1. 21世紀初頭の暗号技術

4. 暗号ハードウェア実装性能と安全性評価

佐藤　証
日本アイ・ビー・エム（株）東京基礎研究所
akashi@jp.ibm.com

山岸 篤弘
（独）情報処理推進機構
atsuhiro@iss.isl.melco.co.jp

暗号技術は日常生活のさまざまな場面で利用されるようになり，小型機器への組み込みから高速なハイエンドサーバまで幅広いアプリケーションにおいて，暗号ハードウェアは必要不可欠である．そして，動作速度や回路規模といった基本性能の研究に加えて，ここ数年，暗号モジュールの実装面からの攻撃とその対策が大きな注目を集めている．そこで本稿では，最も普及している暗号アルゴリズムである DES，AES そして RSA のハードウェア実装のポイントを解説した後，暗号モジュールの安全性評価制度として米国やカナダで運用されている CMVP 制度を取り上げ，その現状を紹介する．

暗号ハードウェアの現状

暗号アルゴリズムは，特殊な演算や数千ビットといった大きな数を扱うため，10年ほど前までは高価な専用ハードウェアが必要で，またその用途も軍事部門や政府そして金融などに限られていた．しかし現在は，MPU性能の向上によりPC上のソフトウェア実装でも速度は十分で，インターネットショッピングなどで日常生活にも広く暗号が浸透してきている．しかしながら暗号ハードウェアが不要となったわけではなく，リソースや消費電力に制限のある小型組み込み用途や，より高い処理能力が求められるハイエンドサーバには欠かすことができない．たとえば，携帯電話の通信暗号化，音楽・映像コンテンツのスクランブル，自動改札など，いたるところに暗号ハードウェアが使用されている．また，ハードウェアの解析には特殊な装置や設備が必要となるため，安全面でも優位性がある．しかしここ数年，ハードウェアの内部解析を行うかわりに，電流や電圧そして電磁波など，暗号処理中の副次的な情報を利用して秘密鍵を推定するサイドチャネル攻撃の研究が進んでいる．そして，標準化活動も暗号アルゴリズムの安全性から，暗号モジュールの安全性評価手法の確立へと移りつつある．

本稿では，業界標準のアルゴリズムである共通鍵暗号のDES[1]とAES[2]，そして公開鍵暗号のRSA[3]を取り上げ，LSIハードウェア化の留意点を解説した後，安全性評価活動の動向を紹介する．

DESとAESの構造と回路実装のポイント

DES[☆1]は1977年に米国で標準化され，最も普及している共通鍵暗号アルゴリズムの1つである．しかし鍵長が56ビットと短く，コンピュータの性能向上によって全数探索で解読が可能となったため，現在は鍵を増やしてDESを3回実行するTriple-DESが主流となっている．さらに米国標準技術研究所（NIST）は安全性を向上させ，かつハードウェアとソフトウェアの実装効率にも優れたAESを2001年に標準化した．

図-1にDESとAESのデータランダム化部の構成を示す．DESは64ビットのデータを左右32ビットに分け，32ビットの変換を交互に繰り返すFeistel型と呼ばれる構造を持ち，またAESの構造は128ビットのデータを一括して変換するSPN型と呼ばれている．ソフトウェア実装では内部関数の複雑さやMPUとの相性，そして反復回数といったトータルな演算量によって速度性能が決まるため，Feistel型かSPN型かといった構造による優劣はほとんどない．これに対してハードウェアでは暗号処理に特化した関数を作ることができ，また任意のビット数を並列処理することも可能である．したがって，32ビット単位で処理するDESよりも，128ビットを一度に処理できるAESの方が高速化に向いているといえる．しかし逆に考えると，DESは1クロックにAESのわずか1/4のビット数を処理するだけなので，必要とされるハードウェアリソースが非常に少ないという利点

