Dリバースエンジニアリング　https://3dprinter.co.jp/product/reverse/

2．1．2　ハードウェアのRE技術　形状・構造

- 非破壊計測による精密形状・構造の分析（X線）

- 透過X線や超音波を用いて、機械部品やコンデンサ等の電子部品や多層プリント基板内部の回路パターンなどを精密に読み取る技術
- 機械部品加工や組立て及び電子部品や電子装置用ボード製造メーカで品質管理用として一般的に用いられている。

X線計測よるスマートフォンの計測例

島津製作所ホームページ
https://www.an.shimadzu.co.jp/apl/electric/device20130723c.htm

２．１．２　ハードウェアのRE技術　形状・構造

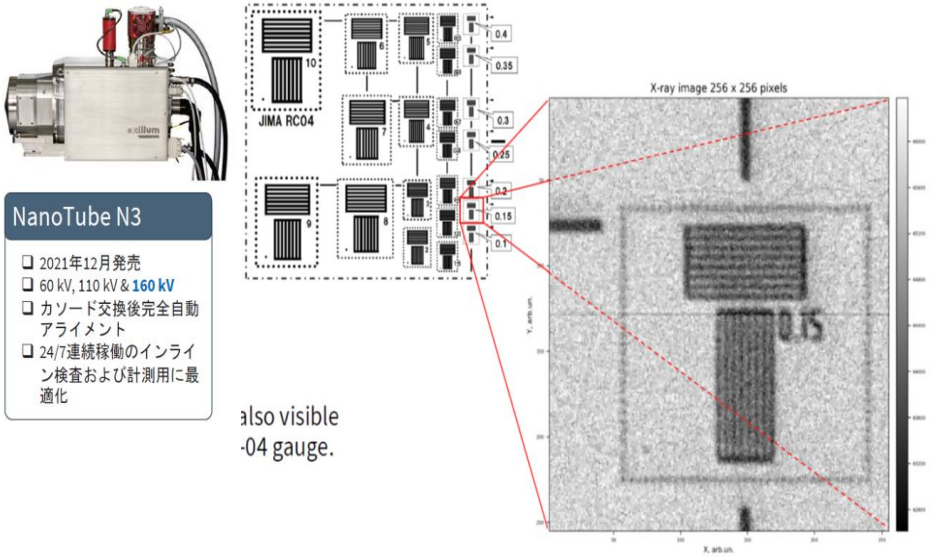
● 非破壊計測による精密形状・構造の分析（X線）

- REに使用可能な最新計測装置
- 高分解能X線透過分析装置：NanoTube N3　(スウェーデン)

民生の品質検査技術や計測技術がRE（攻撃）に利用可能
半導体の構造分析等に使用し製品の品質管理や故障解析に使用する。REツールとして、非破壊で、電子基板、部品、半導体デバイスの構造分析等に使用できる。

（特徴）

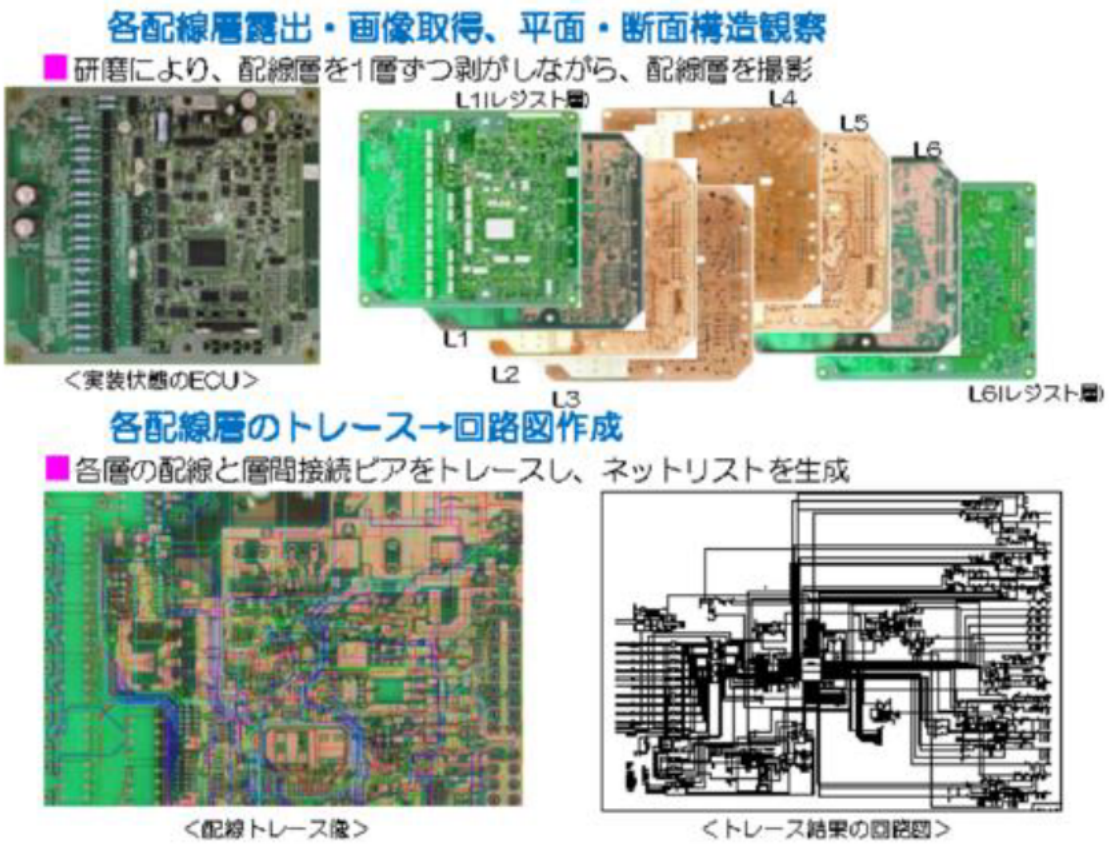
- X線源の電極近くに試料を配置し、X線が拡大発散することを利用して拡大撮像する幾何学的拡大X線撮像システムで分解能150nmを実現している。
- 一般的なX線透過装置の100倍の拡大撮影が可能で高密度化傾向のデバイス情報の取得も可能である。



