Information-technology Promotion Agency, Japan

Japan Cryptographic Module Validation Program

ハードウェアセキュリティ

―IoTの時代に向けて

2015年12月2日

独立行政法人　情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ認証室
佐藤　眞司

サマリ

- 長い期間に渡り、保護やメンテナンスがされない環境で使用されるハードウェア装置があるかもしれない。
- 市場のIoT製品を攻撃する攻撃者は、ハードウェア部分への攻撃をターゲットにし始めている。
- IoT製品の設計関係者は、ハードウェアへの攻撃として物理攻撃、サイドチャネル攻撃、そして故障注入攻撃について最低限の知識は持っているべきである。
- 単独の組織、あるいは企業での対応には限界があり、セキュリティ・コミュニティを形成して連携する必要がある。

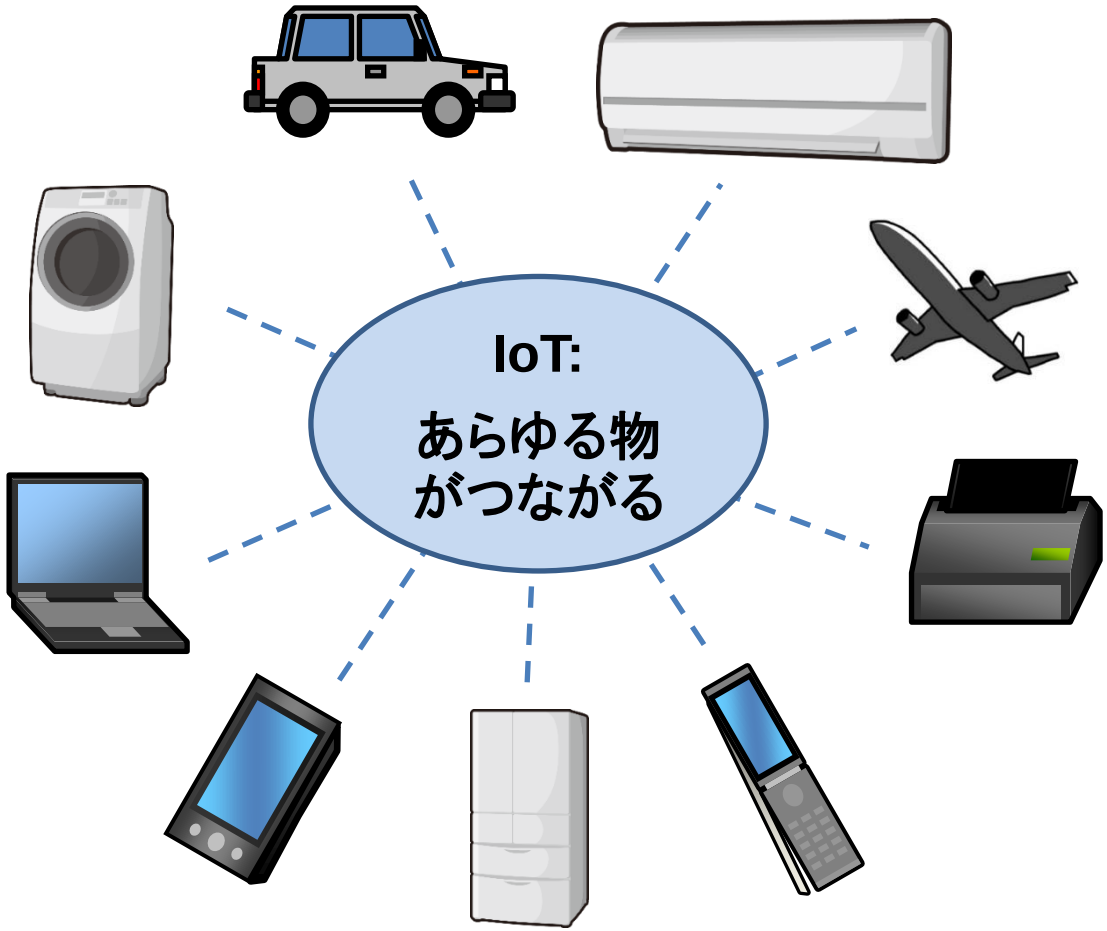
目次

- 第1部 IoTとは
- 第2部 脅威
- 第3部 脆弱性の事例
- 第4部 ハードウェアへの攻撃
  - 物理解析
  - サイドチャネル攻撃
  - 故障注入攻撃
- 第5部 スマートカードでの経験
- 第6部 IPAの取り組み

第1部　IoTとは

- IoT
- **構成、動向**
- **IoTの可能性**

IoT (Internet of Things = モノのインターネット)



あらゆる物がインターネットを通じて
つながることによって実現する新たな
サービス、ビジネスモデル、または
それを可能とする要素技術の総称。
従来のパソコン、サーバー、携帯電話、
スマートホンのほか、ICタグ、ユビキタス、
組込みシステム、各種センサーや
送受信装置などが相互に情報をやりとり
できるようになり、新たなネットワーク社会
が実現すると期待されている。

＊出展:参考資料1

・利用者に情報収集や通信が意識されない場合がある
・利用者には機能の制御ができない場合がある

IoTの活用例

- 医療、ヘルスケア
  - ウェアラブルデバイスを使ったモニタリング
  - スマートビル
  - 幼児のモニタリング
- 産業、製造プロセス
  - スマート工場
  - 産業機械のモニタリング
  - ウェアラブルデバイスを使った作業の効率化
- スマートハウス
  - 空調、照明のスマート化
  - ホームセキュリティ
  - 家庭用アシスタントロボ
- スマートシティ
  - スマートごみ箱
  - スマートグリッド
  - 環境汚染のモニタリング
  - ウェアラブルデバイスを使った作業の効率化
- モビリティ
  - コネクテッドカー
  - カーシェアリング
  - 公共交通機関のリアルタイム位置情報
- 流通
  - 物流のリアルタイム監視
  - 在庫の自動管理
  - 企業間サプライチェーンの統合

＊出展:参考資料2、3

IoTに関する動向

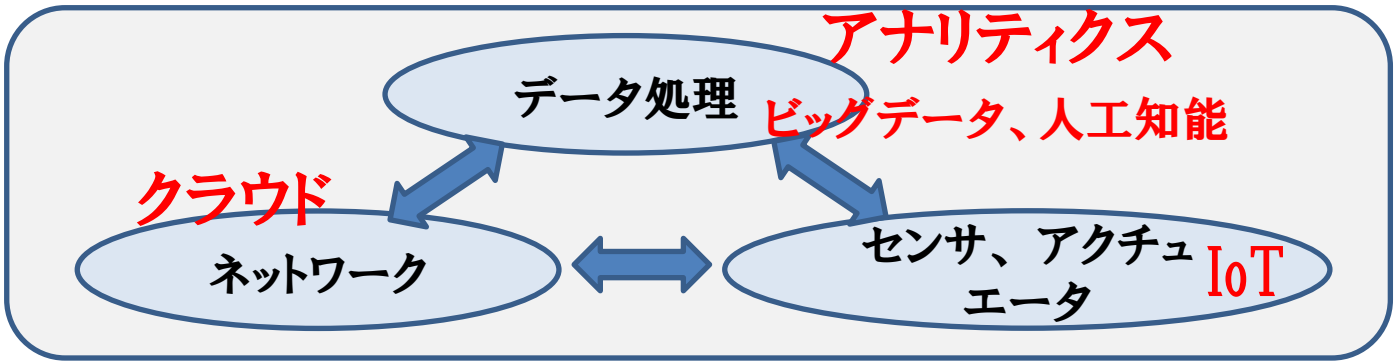
- Industrie 4.0
  - ドイツ政府主導の取り組みであり、「スマート工場」で低コストにて多様なニーズに応じた製造を実現することが目的。

    →ドイツの製造業の国際競争力を高めたい。
  - 化学、機械、プラント、電気、電子機器の領域で大きな効果を見込んでいる。
  - 規格に非対応の機器群は、Administration shellの保護下におく。
  - セーフティ&セキュリティが重要。
- Industrial Internet
  - 米国政府機関NIST(National Institute of Standards and Technology)のPublic Working Groupとして活動。
  - “Internet Thinking”(インターネットで考える)によるビジネス開発が目的。
  - Cyber Physical System:CPS = IoT + 制御 & 判断
- 日本でも経済産業省の主導でIoT推進コンソーシアムを設立

＊出展:参考資料4、5、6

CPS(Cyber Physical System)

- 現実世界のデータをサーバー空間で分析し、分析した情報を現実空間へフィードバックさせる仕組み。
- IoTの普及によって膨大なデータが現実世界から集められ、ビッグデータや人工知能を使った分析が社会の様々な場面で利用される。

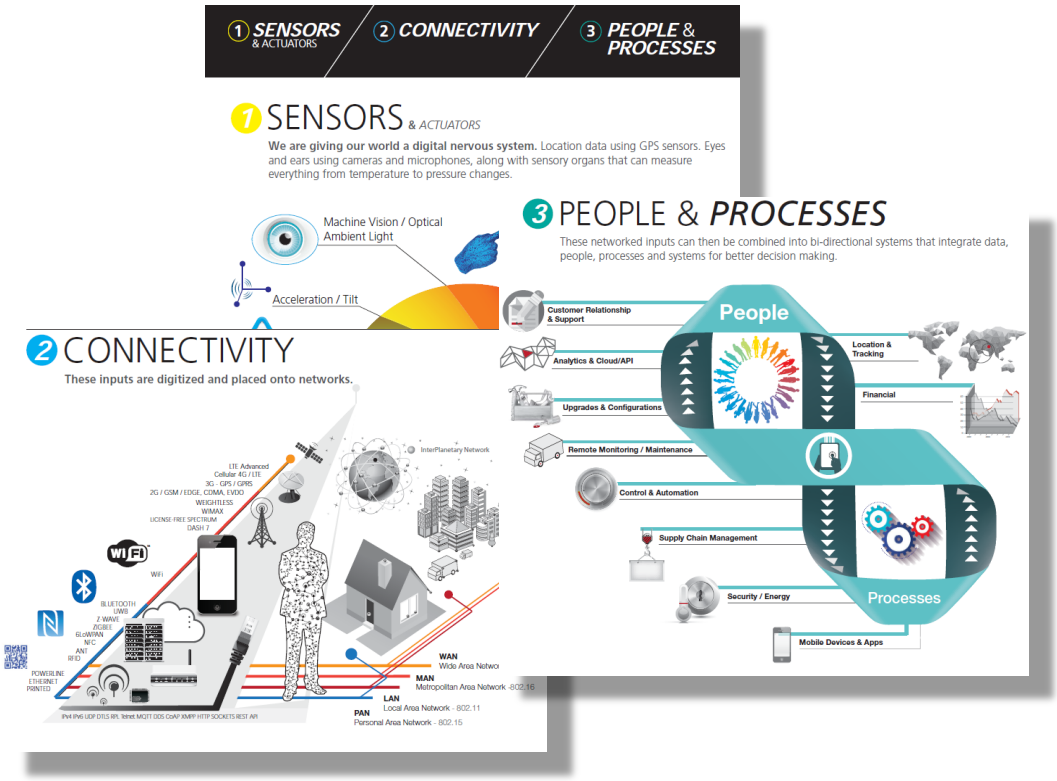


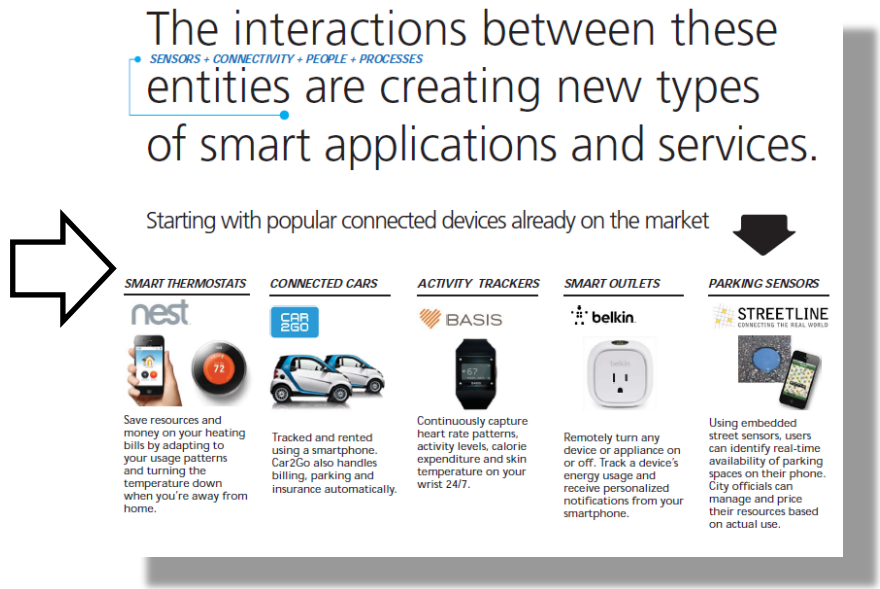
- 背景
  - モバイル技術の発達により小型で性能の高いIoTデバイスの開発が可能になったため、機械のネットワークが多くの分野で進み始めた。
  - ITインフラの整備によって、安価な無線通信サービス、クラウド技術、ビッグデータを用いたアナリティクス、人工知能などIT環境が整備され、無数の機械がインターネットに接続し他の機械が集めたデータを共有することで機械どうしが連携を取ることが可能になった。