☆1 2004年7月27日に，NISTは（Single）DESを標準暗号から取り下げることを提案した．

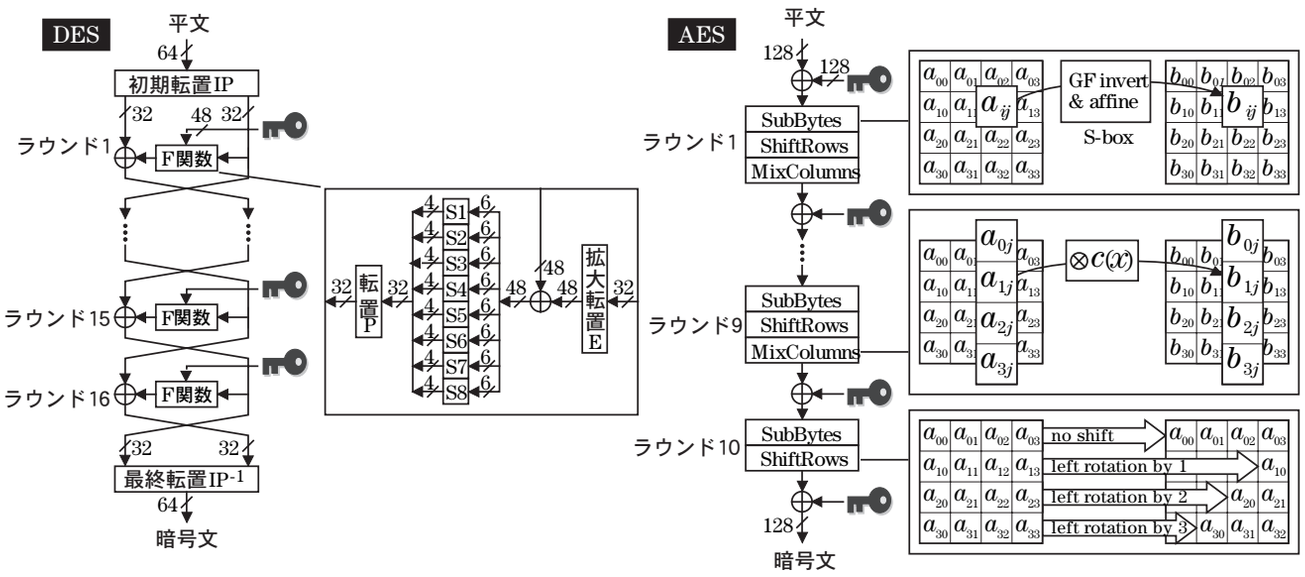

図 -1　DES と AES のデータランダム化部

がある．また，DES の Feistel 型は暗号化と復号化を同じデータパスで実行できるのに対し，AES の SPN 型では暗号化と復号化では逆関数を用いるため，両者を同一のデータパスで処理することはできない．このため単純に構造だけから判断すると，AES は DES の 8 倍ものハードウェアリソースが必要となってしまう．このような理由からハードウェアの高速実装には SPN 型，小型実装には Feistel 型が有利と考えられてきた．

しかしながら，AES の処理ブロックは容易に縦 32 ビットに分割できるので，この 32 ビット処理ブロックを 1 つだけ用意して 128 ビットデータを 4 サイクルで処理するだけで，ランダム化部の回路規模を 1/4 に削減することが可能である．また DES の変換はすべて乱数テーブルで定義されているため設計の自由度が低いが，AES はガロア体 $GF(2^8)$ 上の演算など数学的に定義された関数を使用しているため，演算の最適化によるコンポーネントの小型化・共有化も可能である[4]．**図 -2** は DES と AES をいくつかの異なる回路アーキテクチャで，0.13 μ m の CMOS ASIC ライブラリによって実装したときのゲート数とスループットを比較したものである．SPN 構造を持つ AES は高速性に優れているのと同時に，小型実装においても Feistel 型の Triple-DES に対してまったく遜色ない性能が示されている．

DES が提案された当時の計算機性能と LSI の集積度を考えると，乱数テーブルの使用はソフトウェアおよびハードウェアの両実装において最良の選択であったことに異論はない．しかし，半導体製造技術が飛躍的に進歩し，暗号が組み込み機器からハイエンドサーバまで広く