第11回総合検査機器展（2022.9.14～16）で情報収集

- 破壊による内部構造・部品構成の分析

・プリント回路基板の分析事例



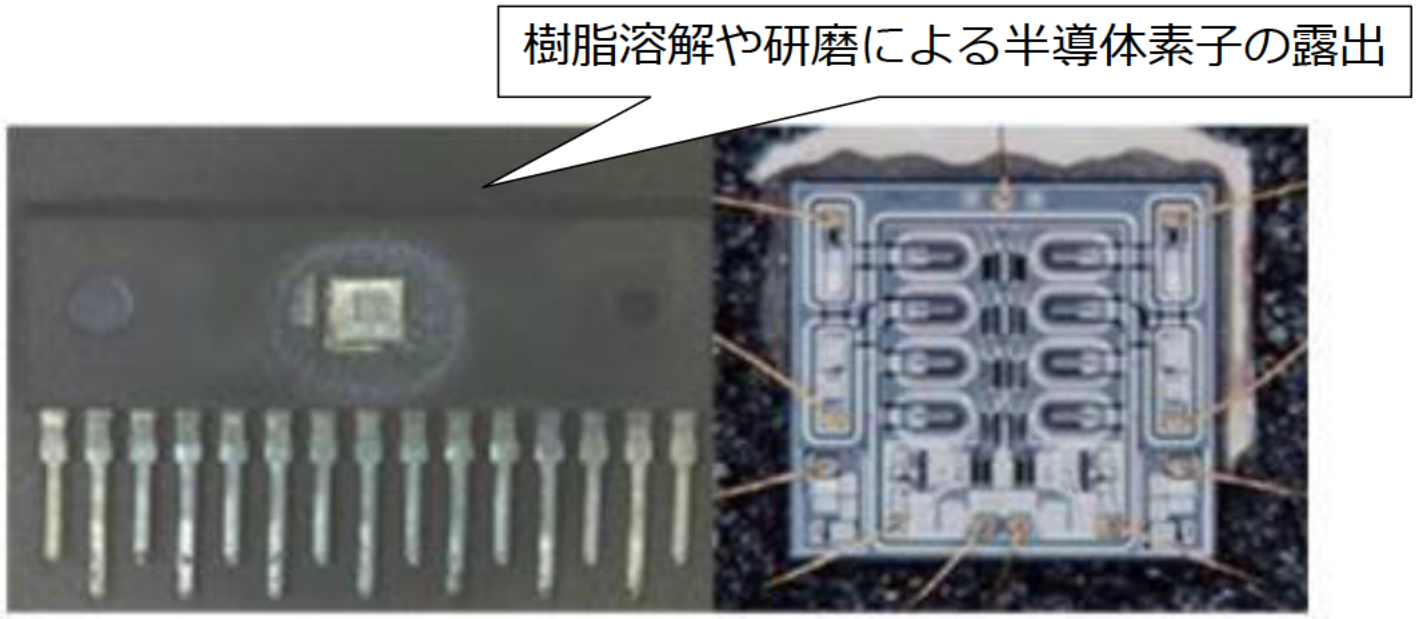
① 実装モジュールの分解調査・放熱構造調査・プリント回路基板材料の熱特性測定

② 実装部品の取り外し・電気測定、データシートの調査、部品表リストの作成

ヴァン･パートナーズ　半導体を解析し特許情報を得るコラボのビジネスモデル
https://www.semiconportal.com/archive/editorial/industry/post-59.html

- 破壊による内部構造・部品構成の分析

- 破壊による内部構造・部品構成の分析、機械部品の内部構造を計測したり、半導体チップのIC回路パターンやトランジスタ構造などを計測したりする技術である。
- 部品加工工場、半導体製造工場及び検査専門会社で品質管理用として一般的に用いられている。



HIC（Hybrid IC）の制御IC部　部分開封事例

パナソニック　半導体の故障解析
https://holdings.panasonic/jp/corporate/pac/electric/design-service/semiconductor.html

２．１．２　ハードウェアのRE技術　部品・構造

- 破壊による内部構造・部品構成の分析　内部分解プロービング解析

・プロービング解析は、ICパッケージの分解・破壊による内部電気信号へのアクセスを前提とした攻撃手段により機能・性能に関する直接的な情報を取得し易いことから、次のような解析が主として行われる可能性が大きい。

- ICパッケージを溶融、研削等の手法により開封し、IC基板を露出した形でIC回路を流れる電気信号を接触又は近接させたプローブ（検出端子）で検出する手法である。
- この解析手法は、ICチップの製造過程における故障解析等に使用されるものである。

半導体の故障解析に用いる電気的マイクロプロービング

MPI Corporation 故障解析
https://www.mpi-corporation.jp/ast/applications/failure-analysis/

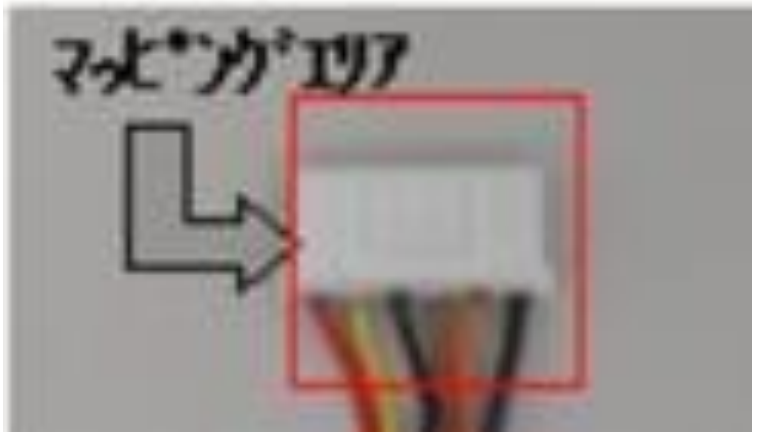
- 素材の特定／成分分析　蛍光Ｘ線分析

- 機械部品の加工組立工場や半導体工場において品質管理に用いられている分析技術で、以下に示す分析を行う。

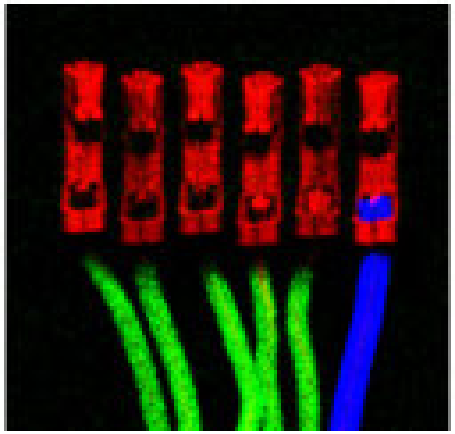
  ① 機械部品に使用されている特殊材料を特定し、成分を取得

  ② パワートランジスタ等の半導体チップの不純物濃度分布等を取得

- 物質に短波長のＸ線を照射すると物質の構成元素に特有の波長を持ったＸ線（蛍光Ｘ線）を放出する。このＸ線の波長や強度を測定することで、物質を構成している元素の種類や濃度を知ることができる。



