［ハードウェアセキュリティの最新動向］

①ハードウェアに対する物理攻撃
―サイバーだけでなくフィジカルも守る―

基般

本間尚文 東北大学　上野　嶺 東北大学

高まる物理攻撃のリスク

Cyber Physical System（CPS）や Internet of Things（IoT）といった新しい情報通信の形態においては，従来のサイバーセキュリティに加えて，実世界との接点となるハードウェアのセキュリティ（ハードウェアセキュリティ）が重要となる．現在，秘匿通信や認証といった情報セキュリティ上の機能は主に暗号技術によって実現されているが，ハードウェアへの物理的なアクセスによる攻撃（物理攻撃）は，暗号技術をも無効化し得る．また，そうした物理攻撃は，しばしば従来の情報セキュリティ技術の想定範囲外となるため，別途脅威分析や対策が必要となる．本稿では，以上の背景から，近年注目が高まるハードウェアに対する物理攻撃とその対策技術を概説する．

物理攻撃とは

本稿で取り上げる攻撃および対策は，主に暗号処理を実行する LSI（大規模集積回路）を対象に研究開発がなされてきたものである．これは，暗号処理の対象となるデータは本来保護されるべきものであり，最も攻撃の標的となり得る（攻撃に成功した場合の価値が高い）ことに起因する．しかし，近年では，これを発展させた汎用プロセッサに対する攻撃や機械学習処理への攻撃などの報告も増加傾向にある．

さて，本稿では，ハードウェアへの物理攻撃の中でも，特に現実的な脅威とされ，多くの事例が報告されている機密性に対する攻撃，すなわち処理中のデータを不正に収奪・解読することを目的とする攻撃について説明する．そのほかにも機能を錯乱・停止する攻撃やデータや処理の改ざん・偽造を行う攻撃，悪意のあるハードウェア機能（ハードウェアトロイなど）の埋込みによる攻撃などがあるが．それらについては本特集の他稿等をご参照いただきたい．

図 -1 に代表的な物理攻撃とその分類を示す．物理攻撃は，攻撃対象のハードウェアに手を加えるかどうかにより侵襲攻撃（Invasive attack）と非侵襲攻撃（Non-invasive attack）に大別される．侵襲攻撃では，LSI パッケージを開封・加工し，高解像度の電子顕微鏡や収束イオンビーム装置などにより，その内部構造や回路動作を静的に解析する．いわゆるリバースエンジニアリングも侵襲攻撃に分類できる．侵襲攻撃は IC カード内の LSI などに対しきわめて高い攻撃能力を持ち得るが，そのような攻撃は一般に高価な装置と高いスキルを必要とするため，実行できる攻撃者は限定される．

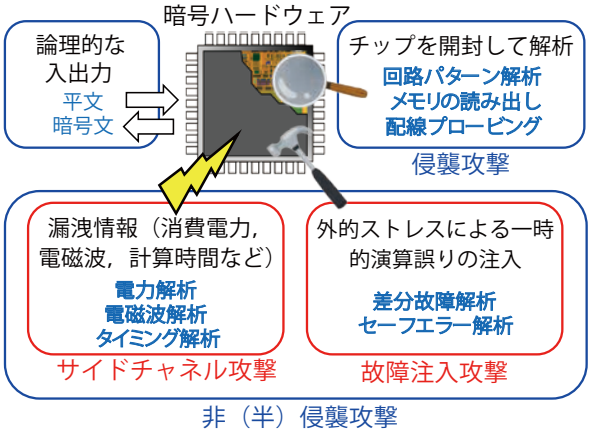


図 -1　代表的な物理攻撃とその分類例

一方，非侵襲攻撃は，その名の通りハードウェアの開封や加工等を伴わない攻撃である．その代表例が，ハードウェア動作中に副次的に生じる物理量（サイドチャネル情報）を観測して情報を奪うサイドチャネル攻撃である．これまでさまざまなサイドチャネル情報を利用する攻撃が報告されており，電力変動を利用する電力解析攻撃，漏洩電磁波を利用する電磁波解析攻撃，処理時間を利用するタイミング攻撃，発生する音を利用した音響解析攻撃などがよく知られている．これらの特徴は，侵襲攻撃と比べて安価な装置で実現でき，基本的に攻撃の痕跡を残さないことである．