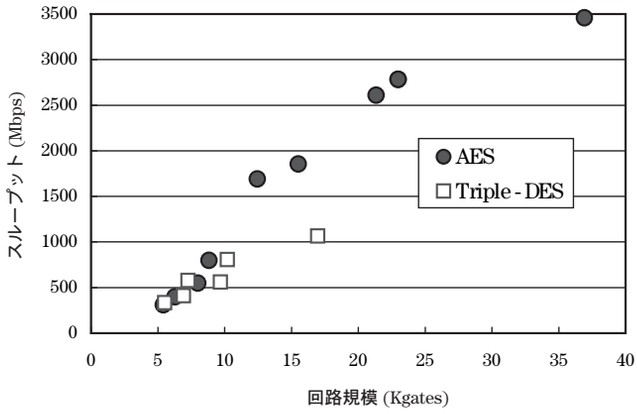

図 -2　DES と AES の ASIC 実装性能

使用されるようになり，またさまざまなアーキテクチャのプロセッサが存在する現在では，AES のようにプラットフォームや要求されるパフォーマンスに応じて柔軟に実装アーキテクチャを変更可能なアルゴリズムに優位性がある．AES のアルゴリズム最終選考においても，ソフトウェアおよびハードウェア実装の柔軟性と効率が勝敗を分けたと言うことができる．AES 選定後にもさまざまな暗号アルゴリズムが提案されているが，特定のプラットフォーム専用なのか汎用なのかということも含めて，その時々の実装技術に合った柔軟なアルゴリズム設計が重要となるであろう．

RSA 暗号の加算器実装と乗算器実装

RSA 暗号は Rivest, Shamir, Adleman が 1977 年に考案し，現在最も普及している公開鍵暗号で，次式のべき乗剰余算で実行される非常にシンプルなアルゴリズムである．

