IMES DISCUSSION PAPER SERIES

サイドチャネル攻撃に対する安全性評価の研究動向とEMVカード固有の留意点

鈴木雅貴(すずきまさたか)・菅原 健(すがわらたけし)・鈴木大輔(すずきだいすけ)

Discussion Paper No. 2015-J-4

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2015-J-4
2015 年 5 月

サイドチャネル攻撃に対する安全性評価の研究動向と EMV カード固有の留意点

鈴木雅貴*・菅原 健**・鈴木大輔***

要　旨

金融業界では、「磁気カード（キャッシュカード、クレジットカード）の偽造」への対策として、「IC カード化」が進められている。一方、学会では、IC カードを含む暗号処理を行う一部の製品において、製品内部に格納された秘密鍵を推定できる可能性があり、その結果、当該製品の偽造に繋がるおそれがあるとの報告も存在する。具体的には、当該製品が暗号処理を行っている最中の消費電力等を計測し、その計測結果から秘密鍵を推定するという攻撃（「サイドチャネル攻撃」と総称される）である。同攻撃については約 20 年にわたる研究が行われており、様々な攻撃手法の提案やそうした攻撃の影響を緩和する対策が示されている。また、最近では、サイドチャネル攻撃に対する IC カード等（「暗号モジュール」と呼ばれる）の耐性を評価する方法も提案されるようになってきた。本発表では、サイドチャネル攻撃の攻撃手法や対策のほかに、同攻撃への耐性の評価手法に関する研究動向を説明する。そのうえで、EMV 仕様に準拠した IC カード（EMV カード）を取り上げ、サイドチャネル攻撃の影響と対策を講じる際の留意点を考察する。

キーワード：暗号モジュール、IC カード、サイドチャネル攻撃、実装攻撃、EMV 仕様、不正取引

JEL classification: L86、L96、Z00

* 日本銀行金融研究所主査（現システム情報局主査、E-mail: masataka.suzuki@boj.or.jp）

** 三菱電機株式会社（E-mail: Sugawara.Takeshi@bp.MitsubishiElectric.co.jp）

*** 三菱電機株式会社主席研究員（E-mail:Suzuki.Daisuke@bx.MitsubishiElectric.co.jp）

本稿の作成に当たっては、防衛大学校の田中秀磨准教授から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいは三菱電機株式会社の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目　次

1. はじめに

金融業界では、磁気ストライプを使った本人認証用のカードの偽造対策として、IC カード化が進められている（金融情報システムセンター[2011] 技 40、図表 1)。国内キャッシュカードの現状をみると、発行済カードに占める IC カードおよび IC カードによる取引が可能な ATM の割合はそれぞれ 23.0%、91.4%であるほか、2012 年 8 月には ATM だけでなく銀行のホストシステムを含めた上流ネットワークまで含めた end-to-end での IC カード対応（いわゆる、全銀協 IC キャッシュカード標準仕様の「基本形」対応）が完了しており、システム全体で IC カードを有効に活用可能な体制が整備されている。また、国内クレジットカードの現状をみると、IC カードおよび IC カード対応端末の割合はそれぞれ 65.6%、63.6%であるほか、今後の IC カード化の推進について 2016 年末までに 80%、東京オリンピック・パラリンピックが開催される 2020 年に 100%を目指すとの目標が掲げられている（日本クレジット協会[2015])。

図表 1. 金融業界における IC カードの導入状況

	キャッシュカード	クレジットカード
IC カードの割合	23.0% (注 1)	65.6% (注 2)
IC カード対応端末の割合	91.4% (注 1)	63.6% (注 3)
偽造カードによる被害額	0.9 億円 (注 4) （ピーク時の 11%）	25.8 億円 (注 5) （ピーク時の 15.6%）

（注 1）2013 年度末現在（金融庁[2014])。（注 2）2013 年末現在（日本クレジット協会[2015])。（注 3）2014 年 6 月末現在（日本クレジットカード協会[2014])。（注 4）2013 年度、ピークは 2005 年度の 8.2 億円（全国銀行協会[2014])。（注 5）2013 年、ピークは 2002 年の 165 億円（日本クレジット協会[2014])。

IC カードの導入に関する海外の状況をみると、欧州 SEPA[1]域内では、既に IC カード対応が完了している。SEPA は、IC カード対応完了後も残存するリスクとして域内で発行された IC カードが域外で磁気カードとして不正使用されることを問題視しており[2]、こうした問題に対応するための新たな運用ポリシー「債務責任の移行[3]」を、2015 年末までに適用する旨を公表している（EPC[2011])。国際決済ブランドの 1 つである VISA も同様に、米国における IC カード対応を促すために、同様の運用ポリシーを 2015 年 10 月 1 日から開始する旨を公表している[4]（VISA[2011])。このように、安全性が高い IC カードへの移行を積極的に進めようとする動きは国

[1] Single Euro Payments Area（単一ユーロ決済圏）。EU 加盟国を含めた 34 ヵ国において、効率的な競争が機能し、ユーロ圏内におけるクロスボーダー決済を国内決済と同じように利用することが出来る、統合された決済サービス市場の実現を目指すプロジェクト。

[2] SEPA 域内では、IC カード未対応の国や加盟店等での利用を想定し、磁気ストライプ付きの IC カードが発行されている。IC カード未対応の加盟店等では、IC カードであっても磁気カードとして扱われるため偽造カードの脅威が残存する。

[3] Liability Shift。加盟店側が IC カード対応していないために IC カードを磁気カードとして処理している状況において、不正使用が発生した場合に、IC カード対応していない側のアクワイアラにその責任を課すという運用ポリシー。

[4] VISA[2011]によれば、ガソリンスタンドにおける取引への同ポリシーの適用は、その特殊な環境を考慮して 2 年間免除する旨が示されている（つまり、2017 年 10 月 1 日開始）。

内外で広まっている。

IC カードのように、暗号アルゴリズムを実装したハードウエアあるいはソフトウエアは「暗号モジュール」と呼ばれ、通常、内部に秘密鍵等が格納されている。こうした暗号モジュールは、内部の秘密鍵が外部からは読み出せないことによって安全性が担保され、データ保護や本人確認等に活用される。他方、暗号モジュールを物理的に破壊することで内部に直接アクセスし秘密鍵を盗取する攻撃（「物理解析（または、侵襲攻撃）」と呼ばれる）が存在することは、フランス等で IC カードの実用化が始まった 1980 年代には既に知られていた[5]。1990 年代に入ると、暗号モジュールを破壊することなく内部の秘密鍵を盗取できるアイデアが示され（「非侵襲攻撃」と呼ばれる）実験環境を用いて実証された（Kocher[1995]）。非侵襲攻撃は痕跡が残らず、しかも比較的安価な装置を用いて実行できるケースもあることから新たな脅威として認識されるようになった。2000 年代に入ると、こうした攻撃によって、実用化されている市販の暗号モジュールからでも内部の秘密鍵を推定できたとされる研究結果が相次いで報告され（Mifare DESFire MF3ICD40＜Eisenbarth, *et al*.[2008]＞、KeeLoq＜Oswald and Paar[2011]＞）、同攻撃が現実的な脅威であると広く認識されるとともに、暗号モジュールの安全性確保の必要性が改めて認識されるようになった。

現在では、暗号モジュールの安全性を試験・評価したうえで認証する制度（CMVP、JCMVP、Common Criteria 等）が整備されており、こうした制度の下で認定を受けた製品（以下、「認証品」）を調達可能になっている[6]。しかし、たとえ認証品であったとしても、攻撃手法が日々高度化し、認証取得時には想定されていない攻撃がでてくるなかで相対的に安全性が低下していくことは避けられない。わが国の一部のキャッシュカードのように、有効期限を設定せずに長期間利用する場合は、そのような変化と付き合っていく必要がある。そのため、金融機関等の調達者にとって、暗号モジュールの安全性について知ることは、ビジネスリスク管理の上で重要である。そのためには、認証品であっても調達した暗号モジュールがどのような試験・評価を受けたのかを把握しておくことが有用であろう。

もっとも、現行の CMVP や JCMVP でも、非侵襲攻撃の 1 つである「サイドチャネル攻撃[7]」を「その他の攻撃」と位置付けているに過ぎず、同攻撃への対策やその有効性を評価する方法等を示していない。また、Common Criteria については、評価機関に求められる評価技術の一例や攻撃の難易度を数値化するための基準は

[5] 例えば、1980 年代中頃には、物理解析への対策を講じた暗号モジュール（IBM 製 μABYSS システム）が発表されている（Anderson[2008] Chap.4）。

[6] CMVP（Cryptographic Module Validation Program）、JCMVP（Japan Cryptographic Module Validation Program）の認証品は、それぞれ下記の URL で公表されている。

・CMVP：http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2015.htm

・JCMVP：http://www.ipa.go.jp/security/jcmvp/val.html

[7] 「コバートチャネル攻撃（covert channel attack）」とも呼ばれる。

示されているものの[8]、具体的な評価方法については公開されていないという状況にあり、調達者が暗号モジュールの評価方法等に関する情報を入手するのはハードルが高い状況にあった。