もう1つの主要な非侵襲攻撃としては故障注入攻撃が知られている．サイドチャネル攻撃がサイドチャネル情報の観測を基本とする受動的な攻撃であるのに対し，故障注入攻撃は外部からハードウェアが誤動作する操作を加えて，その演算結果から情報を奪う能動的な攻撃である．誤動作の誘発には，たとえば電源電圧やクロック信号などに摂動（微細なゆらぎ）を加える方法が知られている．

近年では，チップ開封等を伴うが回路機能を恒久的に破壊せずに，回路動作を動的に解析する半侵襲攻撃（Semi-invasive attack）も見られる．同攻撃では，サイドチャネル情報の高精度な観測に基づくサイドチャネル攻撃や精緻な故障誘発を用いた故障注入攻撃といった，より強力な攻撃が実現されることが知られている．

以降では，典型的な非侵襲攻撃であるサイドチャネル攻撃と故障注入攻撃について述べる．

サイドチャネル攻撃

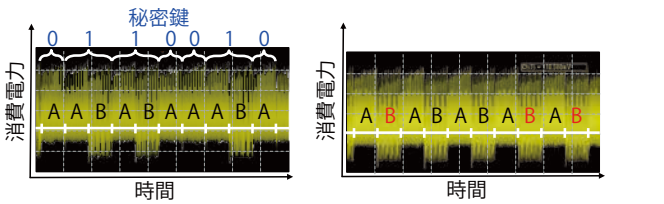
典型的な攻撃手法と対策

典型的なサイドチャネル攻撃の手法を，電力解析攻撃を例に解説する．電力解析攻撃では，ハードウェア動作中に生じる消費電力（電圧）の時間変化をディジタルオシロスコープなどの計測器で観測し，その観測データから処理内容を推定する．1990年代後半にKocherらによって単純電力解析（SPA：Simple Power Analysis）と差分電力解析（DPA：Differential Power Analysis）が発見されて以降，現在もその拡張や対策が盛んに研究されている[1]．なお，ほかのサイドチャネル情報（放射電磁波や動作タイミング）を用いた場合にも同様の解析手法が有効である．

SPAは測定した1つもしくは少数の観測波形を直接調べることで秘密情報を求める攻撃である．一例として，暗号処理を行うソフトウェアでは，しばしば秘密情報により命令系列が異なるため，その違いを波形から読み取ることで鍵を導出できる（図-2（a））．図のRSA暗号ハードウェアでは秘密鍵のビットが0もしくは1の場合にそれぞれ処理A（自乗算）もしくは処理AB（自乗算と乗算）を実行するため，電力波形から処理Aと処理Bを区別することで秘密鍵を推定できる．

DPAは大量の観測波形を統計解析することで秘密情報を求める攻撃である．数百から数十万といった波形数を必要とする一方で，SPAのように攻撃対象のアルゴリズムや構造に関する事前知識を必須とせずノイズに対しても強いという特徴を有する．データ依存性が小さく単一もしくは少数の波形観測では困難であった対象（暗号処理の場合，共通鍵暗号を処理するハードウェアなど）に対しても有効な攻撃とされる．

上記よりも攻撃者が有利な攻撃シナリオとして，攻撃対象の事前解析結果を活用することでより強力に秘密情報を収奪するプロファイリング攻撃もある．



(a) 未対策の電力波形：AとBの2つの演算パターンを消費電力から区別することで秘密情報を推定できる

(b) ハイディング対策を施した電力波形：ダミーの演算を挿入することにより演算パターンから秘密情報が推定が困難に

図-2　暗号ハードウェアへの単純電力解析と対策の例

事前情報の収集には攻撃対象と同等でかつ攻撃者が自由に操作・観測できる参照ハードウェアを用いるため，攻撃の前提条件は SPA や DPA と比べて厳しい．しかし，IC カードのような量産されるハードウェアやオープンソースソフトウェアを利用したシステムでは，考慮されるべきシナリオである．近年では，事前情報の学習に機械学習を用いた攻撃の報告が相次いでいる．

