技術基礎講座

【非接触ICカード技術】

ICカードでは，格納された重要な情報を守るため，さまざまなセキュリティ対策が施されています．特にセキュリティが重要となる公共系や金融系の分野では，使用されるICカードに一定レベルのセキュリティを保証する必要があります．そこで，ISOなどの標準化団体やクレジットカードブランドがセキュリティの認証制度を策定しています．これらの認証制度では，客観性を確保するために，開発者でも調達者でもない中立な立場にある評価機関が評価する制度になっています．ここではICカードのセキュリティ対策と，それを評価する認証制度について解説します．

セキュリティ認証制度の必要性

ICカードは個人識別番号（PIN: Personal Identification Number）やカードを認証する鍵などの秘密情報を格納しています．悪意を持った者が，これらの秘密情報を窃取したり，改ざんしたりすることを防ぐために，ICカードにはさまざまなセキュリティ対策が施されています．このセキュリティ対策が一定のレベルにあることを保証するために，ISOなどの標準化団体やクレジットカードブランドが認証制度を策定しています．特に高いセキュリティが要求される公共系や金融系の分野では，これらの認証に合格したICカードのみをサービスに適用する案件が増加しています．

ここでは，ICカードのセキュリティ対策の考え方と，セキュリティ評価で代表的なISO/IEC 15408〔Common Criteria（CC）認証〕，暗号モジュールに関する認証制度であるISO/IEC 19790とFederal Information Processing Standards（FIPS） 140-2，およびクレジット認定制度について述べます．

セキュリティ対策の考え方

一般的に，セキュリティ対策は**図1**の手順で進めていきます．まず，最初に守るべき資源を決めます．例えばキャッシュカードやクレジットカードならば暗証番号を，電子マネーのカードならば決済に使用する鍵情報など，取得されてしまうと悪用される情報を守るべき資源として決めます．

次に，脅威分析をします．具体的には，どのような技術レベルの者が，どれぐらいの時間をかけて，どのような機材（一般に入手できる機材か，特殊な機材なのか）を使用して，守るべき資源に対してどのような攻撃をするのかという脅威の想定をします．

最後に，守るべき資源と想定した脅威に基づいて，資源を守るためのセキュリティ対策をします．

必要以上のセキュリティ対策は，処理速度の低下により使い勝手が悪くなる，開発期間や開発コストが増加す

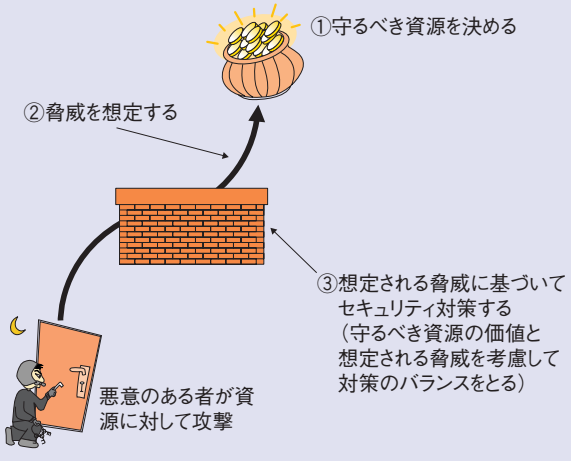

図1　セキュリティ対策の考え方

るなどの問題を発生させます．このため，守るべき資源の価値と想定する脅威を考慮したうえで，バランスがとれたレベルでセキュリティ対策をする必要があります．

続いて，ICカードに行われる攻撃と対策について，発行後のICカードに直接的に行われる攻撃と，発行時のICカードに行われる攻撃の2つについて述べます．

発行後のICカードに行われる攻撃

発行後のICカードに行われる攻撃は，破壊型解析法と非破壊型解析法に大きく分けられます．破壊型解析法は，ICカードのICチップ自体を物理的に開封し，ICチップ内のバスなどに直接測定器のプローブを当てたり，顕微鏡で観察したりして，バスやメモリの内容を読み取る攻撃です．これに対しては，ICチップを物理的に開封した場合は，チップの回路が破壊される構造にするなどの対策がとられます．

非破壊型解析法には，①暗号演算の実行中の消費電流の変化や実行時間の変化を観察するサイドチャネル攻撃，②暗号演算の実行時に異常電圧をかけるなどして誤作動させ，この結果から演算内容を推論する故障利用解析などの攻撃，があります．

これに対しては，暗号の演算時の消費電流を一定にする回路構成にする，演算結果によらず実行時間が一定になるようにプログラムを組む，異常電圧など異常状態を検出するセンサをICチップに搭載する，などの対策がとられます[(1)]．