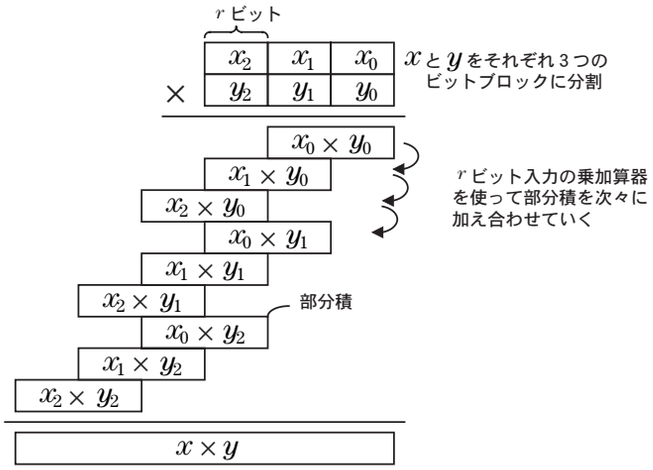

図-3　部分積加算の繰り返しによる多ビット数の乗算

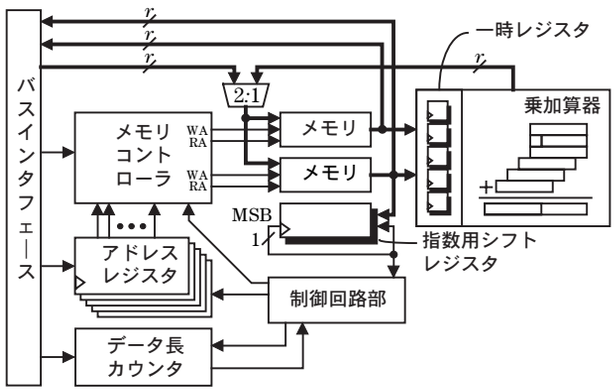

図-4　RSA暗号回路のブロック図

$$\begin{cases} C = M^e \bmod n \\ M = C^d \bmod n \end{cases}$$

ここでMは平文，Cは暗号文，eとnは公開鍵，dは秘密鍵である．式は簡単なものの，MやC，dは1,024～4,096ビットと大きな数を扱うので，このままでは通常の算術演算器などを使うことができない．そこで数年前のLSIでは，1,024ビットや2,048ビットの加減算器を手でレイアウトし，加算と減算の反復処理で実行するといった実装が行われていた．このような大きな加算器ではキャリーの伝播遅延をどのように抑えるかが高速化のポイントであり，さまざまな高速加算方式が提案されている．加算器のレイアウトは規則が高いので，LSIの集積度が低かった当時は小型・高速化に有効な手法であった．しかし現在では，乗算器を使うモンゴメリ乗算アルゴリズム[5]がソフトウェアおよびハードウェア双方で主流となっている．べき乗剰余算は乗剰余算の繰り返しで実行でき，そしてモンゴメリ乗算は乗加算とシフトの繰り返しで乗剰余算を行っている．入力データが乗加算器のビット数rよりも長い場合は，**図-3**のようにrビットの複数ブロックに分割して処理するので，入力データの長さが変わってもループ処理の回数を増減するだけで対応可能である．これに対して，たとえば2,048ビットの加算器を用いた場合は1,024ビットの処理に対して無駄があり，1,024ビットの加算器では2,048ビットの処理が簡単には行えない．また，次世代の公開鍵暗号標準として有望な楕円曲線暗号も主要な処理は乗剰余演算だが，データ長は160～256ビットほどでRSAよりも大幅に短いため，これらを同時にサポートするにはやはり乗算器アーキテクチャが不可欠となる．LSIの集積度向上とCADツールの進歩により，現在では手でレイアウトすることなく高性能な乗算器を利用することができ，逆に1,024ビットといった大きな加算器を使おうとしても，データ入出力バスが広すぎるためCADツールの自動配置配線で問題が生じてしまう．

図-4にモンゴメリ乗算を用いたRSA暗号回路の例を簡単に示す．モンゴメリ乗算では乗加算器の性能が重要であることは言うまでもないが，効率よくデータを流さないと乗加算器を待たせてしまいパフォーマンスが低下してしまう．そこで，この回路例では2つの2ポートメモリと複数の一時レジスタにうまく変数を割り当てることで，乗加算器を常に動作させている．これはDSPや高性能な算術演算器を持つプロセッサ上でデータ処理プログラムを開発するときに，データへのアクセスサイクルを短縮するためにレジスタやメモリ割り当てを最適化する場合と似ている．

表-1は0.13 μm CMOSライブラリを用いて図-4の回路を乗加算器のビット数rを8～128と変えて実装したときの，回路規模と動作周波数，そして1,024ビットのべき乗剰余演算に必要な時間を示している．ビット数rを大きくすれば当然処理能力は向上するが，乗加算器の規模が自乗のオーダーで増大し，それに伴って動作周波数も低下するため，やみくもに大きくするべきではない．乗加算器のビット数を増やすよりも，ビット数はそのままで乗加算器の数を増やしたほうがコスト対性能比の高い場合も多い．RSA暗号が提案されてから4半世紀経った今でも，乗剰余演算回路アーキテクチャやそれを用いたRSA暗号回路・楕円曲線暗号回路実装の論文が多数発表されている．そして今後もLSI製造技術とCADツールの進歩に伴い，またサイドチャネル攻撃などの新たな解析手法への対策も考慮しつつ新たなアーキテクチャが考案されていくことであろう．

暗号モジュールの安全性評価の動向

アルゴリズムの数学的な安全性に関する研究に関しては，NISTのAESプロジェクトや欧州のNESSIEプロジェ

		r = 8 bit	r =16 bit	r = 32 bit	r = 64 bit	r = 128 bit
回路規模 (gate)	乗加算器	2,537	8,031	27,384	92,831	157,817
	制御回路	10,733	10,711	10,736	12,381	18,157
	合計	13,270	18,742	38,120	105,212	175,974
動作周波数 (MHz)		384.6	294.1	222.2	169.5	116.1
1,024 ビットべき乗 剰余演算時間 (ms)		117.95	38.61	13.77	5.18	2.41