＊出展:参考資料2

Postscapes

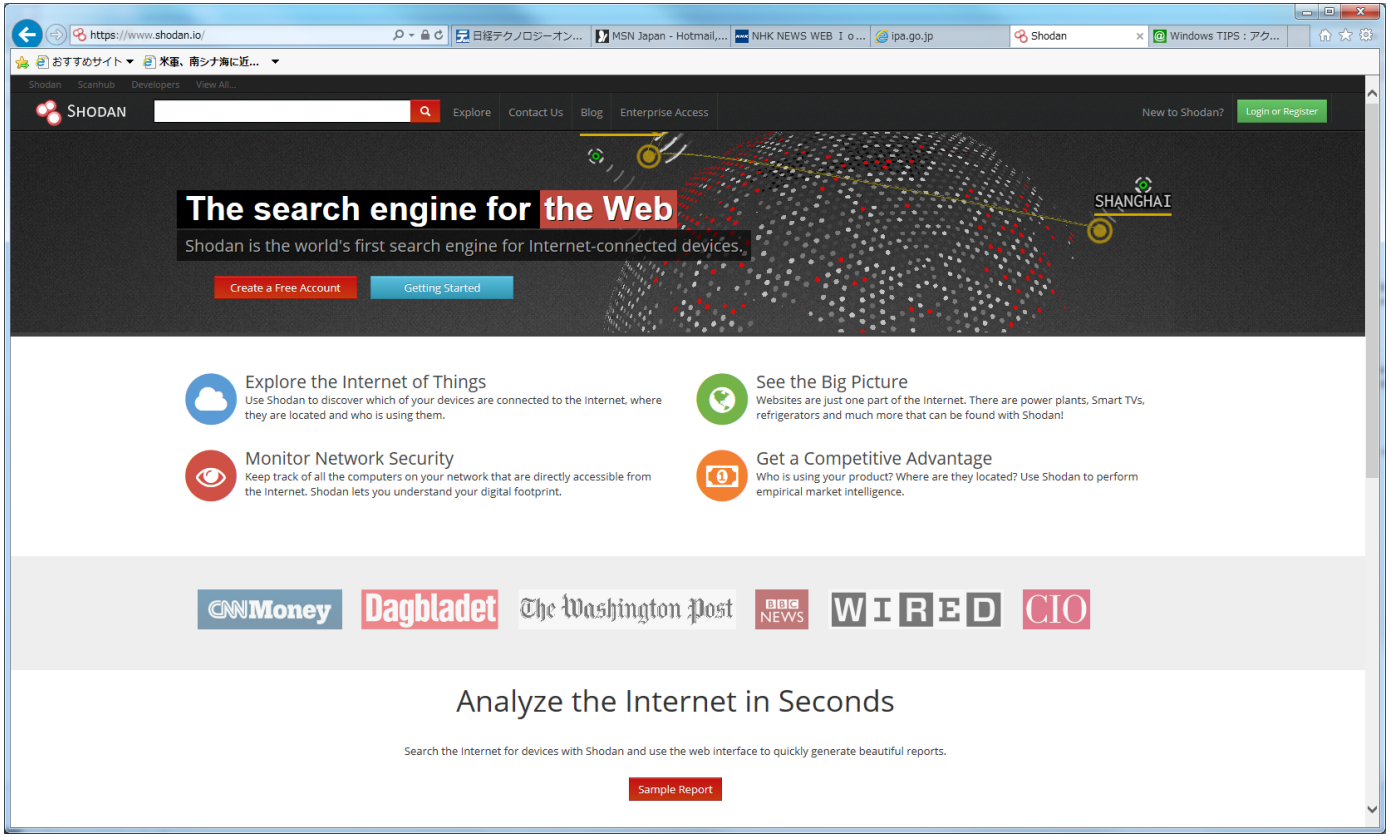
- IoTとは何か？：センサ+つながる+人&プロセス
  →新しいタイプのスマートアプリ、スマートサービス





＊出展：参考資料7

SHODAN: インターネット接続機器の検索サービス



- 2009年より。

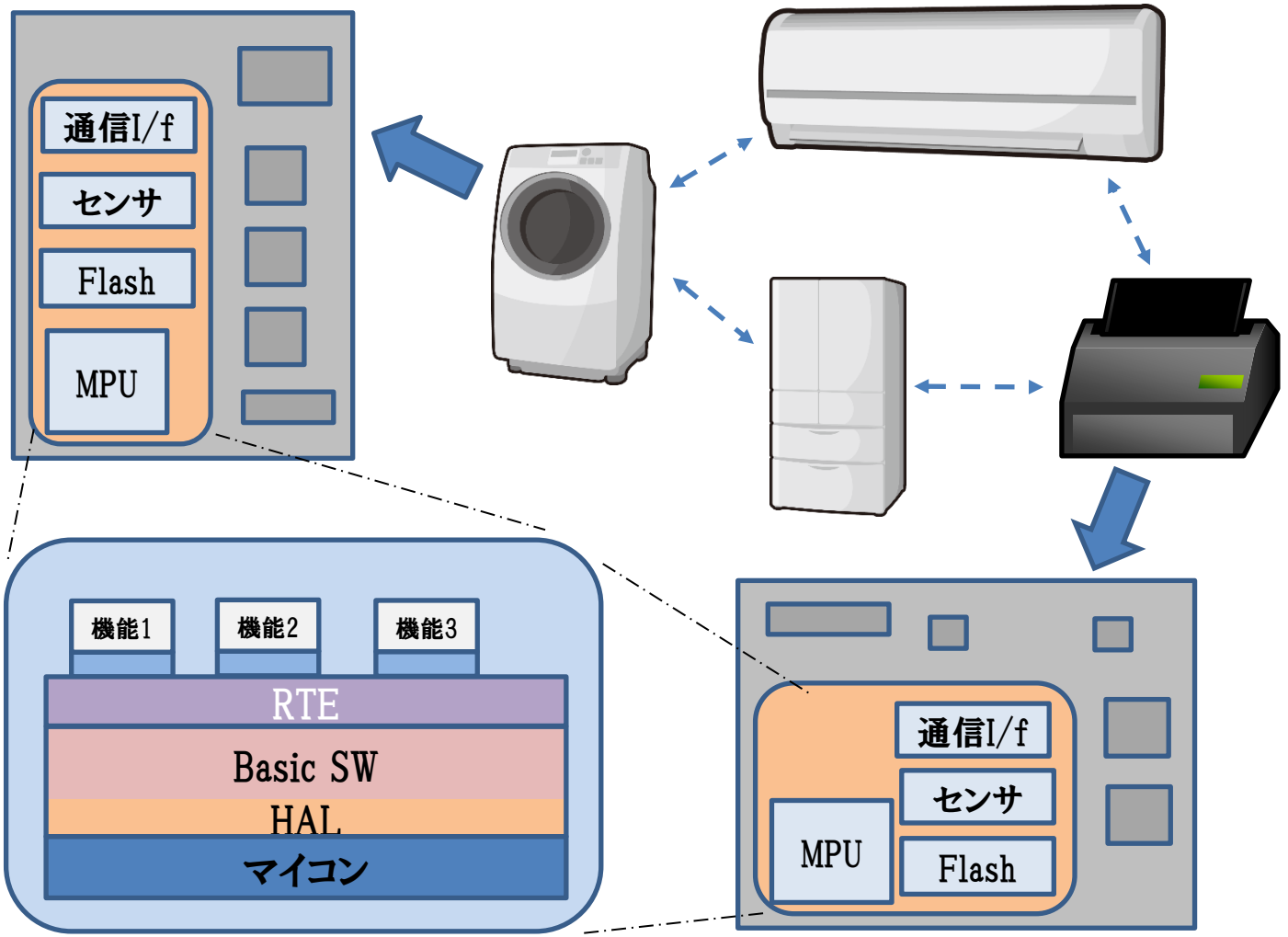
Shodan は、インターネットに接続されている特定のタイプのコンピュータ(ルーター、サーバー等)を、様々なフィルタを使用して24時間探索する検索エンジン。

- 検索可能な機器例
  - Webサーバ
  - Webカメラ
  - ルータやスイッチ
  - NAS
  - 複合機
  - NW対応家電(TV・レコーダなど)
  - ビル管理システム
  - 制御システム(HMI/PLCなど)

＊出展:参考資料8、9 、10

IoTの構成法

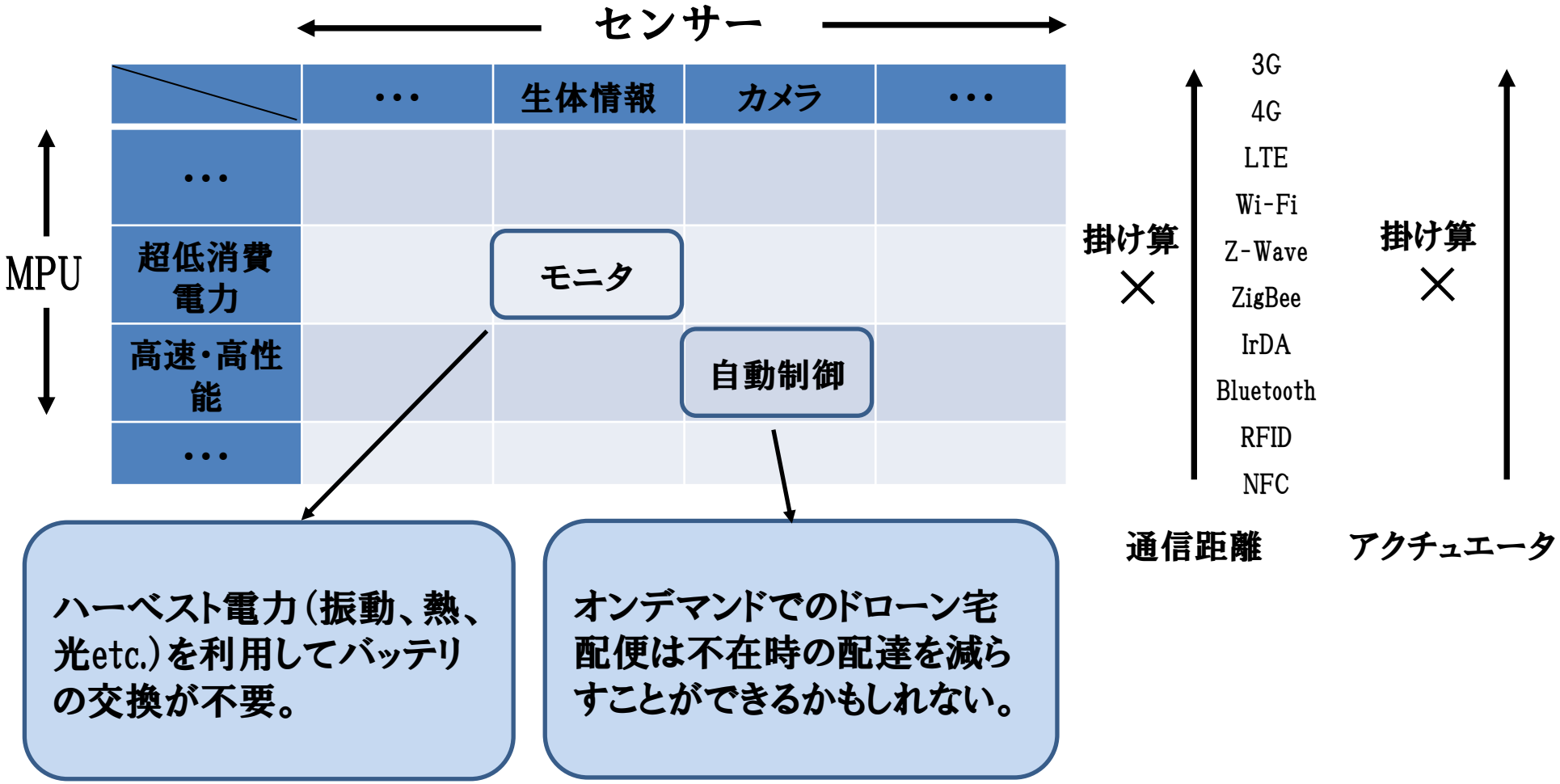
- 共通的な部分の構成法が似てくる。



- ミドルウェア
- アプリケーション
- センサー制御
- アクチュエータ制御
- ネットワーク制御
- センサー
- アクチュエータ
- MPU
- 電源
- 無線

IoTの可能性

- 新しい製品が提案される素地がある。



閑話休題：AI（人工知能）

- **機械学習**
  - パターンを学習して自動化。
- **コンピュータ将棋プロジェクトの終了宣言**
  - コンピュータ将棋は2015年の段階でトッププロ棋士に追いついている。
- **ロボットは東大にはいれるか**
  - 数学の偏差値が64へ。
- **作業員がロボットにつかまれ死亡、独フォルクスワーゲン工場**
  - 機械が人間に対して害を与える意図があったわけではない。単にモノとして扱ってしまっただけ。
- **人工知能分野の専門家の間では、近い将来コンピュータが何らかの意識（意識があれば人類に対して危険な考えを抱く可能性がある）を獲得するという認識はほとんどない。**

特定の機能では、AIは高速・高精度・無休で作業を行うことができるため、人間の能力をはるかに上回ることも可能。しかしながら、応用分野や想定外の事象に対して適切な結果を出せるかは保証されない。AIに制御を委ねる範囲には注意が必要。

＊出展：参考資料23、24、25、26

第2部　脅威

- ネガティブな意見
- 脅威リスト

IoTに対するネガティブな発言

- Apple 共同設立者Steve Wozniak 氏: “IoTはバブルである”
  - 収集されるデータの多くは有用ではない。
  - つながる機器の数が過大に想定されている。
- Computerworld オピニオン:Why the 'Internet of Things' may never happen
  - “Internet of Things”はヒトの介在なしにデバイスが相互につながることを指している。→トースト1枚焼くにもデバイス間の連携は難しい。
  - 複数の規格、標準、アイデアが競争者間で使用される。→多くの機器がインターネットでつながるかもしれないが、相互につながるわけではない。
- Forbes: Who Will Build The 'God Platform' For The Internet Of Things?
  - デバイス間のインタフェースやプロトコルの違いなどを吸収して、あらゆるモノをつなげる統合プラットフォームがない。
- Computerworld オピニオン: The Internet of Things is the grand idea of our time. Unfortunately, that vision may never become reality.
  - 標準が多すぎる。
  - セキュリティの問題→予想外のマルウェアや脆弱性が発見されることを我々は経験している。

＊出展:参考資料11、12、13、14

IoTの脅威（例1：日本クラウドセキュリティアライアンス）

- サービスの妨害、停止
- 誤った情報の流布
- 不正なデータによる機器の乗っ取りや妨害
- 収集された様々な情報の漏洩や悪用
- スクリプト、アプリケーション改ざん
- システムソフトウェア（ファームウェア）改ざん

＊出展：参考資料15

IoTの脅威(例2:OWASP)

- セキュアでないWebインターフェース
- 不十分な認証／認可
- セキュアでないネットワークサービス
- 暗号化されていない転送
- プライバシーの懸念
- セキュアでないクラウドインターフェース
- セキュアでないモバイルインターフェース
- 不十分なセキュリティ設定
- セキュアでないソフトウェア／ファームウェア
- 貧弱な物理的セキュリティ

＊出展:参考資料16

例2:OWASPにおける「物理的セキュリティ」

項目	判定	概要
攻撃エージェント	アプリケーションに依存	デバイスに物理的にアクセスできるものすべて
攻撃ベクトル	Exploitability: AVERAGE	攻撃者はUSBポート、SDカード、あるいは他のストレージ手段を攻撃ベクトルとして利用して、OSとデバイスに保存されているかもしれないすべてのデータにアクセスする。
セキュリティの弱点	Prevalence: COMMON Detectability: AVERAGE	攻撃者がデバイスを分解でき、容易にストレージ手段にアクセスできる場合には、物理セキュリティの弱点となる。構成やメンテナンスを意図した作りを利用して、USBポートや他の外部ポートを介してデバイスにアクセスできる場合にも弱点となる。
技術的インパクト	SEVERE	不十分な物理セキュリティは、デバイスそのものと、そこに保存されたあらゆるデータの弱体化の原因となる。
ビジネスインパクト	アプリケーション／ビジネスに依存	データが盗難、あるいは改ざんされる。デバイスの制御が奪われ、本来の意図に反して制御される。カスタマの害になるか？ブランドの害になるか？