こうしたなか、サイドチャネル攻撃については最近になって、安全性を評価する手法等が学会で提案されるようになってきている。そこで、本稿では、暗号モジュールへの攻撃（「実装攻撃」と呼ばれる）のうちサイドチャネル攻撃に焦点を当てて、同攻撃における攻撃手法や対策を紹介すると共に、既存の安全性評価手法に関する研究動向を紹介する。そのうえで、IC キャッシュカードや IC クレジットカード等に関する国際的な業界標準「EMV 仕様[9]」に準拠した IC カード（以下、「EMV カード」）を取り上げて、サイドチャネル攻撃の影響と同カードに固有の留意点について考察する。

以下、2 節において暗号モジュール・ハードウエアへの実装攻撃を俯瞰したうえで、サイドチャネル攻撃に関する攻撃手法や対策等を紹介し、3 節において同攻撃に対する安全性評価手法の研究動向を解説する。そのうえで、4 節において EMV カードに対するサイドチャネル攻撃の影響と留意点について考察する。

2. サイドチャネル攻撃とその対策

本節では、まず、IC カードのようなハードウエアで実現された暗号モジュールへの実装攻撃[10]を俯瞰する。そのうえで、実装攻撃の 1 つであるサイドチャネル攻撃に焦点を当てて、同攻撃の攻撃手法と対策についてそれぞれ概説する。

(1) 実装攻撃の分類

ハードウエアで実現された暗号モジュールへの実装攻撃は、まず、攻撃対象の IC チップを物理的に破壊したうえでプローブ（探針）を特定の回路にあてて観測する等内部に直接アクセスする「侵襲攻撃（物理解析）」と、そうしたアクセスを行わない「非侵襲攻撃」に分類される[11]。非侵襲攻撃は、さらに、攻撃対象の通常動作を観測・解析を行う「サイドチャネル攻撃」と、何らかの物理的操作を加えることで意図的にエラーを生じさせ、そこで得られる情報を併せて利用する「故障利用攻撃（フォルト攻撃とも呼ばれる）」に分類される[12]（図表 2）。以下、各攻撃の特徴

---

[8] Joint Interpretation Library[2013]。

[9] EMV は、Europay International、MasterCard International、Visa International の頭文字の略。現在は、2011 年に発行された EMV 4.3 が最新（EMVCo[2011abcd]）。

[10] ソフトウエアで実現された暗号モジュールへの攻撃は、プログラムを実行せずに解析する方法「プログラム非実行型（「静的解析」とも呼ばれる）」と、プログラムを実行しながら解析する方法「プログラム実行型（「動的解析」とも呼ばれる）」に分類される（松本・大石・高橋[2008]）。

[11] 侵襲攻撃（invasive attack）および非侵襲攻撃（non-invasive attack）はそれぞれ、「破壊攻撃／非破壊攻撃（情報処理進行事業協会・通信・放送機構[2003]等）」、あるいは、「パッケージ加工攻撃／パッケージ非加工攻撃（松本・石井・高橋[2008]）」とも呼ばれる。

[12] こうした分類は、野崎・藤崎・川村[2009]等にみられる。また、非侵襲攻撃をサイドチャネル攻撃と呼び、そのうち、能

を述べる。

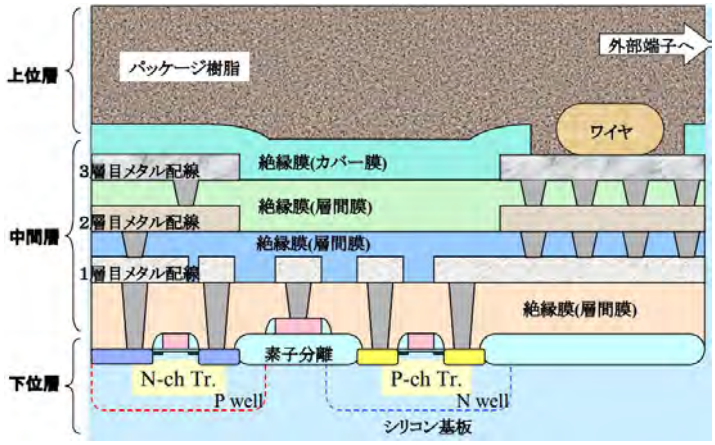
	侵襲攻撃	非侵襲攻撃
通常動作を観測（受動型）	物理解析1980年代には存在 • プローブ攻撃（バスデータの盗聴）、等	サイドチャネル攻撃1995年~ • タイミング解析1995年~ • 電力解析1998年~ • 電磁波解析2001年~、等
異常動作を起こさせたうえで観測（能動型）	• プローブ攻撃（バスデータの改ざん） • 回路配線の破壊・改変、等	故障利用攻撃1996年~

（備考）図中に示した年は、該当する攻撃が初めて提案された年である。

図表 2．暗号モジュール・ハードウエアへの実装攻撃の全体像

イ．物理解析

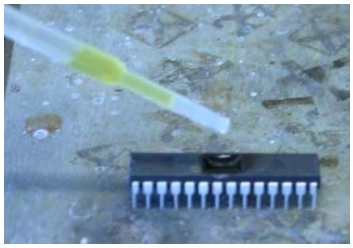
物理解析は、攻撃対象の IC チップのパッケージ樹脂や絶縁膜、メタル配線等（図表 3）を剥離して、内部構造や回路動作を解析する攻撃であり、1980 年代には同攻撃が存在することが知られていた（Anderson[2008] Chap.4）。例えば、パッケージ樹脂等を剥離することでメタル配線を露出させプローブを当てることで、同配線を流れるデータ（秘密鍵等）を直接読み取る攻撃（「プローブ攻撃」と呼ばれる）が存在する（図表 4）。また、IC チップ上の特定回路を破壊したり改変したりすれば、セキュリティ機能をバイパスすることができる。ただし、極めて微細な IC チップに対してこうした攻撃を行うためには、高価な装置・設備と熟練度の高い技術者が必要になる。



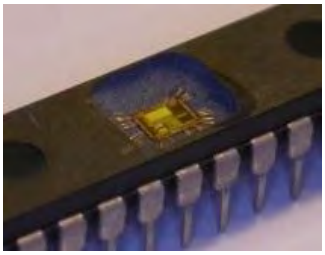
（出典：電子商取引安全技術研究組合[2004] 図 2.2）

図表 3．IC チップの縦断面図（イメージ）

動的なものを故障利用攻撃、受動的なものをタイミング解析、電力解析、電磁波解析と呼ぶ分類もある（本間・青木[2013]）。



(a) IC チップに薬品を垂らす様子

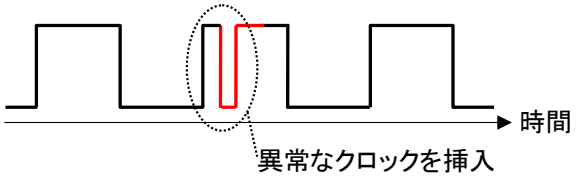


(b) 薬品によりパッケージが溶け、配線が剥き出しになった様子

図表 4．IC チップのパッケージを溶かす様子（Skorobogatov[2005]）

ロ．故障利用攻撃

故障利用攻撃は、攻撃対象に通常ありえない刺激を加えることで内部処理のエラーを誘発させ、同エラーと正常な処理結果の両方を手掛かりに秘密鍵を推定する攻撃であり、1996 年に初めて提案された（Bellcore[1996]、Boneh, DeMillo, and Liption[1997]）。攻撃対象に加える刺激としては、例えば、定格外のクロック周波数（図表 5）、電磁波・放射線・レーザの照射等がある。同攻撃の実現可能性は、①エラーが誘発される期間（一時的、永続的）、②エラー誘発のタイミング（任意、特定）、③エラーの発生対象となるデータ（特定、任意）、④発生するエラーのタイプ（ビット／バイト単位で値の改変、値の固定化、一方向性のエラー＜1→0 のみ等＞、特定命令の無効化等）といったエラーの性質に大きく依存する。



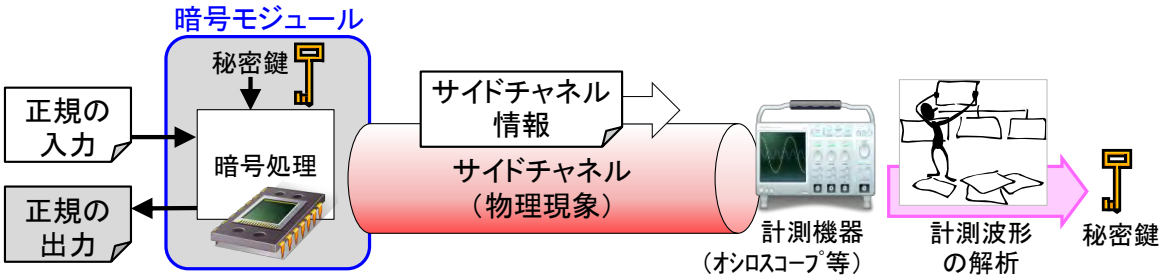
図表 5．定格外のクロック周波数の挿入（イメージ）

ハ．サイドチャネル攻撃

IC チップが計算処理を行うと、電流や電磁波の変化等の物理現象が副次的に生じ、この物理現象を計測することで得られる物理量は、計算内容に応じて変動することが知られている。こうした物理量が得られる物理現象は、計算の入出力をやり取りする正規のチャネルに対し、「サイドチャネル」と呼ばれている。特に、計算内容が暗号処理の場合、秘密鍵に依存して物理量が変動し、秘密鍵に関する情報（「サイドチャネル情報」と呼ばれる）がサイドチャネルを通じて漏洩する可能性がある。