分析対象のコネクタ



分析結果

赤：　銅
緑：　ニッケル
青：　臭素

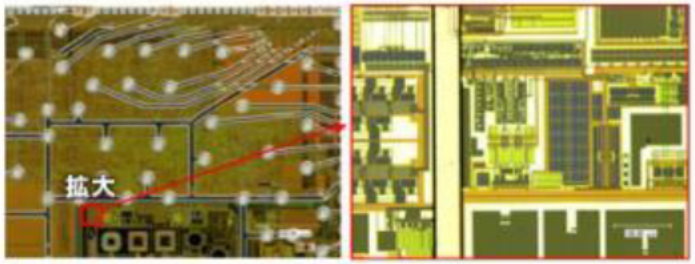
コネクタの蛍光Ｘ線分析の例

日鉄テクノロホームページ 蛍光X線分析装置（XRF）
https://www.nstec.nipponsteel.com/technology/componential/componential09/　）

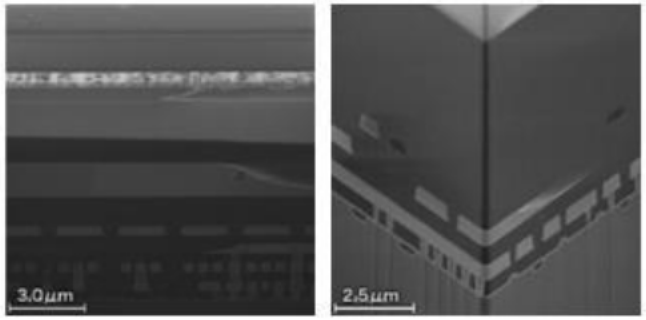
2．1．2　ハードウェアのRE技術　部品・構造

- 電子顕微鏡による構造解析　半導体解析例

• 半導体デバイスは、Si基板上にトランジスタ等の電子回路を形成した複雑な構成となっており、近年、大容量化、サイズの縮小化に伴い、デバイスの微細化が進んでいる。その構造を明確化するため、FIB(Focused Ion Beam：集束イオンビーム加工観察装置) を用いた加工、TEM(Transmission Electron Microscopy：透過型電子顕微鏡)による構造解析をした事例を示す。

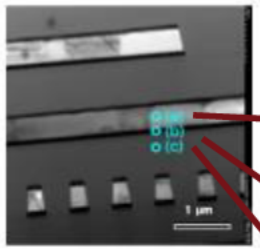


① 光学顕微鏡による半導体構造解析

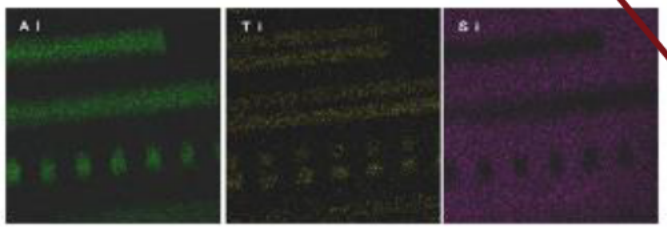


② SIM（Scanning Ion Microscope：走査イオン顕微鏡）による形態観察解析例(断面)

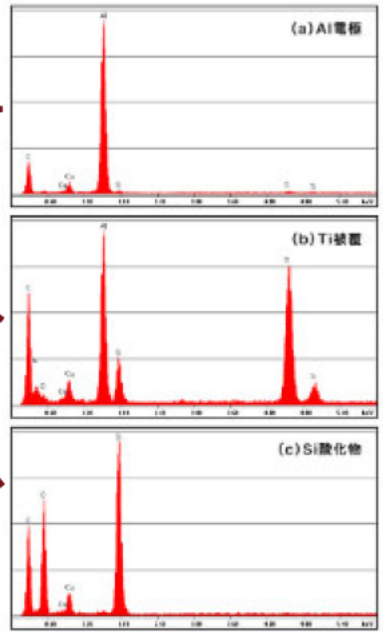
FIB加工により、TEM用薄膜試料を作製後、TEM−EDXにより元素分析（点分析）、元素マッピング分析（面分析）を実施した。



③ 断面観察(TEM像)



④ 元素マッピング分析(面分析）結果
試料面上で電子線プローブの位置情報と特性X線スペクトルを同期させて、二次元の元素分布情報を取得する。



点分析結果（TEM-EDX）

カネカリサーチホームページ
https://www.ktr.co.jp/analysis/case/case_022.html

２．１．１　REとRE対策の概要

２．１．２　ハードウェアのRE技術

２．１．３　ソフトウェアのRE技術

２．１．３　ソフトウェアのRE技術

● REの対象となるソフトウェア

- 装備品等を制御、統制し、通信等を行うための**プログラムとデータがREの対象**になる。これらは通常メモリーチップに格納され、運用時には、CPU等の演算装置とソフトウェアを動作させるFPGA等に格納されたプログラムで実行される。
- プログラムとデータは流出後の不正な解析から保護（防護）するため、暗号化されてメモリに格納されている場合があり、**復号する暗号鍵も攻撃の対象**となる
- ソフトウェアに対するRE手段は、**解析ツール**と**サイドチャネル攻撃**がある。

RE手段	目的	方法
解析ツール	オブジェクトコード・ソフトウェア処理データ等の取得、ソースコード復元解析、プログラム処理構造、アルゴリズムの静的解析及び脆弱性解析、プログラムの暴走を誘発させて内部情報へアクセス	ソフトウェアに対する攻撃方法 ・オブジェクトコード／処理データ取得 ・ソースコード復元解析 ・プログラム処理の静的解析、脆弱性の解析
サイドチャネル攻撃	装置の機能・性能の推定や内部回路動作、内部プログラム処理アルゴリズム、暗号鍵情報等の分析	分析対象の内部信号に直接プロービングできない場合の攻撃 ・放出電波の解析 ・温度・光等のシグネチャ解析 ・外部インタフェース信号の分析 ・プログラム処理への異常電圧印加解析