＜対策例＞

- 機器が容易に分解できないこと
- データ保存用のメディアが容易に取り出せないこと
- 保管時のデータが暗号化されていること
- USBなどの外部ポートを使って不正に機器にアクセスできないこと
- 運用に本当に必要な外部ポートのみが装備されていること
- 管理機能がローカルなアクセスのみに制限されていること

＊出展:参考資料16

IoTの脅威(例3: IoTの将来 ”鍵となる3つのチャレンジ”)

- あらゆるところでデータが収集される
- 消費者のデータが予期されない用途に使用される恐れがある
- セキュリティリスクが高まる

- 設計によるセキュリティ
- データの取り扱いは最低限に
- 予期されない用途の通知と選択

〈〈米〉〉連邦取引委員会議長, Edith Ramirez

＊出展:参考資料17

IoTの脅威(例4:重要生活機器の脅威事例)

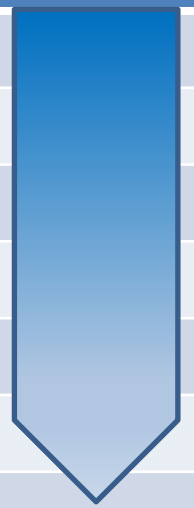
- 組込み機器へのワームの感染
- マルウェアによるPOS上のカード情報の流出
- HDDレコーダーの踏み台化
- 複合機蓄積データの意図せぬ公開
- アイロンの中のハッキングチップ
- ホテルの電子錠の不正な開錠
- 遠隔イモビライザー機能の不正利用
- タイヤ空気圧モニタ(TPMS)の脆弱性
- イモビカッターによる自動車盗難
- スマートキーに対する無線中継攻撃
- 遠隔から車載LANへの侵入実験
- PC接続による自動車の不正操作
- マルウェアに感染したカーナビの出荷
- マルウェアに感染したMP3プレーヤーの配布
- 心臓ペースメーカー等の不正操作
- 標的型攻撃メールによる設計情報漏えい
- ATMのハッキング
- (参考)マルウェアによる工場の生産設備の破壊

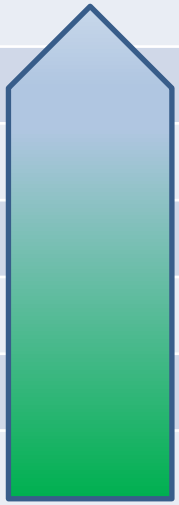
＊出展:参考資料18

IoTの脅威(例5:つながる世界のセーフティ & セキュリティ)

- 広がるセーフティとセキュリティの守る対象範囲

守るべきものの例	保護対象の例	セーフティ	セキュリティ
人	命		
	身体		
	心		
物	システム		
	機械		
金	金銭		
情報	データ、ソフトウェア		
	品質		





- 生活機器の開発では、セーフティ設計が必要
  →ネットワークにつながるようになるとセキュリティ設計も必要。
- セーフティ設計 & セキュリティ設計のために「見える化」が必要。

セーフティ←ハザード

セキュリティ←脅威

＊出展:参考資料19、20

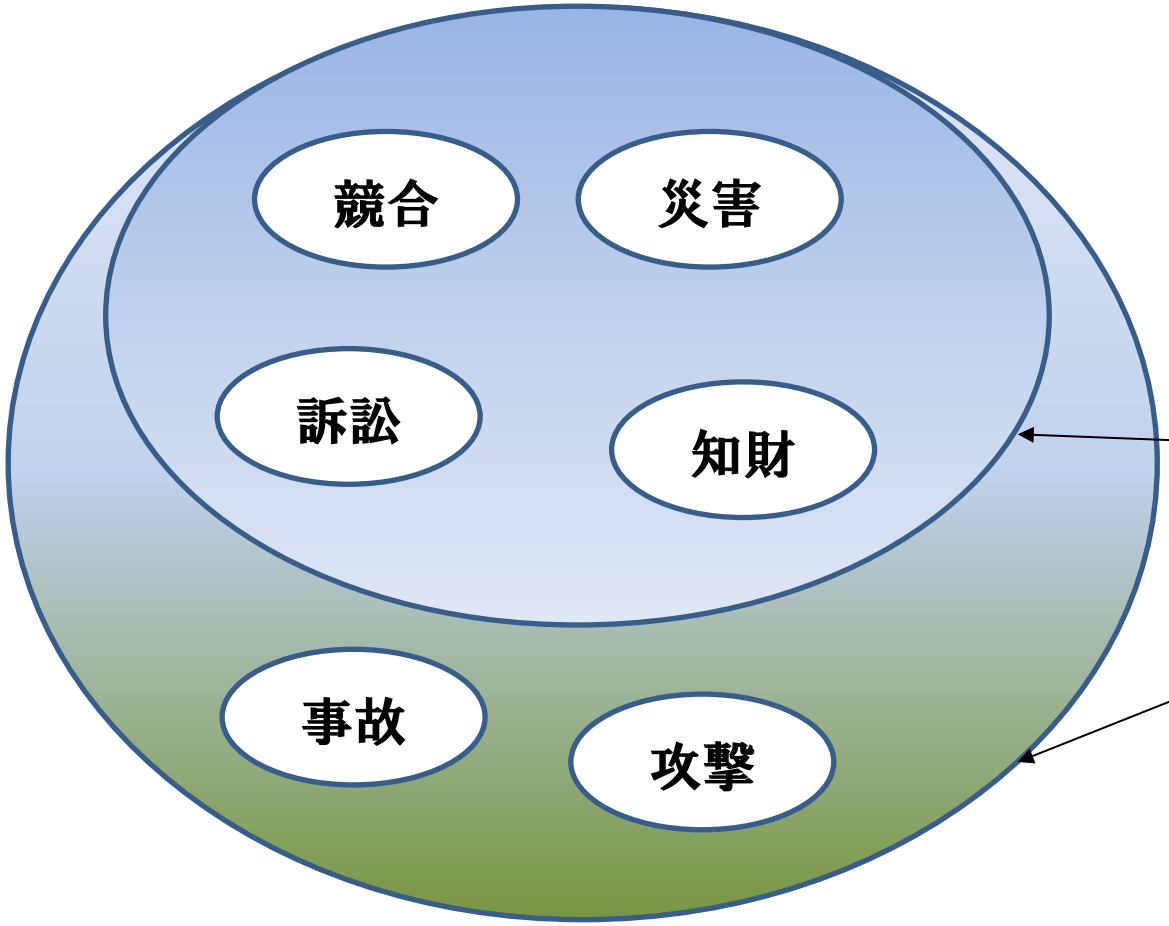
IoTの脅威（補足1）

- ネットワークをサブネット化したり、物理的に距離を置くことでは、他のIoT機器との関わりは排除できない。
- 共通的な部分の構成法は似てくるため、脆弱性が発見された場合の影響範囲は大きい。
- ITセキュリティの侵害が及ぼす影響は、製品種別ごとに千差万別。
- 製品によってはデバイスの寿命が長く、ハードウェアのメンテナンスがされないかもしれない。
- 脆弱性が公知の製品が、インフラ機能やクリティカルな機能をサポートしている可能性もある。

IoT製品のセキュリティ問題の定義は、他のIoT機器とのかかわりの中で初めてクリアになるものであり、製品設計時の想定がすべて満たされるとは限らない。全く想定外の環境で使用される状況が発生することが十分に考えられる。

IoTの脅威(補足2)

- 事業面からのリスク分析では、「事故」と「攻撃」が見えない。



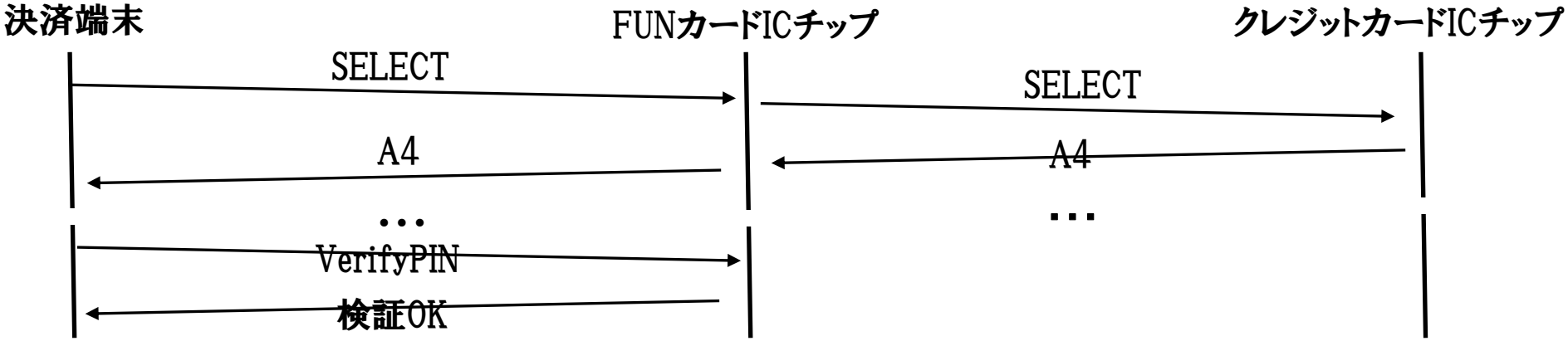
＊出展:参考資料21

第3部　脆弱性の事例

- 発表された事例
- 警告的発表
- 懸念

脆弱性(事例1:ICカード自体はそのままでトリック)

- クレジットカードを改ざんし、2つのICチップが決済端末と通信するようにされていた。(2011年ベルギー)
- 攻撃方法自体は2010年にケンブリッジ大によって発表されていたが、実際に工作しての実行は難しいと考えられていた。
- 決済端末とクレジットのICチップ間の通信をホビー用のICチップ(FUNカード)で媒介する。PINの入力に対しては即時に検証OKを返答する。



- クレジットカードのICチップはまったく別人の物(いずれも盗難)が搭載されていた。
- 技能や知識を持ち寄った犯罪集団が暗躍していた。

＊出展:参考資料29

脆弱性(事例2:BlackHat 2014)

- 以下の製品へのハッキング
  - Philips Hue personal wireless lighting
  - Belkin WeMo baby monitor
  - Belkin WeMo switch
  - Belkin NetCam

遠隔地より
・画像のモニタ
・電源OFF
などができている。

- BadUSB
  - USBデバイスのファームウェアを不正なものに勝手に書き換えられる。
  - USBデバイスの中身は小型のコンピュータとファームウェア
  - 他のデバイス(外付けHDD、ウェブカメラ、キーボード、その他多数)にも同種の攻撃が適用可能。
  - 以下の攻撃の恐れ
    - キーロガーによるユーザ監視
    - コマンド入力による任意の悪意あるコマンド実行。Malwareのインストールを含む。
    - ネットワークの設定を書き換え、悪意あるサーバーを経由するようにする。
    - ユーザーデータを盗み出す
    - その他

＊出展:参考資料30

脆弱性(事例3:CVE-2014-6271)

- UNIXおよびLinuxで広く使われているBash(Bourne Again Shell)に重大な脆弱性が発見された。→攻撃者に任意のコマンドの実行を許可してしまう恐れ。
- 攻撃者一定の条件のもと、特別に細工した環境変数を使って脆弱性を突き、環境変数に含まれる不正なコマンドをリモートで実行できる。
- かなり以前から存在する脆弱性と見られ、20年以上前の古いデバイスも影響を受ける恐れがある。
- UNIXおよびLinuxは多数の重要システムやWebサーバーに使用されており、米AppleのパソコンOS「OS X」もUNIXをベースとしている。

このように予想外の脆弱性の発見が将来も起こるかもしれない。

＊出展:参考資料32

脆弱性(事例2:BlackHat 2015)

- プリンタ内部のICチップのI/Oピンを素早くON/OFFすることで、コンクリートの壁を透過できる強度の電磁波を発生できる。→メッセージを送信することができ、情報の漏洩が可能。

物理的に分離したシステムであってもウイルスを持ち込めば情報送信の恐れ

- Linux搭載の自動照準の長距離狙撃ライフルTP750をリバースエンジニアリングし、システムの制御方法が可能であった。(ただし遠隔制御による発砲機能は無い)

武器もつながってしまう

- Intel X86プロセッサ(1997～2010)にゼロデイの脆弱性があり、Rootkitをインストールできる。BIOSの消去や悪意のあるソフトウェアのインストールが可能。→2010年以前のプロセッサは危険。

インフラ的に広範囲で使用されている製品の思いがけない脆弱性

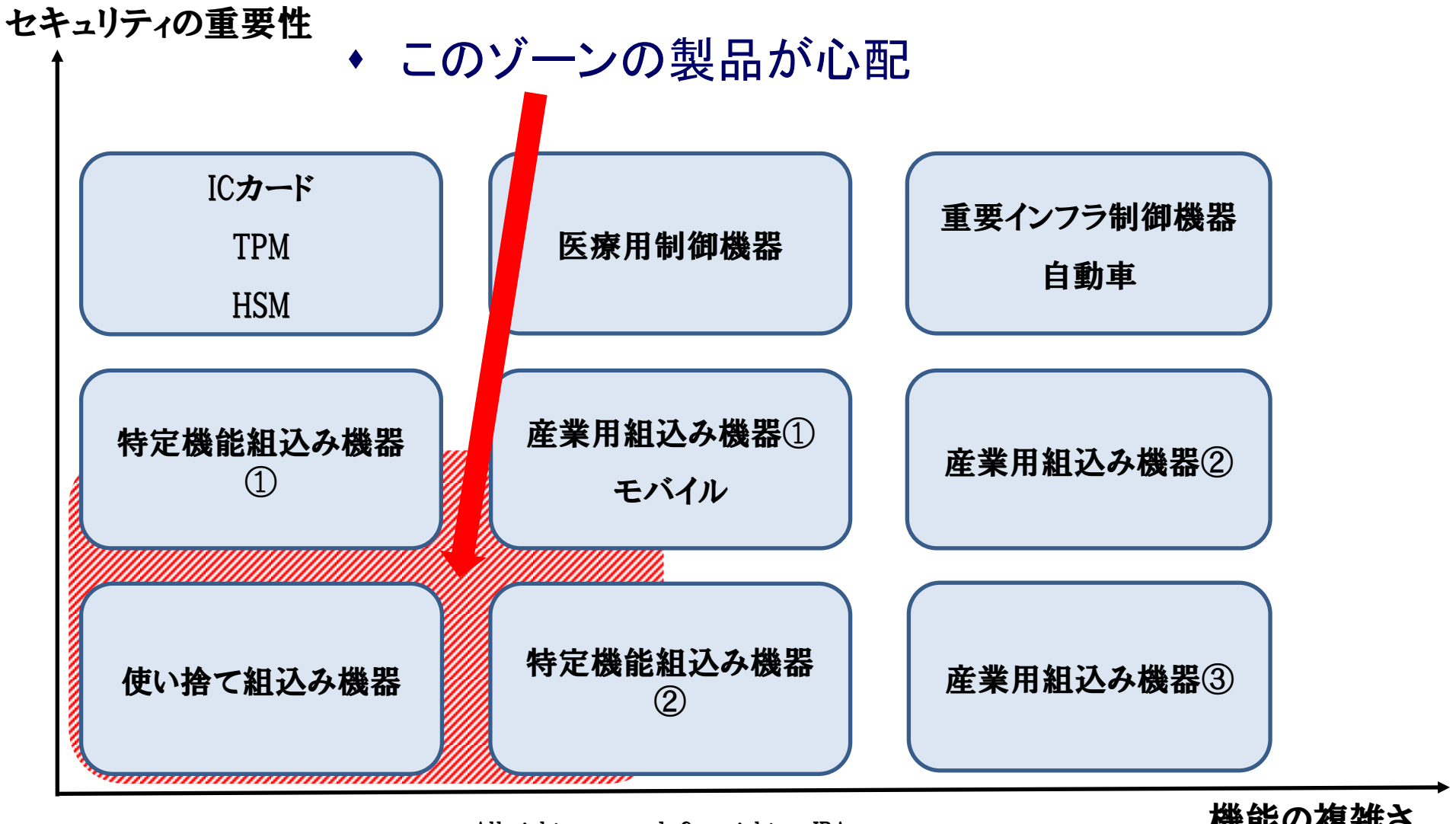
＊出展:参考資料31

警告的発表:BlackHat2010: Hardware is the New Software

- 我々はテクノロジにコントロールされている
  - ほぼすべてのモノにエレクトロニクスが組み込まれている
  - しばしばハードウェアは、「疑わないもの」とされる
  - セキュリティの分野ではハードウェアは大抵無視される
- 時は今
  - ツールも情報もある。
- 悪意によるハードウェアハッキング
  - サービスの盗難
  - 競争／クローニング
  - 利用者認証／なりすまし
- ハードウェアハッキング手法
  - 情報収集
  - ハードウェアの破壊
  - 外部インタフェースの解析
  - シリコンチップの解析
  - ファームウェアのリバース解析
- 共通のテーマ
  - ほとんどの製品設計エンジニアはセキュリティにうとい
  - 多くの製品はチップベンダが公開する参考設計に基づいている
  - エンジニアと製造者は、試験・デバッグのために容易にアクセスできる製品にしたい
  - 単純な攻撃でさえも甚大な影響が続く