上記サイドチャネル攻撃への典型的な対策には，「隠蔽（ハイディング）」と「遮蔽（マスキング）」ある．ハイディングは，ハードウェアのサイドチャネル情報と内部処理や中間値との依存関係を隠す対策である．ハイディングの具体例として，図 -2（b）のようにダミーの演算あるいは相補的な演算を挿入し，内部処理が漏れを防止する対策がある（図 -2 (b)）．このときハードウェアは，単位命令あるいは各クロックで一定量の電力を消費するように設計される．一方，マスキングは，演算に用いる値にあらかじめ乱数を用いて変換し，サイドチャネル情報とアルゴリズムによって決まる真の中間値とを無関係とする対策である．マスキングによる対策は，アルゴリズム，アーキテクチャ，回路方式などさまざまな設計レベルでの適用が報告されている．

アーキテクチャラルサイドチャネル攻撃

近年，報告が急増しているサイドチャネル攻撃として，アーキテクチャラルサイドチャネル攻撃が挙げられる [2]．同攻撃は対象のアーキテクチャ的な特徴を利用することで，攻撃者が自らのプロセスを介して他者が実行中のプロセスの処理内容やデータを取得する．その代表例が 2018 年に報告された Meltdown と Spectre である．

図 -3 にアーキテクチャラルサイドチャネル攻撃のシナリオ例を示す．ここでは，攻撃者と他者がハードウェアを共有し，それぞれの演算コアで自身のプロセスを実行すると想定する．一般に，多くの演算コアでは階層的なキャッシュメモリを採用しており，ユーザはラストレベルキャッシュおよびメインメモリを共有する．攻撃者はたとえば Flush＋Reload や Prime＋Probe と呼ばれる手法を用いて他者のプロセスによるデータ読込を判別し，他者が実行した命令や処理データを収奪する．ここで，Flush＋Reload や Prime＋Probe では，当該データがキャッシュもしくはメインメモリから読み込まれるロード命令にかかる時間を観測することで，被攻撃者が当該データにアクセスしたかどうかを推測する．これにより，たとえば，被攻撃者が単位時間内で自乗算もしくは乗算を実行したか推測できるため，RSA 暗号に対し上述の SPA と同等の攻撃を実行することが可能となる．

アーキテクチャラルサイドチャネル攻撃は，上述の物理的アクセスを伴うサイドチャネル攻撃と異なりリモートで実行可能であるため，現在拡大するクラウドサービスが対象となり得る．特に，オープンソースの暗号ライブラリに対するアーキテクチャラルサイドチャネル攻撃による脆弱性が指摘されている．

故障注入攻撃

故障注入攻撃は，ハードウェアが実行する（暗号）演算に一時的な誤りを誘発し，誤った演算結果から処理内容を解析する．サイドチャネル攻撃対策が施された（暗号）ハードウェアであっても故障注入攻撃により秘密情報が取得される恐れがある．典型的

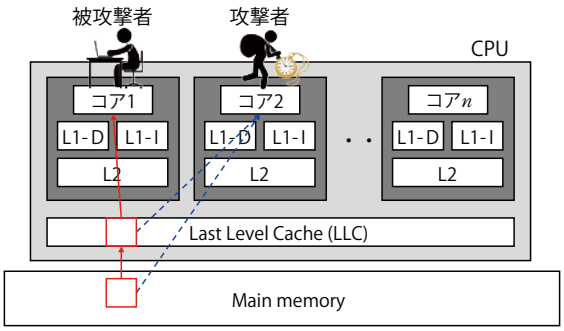


図 -3　LLC に対するアーキテクチャラルサイドチャネル攻撃のイメージ

な故障注入攻撃である RSA 暗号に対する Bellcore 攻撃や共通鍵暗号に対する差分故障解析（DFA：Differential Fault Analysis）では，理想的には 1 回の演算誤りから秘密情報を完全に抽出できる [3]．