表 -1　RSA 暗号回路の性能

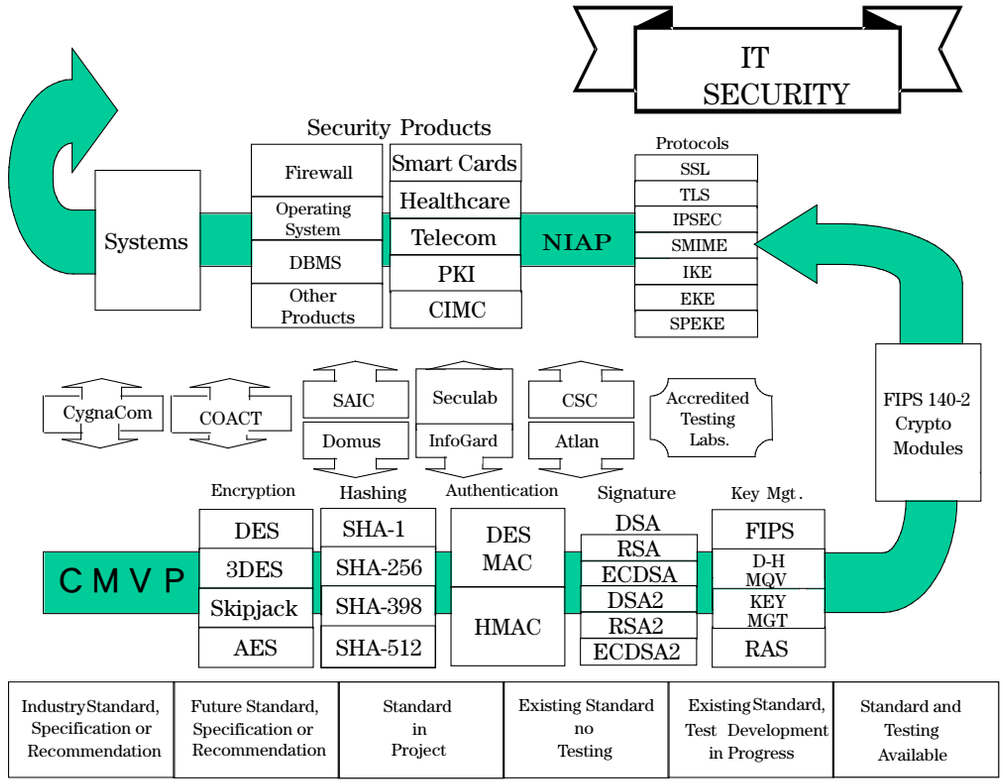

図 -5　暗号モジュール評価の位置付け [11)]

クト，日本の暗号技術検討会 (CRYPTREC プロジェクト) を契機として長足の進歩を遂げている[6)〜8)]．しかし，システムにおいて暗号技術を使用するためには，暗号アルゴリズムをソフトウェア, ファームウェア, ハードウェアとして実装する必要がある．この数学的なアルゴリズムから実装にいたる過程で多くのセキュリティホールが形成される可能性を排除できない．つまり，暗号アルゴリズムが安全だからといって，それを使用したシステムが安全であるとは限らない．

暗号機能を利用する際には，利便性からシステムとして必要なセキュリティ機能をひとまとめにした「暗号モジュール (Cryptographic Module)」を利用することが一般的であり，セキュリティ機能を提供する暗号モジュールの安全性評価が重要となる．この暗号モジュールが満たすべき安全性の基準としては，NISTが定めたFIPS[☆2] PUB 140-2 “Security Requirements for Cryptographic Modules”が広く知られている[9)]．また, IC カード (Smart Card) に特化した評価基準／評価手法はJIL[☆3] として公開されている[10)]．特にFIPS 140-2で規定されている安全性要求基準への適合性を検査する評価制度としては，米国NIST[☆4] とNAVLAP[☆5] およびカナダのCSE[☆6] が共同で運用しているCMVP[☆7] が存在し，1994年以降約450製品が評価されている．米国やカナダにおける暗号モジュール評価の位置付けを**図-5**に示す[11)]．

日本では，2003年度からCRYPTRECの下に暗号モ

☆2 FIPS: Federal Information Processing Standards
☆3 ITSEC Joint Interpretation Library
☆4 NIST: National Institute of Standards and Technology.
☆5 NAVLAP: National Voluntary Laboratory Accreditation Program
☆6 CSE: Communications Security Establishment
☆7 CMVP: Cryptographic Module Validation Program