＊出展:参考資料27

懸念(製品ゾーン)



懸念(運用環境)

- ICカードの運用環境は以下の点が特徴的
  - カード所有者に提供された後は、運用環境を制限できない(一般的に安全でない)。

  →カード所有者も攻撃者になり得る。

  →ICカード自身が単独で攻撃に耐えることが重要である。

  →第3者評価・認証になじむ(一定期間の攻撃耐性が保証される必要)。

  →有効期限を設定し、一定期間後に古いICカードをリプレースする。
- IoT機器の中には以下のような種別のものがあり得る。
  - ICカードと類似の運用環境(安全ではない)。
  - 攻撃への耐性が未知数。
  - 運用される期間が長い。
  - 保護や管理がされない。

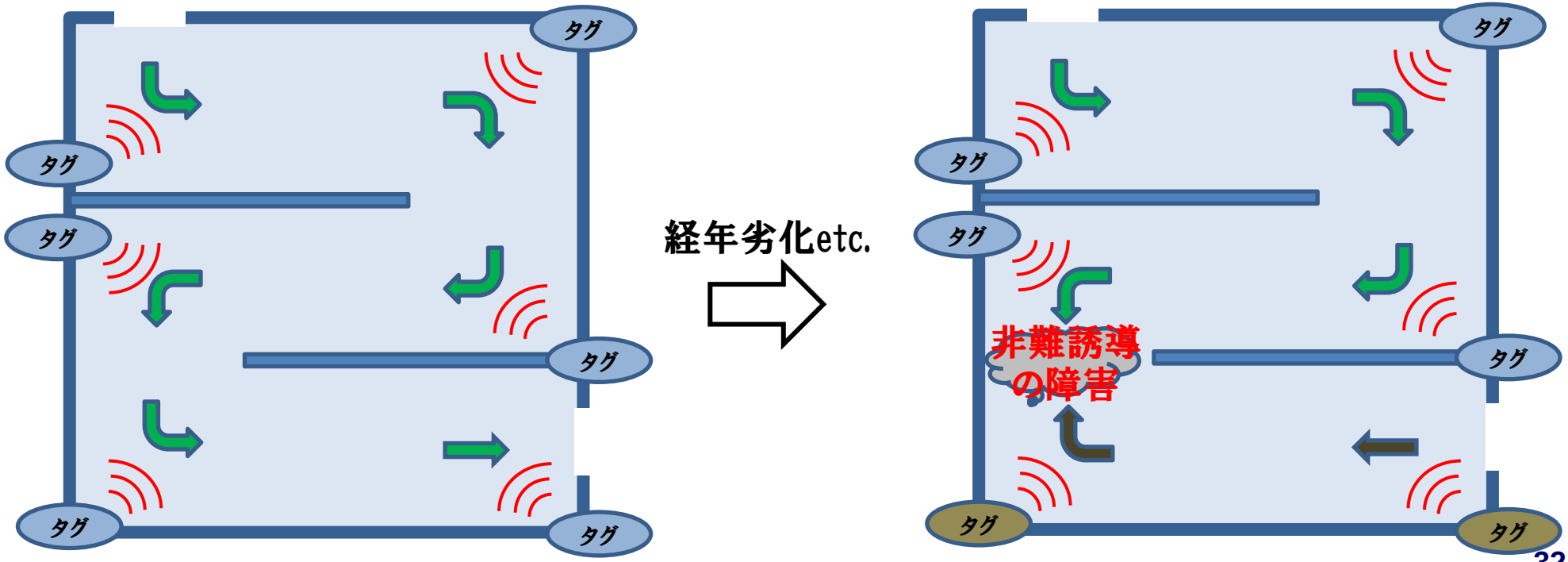
第3者評価・認証のコストを負担できない

自身の設備で試験できない

- 特に容易に持ち運べるIoT機器は想定外の環境で使用される。

懸念（保護・管理されないIoT機器による被害）

- 保護、管理されないIoT機器がインフラとして配置されている場合には、提供される情報が信頼できない恐れがある
  - 例：もしも美術館内での見学順路ガイド用ICタグに不具合があった場合
- 悪意を持って特定のタイミングで一斉に誤動作させられた場合には深刻



第4部　ハードウェアへの攻撃

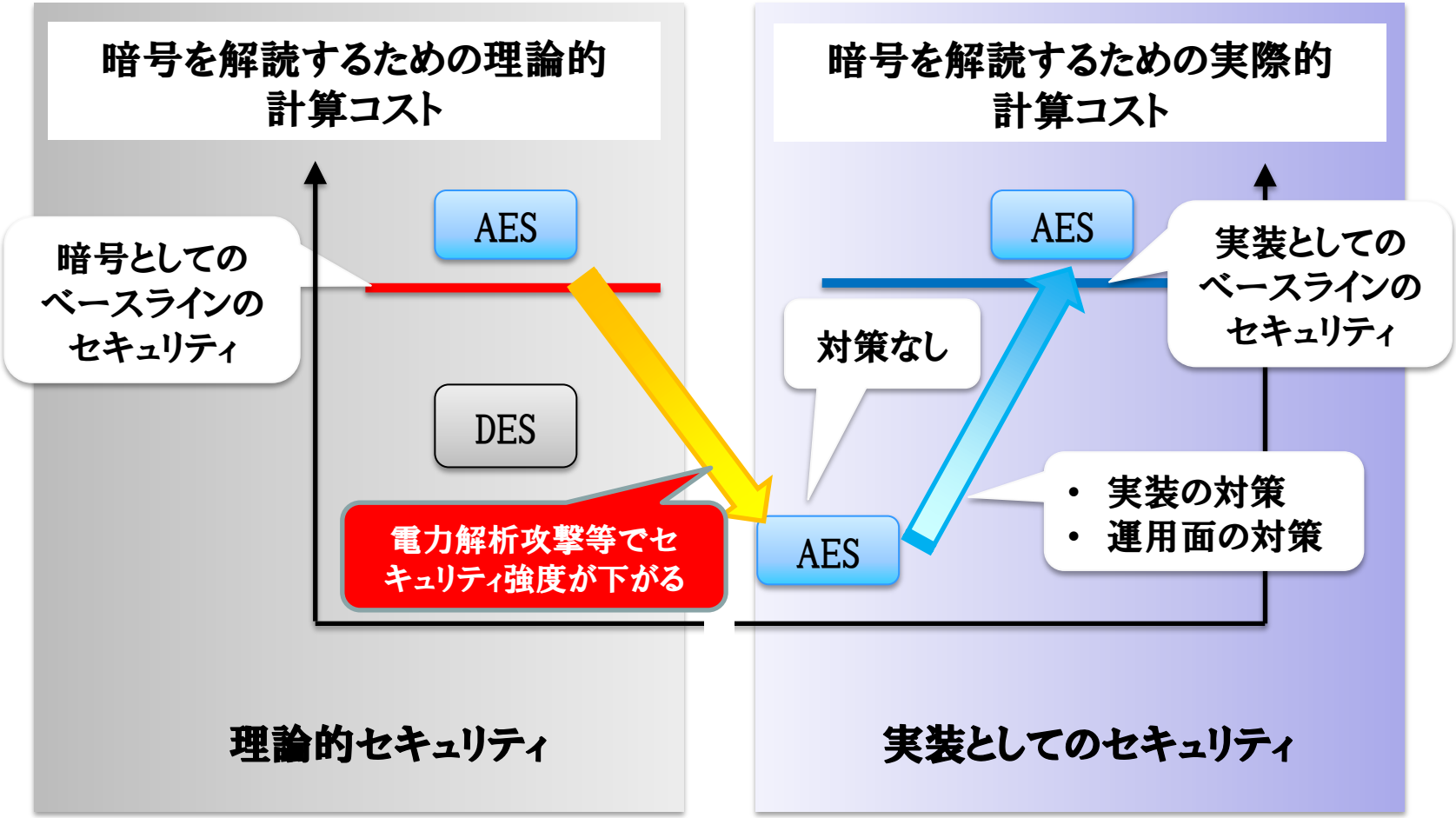
- スマートカード、暗号実装
- 物理解析
- サイドチャネル攻撃
- 故障注入攻撃

スマートカードのハードウェアセキュリティ

- スマートカードの第3者評価・認証の関係者が集まって、考慮すべき「攻撃シナリオ」とその「点数」を規定した文書「アタックメソッド」を作成している。
- 攻撃シナリオでは以下のカテゴリを網羅している。
  - 物理攻撃
  - センサ、フィルタへの攻撃
  - テスト機能の悪用
  - 乱数生成器への攻撃
  - 悪意のあるJavaカードアプリケーション
  - ソフトウェア攻撃
- 代表的なハードウェアへの攻撃カテゴリとして、以下の3つについて最低限の知識を持つ必要がある。
  - 物理攻解析
  - サイドチャネル攻撃
  - 故障注入攻撃

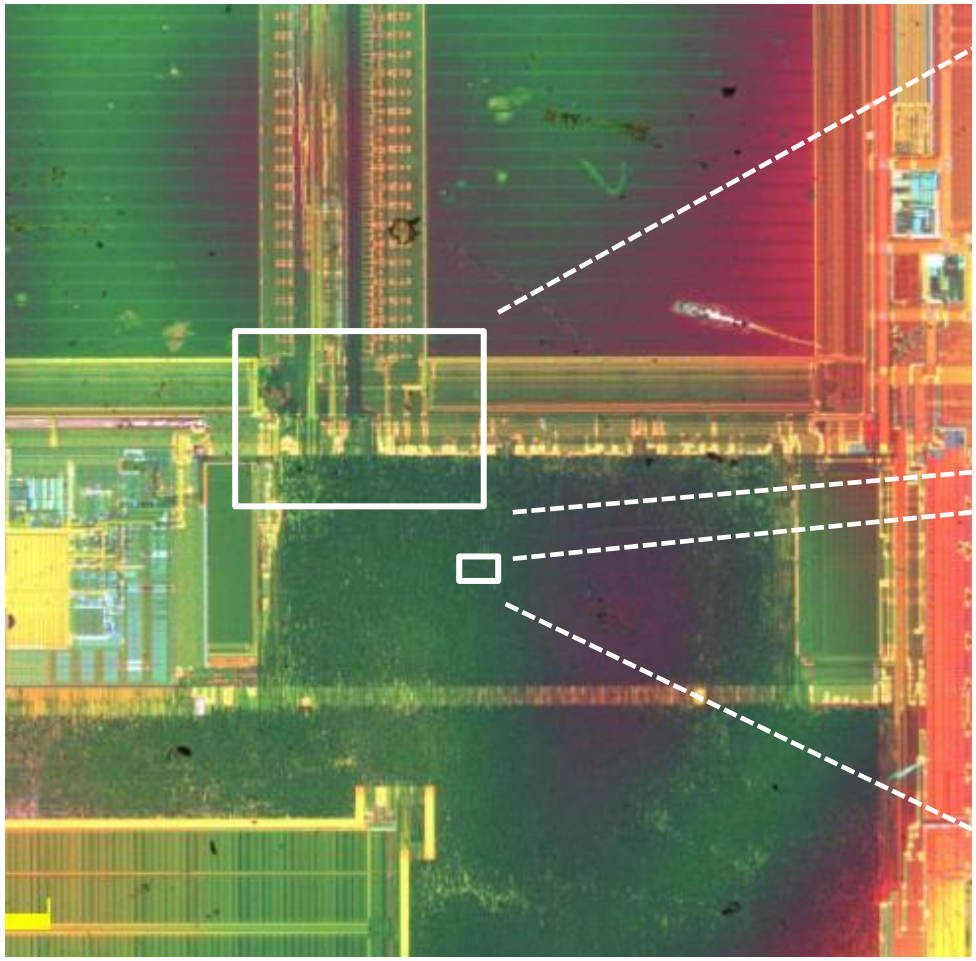
暗号実装のハードウェアセキュリティ
(理論と実装は違う)