２．１．３　ソフトウェアのRE技術

● ソフトウェアに対するREの解析ツール

- ソフトウェアの解析ツールは、静的コード解析と動的コード解析の２種類のツールがある。静的コード解析ツールは、実行ファイルを実行することなく解析を行うことできる。
- 動的コード解析ツールは、ソフトウェアを実行して解析を行うツールである。メモリ部品等から獲得したオブジェクトデータからソースコードを復元するツールや静的コード解析／脆弱性解析に使用可能な解析ツールがある。
- 設計自動化ツールと動作計測ツールとの連携により、高度な動的プログラム解析も行われていると考えられる。

RE技術			
RE手法	プログラム実行状態	ツール	
		名称	機能
静的攻撃	休止状態	逆アセンブラ 逆コンパイル	実行プログラムをプログラミング言語に変換
動的攻撃	実行状態	デバッガ＊	プログラム動作中のCPUとメモリの状態を監視・操作
		仮想マシーン	解析対象ソフトウェアとデバッガの動作環境を作る。

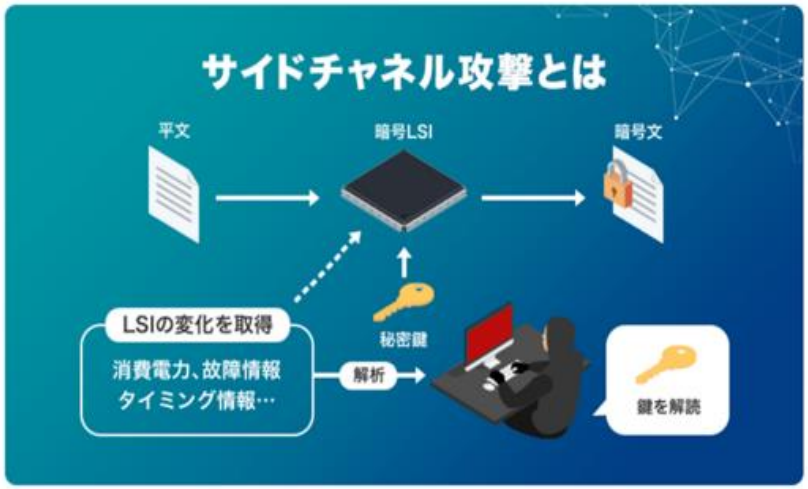
＊：デバッガ：プログラムのバグ（誤りや欠陥）を発見して、それを修正する作業を支援するソフトウェア

２．１．３　ソフトウェアのRE技術

- サイドチャネル攻撃

・サイドチャネル攻撃は、電子機器装置に対するRE攻撃手法の一つである。REの対象とする装置の動作中の物理的な特性の変化を外部から観測・解析することにより、本来読み取ることができない情報を取得する手法である。

サイドチャネル攻撃の**主な対象は、暗号処理機能を組み込んだ半導体製品等**である。これらの機器の内部で、暗号化や復号化を行う際の処理時間や消費電力の変化、外部に発生する電磁波、音、熱などの変動を測定し、重要な情報を取得する。



Office 110

https://office110.jp/security/knowledge/cyber-attack/side-channel-attack

２．２．１　ハードウェアのRE対策技術

（１）開封困難化
（２）開封痕跡
（３）開封時破壊
（４）形状欺瞞
（５）X線透過防止

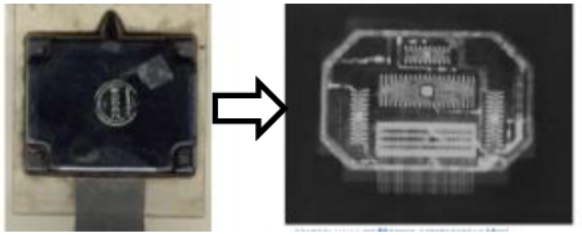
２．２．２　ソフトウェアのRE技術

2．2．1　ハードウェアのRE対策技術

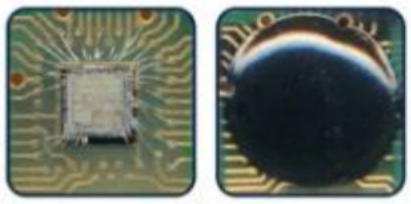
- 開封困難化
- 開封を困難にする手段は多数あり、それぞれの対策の限界を知って利用する必要がある。

No.	手段	概要	対策の限界
1	セキュリティビット	特殊形状のドライバで開封	ドライバセット購入で開封可能
2	高強度接着剤封止	接着剤で封止	加熱で接着剤を軟化封止無効化
3	超音波溶接	超音波プレスした外被で一体化	液体窒素冷却後圧縮空気充填で溶接部に亀裂発生
4	カプセル化	エポキシで充填しカプセル化	X線及び音響顕微鏡でチップ画像が取得可能
5	コーティング	アクリル、エポキシ、シリコン等でコーティング	研磨、薬剤でコーティング剤を除去可能

セキュリティビット　接着剤無効化例



カプセル化とX線顕微鏡による効化例



コーティング例

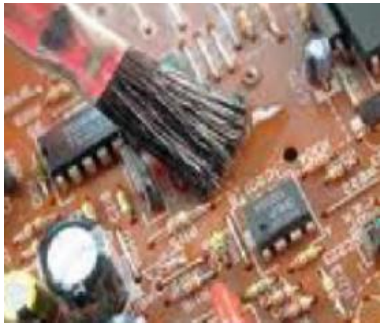
KTH Hardware Security
https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security_2017_05_08.pdf

２．２．１　ハードウェアのRE対策技術 開封痕跡

- 開封痕跡（タンパーエビデント）
- 一度開封したことがわかる機能や仕組みのことであり、装備品等の共同開発や、海外移転等で、開封を禁じている部品等に適用する技術である。開封の痕跡により開封がわかるので開封の抑止となる。

No.	対策	概　要
1	タンパーエビデント収納器	開封すると大きく損傷したり、**開封の跡が残るシール等を用い開封したことがわかる容器に収納する方法。**
2	ブリーディングペイント	1つの色の塗料に対照的な色の塗料を封印した微細なカプセルを混ぜる。塗装面が損傷している場合、**色が混ざり改ざんが容易に識別可能とする方法。**