ICカードの発行時に行われる攻撃

前項のように，ICカード自体には，さまざまな攻撃に対する対策がとられているため，ICカードに格納された秘密情報は容易に読み出せない耐タンパ性があります．しかし，ICカードに格納する前の秘密情報は，発行システムのハードディスクやバックアップテープなどに保管されており，そこから秘密情報が盗取される可能性があります．

また，故障などの原因により発行に失敗したICカードも，セキュリティの機能がきちんと動作していない可能性があり，悪意のある者がこのICカードを入手した場合，ICカード内部を解析してしまう可能性もあります．

このため，①発行システムは，特定の人しか入室できない場所に設置し，さらにパスワードロックをかけて，不特定多数の人が操作できないようにする，②ICカードに搭載する秘密情報を格納したバックアップメディアは鍵がついた書架に保管する，③カードの盗難，すり替えを防ぐために,不特定の人に発行作業や配送作業をさせない，④発行に失敗したカードは悪用されないように廃棄する，など，カードを発行する環境にもセキュリティ対策を行う必要があります．

次に ICカードに関する主なセキュリティ認証制度について述べます．

CC認証（ISO/IEC 15408）

ISO/IEC 15408は，CC認証とも呼ばれています．CC認証では，セキュリティの観点から評価対象（TOE：Target Of Evaluation）が適切に設計され，その設計どおり正しく実装されていることを検証します．このために，CC認証では，評価対象の製品の設計内容の形式，用語と，評価で検証する項目を国際標準として規格化しています[(2)]．

近年，政府調達案件でも，CC認証の取得が要求されることが増加しており，日本では，IPA（社団法人　情報処理推進機構）がCC認証の認証機関として，認証を付与しています．実際の評価は，NITE（独立行政法人　製品評価技術基盤機構）から認定を受けた評価機関が実施し，IPAは評価機関が作成した評価報告書を基に製品を認証します．さらに，CC認証では，CCRA（Commom Criteria Recognition Arrangement）の制度があり，この制度に加入している国ならば，ある国でCC認証を取得した製品は，他の国でも効力を持ちます．また，評価機関による評価方法のガイダンスは，ISO/IEC 18045として標準化されており，評価機関により評価のばらつきが出ない制度を目指しています[(3),(4)]．

CC認証の評価レベルはEAL 1～7まであり，レベルが高くなるほど設計から実装までの開発プロセスの管理を厳密にすることが求められます．EAL 1～4は民生品向きで，EAL 5以上は軍用や高度なセキュリティ製品向きとなっています．例えば，セキュリティ機能の仕様は，民生向きのEAL 1～4では自然言語で記述してもよいですが，最高レベルのEAL 7では数学的な形式言語でより厳密に

記述して管理する必要があります．また，EALのレベルごとに満たすべき項目が決まっており，この項目のうち１つでも，より高いレベルを満たしていれば，レベルに+を付けます．例えば，EAL 4 +ならば，EAL 4 のレベルの項目はすべて満たしており，このうち，１つ以上の項目がEAL 5 以上で規定された項目を満たしていることを意味します．なお，EALのレベルは評価の厳密さのレベルを示し，必ずしも，EALのレベルが高いほどセキュリティ強度が高いわけではないことに注意する必要があります．

CC認証の評価の概要を**図 2** に示します．

CC認証では，最初に，調達者がＰＰ（Protection Profile）と呼ばれるドキュメントで製品に対して要求するセキュリティ機能を定義し，開発者がST（Security Target）と呼ばれるドキュメントで開発する製品で，実現するセキュリティ機能を定義します．例えば，ICカードでは，PPやSTで，評価対象の製品の構成，暗証番号など守るべき資源，想定される脅威としてサイドチャネル攻撃などICカードへの攻撃，これらの脅威に対する対策方針，評価のレベルなどを記載します．さらに，STでは，対策方針に基づいて，暗証番号の検証時間を一定にするなど，具体的なセキュリティ対策も記載します．

そして，評価者は単に完成品だけを評価するのではなく，STで定義したとおりにTOEが正しく実装されているかを，開発ドキュメント，利用者向けの注意事項やマニュアル，製品の製造・使用・廃棄の一連のライフサイクルを規定したドキュメントなどを通して，開発プロセスも含めて厳密に評価します．

このように，CC認証では，セキュリティの観点で守るべき資源がある製品ならば，すべて評価対象とすることができる，非常に汎用的な評価制度になっています．このため，ICカードだけでなく，コピー機のファームウェア，PC用OSなど，CC認証取得製品は多岐にわたっています．