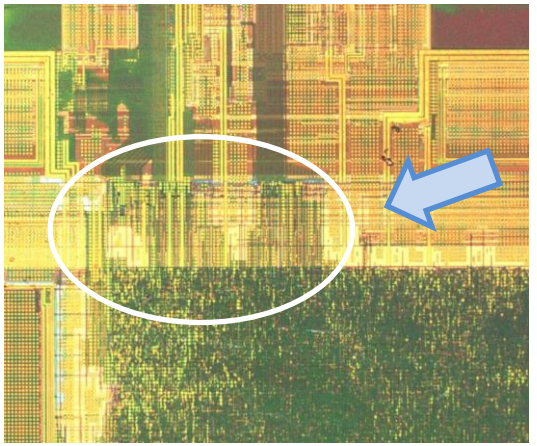
- 実装に不備があると暗号の安全性を脅かす



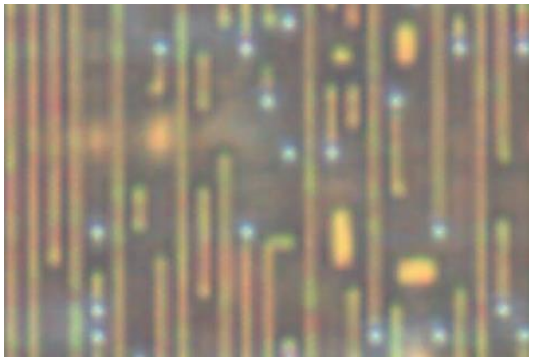
物理解析（事例1: ICの観察）

- スマートカードから取り出したICチップの観察





ランダムロジックからメモリへのアドレス線がレイアウトされていることが観察できる。



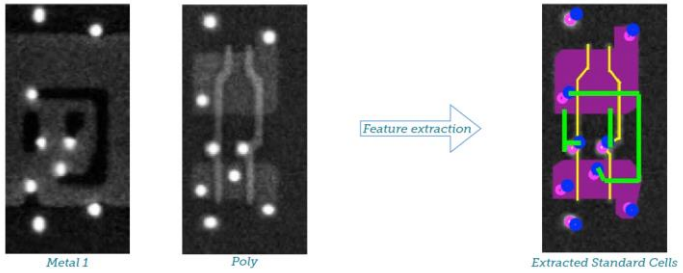
ランダムロジックの配線が観察できる。

レイアウトを探索して、ある配線の信号を直接的に測定されたり、改ざんされたりする恐れがある。

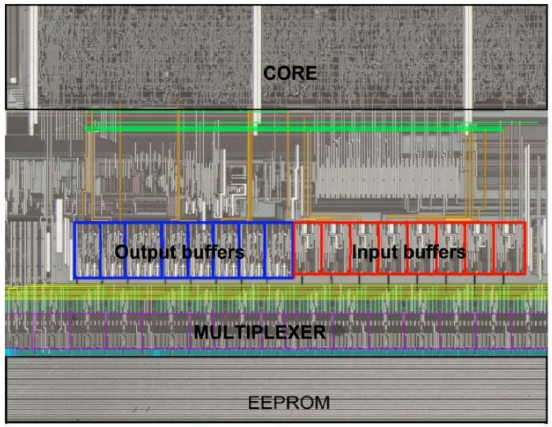
物理解析（事例2：ICチップのリバースエンジニアリング）

- ADVANCED IC REVERSE ENGINEERING TECHNIQUES: IN DEPTH ANALYSIS OF A MODERN SMART CARD (BlackHat USA 2015)

各層のレイアウト写真→パターンを抽出
→レイアウト情報（ポリゴン形式）

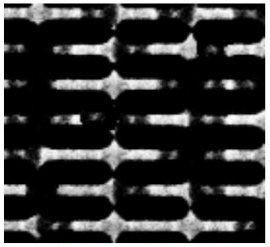


メモリとランダムロジック境界の
リバースエンジニアリング

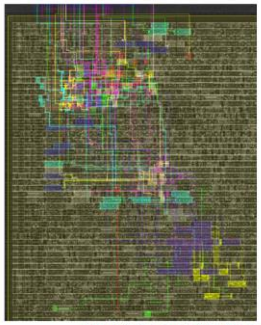


External Flash Buffers

ROMデータの解析


Bits revealed by etching

隠されたマルチプレクサ
の発見


Manual Tracing inside the core

シミュレーション
によるふるまいの
検証と修正

・使われている装置、テクニック、手法が設計者と同じ

・カスタム設計であっても解析ができると結論している。

ICチップのセキュリティビジネスに大きな誤解を与える。

＊出展：参考資料28

物理解析（事例2：ICチップのリバースエンジニアリング続き）

IPA

- 有料TVのスマートカードでのトレンド：常に最先端の対策を進めた事例

～1995	～2000	～2005
・シールドなし	・パッシブシールド	・内部オッシレータ
・スクランブリングなし	・バススクランブリング	・アクティブシールド
・暗号化なし	・暗号化	・バススクランブリング
		・暗号化
		・攻撃センサー
		・ハードウェア冗長化
		・カスタム化ハードウェア

- 今後は、バックドア、IP盗難、偽造、etc.のリスクが高まる恐れ。

＊出展：参考資料28

物理解析（現状についてのまとめ）

- セキュリティ性のある機能はICチップ内に閉じて実装しなければ、最低限の安全性も維持できない。
- ICチップのプロセスの微細化進行に伴い、多くのセキュリティビジネス関係者が、物理解析による攻撃は現実的ではないと考えていた。
- 2010年のBlackHatでのICチップのリバースエンジニアリングの発表は、関係者に衝撃を与えた。
- ICチップ単体の資産の侵害は大きくないが、設計内容を暴露して自身の技術的な宣伝に利用するビジネスが生まれてしまった。
- スマートカード関係者はすでに設計～運用の各フェーズで対策を打っている。
- 今後は、スマートカードよりも簡単に攻撃できる製品が狙われるのではないか？

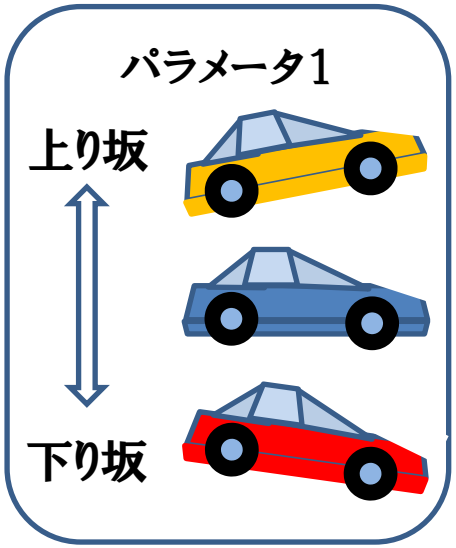
サイドチャネル攻撃とは

左記のような副次的な生成物から
秘密情報を推測する攻撃。

- 設計者や製造者には情報を提供する意図は無い。
- 動作の結果として発生するため、意図的に対策をしない限り、情報の漏洩を抑えられない。

サイドチャネル攻撃（アナロジ1：車のエンジン音）

- 自動車の発生するエンジン音だけでも、走行状態の差が分かる。



パラメータ2：回転数

パラメータ3：吸気温度

パラメータ4：オクタン価

パラメータ5：アクセル開度

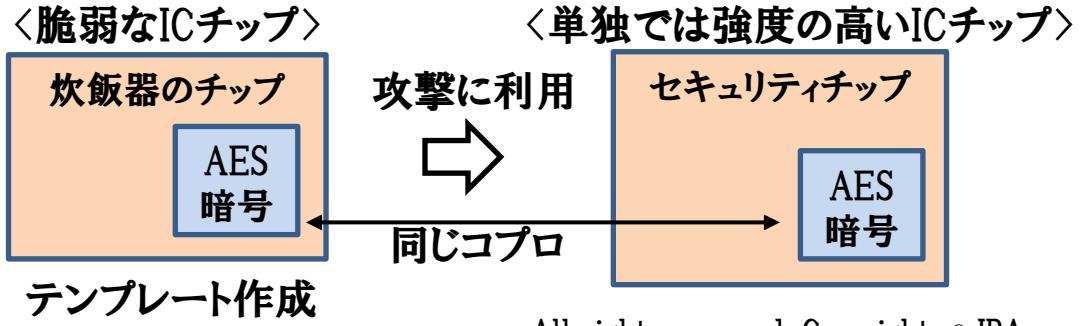
・・・

すべてのパラメータを網羅してエンジン音を記録すれば、辞書データ（テンプレート）が作成できる。

同じエンジンを搭載した車であれば、エンジン音から走行状態を推測できる。

特定の場所からの走行経路が秘密であれば、エンジン音を介して秘密情報が漏えいするとも言える。

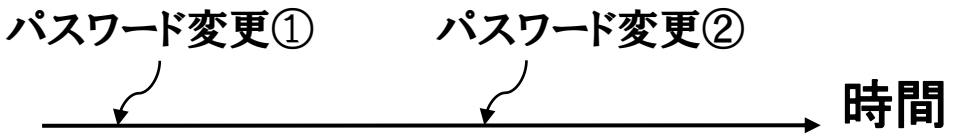
- 攻撃の踏み台があると危険



サイドチャネル攻撃（アナロジ2：パスワードの変更）

- パスワードは定期的に変更することが望ましい。

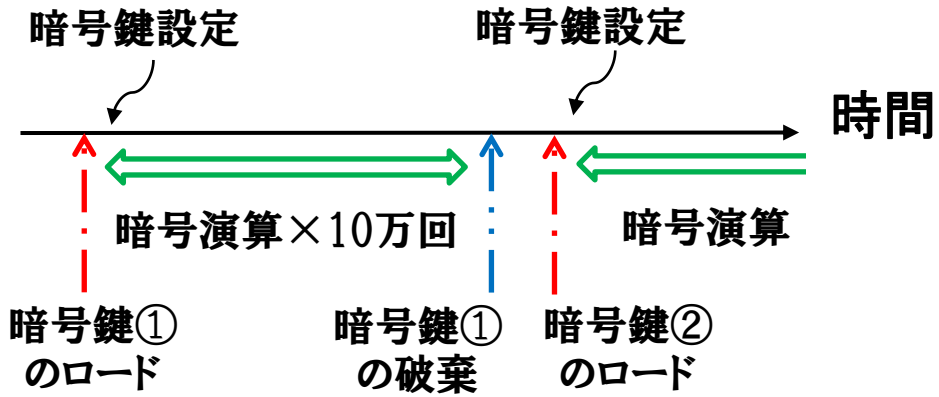
〈Windowsのパスワードなど〉



レインボーアタックなどパスワードを暴露する解析に要する期間よりも短い期間内での変更が望ましい。

- 暗号鍵も定期的に変更することが望ましい。

〈暗号コプロセッサの使用〉



・暗号鍵のロードは攻撃対象。

・暗号鍵の破棄も攻撃対象。

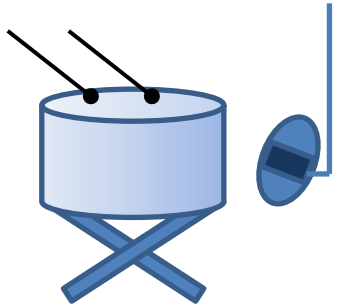
・同じ暗号鍵での暗号演算の繰り返しも攻撃対象。

・適切な頻度での変更が必要。

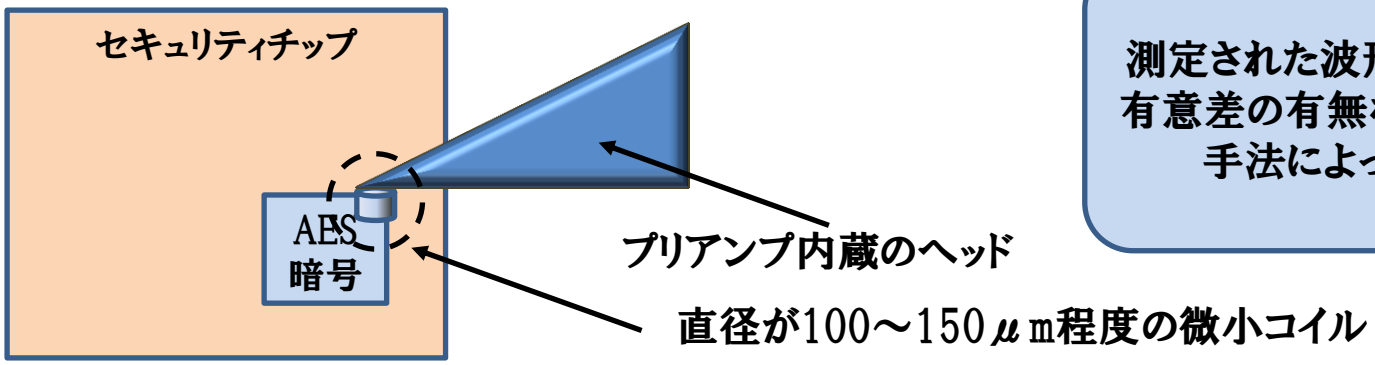
・不揮発性メモリ中に、あらかじめ複数の暗号鍵を用意しておく場合には、メモリ解析による直接的な読み出し（物理解析）を、警戒しておく必要。

サイドチャネル攻撃(アナロジ3:オーケストラ)

- オーケストラでは多数の楽器が同時に演奏している楽章で、特定の楽器の音を選択的にとらえることは難しいが、特別にマイクを近づければ可能。



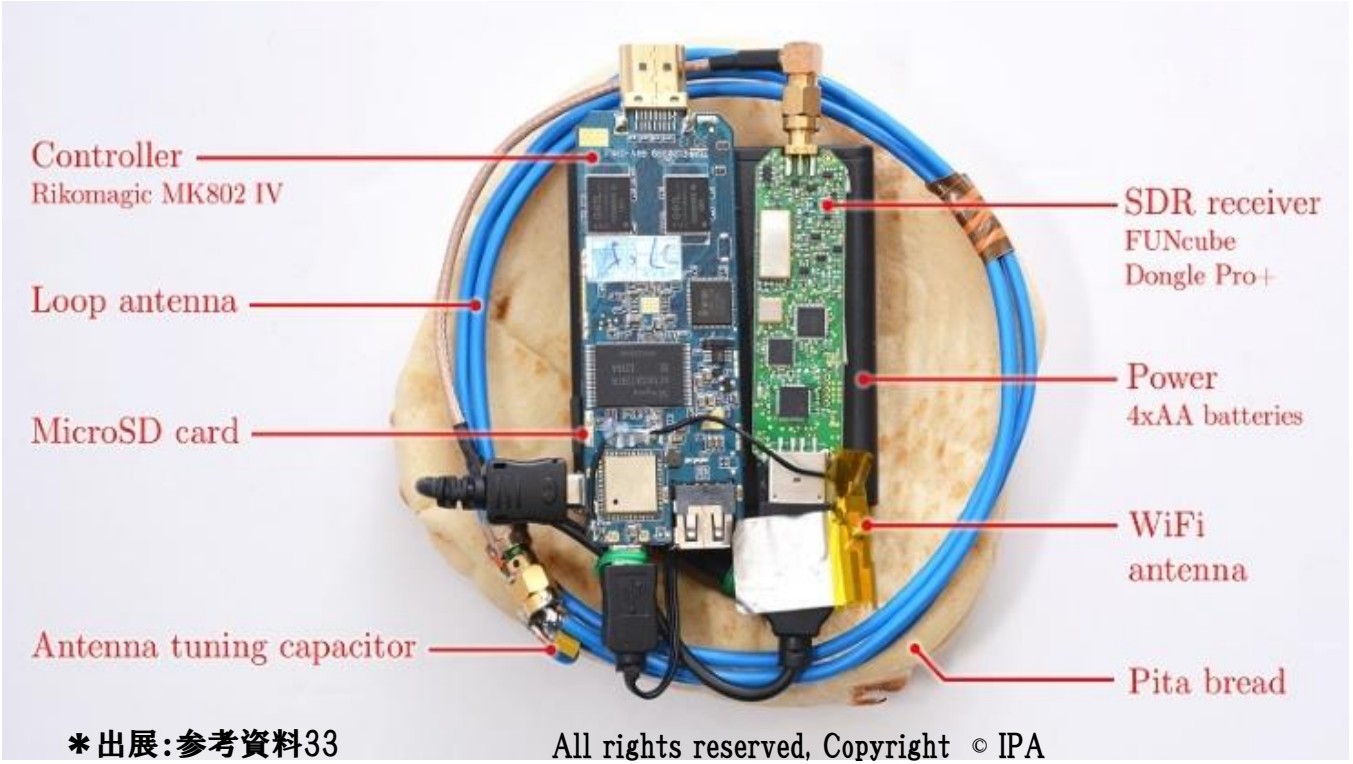
- 暗号コプロの近傍に微小コイルを接近させれば、他のノイズ源に邪魔されずに暗号演算の電磁波を観測することができる。