タンパーエビデント



ブリーディングペイント

KTH Hardware Security
https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security_2017_05_08.pdf

２．２．１　ハードウェアのRE対策技術

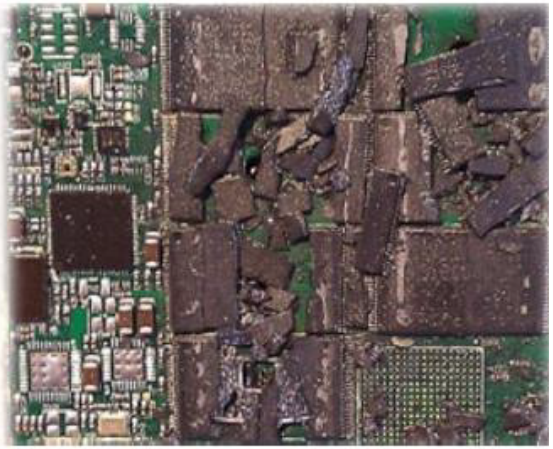
- 開封時破壊
- 開封されると物理的に破壊するという方法であり、高いセキュリティが要求されるデバイスで用いられる。

①火工品

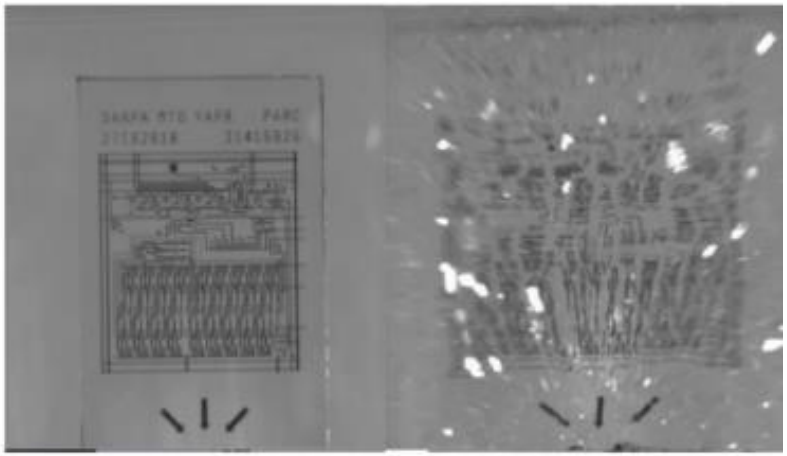
小さな火薬を用いて焼損させる。民生品には適していいない。

②自己破壊する強化ガラス製チップ

シリコン製コンピュータ・ウェハーをあらかじめ内部応力を持たせた強化ガラス製に取り付けることにより、一か所でも**刺激**（通電、加熱、圧力）**が加わると自己破壊させることができる。**



① 改ざん検出に応じて破壊されたチップの事例

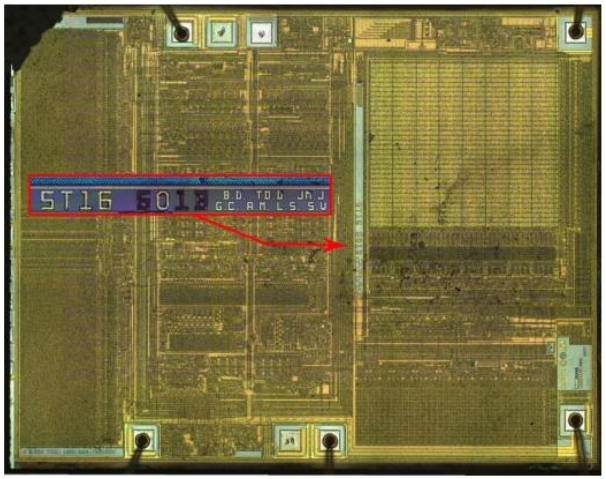


② 強化ガラス製チップの事例

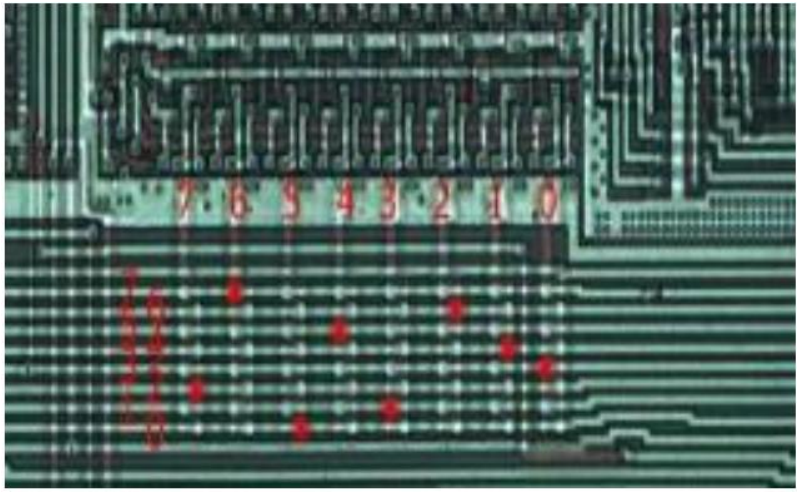
https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security_2017_05_08.pdf

- 形状欺瞞

- RE攻撃では**X線や超音波を用いた**非破壊検査により**精密形状・構造を分析**することが行われえる。
- ダミー回路、配線等により**形状を欺瞞して攻撃者を混乱**させる方法がある。
- 対策例としてスマートメモリカードのレイアウト（下図左）やデータバス（下図右）のREる対策例を示す。