サイドチャネル攻撃は、こうしたサイドチャネル情報を含んだ物理量を計測し、これを解析することで秘密鍵を効率よく推定する攻撃であり（図表 6）、1995 年に初めて提案された（Kocher[1995, 1996]）。同攻撃を実行するには、物理量を計測するための機器（オシロスコープ等）や計測した物理量を解析するための計算機（PC

等）等が必要となるが、これらは物理解析に用いられる装置・設備と比較すれば一般的に安価である。



図表 6. サイドチャネル攻撃の全体の流れ

攻撃者は暗号モジュールの最弱点を狙って攻撃をする。そのため、暗号モジュールとしては、ここまで述べた攻撃すべてに対応する必要があるが、サイドチャネル攻撃に対する安全性評価は特に重要度が高いと考えられる。攻撃が受動的に行われる性質上、攻撃を検出してリアクションを取る等の事後的な対策は困難であり、情報の漏洩を減らすことが最大の対策になるため、より厳密な安全性評価が求められる。そこで、本稿では、サイドチャネル攻撃に焦点を当てる。

(2) サイドチャネル攻撃の攻撃手法

イ. 漏洩モデル

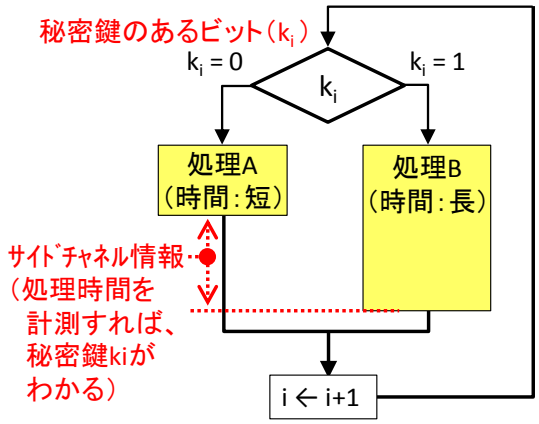
サイドチャネル攻撃は、どんな情報が漏洩しうるのかという物理的な側面と、漏洩を使っていかに暗号解読をするかという暗号学的な側面を持つ。両者をつなげるために、何が漏洩するかを「漏洩モデル[13]」として抽象化するのが一般的である。次に、代表的な 2 つの漏洩モデルを紹介する。

① 処理時間モデル

秘密鍵の値に応じて処理時間が変化する場合には、処理時間から秘密鍵に関する情報が漏洩する。例えば、秘密鍵の特定のビットの値が 0 の場合には処理時間の短い処理 A が、1 の場合には処理時間の長い処理 B がそれぞれ実行されるとする。この場合、計測した物理現象から当該処理にかかる時間を求め、処理時間が短い場合には秘密鍵の当該ビットが 0、長い場合には 1 であると推定できる可能性がある（図表 7 (a)）。具体的な暗号アルゴリズムの例として、バイナリ法[14]を用いて実装された RSA の復号処理が挙げられる（図表 7 (b)）。同実装では、該当する秘密鍵の 1 ビットの値が 0 の場合には内部の一時データの二乗（処理 A に相当）を、1 の場

[13] このほか、「電力モデル」や「リーク・モデル」等とも呼ばれる。
[14] バイナリ法は、剰余演算を高速化するための実装方法。

合には一時データの二乗および一時データと暗号文の乗算（処理 B に相当）をそれぞれ行う。処理 B の方が演算内容が多いため、処理時間が長くなる。



(a) 処理時間モデル（イメージ）

処理A（$k_i = 0$）	処理B（$k_i = 1$）
・$m \leftarrow m^2 \bmod N$	・$m \leftarrow m^2 \bmod N$ ・$m \leftarrow m \times c \bmod N$

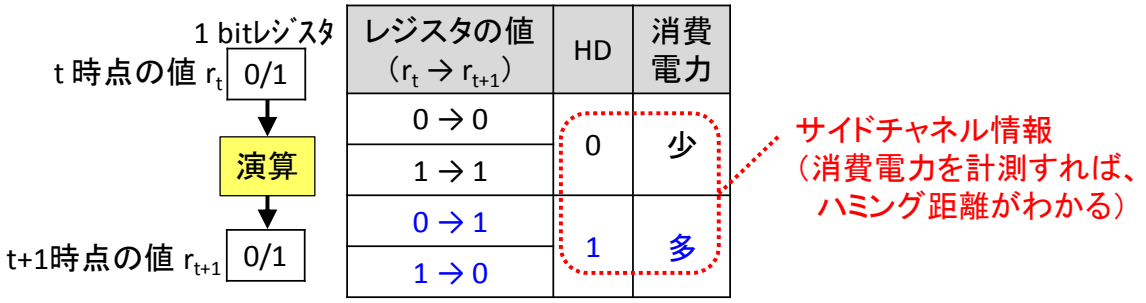
（m：内部の一時データ、c：暗号文、
N：公開鍵、k：秘密鍵、i = 0～2,048）

(b) バイナリ法を用いて実装した RSA の復号処理

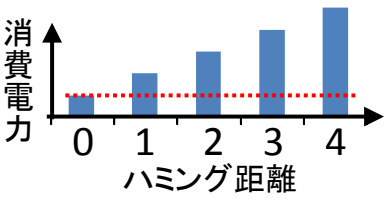
図表 7. 処理時間モデル

② ハミング距離モデル

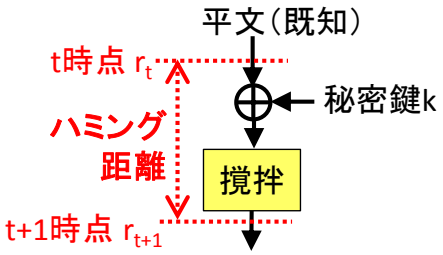
IC チップには、演算に用いるデータを一時的に記録しておく領域（「レジスタ」と呼ばれる）があり、暗号処理は、レジスタを順次上書きすることで行われる。ハミング距離モデルでは、ある上書きにおいて、値が書き換わった時に限って電力を消費すると考える（図表 8 (a)）。つまり、ある計算をする際の電力の変化を観測すれば、レジスタの値が書き換わったかどうかを推定でき、レジスタが書き換わったかどうかの情報を使えば、計算に利用された秘密情報が復元できる可能性がある。値が変化した時に電力を消費するという性質は、CMOS 回路の電気的な性質に由来する。なお、複数ビットのレジスタで考えた場合、書き換えられたビットの数が多い（ハミング距離が大きい）ほど、消費電力は大きくなる（図表 8 (b)）。具体的な暗号アルゴリズムの例として、AES の暗号化処理が挙げられる（同(c)）。暗号処理中のある時点の値（同 r_{t+1}）は、平文（同 r_t）と秘密鍵に依存する。このため、攻撃者は、ある時点（同 t+1 時点）の消費電力を計測し、その値からハミング距離を推定したうえで、このハミング距離となるような秘密鍵を探索するというアプローチにより、秘密鍵を推定できる。



(a) ハミング距離モデル（イメージ）



(b) 4 ビットのレジスタの場合



(c) AES の暗号化処理の冒頭一部

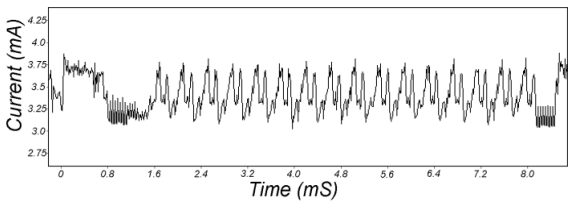
図表 8. ハミング距離モデル

ロ. 計測波形

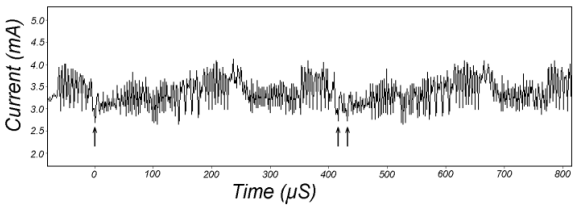
暗号処理中に発生する物理現象の物理量は刻々と変化する。それを計測機器で観察すると、図表 9 のような「波形[15]」が得られる（以下、計測した波形を「計測波形」と呼ぶ）。

計測波形には、サイドチャネル情報とノイズが含まれるが、多くの場合、ノイズ成分が支配的である。攻撃者は、波形をたくさん集め、それらに信号処理・統計処理を適用することでサイドチャネル情報の抽出を試みる。波形をたくさん集めるほど、サイドチャネル攻撃の成功率は高まる。