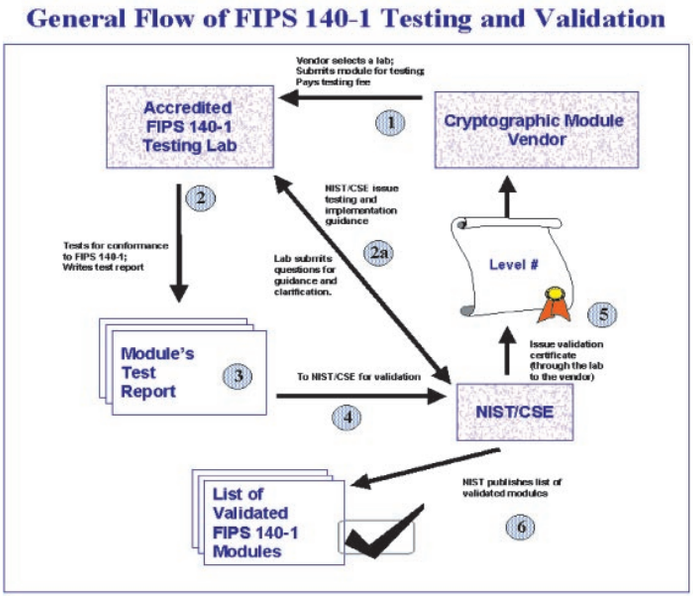

図 -6　暗号モジュール評価の枠組み [12)]

ジュール委員会を組織し，暗号モジュールに対する安全性要求基準やその評価手法を検討している．2004 年 3 月には，米国・カナダの CMVP をベースとした安全性要求基準や評価手法の第 0 版として，FIPS 140-2 とその試験基準である DTR[☆8] の日本語訳を公開した[8)]．

暗号モジュール評価プロジェクト (CMVP)

実際に暗号モジュールの評価制度を運用している CMVP の枠組みを**図 -6** に示す．暗号モジュールの製造者は，目標とするセキュリティレベルを定め，それに対する FIPS 140-2 の要求基準を満足することが求められる．できあがった暗号モジュールは，NAVLAP の認定した CMT[☆9]（評価機関）において，DTR に沿った評価が実施され，その評価結果は NIST と CSE に提出される．そして NIST/CSE は CMT からの報告書を点検し，問題がなければ対象となった暗号モジュールを認証する．ただし，この標準は暗号モジュールが FIPS 140-2 で定められた要求基準に適合していることを確認するものであって，無条件に安全であることは保証していない．この暗号モジュールの安全性評価については，現在 ISO/IEC JTC 1 SC 27 WG 3 において，米国とカナダからの共同提案として国際標準化が進行中である．CRYPTREC 暗号モジュール委員会で検討中の安全性要求基準も，この新たな国際標準に準拠して変更を加えるとともに，それに対応した評価手法の開発も行う予定である．

今後解決しなければならない具体的な課題としては，評価制度の確立と，現在の FIPS 140-2 においても未解決であるサイドチャネル攻撃に対する評価手法の研究が挙げられる．

参考文献
1) National Institute of Standards and Technology (NIST): Data Encryption Standard (DES), FIPS Publication 46-3, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf(Oct. 1999).
2) National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES), FIPS Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf(Nov. 2001).
3) Schneier, B.: 暗号技術大全，ソフトバンクパブリッシング，ISBN:4797319119(May 2003).
4) 暗号回路設計のトライ＆エラー，デザインウェーブマガジン 2004 年 6 月号，pp.91-113(2004).
5) 佐藤，高野，大庭: GF(p) 上の楕円曲線暗号回路のスケーラブルアーキテクチャ，信学論，Vol. J85-A (11), pp.1264-1272(Nov. 2002).
6) Report on the Development of the Advanced Encryption Standard (AES), NIST, http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf(Oct. 2000).
7) NESSIE Security Report, Version 2.0, NES/DOC/ENS/WP5/D20/2, NESSIE, 2003, https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/D20-v2.pdf
8) CRYPTREC Report 2003, IPA, 2003, http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/c02_2.pdf
9) FIPS PUB 140-2 : Security Requirements for Cryptographic Modules, NIST(2002), http://csrc.nist.gov/cryptval/
10) ITSEC Joint Interpretation Working Group (JIWG): Requirement to perform Integrated Circuit Evaluations(V1.1) (July 2003), http://www.cesg.gov.uk/
11) NIST: Cryptographic Module Validation Program CONFERENCE 2002, CMVP2603.pdf (Mar. 2002), http://csrc.nist.gov/cryptval/(Announcements)
12) NIST: Cryptographic Module Validation Program, http://csrc.nist.gov/cryptval/

(平成 16 年 9 月 30 日受付)

☆8 DTR: Derived Test Requirements for FIPS PUB 140-2
☆9 CMT: Cryptographic Module Testing laboratory