STMicroelectronics ST16601 smartcard MCU



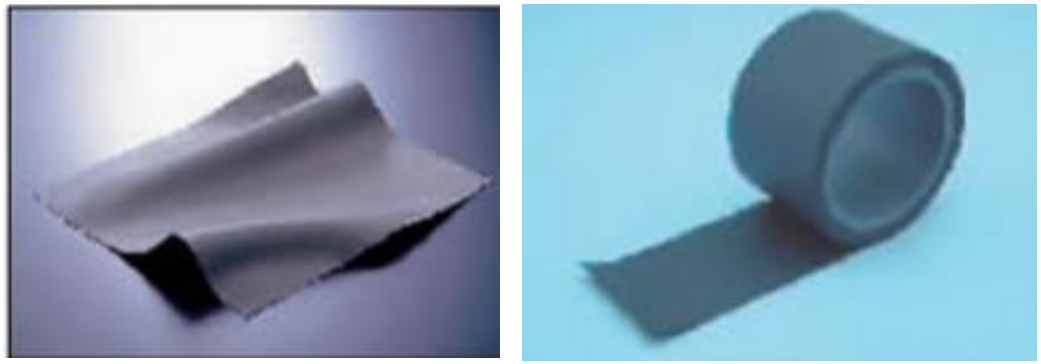
Motorola SC27/28 smartcard MCU

スマートMCU（Memory Control Unit）の例

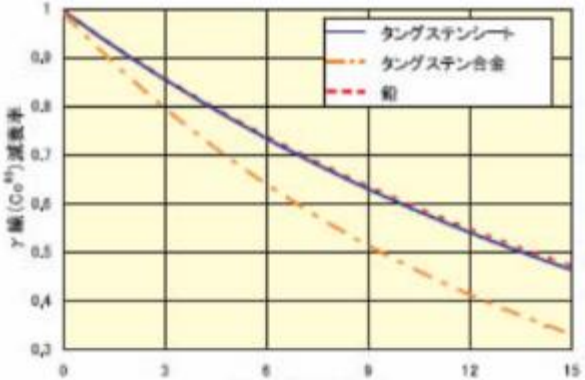
KTH Hardware Security
https://www.kth.se/social/files/59102ef5f276540f03507109/hardware_security_2017_05_08.pdf

● X線透過防止

- ハードウェアの精密形状や構造は、装置又は部品の外側から非接触でX線により内部の画像を取得することによって計測できます。これを防ぐために**X線を透過しない遮蔽シート等により透過を防止する。**
- X線を含む放射線の遮蔽シート等は、その遮へい能力が優れ安価である鉛や鉛含有材料、またタングステンを主成分とするタングステン合金が放射線遮へい能力が高い放射線遮へい材です。環境への影響や人体への影響等から近年ではタングステン合金材が用いられてる。
- タングステンと有機材料からなる全く新しい高密度の複合材料が開発され、環境に優しい「タングステンシート」として商品化されている。



放射線(Ｘ線含む)遮へいシート等の例



放射線(Ｘ線含む)遮へい特性

日本タングステン社カタログ
https://www.nittan.co.jp/tech/gihou/tungsten_sheet4_040.html

２．２．１　ハードウェアのRE対策技術

２．２．２　ソフトウェアのRE対策技術

2．2．2　ソフトウェアのRE対策技術

- プログラムの「難読化」と「暗号化」

• ソフトウェアのRE対策として、オブジェクトコードや各種データの解析取得、ソースコードの復元解析を困難とする技術が用いられる。

• 「難読化」にはさまざまな手法があり、ダミーコードによる制御フローの難読化はその一例です。これは、**無意味な命令列（ダミーコード）をプログラムに挿入**することで解析作業を煩雑にする手法である。また、RE専用のデバッガを通じて行われることも多いため、デバッガ*の監視下にあることを検知し、制御フローを変える「アンチデバッグ機能」が組み込まれることもある。

• 「暗号化」は、プログラムやデータを暗号化し、**第三者には解読できない状態に変換**します。暗号化されたデータをもとに戻す「復号鍵」がないと中身を見られないようにする技術である。

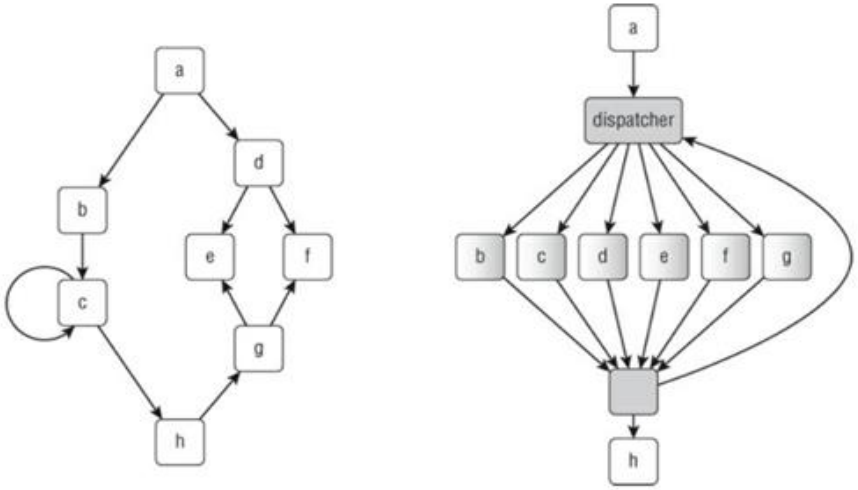
RE対策手法		概要
難読化		ダミーコードの挿入やプログラム変換を行い実行モジュールからソースコード作成を困難にする。
暗号化	プログラムやデータの暗号化	保護したプログラムやデータを暗号化しFPGA 等で処理する。
	プログラム分割	ノウハウ等重要データをプログラムから分割して暗号化する。
	パッキング	プログラムを暗号化して圧縮することで、不揮発メモリ内容の解析が困難となる。

＊　プログラムのバグ（誤りや欠陥）を発見して、それを修正する作業を支援するソフトウェア

2．2．2　ソフトウェアのRE対策技術

- 難読化
- ダミーコードによる制御フローの難読化
- 無意味な命令列（ダミーコード）をプログラムに挿入することで解析作業を煩雑にする手法である。
- RE専用のデバッガ　を通じて行われることも多いため、デバッガの監視下にあることを検知し、制御フローを変える「アンチデバッグ機能」がある。
- 制御フローの平坦化（CFF：Control Flow Flattening)の例を示す。

CFFは、**制御フローを平らにすることで、解析を困難**にする。元の制御フローは、条件分岐やループ処理などの構造が分かりやすく、どのような処理を行っているかを推測しやすい。一方、CFFを適用した制御フローは、それぞれの処理が同じ個所（dispatcher）を通るようになっており、各処理の依存関係が隠されて解析が難しい。CFFではこのように、条件分岐に応じてdispatcherが各処理（b~g）に制御を割り振るようにすることで、CFF適用前と同じ処理を、平らな制御フローで実現する。



