L-003

認証局運用規定おける暗号モジュールセキュリティ要件の記述に関する検討
A Note of the Security Requirements for Cryptographic Modules Description in Certification Practice Statement

小川　博久†
Hirohisa OGAWA

1. はじめに

認証局の証明書ポリシ及び認証局運用規定は，信頼できる電子認証基盤を形成するうえで，重要な規定である．証明書ポリシ及び認証局運用規定内で規定されている鍵ペア生成・管理に対する要求事項は，暗号モジュールセキュリティ要件を参照する構造で記述されている．証明書ポリシ及び認証局運用規定は，参照する暗号モジュールセキュリティ要件が改正されること，又は 2006 年に国際標準化されたことに伴い改訂を検討する必要がある．本検討では，改訂の記述及び改訂に関する考慮事項について検討する．本稿の構成は，2 章で証明書ポリシ及び認証局運用規定に求められる暗号モジュールセキュリティ要件の概要を示す．3 章で現状の記述内容の調査結果を報告し，4 章で現状の記述方法の問題点を示す．また，5 章では改訂記述を考察し，6 章でまとめる．

2. CPS における暗号モジュールセキュリティ要件

認証局の証明書ポリシ：Certificate Policy（以下，CP とする）及び認証局運用規定：Certification Practice Statement（以下，CPS とする）は，認証局の鍵ペア生成及び管理を規定している．CP/CPS での規定要求として参照される RFC2527[1]及び RFC 3647[2]では，鍵ペアを生成するために利用される暗号モジュールの要求事項が記述されている（暗号モジュールの境界，インプット/アウトプット，役割およびサービス，有限状態機械，物理的セキュリティ，ソフトウェアセキュリティ，OS セキュリティ，アルゴリズムの準拠性，電磁的互換性，自己テスト等）．また，同 RFC では，暗号モジュールセキュリティ要件の FIPS 140-1[3]に準じた暗号モジュールを利用する場合には，FIPS 140-1 での要求レベルを記述することを求めている．以上のように暗号モジュールに求められるセキュリティ要件を明確に定め，参照要件を満たした暗号モジュールで鍵ペアの生成及び保管を行うことで信頼できる電子認証基盤が形成される．そのうえで，認証局が定める暗号モジュールセキュリティ要件の記述は重要な要求事項であり，認証局の利用者にとって理解しやすい記述が求められる．

3. 現状の記述

CP/CPS における暗号モジュールセキュリティ要件の記述を検討するうえで，現状の記述内容の調査を行った．調査した結果を 表 1 に示す．調査方法としては，調査時点で公開されている CP/CPS 及び CP/CPS のガイダンスやサンプルについてランダムに抽出し調査を行った．調査の結果，以下のような記述がみられた．

表1 参照規格の記述分類

	参照要件	要件バージョン	要件レベル	補足事項
1	FIPS140	―	―	―
2	FIPS140	―	―	レベル
3	FIPS140	-1	レベル 1/2	相当/―
4	FIPS140	-1	レベル 3	相当/―
5	FIPS140	-2	レベル 1/2	相当/―
6	FIPS140	-2	レベル 3	相当/―
7	FIPS140	-1 / 2	レベル 1/2	相当/―
8	FIPS140	-1 / 2	レベル 3	相当/―

表内のレベル 1 及び 2 は主に証明書利用者等の鍵生成及び保管に求められるレベルであり，レベル 3 は主に認証局の鍵生成及び保管に求められるレベルである．一部の記述では，「暗号機能のコンポーネント化」や「耐タンパ性」を要求するのみで参照要件が記述されていない CP/CPS のガイドラインも存在した．一方，参照要件の記述がない CP/CPS のガイドラインを除いては，参照要件名，要件のバージョン，要件のレベル，補足事項という構成で記述されていることがわかった．なお，補足事項では，CP/CPS 及び CP/CPS のガイダンスやサンプルの策定時点で，日本国に暗号モジュール試験及び認証制度が存在しなかったために「相当」を追記していると報告されている[6].

4. 記述の問題点

RFC2527 及び RFC 3647 からもわかるように，暗号モジュールセキュリティ要件を規定するためには，参照要件名（及び，要件バージョン），参照要件でのレベルの記述（表内では要件レベル）が必要であるが，一部の CP/CPS では，参照要件のレベルの記述がないものが存在した．参照要件でのレベルの記述がない場合は，利用する暗号モジュールに対して耐タンパ性を求めるのか否か等のセキュリティ要件が明確でないため，信頼できる認証基盤が形成できるとは言い難い．

なお，既に他の調査報告書[7]でも指摘されている通り，補足事項として「相当」を付加する場合は，相当の意味する範囲やその範囲に関する評価方法を検討しておく必要があり，更にその範囲を CP/CPS に明記した方が利用者にとって理解しやすい．

5. 改訂の考察

以上の問題点を踏まえ，改訂記述について考察する．上記の問題点に関しては，参照要件の要求レベルを記述することで改善できる．また，現在では参照できる要件

†みずほ情報総研株式会社
Mizuho Information & Research Institute, Inc.