以上の理由から、攻撃成功に必要な波形数は、暗号モジュールの安全性を示す指標（セキュリティパラメータ）として利用されることがある。利用者は、その指標を用いて、秘密鍵の更新までに何回暗号化してよいか決めることができる。一方、攻撃者にとって、サイドチャネル攻撃の労力のほとんどは波形の計測・処理に充てられるため、収集する波形数は、攻撃者の労力の指標にもなっている。



(a) DES 全体



(b) DES の第 2, 3 ラウンド

[15] トレース（trace）、サンプル等とも呼ばれる。

（出典）Kocher, Jaffe, and Jun[1999]

図表 9．IC チップ内で DES を実行した際の物理量（電流）

ハ．攻撃手法の分類

サイドチャネル攻撃は、①攻撃に利用する物理現象の選択と②計測した物理現象（計測波形）を解析する方法の組合せで表現される。攻撃に利用する物理現象（上記①）には、攻撃対象の消費電力、攻撃対象から放射される電磁波、攻撃対象の処理時間等があり、こうした物理現象を利用した攻撃はそれぞれ「電力解析」（Kocher, Jaffe, and Jun[1998, 1999]）、「電磁波解析」（Gandolfi, Mourtel, and Olivier[2001]）、「タイミング解析」（Kocher[1996]）と呼ばれている[16]。また、計測波形を解析する方法（上記②）には、「差分解析」や「相関係数解析」等がある（図表 10）。上記①②を組み合わせることで、例えば、消費電力を用いた差分解析は「差分電力解析」、電磁波解析を用いた相関解析は「相関電磁波解析」とそれぞれ表現される。

図表 10．計測波形を解析する方法

解析方法	概要
差分解析	秘密鍵のある 1 ビットを予想し、その予想に基づき計測波形を 2 つのグループに分け、各グループの平均値に差分があるかどうかを検証する。予想したビットが正しければ、各グループの平均値に顕著な差分が現れる可能性が高いとみなし、秘密鍵の他のビットについても同様の解析を繰り返し、最終的にすべてのビットについて推測するという解析方法。
相関係数解析	秘密鍵候補の値が正しければ、同秘密鍵候補の下で算出した予測波形と計測波形の相関係数が高くなるという前提の下、秘密鍵候補の値を 1 つずつ変えながら予測波形を算出し、同予測波形と計測波形との相関係数を求める。最も高い相関係数が得られたときの秘密鍵候補を正しい秘密鍵と見なすという解析方法。

(3) サイドチャネル攻撃への対策

イ．対策の評価

サイドチャネル攻撃への安全性について議論するには、攻撃に要する労力・費用の観点が不可欠である[17]。もっとも、それらを机上で見積もるのは簡単ではなく、実際に攻撃を行ってみるのが現実的である。こうした背景より、Common Criteria では、第三者評価機関によるペネトレーションテストが行われる。評価対象の暗号モジュールは、図表 11 に挙げた所要時間や必要機材などの攻撃の実現可能性に関する評価項目に従い、予め決められた評価尺度によってスコアが付けられ、このス

[16] 計算機が動作中のノイズ音を利用する攻撃「音響解析（Genkin, Shamir, and Tromer[2014]）」等も提案されている。
[17] 暗号モジュールの対策に関する評価軸は、安全性のほかに、性能（処理速度、回路サイズ等）もある。

コアに応じて認証取得の可否が決まる。

図表 11. 攻撃手法の実現可能性に関する主な評価項目

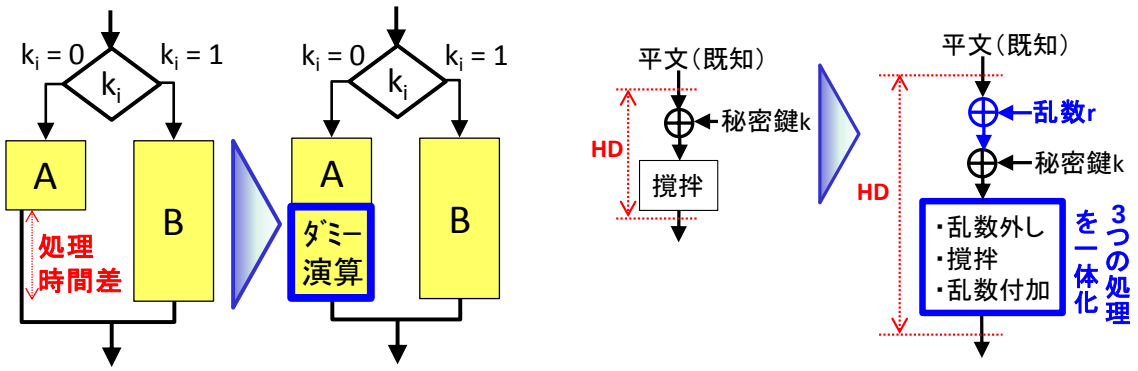
要素	概要
所要時間	攻撃に要する時間。「1 時間未満」、「1 日未満」、「1 週間未満」、「1 ヶ月未満」、「1 ヶ月以上」、「実際的でない」、という 6 段階に分けられている。
専門知識	IC カードに対する新しい攻撃と必要なツールを定義する能力や、開発者と同程度に評価対象に関する知識を有しているかという観点から 4 段階に分けられている。
評価対象に関する知識	評価対象に関する知識を入手する難しさの観点から 5 段階に分けられている。公知の情報が最も入手し易く、非常に重要なハードウエア設計書が最も入手困難と分類されている。
評価対象へのアクセス	攻撃を成功させるまでに必要となる暗号モジュール機器等のサンプル（IC カード）の数。攻撃の成功確率が低い場合や、多くのサンプルから情報を収集する必要がある場合ほど、多くのサンプルが必要となる。「10 サンプル未満」、「100 サンプル未満」、「100 サンプル以上」、「実際的でない」という 4 段階に分けられている。
攻撃に必要な機器	価格と入手のし易さから、「なし」、「標準」、「特殊（大学の研究室が所持する程度のもの）」、「特別注文」、「複数の特別注文」という 5 段階に分けられる。

（出典：Joint Interpretation Library[2013]）

ロ．対策例

前述の 2 つの漏洩モデルにおける対策の一例を挙げる。処理時間モデルについては、秘密鍵の値にかかわらず処理時間が一定になるようにすることが対策となる（図表 12 (a)）。例えば、秘密鍵の値が 0 のとき、処理 A のほかに、ダミー演算を実行することで処理時間が処理 B と同程度になるように調整することが考えられる。

ハミング距離モデルについては、暗号化処理の冒頭において平文に乱数を加えることでマスクし、このマスクされた状態のまま暗号化処理を行うという対策（「マスキング」と呼ばれる）が挙げられる（図表 12 (b)）。理論的には、撹拌の処理を行う前にマスク（乱数）を外し、撹拌後にマスクを加えるという流れになるが、この一連の流れを一体化することで、マスクを外した状態に戻すことなく暗号化処理を実行できる。このため、計測した消費電力から求めたハミング距離には、マスクの影響が残っており、秘密鍵を推定することができないと期待される。



(a) 処理時間モデル　　(b) ハミング距離モデル

図表 12. 各漏洩モデルにおける対策例

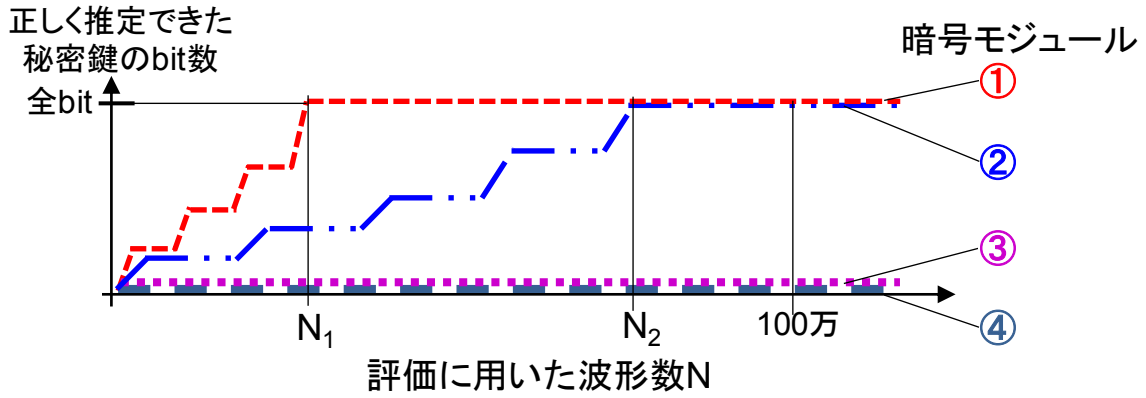
3. IC カードの安全性評価手法に関する研究動向

前節において、暗号モジュールの安全性評価には、ペネトレーションテストを行う必要があることを述べた。ペネトレーションテストを行う評価者（すなわち攻撃者）は、限られた時間の中で、できる限りの評価を行う。そのため、評価の効率化は必須であり、そのための方法がいくつか知られている。本節では、安全性評価に焦点を当て、既存の 3 つの安全性評価手法を紹介したうえで各評価手法を比較する。