測定された波形データは統計的に有意差の有無を検証する数学的な手法によって解析される。

サイドチャネル攻撃(新たな盗聴デバイス)

- Portable Instrument for Trace Acquisition (PITA)
- 19インチ離れたPCの電磁波を観測する盗聴デバイスを＄300で開発。
- PITAサンドに隠れるサイズで、新たなスキマーと言える。
- 通信の観測や記録が可能であり、暗号鍵の解析はオフラインで。



＊出展:参考資料33

・ループアンテナ
・マイクロSDカード
・Wi-Fiアンテナ
・単３電池×4
・ラジオレシーバ

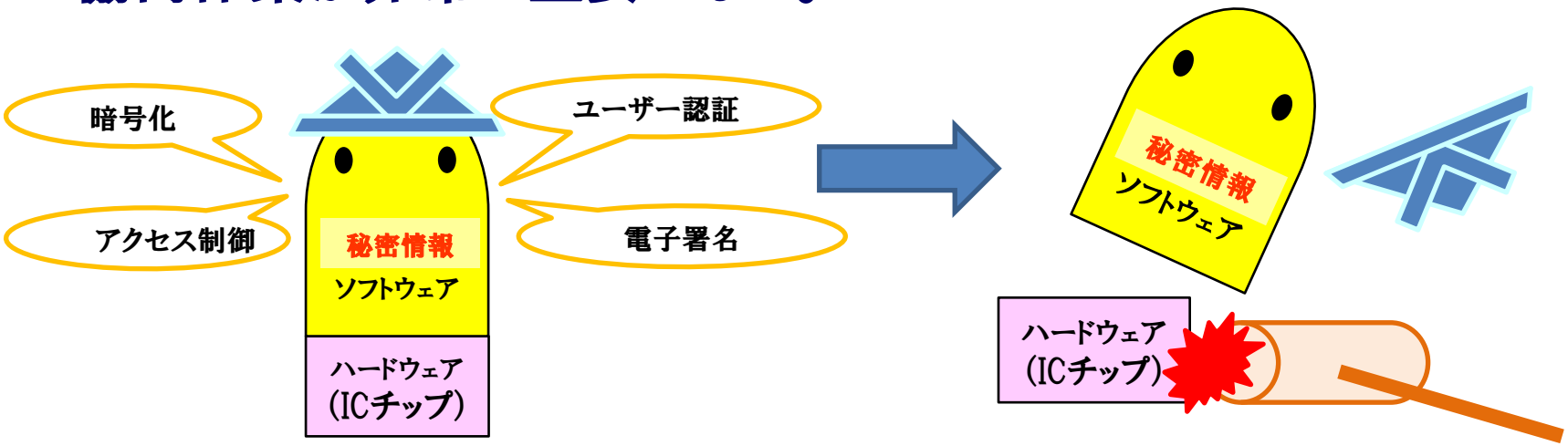
サイドチャネル攻撃（現状についてのまとめ）

- サイドチャネル攻撃に長期間かつ完全に対抗できるハードウェアはコスト的に難しい。
- 乱数を利用したマスキングやブラインディングでも限界がある。
- 暗号鍵も定期的に更新する必要がある。
- プロトコルのレベルで暗号機能の利用を制限したり、入力の制御や出力の観測を防止したりする対策が必須である。
- 同じハードウェアが、セキュリティ的に弱いICチップに搭載されている場合には、踏み台となるため、設計流用を追跡すべしという議論もある。
- 観測した波形を分析する数学的手法は、進歩がはやく頻繁なキャッチアップが必要。統計的な有意差の有無を検証する手法が台頭してきている。

暗号機能の長期間メンテナンスフリーはセキュリティ性の高い製品では不可能

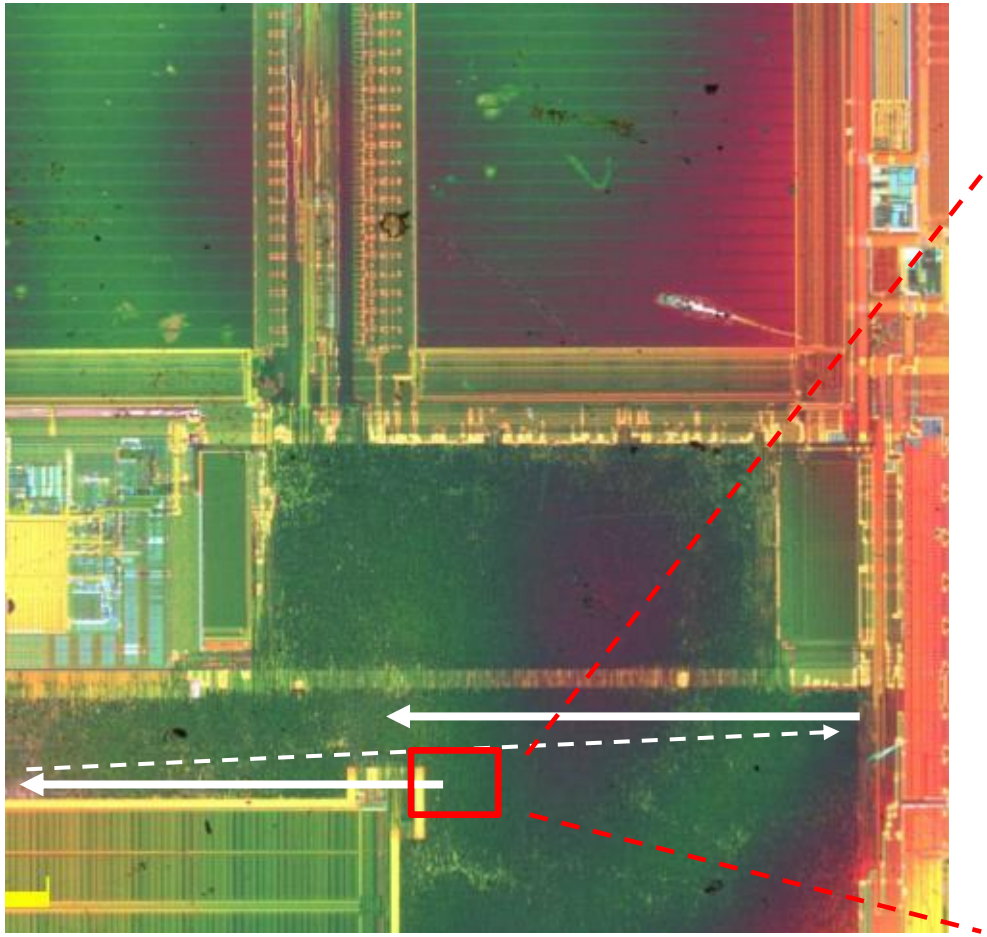
故障注入攻撃

- ソフトウェアのセキュリティが万全であっても、ハードウェアのセキュリティ機能に障害があれば、正常動作は期待できない。
- ハードウェア単独でも、セキュリティ機能を万全にできない。
- 暗号機能の故障動作から暗号鍵を推測できる場合がある。
- セキュリティが目的のエラー処理を悪用した攻撃もある。
- このカテゴリの攻撃に対抗するためには、ソフトウェアとハードウェアの協同作業が非常に重要になる。



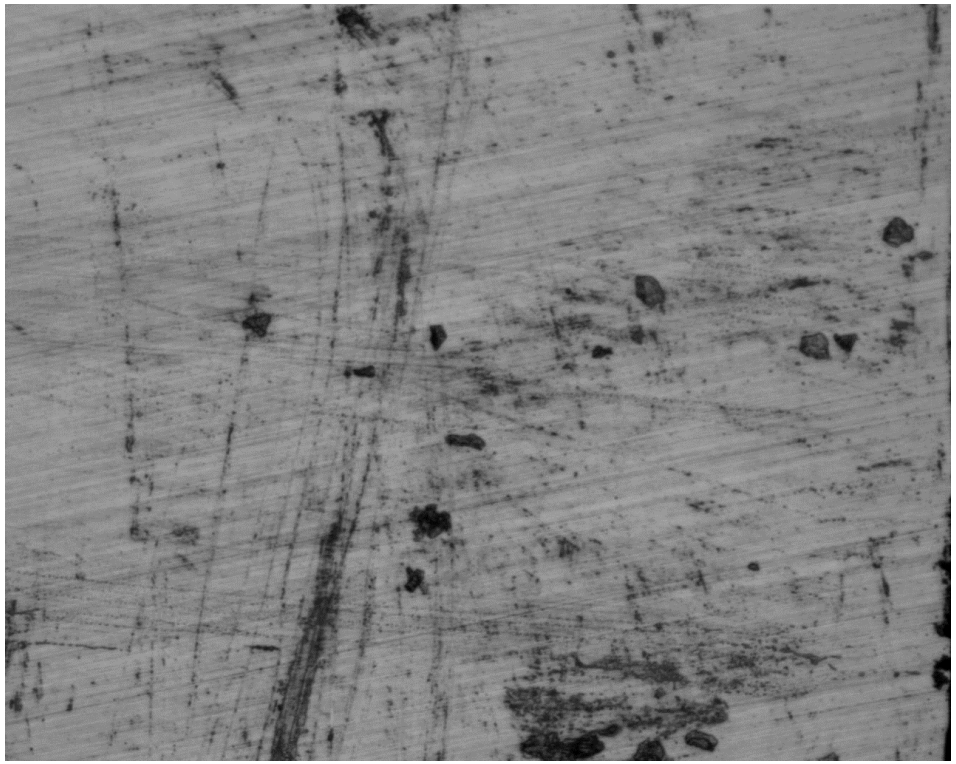
故障注入攻撃(レーザー照射攻撃(1/4))

- レーザー照射攻撃の事例



表面からの画像

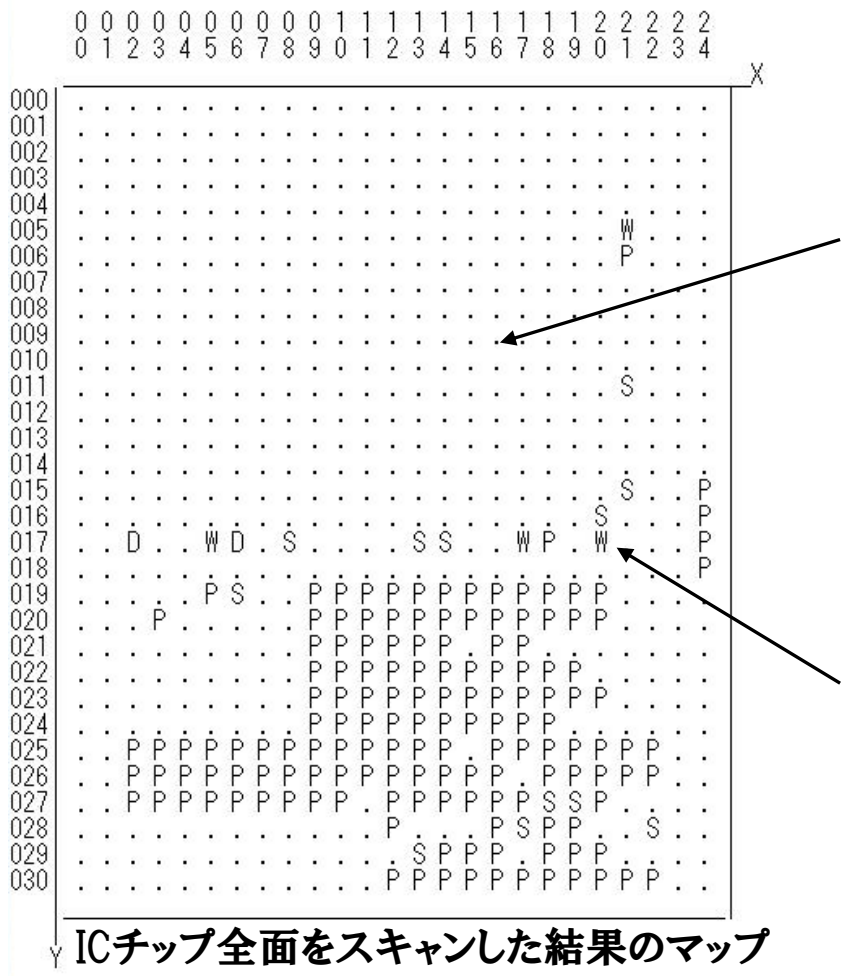
ICチップの裏面からレーザー照射のスキャンを実施している。(近赤外:1064nm)



裏面へのレーザー照射

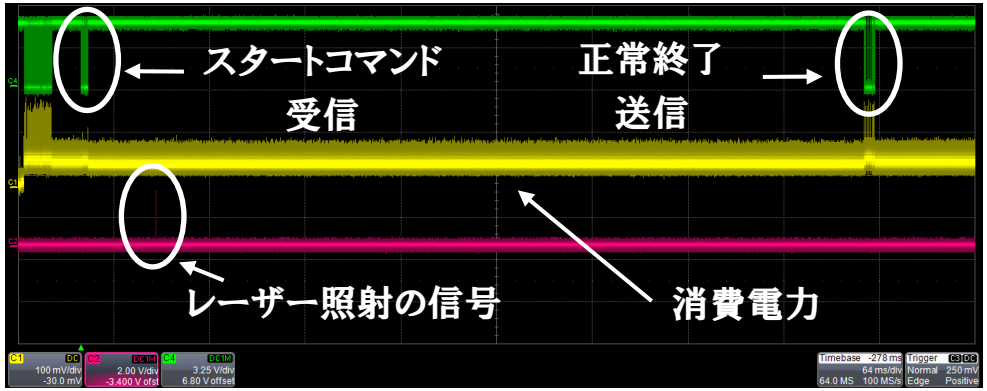
故障注入攻撃(レーザー照射攻撃(2/4))