暗号モジュールの認証（ISO/IEC 19790とFIPS 140-2）

FIPS 140-2は米国のNIST（National Institute of Standards and Technology）において，暗号モ

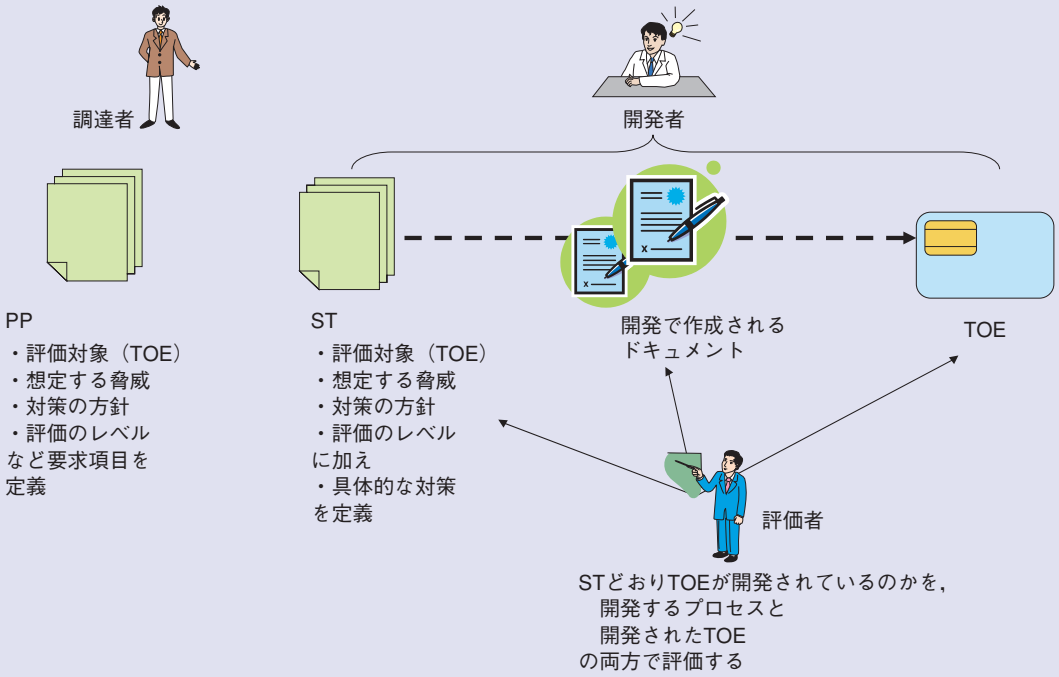

図 2　CC認証の評価の概要

ジュール（暗号演算を行うハードウェア，ソフトウェア，ファームウェア）が満たすべき要件を規定した規格で，このFIPS 140-2を基にISOで規格化したものがISO/IES 19790です．これらの認証では，HSM（Hardware Security Module）や暗号ライブラリなどのような暗号製品を，暗号演算の正しさと，暗号モジュールのセキュリティの観点で評価します．ICカードでもこのような暗号モジュールを実装した製品が多くあり，この認証を取得した製品もあります．

CC認証と異なり，FIPS 140-2では，評価可能な暗号アルゴリズムの種類や乱数生成のアルゴリズムは具体的に決められており，これらは，承認されたセキュリティ機能と呼ばれています．承認されたセキュリティ機能以外は，暗号演算とみなされず，評価を受ける製品は承認されたセキュリティ機能を最低限１つは実装している必要があります．なお，承認されたセキュリティ機能は暗号技術の進展により，安全性を考慮して改定されており，例えば，共通鍵暗号演算については，2001年からAESが新たに追加されました．

認証にあたっては，開発者は，暗号モジュールを物理的に格納して外部と区別する暗号境界を定義し，セキュリティポリシとして，提供するサービス，オペレータがアクセスするときに使用する暗証番号やパスワードなどの認証機能，セキュリティを守るための暗号鍵の管理，開封したら破壊されるなど物理的なメカニズム，起動時などに正常に動作することを確認する自己テスト，動作環境，インストール手順，開発手順などを定義します．

これらから，レベル１～４に分けて規定された要件に基づいて製品は評価され，さらに，承認されたセキュリティ機能を暗号モジュールが正しく演算することも評価されます．なお，FIPS 140-2の要件はCC認証よりも具体的に規定されており，レベルが上がるにつれ要件は多くなり，セキュリティ強度も高くなります．例えばレベル１では，特別な物理的なメカニズムは要求されませんが，レベル４では，電圧や温度などの適正作動範囲からの変動を検知して，異常なときには攻撃されたとみなして，暗号鍵などの秘密情報をクリアするなどの耐タンパ性を確保するための対策を行っていく必要があります．

FIPS 140-2は，米国のNISTとカナダのCSE（Communication Security Establishment）が共同で運用しているCMVP（Cryptographic Module Validation Program）の枠組みによって評価されます．CMVPでは，CMTラボ（Cryptographic Module Testing Laboratory）と呼ばれる試験機関が認定されており，認証の申請者はCMTラボに試験を依頼し，この試験結果をNISTやCSEに提出して合格したものが認証されます[5]．