(1) 評価手法 1：波形数を用いる評価手法

波形数を用いる評価手法（以下、「評価手法 1」）は、まず、評価対象の暗号モジュールにサイドチャネル攻撃を適用することで未知の秘密鍵の推定に要した波形数（計測波形の数）を求めるものである（図表 13）。同手法は、攻撃手法や対策に関する既存研究において広く採用されている。特に、製品の評価では、「100 万波形以下では秘密鍵を推定できないこと」等の安全性要件（以下、「N 波形安全」）が充足されるか否かの評価が行われる。例えば、図表 13 のような評価結果が得られた場合には、(i) 暗号モジュール①②は要件を満たさないが、(ii) 暗号モジュール③④は要件を満たすことが分かる。その結果、暗号モジュール①②は、要件を充足しないと判断される[18]。

[18] 暗号モジュール①より②の方が相対的に安全性は高いが、どちらも秘密鍵を推定されているため、製品として実用に耐えるかという観点からはいずれも選択すべきではないといえる。



図表 13. 波形数を用いる評価手法（イメージ）

(2) 評価手法 2：仮説検定を用いる評価手法

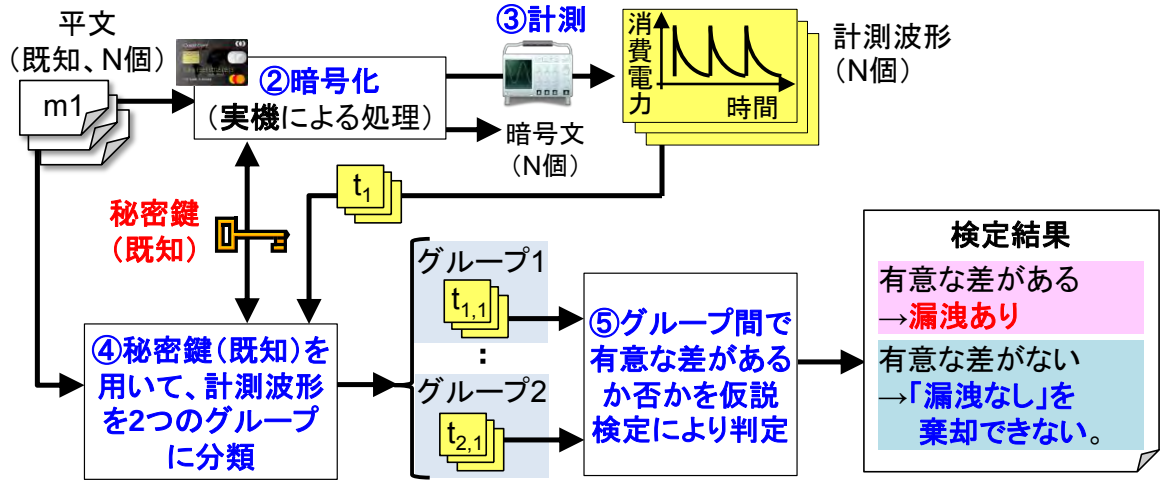
評価者は、本物の攻撃者よりも多くの前提知識を活用して評価することが可能である。特に、鍵の真の値を、あらかじめ知った上でこれを利用して評価することもできる。その条件の元では、鍵候補の探索を行うことなく、鍵に関する情報のサイドチャネルからの漏洩有無を直接調べることができる。

仮説検定を用いる評価手法（以下、「評価手法 2」）は、まず、「サイドチャネル情報を漏洩していない」という帰無仮説を立てておき、計測した物理現象（計測波形）が同仮説の下では非常に稀にしか観測し得ないことを示すことで同仮説を棄却し、対立仮説である「サイドチャネル情報を漏洩している」ことを示すという手法である[19]。なお、同手法は、サイドチャネル情報の漏洩の有無を調べることが目的であり、そうした漏洩があった場合に、それをどう利用すれば秘密鍵を推定できるかといった攻撃手法の構築や、そうした攻撃手法による秘密鍵推定の困難さについては評価対象外としている。

具体例として、計測波形に秘密鍵に依存した偏りがあるか否かを仮説検定で調べる方法を示す（図表 14）。検定の結果、こうした偏りがあると判定された場合には、計測波形と秘密鍵の依存関係を利用して計測波形から秘密鍵を推定される可能性があるといえる。具体的な手順は、次のとおりである。

[19] Goodwill, Jun, Jaffe, and Rohatgi[2011]、Jaffe and Rohatgi[2011]。

① まず、帰無仮説と対立仮説を立てる。なお、グループとは、既知の秘密鍵に基づき分類された計測波形の集合（下記④を参照）を指す。
帰無仮説：グループ間に有意な差がない（漏洩なし）
対立仮説：グループ間に有意な差がある（漏洩あり）
② 用意した N 個の平文（既知）を、暗号モジュールを用いて暗号化する。
③ 上記②の暗号化において、各暗号化処理における消費電力を計測し観測し、N 個の計測波形を得る。
④ 既知の秘密鍵のビットの値に基づき、計測波形を 2 つのグループに分類する。
⑤ 仮説検定により、グループ間に有意な差があるか否かを判定する。検定結果が「有意な差がある」の場合には、帰無仮説を棄却し漏洩ありとみなし、「有意な差がない」の場合には、帰無仮説を棄却できない（漏洩があるとはいえない）。



図表 14. 仮説検定を用いる評価手法（イメージ）

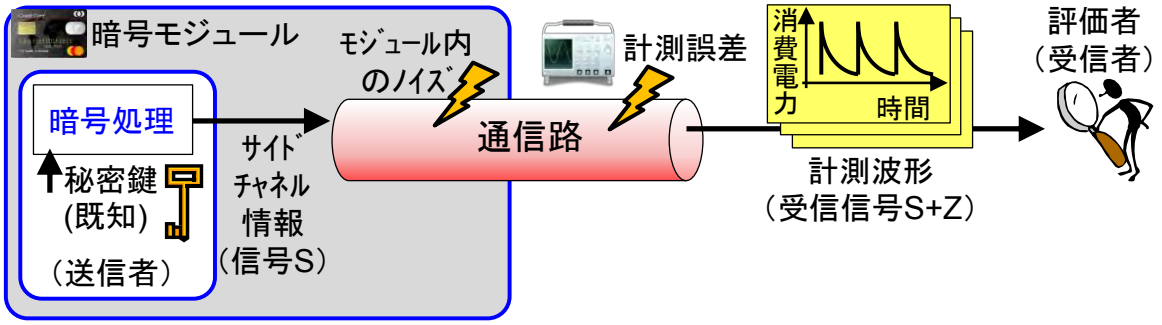
(3) 評価手法 3：通信路容量を用いる評価手法

評価手法 2 は、鍵が既知の条件で、漏洩の有無を調べるというものであった。このアプローチをさらに進めて、漏洩の「量」を調べようというアプローチがある。1 つの方法は、通信路容量を用いる評価手法（以下、「評価手法 3」）である。

評価手法 3 では、サイドチャネル攻撃の一連の流れを「サイドチャネル情報を送信する通信」と見なし、1 つの計測波形（サンプル）で伝送可能なサイドチャネル情報の量（「通信路容量」と呼ばれる）が少ないほど安全性が高いとする手法である（水野ら[2014]、Mizuno, *et al.*[2014]、図表 15）。より厳密には、暗号モジュール（送信者）がサイドチャネル情報（信号 S）を送信し、同モジュール内でノイズが加わったり、計測時に読取誤差が発生するといった「雑音 Z」が加わったデータ（S+Z）を攻撃者や評価者（受信者）が受信するという通信路モデルとみなしている。雑音のある通信路における通信路容量は、シャノン・ハートレーの定理により次式のように定式化されている。同式からは、信号 S が小さく、雑音 Z が大きいほど、通

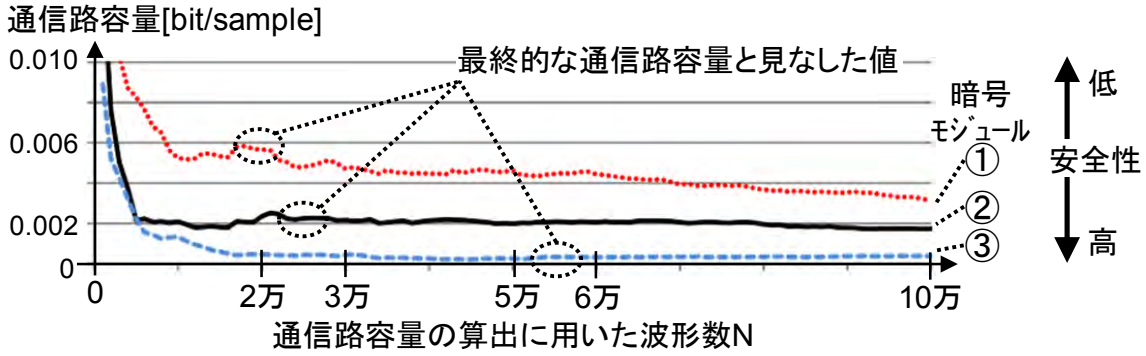
信路容量が小さくなる（安全性が高くなる）ことがわかる。このため、通信路容量の算出に必要な波形数は、評価対象毎に異なる。

$$\text{通信路容量 C} = \frac{1}{2} log_2 \left(1 + \frac{\text{信号 S}}{\text{雑音 Z}}\right) [bit/sample]$$