一例として，図 -4 に RSA 暗号に対するセーフエラー解析攻撃を示す．図 -2（b）のように解析対象のハードウェアは演算 B のダミーを挿入するハイディング対策が施されており SPA では秘密鍵を推定することができないとする．そこで，攻撃者は演算 B（本来秘密鍵ビットが 1 のときのみに実行される乗算）実行時に誤りを発生させて，最終出力結果が正しいかを確認する．故障を注入した演算 B がダミーであった場合，故障の影響は最終結果に影響しない（図 -4（a））．一方，演算 B が本来の演算の場合，故障の影響が伝搬し，最終結果は誤りを含む出力となる（図 -4（b））．こうして，攻撃者はハイディング対策によって挿入されたダミーの演算 B と本来の演算 B を区別することができ，ダミーの演算 B を取り除くことによりハイディング対策を無効化し，秘密鍵を推定することが可能となる．

故障注入攻撃に対する対策は，センサやシールドを用いる対策と冗長性による対策がよく知られている．前者は物理的変動を検知・阻害するハードウェアを用いて攻撃の兆候を検知あるいは攻撃そのものを阻害する．たとえばレーザ照射によるメモリのビットフリップを検知するセンサなどが考案されている．後者は検算（たとえば，同じ処理を複数回実行し結果を確かめるなど）や誤り訂正符号により計算結果が正しいことを検証し，誤りを検知した場合は出力の停止等を行う．ただし，これらの対策により故障を検知しても検知後の処理内容から情報が漏洩する可能性がある点に注意が必要である．また，上述のセーフエラー攻撃では演算誤り発生の有無という情報のみを用いて秘密情報を取得するため，検算型対策のみでは防ぐことは難しい．このように想定される攻撃に応じて適切な対策を施すことが求められる．

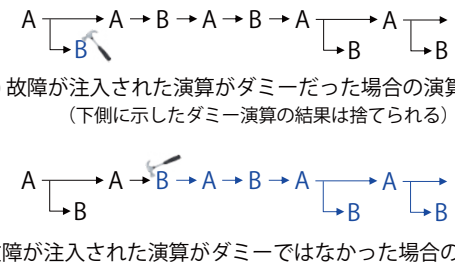


図 -4　RSA 暗号ハードウェアへの故障注入攻撃（セーフエラー解析）

今後の展望

本稿では，ハードウェアに対する物理攻撃の脅威と対策について概説した．サイドチャネル攻撃に代表される物理攻撃は，報告から 20 年が経過した今でも，日々新たな手法が報告されており，今後も半導体製造技術や計測・解析技術の進歩によって発展していくと予想される．ハードウェア設計者は，どのような物理攻撃の脅威が設計対象にあるかを考え，あらかじめ対策を施すことが肝要である．本稿がそうした脅威を把握する一助となれば幸いである．

参考文献

1) Mangard, S. et al. : Power Analysis Attack : Revealing the Secrets of Smart Cards, Springer (2007).
2) Yarom, Y. : Mastik : A Micro-Architectural Side-Channel Toolkit, https://cs.adelaide.edu.au/~yval/Mastik/ (Jan. 2020).
3) Joye, M. and Tunstall, M. : Fault Analysis in Cryptography, Springer (2012).

（2020 年 2 月 4 日受付）

本間尚文（正会員）　homma@riec.tohoku.ac.jp

東北大学電気通信研究所教授．専門は計算機システムおよび情報セキュリティ．用途や環境に応じた安全な情報システムの構築に興味がある．日本学術振興会賞，ドイツイノベーションアワードなどを受賞．博士（情報科学）．

上野　嶺（正会員）　ueno@riec.tohoku.ac.jp

東北大学電気通信研究所助教．専門は情報セキュリティおよび暗号実装．暗号を用いた情報システムの安全性評価に興味がある．Kenneth C. Smith Early Career Award in Microelectronics，船井研究奨励賞などを受賞．博士（情報科学）．