- IF文の動作が影響された事例。

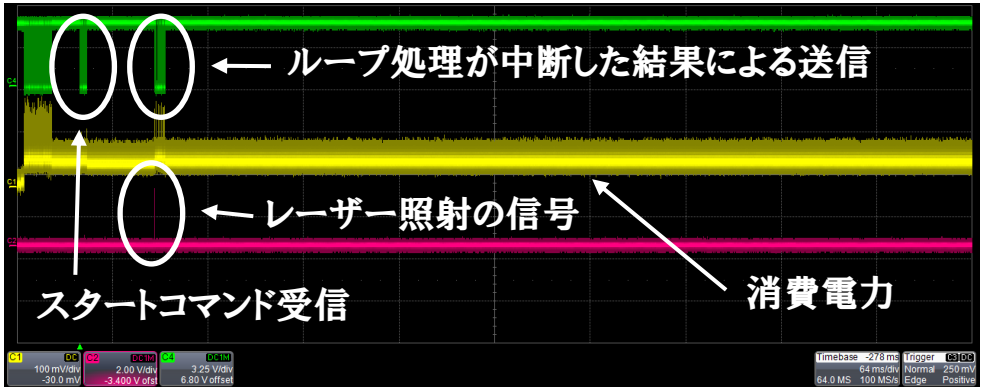


ICチップ全面をスキャンした結果のマップ

ICチップ正常動作時のオシロスコープ画面



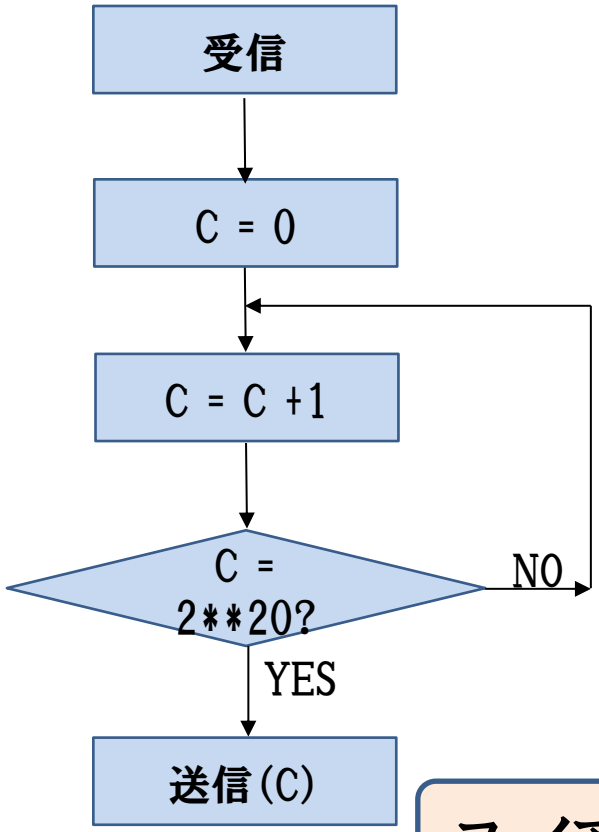
ICチップ誤作動時のオシロスコープ画面



故障注入攻撃(レーザー照射攻撃(3/4))

- レーザー照射によって、ループ処理が途中で終わってしまった。

ループ処理の流れ



ループ処理のアセンブラコード

```
...
LOOP
        cmp r1, r2    ; if A==B
        bne Fail1     ; firewall << 1st attack point
        nop
        ～
        nop
return_pass
...
```

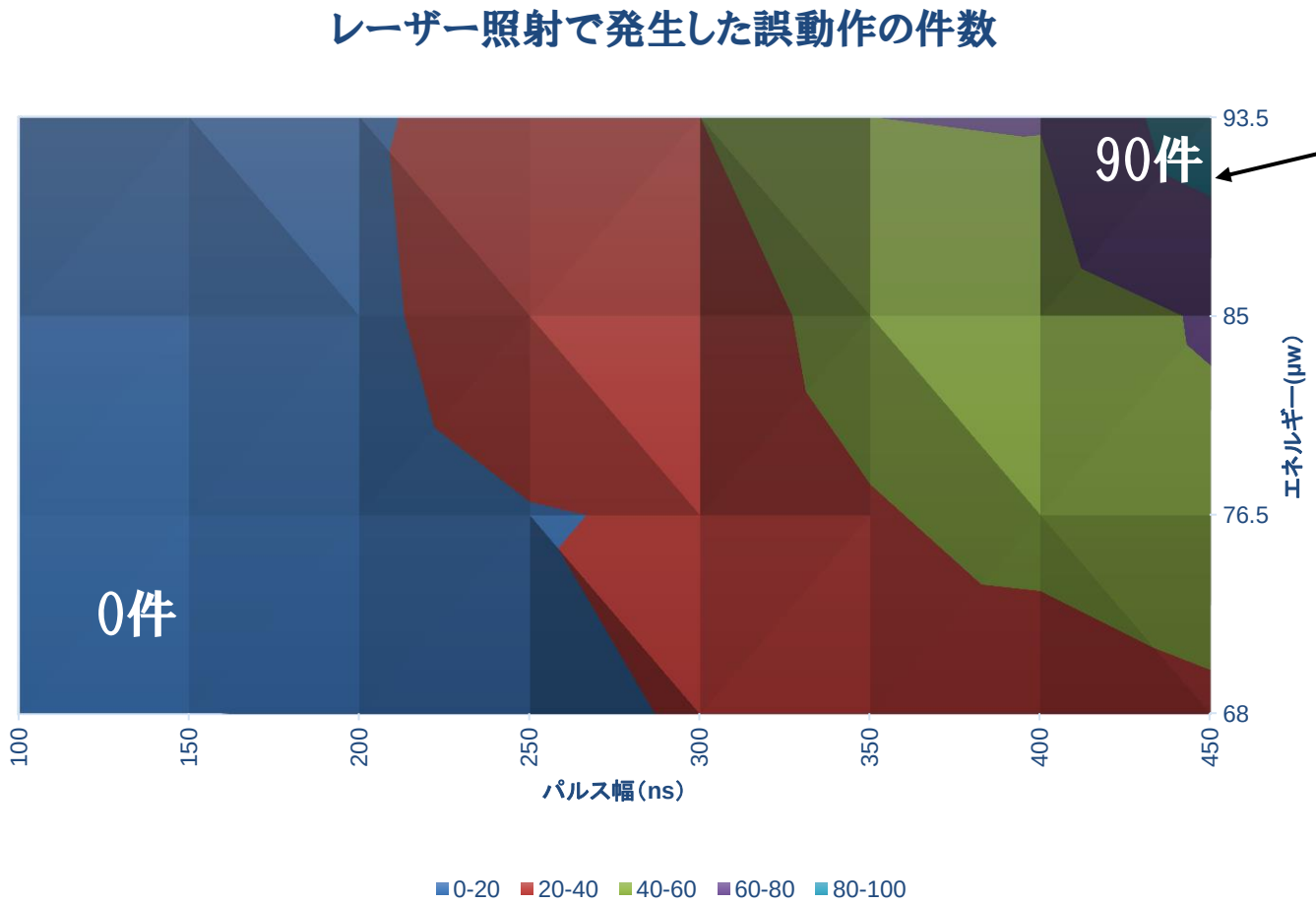
レーザー照射

レーザー照射によって分岐先が改変され、ループ処理が中断してしまった。

ファイアウォールやハイパバイザーの判定も改ざんされる恐れ

故障注入攻撃(レーザー照射攻撃(4/4))

- ICチップに発生した誤動作の件数の例と照射の電力。



数十μWのエネルギーで誤動作が発生している。

レーザー照射による侵入試験は制御性が良く、再現性も高いために採用している。特別に高いエネルギーを照射しているわけではない。

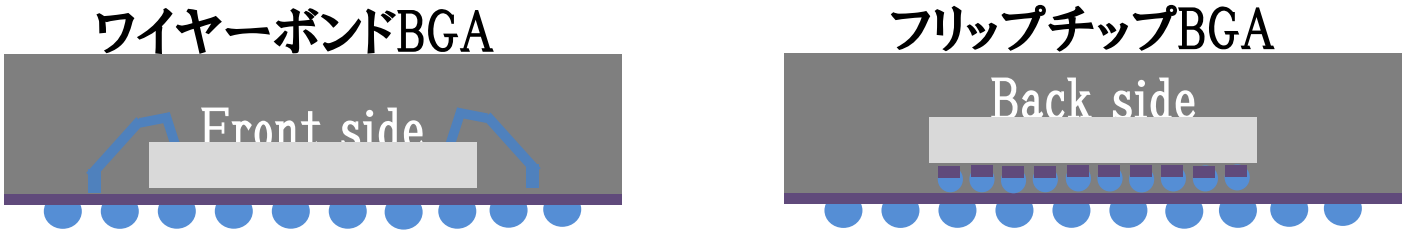
故障注入攻撃(レーザー照射攻撃への対策例)

- センサーの強化
  - メモリ周辺への光センサを充実させる。
- 冗長化
  - 必要な情報量よりも多くのビット数を使う。
  - データの読み出しを複数回行う。
  - データの複製を、ICチップ内の離れた場所に置く。
- 完全性の検証
  - パリティなど、データの完全性を検証するためのコードを付加して検証する。
  - プログラムのフローを一定間隔で検査する。
- レーザー攻撃では改ざんし辛い値の採用
  - レーザー攻撃で実現しやすい0xFFや0x00などの値は、重要なフラッグ値として使用しない。
  - “0101”のような、隣接するビットの値が異なる値を使用したり、エントロピーの小さいコードを使用する。

故障注入攻撃(EMFI:Electro-Magnetic Fault Injection)

- SoC (System on Chip)への攻撃
  - 組込み機器の基板上にあるBGAパッケージに搭載されたチップに対してレーザー攻撃を実行することはハードルが高い
  - BGAパッケージへの別の種別の攻撃方法
    - ワイヤーボンディングで表面(Front side)が上にある場合　タイプ1

    →Electro-Magnetic Fault Injection
      - 乱数生成器:　　微小コイルによるHarmonic Injection
      - ロジック、メモリ:　　微小コイルによるPulse Injection
    - フリップチップで裏面(Back side)が上にある場合→Forward Body Bias Injection　タイプ2



＊出展:参考資料22

故障注入攻撃(EMFIに必要な装置例)

タイプ1

- **電磁照射**

〈Harmonic Injection〉

任意波形生成装置

パワーアンプ

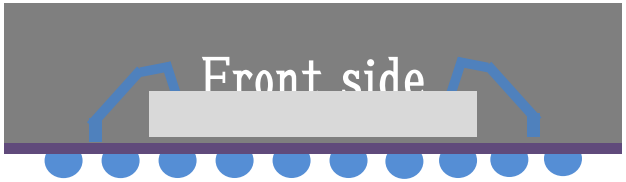
マイクロプローブ

〈Pulsed Injection〉

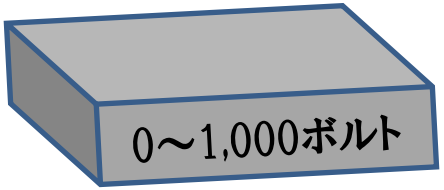
市販のパルス生成装置

微小コイル

ワイヤーボンドBGA



自作のナノパルス生成装置



微小コイル

要注意！
組込み機器への攻撃がレーザー照射よりも簡単

＊出展:参考資料22

故障注入攻撃(Forward Body Bias Injection)

タイプ2

市販のパルス生成装置

- パッケージ表面を削る
- ↓
- ICチップ裏面にニードルを当てる
- ↓
- ニードルに電圧パルスを入力
- ↓
- ICチップ内部のGND電位が変化

要注意！
組込み機器への攻撃がレーザー照射よりも簡単

＊出展:参考資料22

第5部　セキュリティコミュニティ

- スマートカードでの経験
- 最先端の攻撃レベルに対応する活動

セキュリティコミュニティ(スマートカードでの経験)

- スマートカード関係者が定期的に集まって、最新の攻撃手法の情報共有と「アタックメソッド」の更新を行っている。(国際的なセキュリティコミュニティ)
- テストラボが切磋琢磨することで、セキュリティコミュニティとして高いレベルでの侵入試験能力を維持している。
- 特に以下のカテゴリでの攻撃手法の進歩が早い。
  - サイドチャネル攻撃
  - 故障注入攻撃
- 以下のカテゴリの攻撃に対する対抗力は、セキュリティ関連製品開発の経験の有無が大きな差を生む。
  - 物理解析
- スマートカードのCC評価・認証では、おおよそ2年程度で認証の再査定をする国がある。

セキュリティコミュニティ(最先端の攻撃レベルに対応する活動)

- 公知の攻撃方法に対してアドバンテージを持つ
- 実際のフィールドに存在する攻撃者の行動に関心を持つ
- ハイレベルな議論によって詳細情報の漏洩を防止する
- アカデミック研究者のコミュニティとコンタクトを持つ
- 競争と協同のバランスを取る
- 貢献度を常にチェックする
- セキュリティとビジネスのバランスを考慮する
- 形式にはこだわらない

セキュリティコミュニティ(公知の攻撃方法に対してアドバンテージを持つ)

- 国際学会等で(セキュリティ・コミュニティ外のメンバーから)発表される攻撃方法がコミュニティから見て数年遅れている状況が望ましい。
  →その時間差が評価・認証された製品の安全マージンとなる。ライフの長い製品の場合には難しいケースもある。
- テストラボが新たに考案した攻撃方法は、一定期間経過後に国際学会等で(ハイレベルな内容にとどめて)発表することが望ましい。
  →セキュリティ・コミュニティ内では、それ以前に発表や指導などを実施する。(有料のセミナ形式にすることで、考案したテストラボは収入を得る。このような活動はテストラボ間の技術レベルの平準化にも寄与し、試験基準の議論を効率的にする。)
- テストラボは得意な攻撃をさらに高度化することで、セキュリティ・コミュニティ内での存在感を高めることができる。

セキュリティコミュニティ（実際のフィールドに存在する攻撃者の行動に関心を持つ）

- 実際にフィールドで製品に攻撃を実行する攻撃者のふるまいのイメージを明確に持つことが重要。そうでなければ試験基準の議論は収束しない。
- 攻撃者のふるまいの変化にも敏感に反応する必要がある。→ビジネスとして特定の製品を攻撃するケースが増えている（BlackHatなど）
- リスクアセスメントの議論では、実際には存在しないタイプの攻撃者が実施するかもしれない攻撃シナリオに、無駄な時間を割いてしまうことがある。
- セキュリティ・コミュニティ内のテストラボと実際の攻撃者で何が決定的に異なるのか？は重要。→テストラボにアドバンテージを与えることが必要なケースもある（非常に特殊なサンプルの提供など）。
- 国際会議での攻撃方法の発表から、実際のインシデント事例の発生までが短くなってきている。

セキュリティコミュニティ(ハイレベルな議論によって詳細情報の漏洩を防止する)