図表 15. 通信路容量を用いた評価手法（イメージ）

評価対象の通信路容量を算出する際、水野ら[2014]は、同モジュールの暗号処理中に計測した計測波形と既知の秘密鍵を用いている（図表 16）。同図表では、3 つの暗号モジュール（①②③）の通信路容量を示しており、全体の傾向としてモジュール③の安全性が高いことがわかる。しかし、各モジュールの通信路容量は、算出に用いた波形数によって変化するため、どの地点の値を最終的な通信路容量と定めればよいかという課題がある。この課題に対して水野ら[2014]は、波形数を増やした時の通信路容量の変化率が一定水準以下であれば収束したと見なし、その時点の値を最終的な値とするという対応を採っている。



（備考）水野ら[2014] 図 6 を基に作成。

図表 16. 3 つの暗号モジュールの通信路容量の評価結果の例

(4) 各評価手法の比較

評価手法 1 は、攻撃者と全く同じ攻撃を試してみることになるため、最も現実に近い評価を行っていると言える。特に、前述の「100 万波形以下では秘密鍵を推定できないこと」のような要件の充足可否に答えられるのはこの方法だけである。し

かし、評価では鍵の探索を行うため、計算時間がかかるほか、存在する複数の攻撃手法をすべて試すことは現実的には難しい。

一方、評価手法 2 と 3 は、秘密鍵の推定を行う必要はないため、評価に要する時間が短くて済む。また、秘密鍵が既知という攻撃者よりも有利な条件で評価を行うため、より安全サイドに倒した評価結果が期待できる。一方で、攻撃者が秘密鍵を推定できるか否かを直接的に知ることはできない。特に、秘密鍵の推定に繋がらない漏洩が存在する点に注意が必要である。

以上の議論を図表 17 にまとめる。同図表から分かるように、各評価手法が評価可能な項目は異なっており、いずれかの評価手法を単独で利用するというよりも、組み合わせて利用することが現実的である。例として、評価手法 1 と 2 を組み合わせた評価フローは次のとおりである。

Step 1. まず、評価手法 2 を用いて、漏洩の有無を調べる。
Step 2. 漏洩の存在が明らかになった場合、その漏洩が秘密鍵の推定に繋がるか否かを判断する。
Step 3. 秘密鍵の推定に繋がると判断した場合には、どのような攻撃手法が有効かを決定する。
Step 4. Step 3 で決定した攻撃手法を用いて、評価手法 1 を行う。

最後に、評価手法 2 と 3 を比較する。評価手法 1 を実施するのに、波形数をどれくらい計測すべきかという問題がある。「100 万波形以下では秘密鍵を推定できないこと」という要件を検証するには、もちろん 100 万波形を利用する必要がある。しかし、例えば 1,000 波形で解読できるのに 100 万枚計測するのは無駄である。評価手法 3 で漏洩の容量が分かれば、評価手法 1 において、何波形程度で攻撃が成功するか見積もることができる。これにより、実験に必要な波形数を削減でき、評価に要する時間の短縮に繋がると期待される。

図表 17. 各評価手法の比較

	安全性評価手法		
	評価手法 1 （波形数）	評価手法 2 （仮説検定）	評価手法 3 （通信路容量）
秘密鍵の推定を行うか	行う（攻撃手法を構築するコストが発生）。	行わない（秘密鍵は既知）。	
評価に要するコスト	大きい	小さい	
評価手法の出力	波形数	漏洩の有無	通信路容量
その他の特徴	・N 波形安全という安全性要件の充足を検証可能。	・秘密鍵の推定に繋がらない漏洩を検知する可能性がある。	・秘密鍵の推定に繋がらない漏洩を検知する可能性がある。 ・攻撃に必要な波形数の下限を理論的に算出可能。

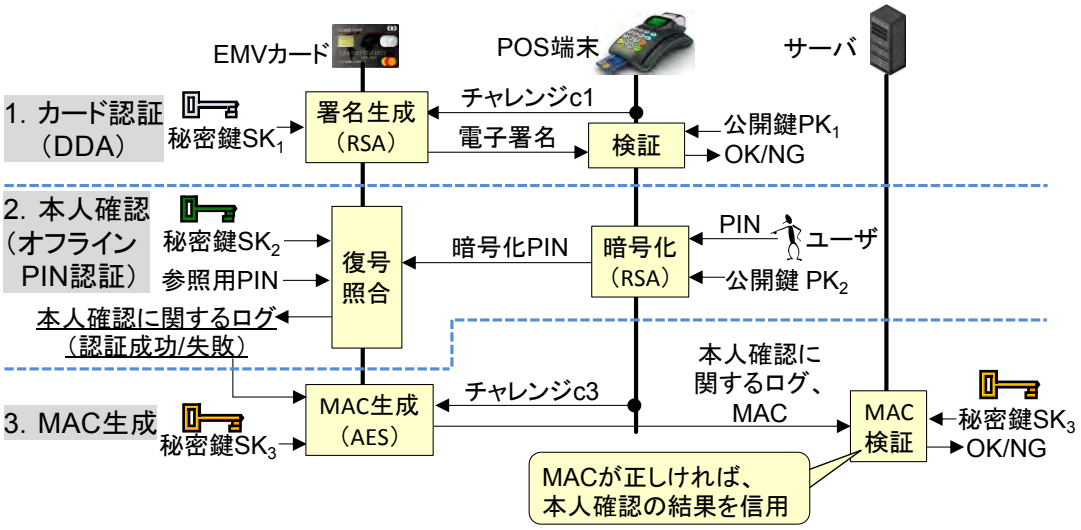
4. 考察：EMV カードへのサイドチャネル攻撃の影響と留意点

本節では、EMV カードを用いた取引について想定する取引フローを示したうえで、サイドチャネル攻撃により EMV カードから秘密鍵が漏洩した場合の影響を考察する。また、EMV 仕様上の制約を加味した場合の留意点等について考察する。

(1) 想定する取引フロー

EMV カードを用いた典型的な取引では、カードの真正性を端末（POS 端末、ATM）が検証する「カード認証」、カード所持者（ユーザ）が本人であることを確認する「本人確認」、取引データ（金額、本人確認に関するログ等）が改ざんされることを防止するための「MAC 生成[20]」の 3 つの処理が行われる。各処理を実施する順番[21]や、複数存在する各処理の実現方法のうちどれを選択するかについては、カード発行者のビジネス判断に依存するが、本稿では、クレジットカードを用いた取引において通常行われることが多いと思われるカード認証、本人確認、MAC 生成の順に実施される取引フローを想定する（図表 18）。各処理の実現方法は以下のとおりとする。

[20] Message Authentication Code（メッセージ認証子）。EMV 仕様では、「Application Cryptogram Generation」と表記。
[21] 本稿では、カード認証、本人確認、MAC 生成の順番を想定するが、カード認証の前に本人確認を行ったり、本人確認を省略するフローも EMV 仕様上はありうる。



図表 18. 想定する取引フロー

カード認証：カードは、秘密鍵 SK_1 を用いて、端末から受信したチャレンジ（乱数）に対するレスポンスとして電子署名を生成し、端末に送信する。端末は、カードの公開鍵 PK_1 を用いて同電子署名を検証する。EMV 仕様では、同実現方法を「動的データ認証[22]」と呼び、公開鍵暗号として RSA を利用する。なお、鍵ペア SK_1/PK_1 は、カード内に格納されており、公開鍵 PK_1 については、取引時にカードから端末に送信される。本人確認に用いる鍵ペア SK_2/PK_2 についても同様[23]。

本人確認：端末は、ユーザが端末に入力した暗証番号（PIN）を、カードの公開鍵 PK_2 で暗号化したうえでカードに送信する。カードは、対応する秘密鍵 SK_2 を用いてこれを復号したうえで、カード内に予め格納されている参照用 PIN と照合する。EMV 仕様では、同実現方法を「オフライン PIN 認証」と呼び、公開鍵暗号として RSA を利用する。本稿では、認証成功のログをサーバが確認したときに、本人確認をパスしたとみなす。なお、このログは、MAC 生成における保護対象である取引データの 1 つであるため、本人確認をパスするには MAC 生成をパスすることが前提となる。

MAC 生成：カードは、秘密鍵 SK_3 を用いて、本人確認に関するログ（認証成功／失敗）等の取引データに対する MAC を生成する。カードは、同 MAC を端末経由でカード発行者のサーバに送信する。サーバは、カードと秘密鍵 SK_3 を共有できるため、同 MAC を検証し、MAC が正しければ本人確認に関するログを信用する。秘密鍵 SK_3 は、取

[22] Dynamic Data Authentication。このほか、EMV 仕様では、カードに格納されたクライアント証明書を端末に送信し、端末がそれを検証するという実現方法「静的データ認証（Static Data Authentication）」も定義されている。
[23] EMV 仕様では、鍵ペア SK_1/PK_1 を鍵ペア SK_2/PK_2 として使い回す運用も認められている。