CFFの概念図　左: 元の制御フロー右: CFF適用後の制御フロー

Bruce Dang. “Practical Reverse Engineering.” John Wiley & Sons, Inc., 2014, ISBN: 978-1-118-78731-1 (USA)

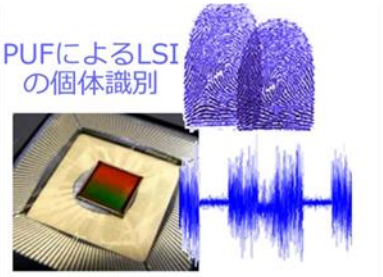
● 暗号化

- 暗号化は、プログラムやデータを暗号化し、**第三者には解読できない状態**に変換する。暗号化されたデータをもとに戻す「復号鍵」がないと中身を見られないようにする技術である。
- バイナリデータを暗号化しておき、実行時に復号することで元のコードを実行する。暗号化により、データサイズは増加する傾向にある。
- 暗号化では**復号に秘密鍵が必要**である。

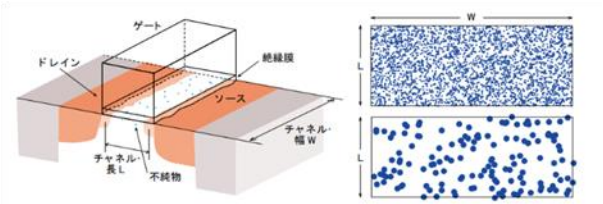
2．2．2　ソフトウェアのRE対策技術

- 鍵管理の方法

- 復号に使う秘密鍵を攻撃者が見ることのできるバイナリ自身に埋め込む方法である。攻撃者がバイナリを全て見ることができても秘密鍵が漏洩しないような技術は、**ホワイトボックス暗号として研究**が進められている。
- 復号に使う鍵を、**セキュアなストレージに保管する**方法である。セキュアなストレージとして、HSM (Hardware Security Module) やTPM (Trusted Platform Module) といったモジュールが良く用いられる。また、ICの製造時のばらつきを利用して**固有の情報を抽出するPUF** (Physically Unclonable Function) という技術を用いて、鍵を生成・管理する方法がある。PUFでは回路の動作時にしか鍵が出現しないことから、バイナリ解析に特に有効だと考えられる。



PUF技術のイメージ図 *1



半導体チップのばらつきの例
(FETのゲート不純物) *2

*1 産業技術総合研究所「暗号LSIの安全性評価に関する国際標準化の動向 の安全性評価に関する国際標準化の動向」
https://www.jst.go.jp/crest/dvlsi/list/pdf/h221001fujinot00sato.pdf

*2 新技術説明会　京都大学大学院佐藤高史　固有値を共有する物理複製困難関数回路
https://shingi.jst.go.jp/pdf/2019/2019_kyoto-u_6.pdf

2．2．2　ソフトウェアのRE対策技術

- サイドチャネル攻撃に対するRE対策
- サイドチャネル攻撃の代表的な方法とそのRE対策を表に示す。外部からのサイドチャネル攻撃に対して、観測した情報とプログラム処理やデータの動作情報との関係を隠蔽・遮へいする対策をとる。

サイドチャネル攻撃		RE対策例
手法	攻撃概要	
放出電波の解析（電磁波計測）	プログラムが格納されたメモリからCPU、RAM、FPGAへプログラムを書き込む際に**データの流れとともに発生する電磁波を外部の電磁波計測装置で読み込む**方法	観測した動作情報とモジュール等での内部情報の関係を隠す方法（ハイディング）で、例えば放射する電磁波、温度・光及び消費電力を**処理内容とは無関係にランダム化**や一定量にして解析を不可能にする。 一方、遮へい（マスキング）では、演算に用いる値にあらかじめ乱数により変換しサイドチャネル情報とアルゴリズムの関係を解析することを困難にする。
温度・光等のシグネチャ解析	温度・光等によるシグネチャ解析は、**メモリ内やFPGA内**でどの部位のロジック回路やトランジスタが活性化（データのやり取りがされている。）したかを**発生する熱や放出される光を外部から検出**することによってデータのパターンを読み取る技術	
消費電力解析	暗号モジュール等の動作中の電力（電圧）をデジタルオシロスコープで観測しその**観測波形から暗号化・復合化を実施**	
ソフトウェア処理時の過電圧印加解析（故障モード解析）	ソフトウェア処理時の過電圧印加解析（故障モード解析）は、動作中のFPGAに対し**故意に外部から過電圧を印加することで、処理を異常終了**させ、FPGAの論理素子アレイに部分的に揮発せずに残っているプログラムの断片情報を取得する。これを複数回繰り返すことにより、プログラムの全体構成を得るものである。この手法は、プログラム読み取りのために開発された手法	過電圧検知器により過**電圧を検知すると情報を消去**することにより情報接種を防ぐ。

2．2．2　ソフトウェアのRE対策技術

- 特許の事例

・ ハードウェアの機能追加等によるサイドチャネル攻撃対策（1/2）

No.	特許等	概　要
1	特願2019-208908 暗号攻撃に対する防御のためのクロック周期ランダム化 (2020.4.9)	暗号化動作中に**デバイスクロックをランダムに変化させる装置**。クロック周期ランダマイザにより、暗号化動作中にランダムなクロックレートでデバイスを駆動する出力可変クロックの周期をランダムに発生させる。
2	US特許 US-A-190279947, 2021/10/7 US-A-210313280 INTEGRATED CIRCUIT PROVIDED WITH DECOYS AGAINST REVERSE ENGINEERING AND CORRESPONDING FABRICATION PROCESS（2019.9.12）	**動作電圧の異なる2つの回路で同じ処理**を行い、**不正アクセスが行われる**ことにより異なる電圧変化を検知すると**デコイ処理に誘導**して混乱させる手法。
3	US特許 US-A-200401733 BUFFER ACCESS FOR SIDE-CHANNEL ATTACK RESISTANCE）（2020.12.24 ）	**データ処理ブロックをランダムに処理することによる難読化**。暗号プロセッサは、処理対象のデータブロックをメモリから取得し、入力バッファに一定数のデータブロックが格納されるまで待機する。その後、入力バッファからランダムにデータブロックを選択して処理することにより、データブロックの処理順序がランダムになるため処理内容の解析が困難になる。