日本では，ISO/IEC 19790に対応するものとして，JIS規格 JIS X 19790が制定されました．総務省および経済産業省が公表した電子政府推奨暗号リスト等に記載されている暗号演算を実装した暗号モジュールを，暗号モジュール試験および認証制度（JCMVP：Japan Cryptographic Module Validation Program*）の枠組みで評価しています．JCMVPはIPAで運用され，申請者はNITEで認定された暗号モジュール試験機関で試験し，この試験結果をIPAに提出することにより認証を受けます[6]．

クレジットカード認定

クレジットカード認定は，ICカードが，ICクレジットカードとして必要な機能とセキュリティを備えていることを検証するための認定制度で，この認定を取得していないICカードはICクレジットカードとして使用することはできません．

今までに述べた認証制度と異なり，クレジットカード認定は，認定の基準や評価方法がクレジットカードブランドごとに異なっています．

クレジットカード認定では，おおむね次の項目を評価します．

① チップの評価：ICクレジットカードに使用するチップが，クレジットカードブランドが指定するセキュリティ対策を行っているか．

② ソフトウェアの評価：ICクレジットカードに搭載するソフトウェアがクレジットカードとして使用するために必要なコマンドを実装しているか，すなわち，クレジットカードブランドが指定したコマンド，暗号

＊ JCMVPは，IPAの登録商標です．

表　ICカードに関するセキュリティ認証制度

	CC認証	ISO/IEC 19790とFIPS 140-2	クレジットカード認定
規定している項目	・製品の設計内容の形式，用語 ・評価で検証する項目	暗号モジュールが実装すべき暗号アルゴリズム，セキュリティの強度	クレジットカードに必要な機能とセキュリティ強度
評価の観点	・セキュリティに関する機能がSTどおりに実装されているか ・EAL 1 ～ 7 の厳密さのレベルで評価される	・暗号モジュールが正しく暗号演算するか ・規定されたセキュリティ強度を持っているか ・レベル 1 ～ 4 のレベルで評価される	・クレジットカードの機能が実装されているか ・セキュリティ強度が十分か
提供すべき暗号	STで開発者が規定する	・承認されたセキュリティ機能のうち，最低限，1つは提供する必要がある ・承認されたセキュリティ機能以外は暗号演算とみなされない	暗号演算，鍵長とも，各クレジットカードブランドが個別に指定する
想定される攻撃	・STで開発者が規定する ・EALのレベルが高いほどセキュリティ強度が高いわけではない	・レベルごとに想定される攻撃は決まっている ・レベルが高いほどセキュリティ強度が高い	各クレジットカードブランドが個別に指定する
カードの発行環境	発行環境が評価対象に含まれるのかは，STで開発者が規定する	評価対象外	・評価対象に含まれる ・各クレジットカードブランドが個別にセキュリティ対策を指定する
開発プロセス	・評価対象に含まれる ・EALのレベルが高いほど厳密な管理が要求される	・評価対象に含まれる ・レベルが高いほど厳密な管理が要求される	通常は評価対象に含まれない
評価される製品例	ICカード，OS，ファームウェアなど，守るべき資源があれば，どの製品でも適用可	ICカード，HSM，暗号ライブラリなど，暗号演算機能があるもの	ICクレジットカード

演算，暗号の鍵長を実装しているか．さらに実装されたソフトウェアはクレジットカードブランドが指定したセキュリティ対策を行っているか．

③　ICカードの券面の評価：ICクレジットカードの券面のデザイン，エンボス（クレジットカード番号などを記載した凹凸），偽造防止のホログラムがクレジットカードブランドの指定どおりになっているか．

④　カード発行工場の評価：ICクレジットカードを発行する工場で，クレジットカード情報が漏洩しないように，クレジットカードブランドが指定したセキュリティ対策を実施しているか．

ま と め

これまで説明したICカードに関連する認証制度を**表**に示します．これらの認証制度は認証の目的により評価の観点や評価項目が異なっており，適用先に応じて，どの認証を取得すべきかを検討する必要があります．

現在，バイオメトリクス認証のセキュリティ評価の標準としてISO/IEC 19792が策定中であり，今後は，バイオメトリクス認証の認証制度も実施されると予想されます．

■参考文献

⑴ http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/node2.html
⑵ http://www.commoncriteriaportal.org/
⑶ http://www.ipa.go.jp/security/jisec/
⑷ http://www.ipa.go.jp/security/jisec/documents/pamph_0611.pdf
⑸ http://csrc.nist.gov/groups/STM/cmvp/
⑹ http://www.ipa.go.jp/security/jcmvp/

◆問い合わせ先

NTTサービスインテグレーション基盤研究所
ICカードサービス推進プロジェクト
E-mail　sd-info@lab.ntt.co.jp