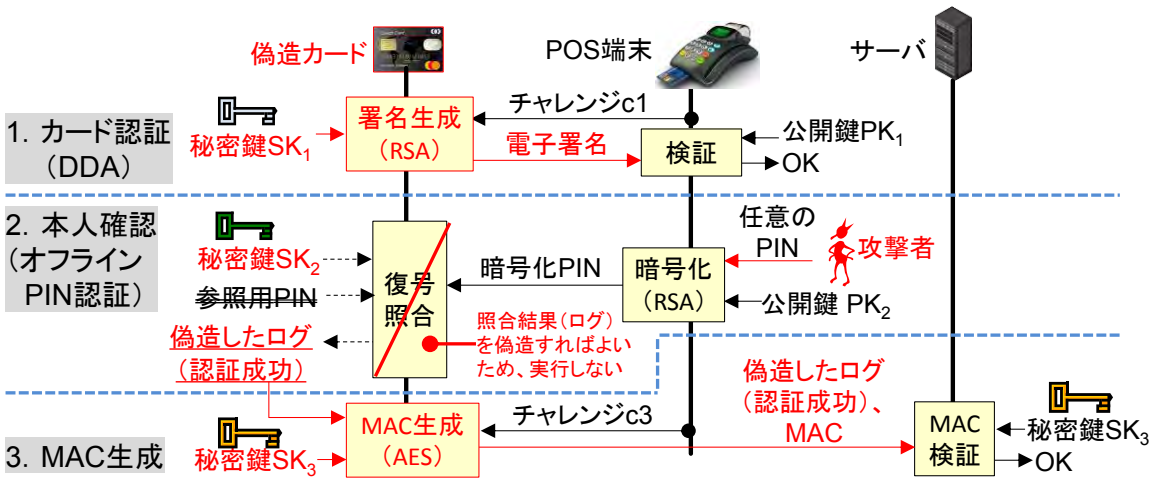
引毎にカード内およびサーバ内で生成・共有される。詳細については本節(3)を参照のこと。なお、端末は、カードと秘密鍵 SK_3 を共有できないため、MAC を検証できない。EMV 仕様では、MAC の生成方法についてカード発行者独自の生成方法を認める一方で、代表的な共通鍵暗号である AES を用いた方法も例示している。

(2) サイドチャネル攻撃により秘密鍵が漏洩した場合の影響

サイドチャネル攻撃により EMV カードから秘密鍵が漏洩した場合に、不正取引が成立するか否かについて考察する（図表 19）。想定する攻撃者と不正取引の成立条件は、それぞれ次のとおりとする。

想定する攻撃者:他人の EMV カードを盗取し、サイドチャネル攻撃により同カードから各鍵ペア（SK_1/PK_1、SK_2/PK_2、SK_3/PK_3）を入手している。さらに、各鍵ペアを格納した偽造カードを作成している。ただし、同カードの正規 PIN については入手していない。

不正取引の成立条件：想定する取引フローにおける 3 つの処理（カード認証、本人確認、MAC 生成）について、POS 端末あるいはサーバの検証をパスできた場合に取引が成立したとみなす。



図表 19. 偽造カードを用いた不正取引手続き

攻撃者が各処理をパスできるか否かについて考察する。まず、カード認証については、攻撃者は、秘密鍵 SK_1 を利用可能なため、正しいレスポンス（電子署名）を生成可能である。このため、カード認証については、POS 端末の検証をパスできる。本人確認については、本来はカード内で照合が行われるが、偽造カードであれば照

合を行うことなく認証成功というログを偽造可能である[24]。よって、攻撃者は、オフライン PIN 認証を行っているように見せるために、POS 端末に任意の PIN（ランダムな数字で構わない）を入力するものの、カード内では照合を行わずに認証成功のログを偽造する。MAC 生成については、攻撃者は、秘密鍵 SK_3 を利用可能なため、偽造したログ等の取引データに対する正しい MAC を生成可能である。このため、サーバは、正しい MAC であると誤って判断し、さらに、本人確認も成功したと判断するため不正取引が成立する可能性がある。

以上を整理すると、攻撃者が、SK_1、SK_2、SK_3 を利用可能な場合には、正規 PIN を知らなくとも、本人確認に関するログ（認証成功）を偽造したうえで適切な MAC を生成可能であり、オンラインでサーバが MAC を検証したとしても、不正取引が成立する可能性があることがわかる。なお、ATM における IC キャッシュカードを用いた取引（預金引出等）への影響については、次の Box を参照のこと。

Box　ATM における IC キャッシュカードを用いた取引への影響

想定する攻撃者：他人の IC キャッシュカードを所持しており、同カード内の秘密鍵をサイドチャネル攻撃により入手可能。一方、同カードに対応する正規の PIN は入手していない。

想定する ATM 取引：IC キャッシュカード、生体認証、PIN の 3 要素認証を行うとする。

- 1 つ目の認証要素である IC キャッシュカードについては、サイドチャネル攻撃により同カードから秘密鍵を盗取することが「短時間で」実行可能な状況を想定する。この場合、攻撃者は、他人から IC キャッシュカードを盗取し、直ちに秘密鍵を推定したうえで、同カードを密かに本人に戻すことで、本人に気付かれることなく偽造カードを作製できるという潜在的なリスクがある。
- 2 つ目の認証要素である生体認証については、カード内で生体認証を行う形態（「Match on Card」と呼ばれる）を想定する。この場合、ATM や銀行ホストシステムが照合を行わないため、前述のオフライン PIN 認証と同様に、偽造カード内で生体認証の照合結果を偽造されるという潜在的なリスクがある。
- 3 つ目の認証要素である PIN については、ATM における取引では、ユーザが ATM に入力した PIN は、銀行ホストシステムに送信され、同ホストシステムで照合が行われる（「オンライン PIN 認証」と呼ばれる）。このため、前述の 2 つの認証要素（IC キャッシュカード、生体認証）が破られたとしても、攻撃者が正規の PIN を知らない限り、不正取引は成立しない。

[24] 厳密には、オフライン PIN 認証の最後に、カードから POS 端末に本人確認に関するログが送信される。しかし、このログは暗号技術により保護されていないため改ざんや偽造が可能であり、攻撃者がログを偽造することで POS 端末を騙すことが可能である。こうした攻撃や対策については、Murdoch, *et al.*[2010]や鈴木・廣川・古原[2012]に詳しい。

(3) EMV 仕様上の制約等を加味した場合の留意点

まず、他人の EMV カードを所持している攻撃者が、不正取引を成立させるために不可欠な秘密鍵が前述の 3 つ（SK_1、SK_2、SK_3）のうちどれかについて分析する。カード認証については、秘密鍵 SK_1 を入手していなくとも、正規カードにレスポンスの生成を行わせることで、POS 端末の検証をパスできる[25]。このため、秘密鍵 SK_1 は必須とはいえない。本人確認については、前述のとおりカード内で照合を行う必要がないため、秘密鍵 SK_2 も必須とはいえない。MAC 生成については、正規カードに MAC 生成を行わせた場合、偽造したログ（認証成功）を外部から正規カードに与えることができないため、認証失敗のログに対する MAC が生成される。偽造したログに対する正しい MAC を生成するためには、秘密鍵 SK_3 が必須となる。よって、不正取引の成立には、秘密鍵 SK_3 のみが不可欠であることがわかる。

次に、秘密鍵 SK_3 に関する EMV 仕様上の制約等を示す。

① 秘密鍵 SK_3 は、カードのマスタ鍵を用いて取引毎に異なる値となるように生成される。EMV 仕様では、SK_3 の生成方法についてカード発行者独自の方法を認めている一方で、取引毎に更新されるカウンタ[26]をマスタ鍵で暗号化したものを秘密鍵 SK_3 とする生成方法を例示している。

② 上記①の生成方法によって生成された秘密鍵 SK_3 をサーバと共有するために、カードは、カウンタの値を POS 端末経由でサーバに送信する。なお、マスタ鍵は、カード発行時にカードに格納されるため、カードとサーバ間で事前に共有できている。

③ 1 回の取引で行われる MAC 生成は、高々2 回である。

④ カウンタは 16 ビットのデータであり、その上限は 65,536（$= 2^{16}$）回である。EMV 仕様では、カウンタが上限に達した場合には、カードを取引できない状態（ブロック状態）にすることが求められている。