2．2．2　ソフトウェアのRE対策技術

● 特許の事例

• ハードウェアの機能追加等よるサイドチャネル攻撃対策（2/2）

No.	特許等	概　要
4	US特許 US-A-210374249 POWER SIDE-CHANNEL ATTACK VULNERABILITY ASSESSMENT SYSTEMS AND METHODS（2021.12.2 ）	**FPGAに電力監視回路を内蔵**し、**電力をモニターしながら攻撃された際に電力を制御**する方法。電力監視回路用のFPGAとパワー・モニタリング回路を内蔵し、電力解析サイドチャネル攻撃を受けた際にパラメータを操作することにより出力電圧を変えて難読化する。

• AIによるソフトウェア解析技術を応用するRE

No.	特許等	概　要
1	EP特許EP-A-003872626 UTILIZING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING MODELS TO REVERSE ENGINEER AN APPLICATION FROM APPLICATION ARTIFACTS（2021.9.1）	プログラム設計の過程で生じた**バグをAIにより消去して整理する技術**を用い、RE対策として仕込ませた無意味なプログラム処理も同様に削除することが可能である。**RE対策を無力化**できる。
2	US特許US-A-190138719 METHODS AND APPARATUS FOR DETECTING A SIDE CHANNEL ATTACK USING A CACHE STATE (2019.5.9)	**ヒストグラム生成器と機械学習によりサイドチャネル攻撃を識別する方法**。ヒストグラムアナライザは、ヒストグラムに基づいて統計量を算出し、機械学習モデルプロセッサは、機械学習モデルにより、サイドチャネル攻撃を識別する。

用語集 (1/3)

用　　語	意　　味
CPU（Central Processing Unit ）	中央演算処理装置
DRAM(Dynamic Random Access Memory)	主記憶として用いられる不揮発性の半導体メモリ
DSP(Digital Signal Processor)	信号処理向けのマイクロプロセッサ
FIB(Focused Ion Beam)	集束イオンビーム装置のこと。集束したイオンビームを試料に照射し、加工や観察を行う装置
FPGA(Field Programmable Gate Array)	書き換え可能なLSI
ICチップ	高度な機能を持つ電子部品の一つで、トランジスタ、抵抗、コンデンサ、ダイオードなど、多数の微細な電子部品を一つの基板の上で連結し、全体として複雑な処理を行ったり、大量のデータの記憶を行ったりできるもの。形態が数cm角程度の小片であるため「チップ」（chip）と呼ばれる。
JTAG(Joint Test Action Group)	シリアル通信で、IC内部に設けられたテスト用の回路にアクセスし、ICの内部回路と通信することができる技術でCPUのデバッグやデバイスのプログラミング機能がある。
PUF(Physically Unclonable Function)	LSIの指紋（固有ID）のことであり、製品ごとに異なるので複製が不可能であるため暗号鍵に利用すると強度の高い暗号化が可能となる。
SEM（scanning electron microscope）	走査型電子顕微鏡

用語集 (2/3)

用　　語	意　　味
TEM（transmission electron microscope）	透過型電子顕微鏡
X線CT（Computed Tomography）	X線撮影を360度全方向から行い、物体の内部がどうなっているかを調べる技術 （CT：コンピュータ断層撮影）
アセンブラ	アセンブリ言語で記述されたソースコードを、コンピュータが直接解釈・実行できる機械語（マシン語）による表現（オブジェクトコード）に変換するソフトウェア
アルゴリズム	コンピュータにプログラムの形で与えて実行させることができるよう定式化された処理手順の集合のことを指すこと。
オブジェクトコード	コンピュータプログラムの形式の一つで、コンピュータによる解釈・実行に適した言語や コード 体系で記述されたもの。
筐体	機器類を入れる箱。装置の外装部をいう。
サイドチャネル攻撃	装置の物理的な特性の変化を外部から観測・解析することにより、本来読み取ることができない情報を取得する手法
ソースコード	プログラミング言語などの人間が理解・記述しやすい言語やデータ形式を用いて書き記されたプログラム
ダミーソフト	その実行に意味のないソフトウェア。ダミーソフトの挿入して計算量を増減させるとサイドチャネル攻撃などによる解読を困難にする。

用語集 (3/3)

用　　語	意　　味
デバッガ	プログラムのバグ（誤りや欠陥）を発見して、それを修正する作業を支援するソフトウェア
デバッグ	プログラムの欠陥を取り除くこと。
デバッグボード	プログラムのバグを見つけ、これを排除するのに使用するボード
プロービング	測定対象に接触させて、信号を検出し、測定器まで伝送して波形観測をすること。
プロービング	測定対象に接触させて、信号を検出し、測定器まで伝送して波形観測をすること。
ホワイトボックス暗号	DES 、 AES等の一般的な対称鍵 (共有鍵) ブロック暗号のラウンドを難読化することで、結果的に暗号化/復号化処理機能に公開鍵暗号のような非対称性を持つ。


DTF
一般財団法人 防衛技術協会
DEFENSE TECHNOLOGY FOUNDATION

（様式２）

二次利用未承諾リスト

報告書の題名
令和4年度重要技術管理体制強化事業安全保障上重要となる機微技術の流出防止にかかる調査　調査報告書

委託事業名　令和4年度重要技術管理体制強化事業安全保障上重要となる機微技術の流出防止にかかる調査

受注事業者名　一般財団法人　防衛技術協会

頁	図表番号	タイトル
8		非破壊計測による精密形状・構造の分析（3Dスキャナ）
9		Ｘ線計測によるスマートフォンの計測例
10		高分解能X線透過分析装置：NanoTube N3
11		プリント基板の分析事例
12		破壊による内部構造・部品構成の分析 HIC(Hybrid IC)の制御IC部　部分開封事例
13		半導体の故障解析に用いる電気的マイクロプロービング
14		コネクタの蛍光X線分析の例
15		電子顕微鏡による構造解析　半導体解析例
19		サイドチャネル攻撃とは
21		開封困難化
22		タンパーエビデント、ブリーティングペイント
23		改ざん検出に応じて破壊されたチップの事例
23		強化ガラス製チップの事例
24		STMicroelectronics ST16601 smartcard MCU
24		Motorola SC27/28 smartcard MCU
25		放射線(Ｘ線含む)遮へいシート等の例
25		放射線(Ｘ線含む)遮へい特性
28		CFFの概念図