- 試験基準を議論する際に、詳細な攻撃手順にまで踏み込まないハイレベル(いわゆる抽象的レベル)での議論が必要。
  →ビジネスで競争する者どうしが議論するために必要な工夫。
- テストラボが国際会議等で発表する際も、対抗策をより詳細に。
  →攻撃方法を詳細に説明する必要は無い。
- 技術レベルがバランスしていれば、攻撃手順の詳細まで言及しなくても、コミュニケーションが可能。

セキュリティコミュニティ(アカデミック研究者のコミュニティとコンタクトを持つ)

- 理工学、数学、化学、生物学等の研究者とのコンスタントな交流は必要。
- 半導体の物性、信頼性、そして故障の解析に使用する装置は、高度な攻撃に利用できる。→フィールドで実際の製品に対して攻撃に利用されることはまれであるが(＊一般的に管理者が用途や使用を監視している)、認識は必要。どこかの国で無頓着にレンタル開始されたら危険。
- 新しい測定技術、解析技術は新しい攻撃方法につながる可能性がある。
- 最先端の微細化テクノロジに対応して故障解析できる装置は、裏返せば最先端のデバイスを攻撃できる。
- 最近の傾向として攻撃の複合化が進んでいる。

セキュリティコミュニティ(成果物)

- アタックメソッド文書の作成と合意
  - 攻撃シナリオを列挙し、評価・認証で考慮すべき攻撃手法を明確にした。
  - 攻撃シナリオの難易度を議論し、関係者が点数づけに合意した。
  - 該当する攻撃シナリオにすべて耐性が無ければ合格しない。
- アタックメソッド文書の内容は頻繁に見直される。
- 最新のアタックメソッド文書はコミュニティ内で管理され、攻撃者には情報を提供しない。
- アタックメソッド文書が、正式にテスト基準として使用されるまで一定の猶予期間をおき、設計、製造や環境の対応ができるようにする。

第6部　IPAの取り組みの紹介

- ハードウェアセキュリティセミナー
  - 導入～入門～実践
- 装置・評価ツールの利用
- テストビークル（評価対象）の利用
- プロテクションプロファイル

セキュリティセミナー

- 導入編から技術編までの開催

導入コース

対象：
セキュリティに関心を
持つ一般の方

内容：
ICチップの仕組み
攻撃と対策
評価された製品

技術コース（入門編）

対象：セキュリティに関心
を持つ開発者

内容：暗号アルゴリズム
実際の攻撃

技術コース（実践編）

対象：セキュリティに関心
を持つ開発者

内容：暗号の実装
実際の対策

評価ツールの利用

- Riscure社Inspector SCA/FI
  - ダイオードレーザ

#	モード	波長	出力	スポット	反復レート
1	マルチ	808nm	14w	6×1.4μm	25MHz
2	マルチ	1064nm	20w	6×1.4μm	25MHz

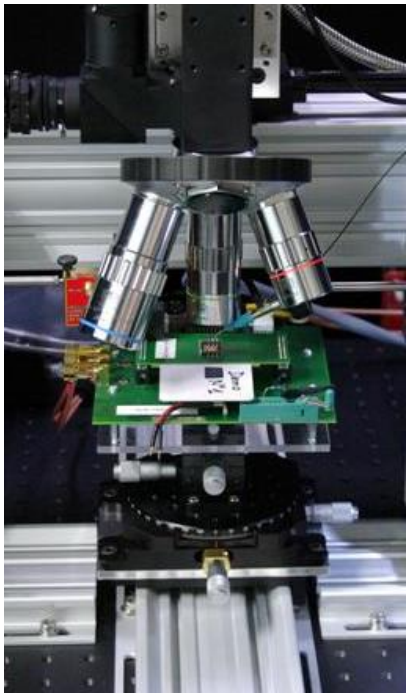
  - アドバンスト・トリガ生成装置
    - 200MS/s×8bit入力
    - 波形登録:512×1、256×2
    - トリガ生成遅延:パターン入力後500ns
  - サイドチャネル(PA、EMA)評価装置
  - グリッチ(VCC、CK)評価装置

評価ツールの利用

- Trusted Labs社DLFI
  - レーザ

#	モード	波長	出力	スポット径	反復レート
1	モノ	976nm	1.7w	6μm	250MHz
2	マルチ	976nm、1064nm	4.5w	6.6μm	250MHz

  - トリガ生成装置
    - 調整可能なトリガ生成ロジック(最大8つ)
    - リアルタイムシンクロナイゼーション機能
      - 電力波形／電磁波波形を
        計2チャンネル同時サンプリング(12bit量子化)
      - 入力:～1.8GS/s
      - 検知波形登録:～700ポイント
      - 登録波形の検知を4段階までチェーン化した
        トリガ生成が可能
  - プローブ
    - 150μm径、～6GHz、水平、垂直



評価ツールの利用

- Secure-IC社Analyzer
  - EMA
    - プローブ径:＜1mm
  - EMフォールト注入
    - 100MHz～1GHz
    - 出力:～140W
  - スマートトリガ
    - 入力:250MS/s×8bit
    - 検知波形登録:1024×1、512×2
    - トリガ生成遅延:パターン入力から＜2μs
  - XYZステージ
  - シールドボックス

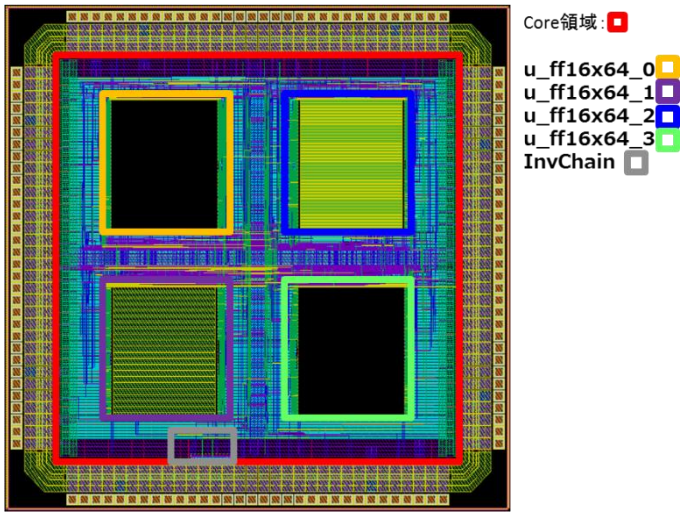
テストビークル(評価対象)の利用

- ICカードのテストビークル用ICチップ
  - JHAS [ATTACK METHOD]に記載されている下記4項目を評価できる。
    - Perturbation Attacks
    - Fault Attacks
    - Side Channel Attacks
    - Attacks on RNG

  - ICカードのR/WまたはSASEBO-Wで評価可能
    - ARM, DES, AES, RSA, V/F-センサ、暗号Lib付き
    - ICSS-JC、大学、JHASメンバーは利用可能

テストビークル(評価対象)の利用

- テストビークル用ICチップ(カスタム回路)
  - 攻撃シナリオに対抗するカスタム回路
    - CHES, SCIS等で報告のあったシナリオ、対抗策
    - 要素回路を実装した評価チップ
      - 基本特性
        DFFアレー、インバータチェーン
      - 複数の実装によるAES

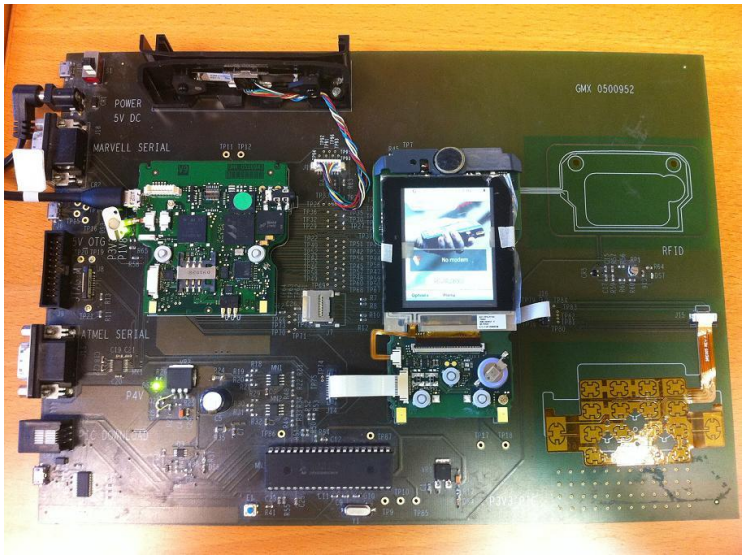


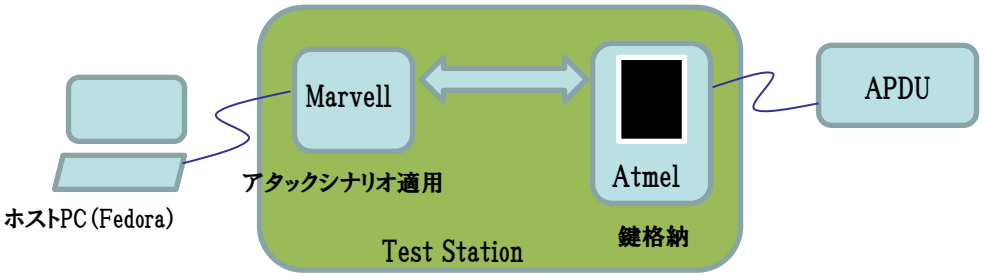
  - カスタム回路の評価環境
    - 評価ソフト
    - 評価ボード(SASEBO-R、SASEBO-W)
    - ホワイトボックスの実装仕様書

テストビークル(評価対象)の利用

- **決済端末テストビークル**
  - GMX社SK-20端末をボード上に展開
  - JTEMS (JIL Terminal Evaluation Methodology Subgroup)の ATTACK METHODに記載のシナリオが評価可能
    - Intrusion of Sensors, Switches and Filters
    - Software Attacks

    など
  - 全体の接続イメージ





プロテクションプロファイル: TPM-thin

- TPMのプロテクションプロファイルが開発されている。
- 車載EUCなどでの利用を想定している。
- TPM-thinのドラフトが、３月をめどに完成する予定。
- IPAは、来年度にプロテクションプロファイルのCC評価・認証を推進する。

参考資料(1/2)

- 参考資料1:デジタル大辞泉 IoT https://kotobank.jp/word/IoT-676428
- 参考資料2:国におけるIoT(モノのインターネット)に関する取り組みの現状 ニューヨーク便り 2015年8月 https://www.ipa.go.jp/files/000047543.pdf
- 参考資料3: Postscapes http://postscapes.com/
- 参考資料4: Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) https://www.vdi.de/fileadmin/user_upload/VDI-GMA_Statusreport_Referenzarchitekturmodell-Industrie40.pdf
- 参考資料5: Industrial Internet Consortium http://www.iiconsortium.org/
- 参考資料6: IoT推進コンソーシアム http://www.iotac.jp/
- 参考資料7: What Exactly Is The "Internet of Things"? https://s3.amazonaws.com/postscapes/IoT-Harbor-Postscapes-Infographic.pdf
- 参考資料8: SHODAN https://www.shodan.io/
- 参考資料9: IPA テクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」～SHODANを活用したインターネット接続機器のセキュリティ検査～ https://www.ipa.go.jp/files/000036921.pdf
- 参考資料10:一般社団法人 JP CERT コーディネーションセンター SHODANを悪用した攻撃に備えて ―制御システム編― https://www.jpcert.or.jp/ics/20150609ICSR-shodan.pdf
- 参考資料11: http://www.fool.com/investing/general/2015/06/10/apple-inc-co-founder-steve-wozniak-believes-the-in.aspx
- 参考資料12: http://www.computerworld.com/article/2487816/emerging-technology/why-the--internet-of-things--may-never-happen.html
- 参考資料13: http://www.forbes.com/sites/oreillymedia/2014/09/23/who-will-build-the-god-platform-for-the-internet-of-things/
- 参考資料14: http://www.computerworld.com/article/2687741/why-the-internet-of-things-may-never-happen-part-2.html
- 参考資料15: IoT(M2Mもしくはスマート家電ネットワークサービス等)への主な脅威候補 (般)日本クラウドセキュリティアライアンス http://www.cloudsecurityalliance.jp/WG_PUB/IoT_WG/Threats-IoTCloud%20Service-final%20(%20Reviewed).pdf
- 参考資料16: OWASP Internet of Things Top Ten https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

参考資料(2/2)

- 参考資料17: Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show
- 参考資料18: 重要生活機器の脅威事例集 Ver. 1.2 一般社団法人重要生活機器連携セキュリティ協議会
- 参考資料19: つながる世界のセーフティ&セキュリティ設計入門 https://www.ipa.go.jp/files/000005118.pdf
- 参考資料20: 組込みシステムの安全性向上の勧め(機能安全編) https://www.ipa.go.jp/files/000048104.pdf
- 参考資料21:「つながる」システムに向けたソフトウェア品質向上のためのガイドブックを作成 ～「つながる世界のソフトウェア品質ガイド(ダイジェスト版)」を先行公開～ https://ipa-rcpt.ipa.go.jp/cgi-bin/enquete/registEnquete.cgi?EID=b913e41893bb730bde37e8a4f561c6b3
- 参考資料22: FDTC 2012: Techniques for EM Fault Injection: Equipments and Experimental Results http://conferenze.dei.polimi.it/FDTC12/shared/FDTC-2012-keynote-1.pdf
- 参考資料23: 作業員がロボットにつかまれ死亡、独フォルクスワーゲン工場http://www.cnn.co.jp/business/35066855.html
- 参考資料24: コンピュータ将棋プロジェクトの終了宣言 http://www.ipsj.or.jp/50anv/shogi/20151011.html
- 参考資料25: 本当に恐い人工知能はもう普通に働いている http://toyokeizai.net/articles/-/77118?page=3
- 参考資料26: ロボットは東大にはいれるか http://21robot.org/
- 参考資料27: BlackHat2010: Hardware is the New Software
- 参考資料28: ADVANCED IC REVERSE ENGINEERING TECHNIQUES: IN DEPTH ANALYSIS OF A MODERN SMART CARD https://www.blackhat.com/docs/us-15/materials/us-15-Thomas-Advanced-IC-Reverse-Engineering-Techniques-In-Depth-Analysis-Of-A-Modern-Smart-Card.pdf#search='blackhat+smartcard‘
- 参考資料29: How a criminal ring defeated the secure chip-and-PIN credit cards http://arstechnica.com/tech-policy/2015/10/how-a-criminal-ring-defeated-the-secure-chip-and-pin-credit-cards
- 参考資料30: Black Hat USA 2014 https://www.blackhat.com/us-14/briefings
- 参考資料31 : Black Hat USA 2015 https://www.blackhat.com/us-15/briefings
- 参考資料32: 更新:bashの脆弱性更新について(CVE-2014-6271等) https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html
- 参考資料33: ＄300 ‘PITA’ Device Steals PC Encryption Keys http://www.pcmag.com/article2/0,2817,2486651,00.asp

ご清聴ありがとうございました。

当セミナーに関する質問は以下のメールアドレスまでどうぞ。

jcmvp-info@ipa.go.jp