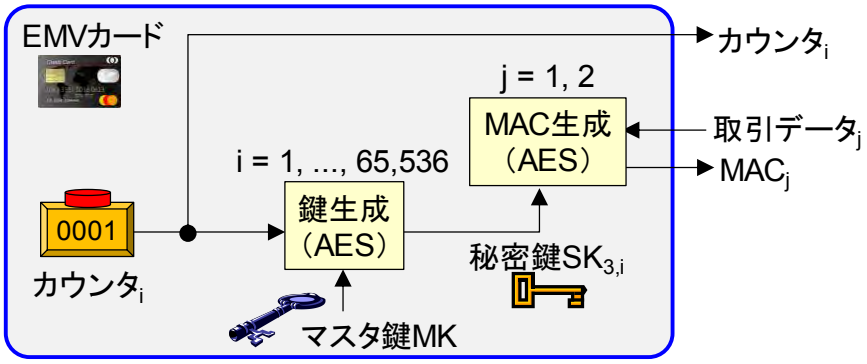
これらの制約等を踏まえ、秘密鍵 SK_3 およびマスタ鍵（上記①）をサイドチャネル攻撃で推定する際の攻撃条件や秘密鍵生成から MAC 生成の流れを整理するとそれぞれ図表 20、図表 21 のとおりである。秘密鍵 SK_3 とマスタ鍵のそれぞれの攻撃時の条件を比較すると、相対的に計測回数の多いマスタ鍵の方が、攻撃者が推定し易いと考えられる。そこで、マスタ鍵の攻撃時の条件を攻撃者にとって厳しくする（攻撃のハードルを上げる）ための運用面での対策を 2 つ示す。1 つは、カウンタの上限を引き下げるという対策である。この対策は、EMV 仕様上も認められている。もう 1 つは、マスタ鍵を定期的に更新するという対策である。具体的には、①予め複数のマスタ鍵をカード内に格納しておき、それに切り替えるというオフライ

[25] こうした攻撃は、「リレー攻撃」や「中間者攻撃（Man-in-the-Middle）」等と呼ばれる。
[26] EMV 仕様では、「Application Transaction Counter」と呼ばれる。

ン型の方法と、②カードとサーバの通信機能である「Issuer Script」を用いてマスタ鍵を更新するというオンライン型の方法が考えられる。このほか、システム全体で考えれば、サイドチャネル攻撃の影響を受け難い独自の鍵生成方法をシステム設計時に選択しておくことも考えられる。なお、本稿では、カウンタを改ざんする攻撃（例：故障利用攻撃）については、検討対象外としている。

図表 20. EMV カードにおけるサイドチャネル攻撃時の制約

推定対象	攻撃時の条件
秘密鍵 SK_3	・ 高々2 回の MAC 生成を計測可能。 ・ その際の入力（取引データ）および出力（MAC）は、入手可能。
マスタ鍵	・ 最大 65,536 回の鍵生成処理（AES による暗号化）を計測可能。 ・ その際の入力（カウンタ）は入手可能であるが、出力（秘密鍵 SK_3）は入手困難。



図表 21. EMV カードにおける秘密鍵生成と MAC 生成

5. おわりに

我々の生活に情報システムが浸透するにつれ、暗号アルゴリズムを実装した暗号モジュールの安全性の重要性が増している。暗号モジュールへの実装攻撃をみると、物理解析や故障利用解析については、攻撃時の IC チップの破壊や IC チップへの刺激挿入といった操作を検知するとともに、内部の秘密鍵を消去する等の対策が有効といえる。これに対しサイドチャネル攻撃は、暗号モジュールの物理現象を計測するだけという受動的な攻撃であるため、同攻撃を検知することは難しく、サイドチャネル情報の漏洩を減らすという対策に頼らざるを得ず、そうした対策の効果を厳密に評価することも求められる。

サイドチャネル攻撃が提案されてから約 20 年が経つなかで同攻撃を含め、暗号モジュールの安全性を評価・認証する制度（Common Criteria）が整備され、認証品を調達可能な状況になってきている。しかし、暗号モジュールの安全性は、理論的

に安全性を確保可能な暗号アルゴリズムとは異なり実装に大きく依存することから、技術の陳腐化の影響や想定する攻撃者の資金力によっては、その安全性を確保できなくなるケースが発生しうることに留意が必要である。特に、わが国の一部のIC キャッシュカードについては、有効期限が設けられておらず、一度発行したICカードを長期間利用することが想定されているようである。新たなサイドチャネル攻撃手法の考案等、安全性が経年劣化していくなかで、危殆化するリスクが高まっていくことにも留意し続けることが求められる。

これらを考慮すると暗号モジュールの調達者は、認証品を調達することに加え、発行済み IC カードの安全性を定期的に評価することが有用であろう。また、暗号モジュールから秘密鍵等が漏洩することを前提に、被害を早期検知するための仕組みや被害拡大を防止する仕組み等について検討することが望ましい。

以　上

参考文献

金融情報システムセンター、「金融機関等コンピュータシステムの安全対策基準・解説書（第 8 版）」、2011 年

金融庁、「偽造キャッシュカード問題等に対する対応状況（平成 26 年 3 月末）」、2014 年 8 月 27 日

情報処理進行事業協会・通信・放送機構、「暗号技術評価報告書（2002 年度版）」、2003 年 3 月

鈴木雅貴・廣川勝久・古原和邦、「IC カード利用システムにおいて新たに顕現化した中間者攻撃とその対策」、『金融研究』第 31 巻第 3 号、2012 年

全国銀行協会、「盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正使用に関するアンケート結果について」、全銀協ニュース、2014 年 11 月 27 日

日本クレジットカード協会、「IC カード対応端末の設置台数が 100 万台を突破」、2014 年 7 月 14 日

日本クレジット協会、「クレジットカード不正使用被害の集計結果について」、2014 年 12 月 26 日

————、「クレジットカードの不正使用防止対策と IC 化の取組み状況について」、ニュースリリース、2015 年 2 月 27 日

野崎華恵・藤崎浩一・川村信一、「暗号モジュールの実装攻撃対策技術」、東芝レビュー vol.64 no.7、2009 年、28～31 頁

本間尚史・青木孝文、「暗号モジュールから漏洩する情報を利用するサイドチャネル攻撃」、『システム制御情報学会誌』vol.57 no.12、2013 年、505～510 頁

松本 勉・大石和臣・高橋芳夫、「実装攻撃に対抗する耐タンパー技術の動向」、『情報処理学会誌』 vol.49 no.7、2008 年、799～809 頁

水野弘章・岩井啓輔・田中秀磨・黒川恭一、「サイドチャネル攻撃に関する情報理論的解析(3)」、暗号と情報セキュリティシンポジウム、2A4-3、2014 年

Anderson, Ross, “Security Engineering Second Edition,” Wiley, 2008.

Bellcore, “Now, Smart Cards Can Leak Secrets,” Bellcore Media Advisory, 25 Sept. 1996.

Boneh, Dan, Richard A. DeMillo, and Richard J. Liption, “On the Importance of Checking Cryptographic Protocols for Faults,” EUROCRYPT ’97, Lecture Notes in Computer Science (LNCS) vol.1233, 1997, pp.37-51.

Eisenbarth, Thomas, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani, “On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme,” CRYPTO 2008, LNCS vol.5157, 2008, pp.203-220.

EMVCo, “EMV 4.3 Book 1 – Application Independent ICC to Terminal Interface Requirements,” EMVCo, 2011a.

————, “EMV 4.3 Book 2 – Security and Key Management,” EMVCo, 2011b.

————, “EMV 4.3 Book 3 – Application Specification,” EMVCo, 2011c.

————, “EMV 4.3 Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements,” EMVCo, 2011d.

European Payments Council (EPC), “Resolution: Preventing Card Fraud in a mature EMV Environment,” Doc EPC424-10, 31 Jan., 2011.

Gandolfi, Karine, Christophe. Mourtel, and Francis. Olivier, “Electromagnetic analysis: concrete results,” Cryptographic Hardware and Embedded Systems (CHES) 2001, LNCS vol.2162, pp.251-261.

Genkin, Daniel, Adi Shamir, and Eran Tromer, “RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis,” CRYPTO 2014, LNCS 8616,2014, pp.444-461.

Goodwill, Gilbert, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi, “A testing methodology for side-channel resistance validation,” Non-Invasive Attack Testing Workshop (NIAT), 2011.

Jaffe, Josh and Pankaj Rohatgi, “Efficient side-channel testing for public key algorithms: RSA case study,” NIAT, 2011.

Joint Interpretation Library, “Application of Attack Potential of Smartcards,” version 2.9, 2013.

Kocher, Paul C., “Crytptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks,” extended abstract, 1995.

————, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” CRYPTO ’96, LNCS vol.1109, 1996, pp.104-113.

————, Joshua Jaffe, Benjamin Jun, “Introduction to Differential Power Analysis and Related Attacks,” 1998.

————, ————, and ————, “Differential Power Analysis,” CRYPTO ’99, LNCS vol.1666, 1999, pp.388-397.

Mizuno, Hiroaki, Keisuke Iwai, Hidema Tanaka, and Takakazu Kurokawa, “Analysis of Side-Channel Attack Based on Information Theory,” IEICE Trans. Fundamentals, vol.E97-A no.7, 2014, pp.1523-1532.

Murdoch, Steven J., Saar Drimer, Ross Anderson, and Mike Bond, “Chip and PIN is Broken,” 2010 IEEE Symposium on Security and Privacy, 2010.

Oswald, David, and Christof Paar, “Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World,” CHES 2011, LNCS vol.6917, 2011, pp.207-222.

Skorobogatov, Sergei P., “Semi-invasive attacks - A new approach to hardware security

analysis," UCAM-CL-TR-630, 2005.
VISA, "Visa Announce U.S. Participation in Global Point-of-Sale Counterfeit Liability Shift," VISA BULLETIN, 9 Aug., 2011.