は FIPS140-1/2 だけではなく，他の暗号モジュールセキュリティ要件も存在する．以下に参照できる 3 つの暗号モジュールセキュリティ要件を示す．

1. FIPS140-1/2/3[3][4][5]
2. ISO/IEC 19790[8]
3. JIS X 19790[9]

FIPS140-1/2/3 は，北米が運営する暗号モジュールセキュリティ要件であり，現状の記述調査でも多く見られた参照要件である．また，FIPS140-2 を基に 2006 年 3 月に国際標準化された ISO/IEC 19790 があり，国家規格である JIS X 19790 が存在する．以上の 3 つの参照要件を用いて改訂する場合に考慮すべき事項を整理する．なお，FIPS140-2 を基に国際標準化されたからといって，直ちに ISO/IEC 19790 への参照に改訂する必要があるわけではない．また，FIPS140-1/2/3 においても改正以前の認証取得製品に対する認証が無効になるわけではなく，FIPS140-1/2 の認証は引き続き有効である．そのため FIPS140-1/2 認証取得した暗号モジュールの製造，販売が完了し，FIPS140-3 認証取得の暗号モジュールを利用する場合を考慮して CP/CPS の改訂を検討することが賢明である．

5.1 FIPS140-3 での改訂記述

FIPS140 は，5 年ごとに見直しが行われ都度，改正版が発行される．現在，運用されている FIPS140-2 の改正についても，当初は 2008 年度中に FIPS140-3 に移行する予定であった．（現在，FIPS140-3 はドラフトの段階であり，以降の内容もドラフト段階の内容に基づいている．）このドラフト段階の FIPS140-3 では，暗号モジュールのレベル設定が変更されている．FIPS140-2 ではレベルが 1 から 4 まで設定されていたが，FIPS140-3 ではレベルが 1 から 5 までに拡張されている．なお，拡張されたレベルについては，FIPS140-2 ではレベル 3 とレベル 4 の間で要求に大きな差があったために，その間に新規にレベルを設けた構造になっている．そのため，現状の認証局の HSM（Hardware Security Module）のセキュリティ要件で多く記述されている「FIPS140-1 及び 2 のレベル 3」という記述を「FIPS140-3 のレベル 3」と改訂しても大きな差は発生しない．

5.2 ISO/IEC 19790 での改訂記述

暗号モジュールセキュリティ要求として ISO/IEC 19790 が 2006 年 3 月に国際標準化されたために，同参照要件に基づいた記述に改訂することも考えられる．しかし，ISO/IEC19790 は，FIPS140-2 を基に作成されているが，FIPS140-3 は参照されていない．また，現時点では，暗号モジュール試験及び認証制度に関しては国際相互承認スキームが存在しない．そのため，国際相互承認スキームが整備されるまでは「相当」等の追記が必要となり，相当の範囲を FIPS140 及び JIS X 19790 のレベル 1 及び 3 とする等の記述が必要となる．

5.3 JIS X 19790 での改訂記述

日本国においても，ISO/IEC 19790 を基に，暗号モジュールセキュリティ要件である JIS X 19790 及び同評価基準である JIS X 5091[10]が発行され，2007 年 4 月から JCMVP（Japan Cryptographic Module Validation Program）[11]を正式運用している．前述した CPS の記述で補足事項に用いられる「相当」については，日本国に暗号モジュール試験及び認証制度が存在しなかったために，「相当」という補足事項を追記したと報告されている．しかし，国家規格が制定された現在では，JIS X 19790 の要件を満たした暗号モジュールを用いることで，「相当」という補足事項を追記する必要はない．また，電子政府推奨暗号を利用する場合であれば暗号モジュール試験及び認証制度が JIS X 19790 だけに限定される場合も存在する．以上のことから，日本国の電子政府として推進する認証基盤（GPKI，LGPKI 等）であれば，国家規格に準拠することが望ましく，JIS X 19790（MSR-01）での記述に改訂することも考えられる．一方，現時点で JIS X 19790 の認証を取得した HSM やハードウェアトークン等は存在しない．そのため，JIS X 19790 の認証を取得した暗号モジュールが製造，販売されるまでは，暫定的に ISO/IEC 19790 での改訂記述と同様に補足事項として「相当」を付加する必要がある．

6. まとめ

本検討では，CP/CPS の暗号モジュールセキュリティ要件記述を調査し，問題点を示した．また，記述の改訂に対して考慮すべき点を整理した．整理した結果，最もスムーズに改訂が可能な参照要件としては，北米で運営されている FIPS140-3 であることを示した．一方，日本国の電子政府として推進する認証基盤であれば，JIS X 19790 での記述改訂が有効である点を示した．また，国際標準である ISO/IEC 19790 は暗号モジュール試験及び認証制度に関する国際相互承認スキームが存在しないため補足事項として「相当」の追記が必要であることを示した．

今後は，参照要件である FIPS140-3 の正式版発行及び，ISO/IEC 19790，JIS X 19790 の改正後に同様の調査を行い，記述改訂を検討する予定である．

参考文献

[1]RFC 2527 , Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework ,S. Chokhani,W. Ford, March 1999.
[2]RFC 3647 , Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani,W . Ford,R. Sabett, C. Merrill, S. Wu, November 2003.
[3]FIPS PUB 140-1, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology ,October 2001.
[4]FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology ,January ,1994.
[5]FIPS PUB 140-3 (DRAFT), Security Requirements for Cryptographic Modules, National Institute of Standards and Technology , 07,2007.
[6]電子認証ポリシーガイドライン（案）基準規範編 評価報告書, 財団法人日本情報処理開発協会, 平成 18 年 3 月.
[7]本人認証技術の現状に関する調査報告書, 独立行政法人情報処理推進機構, 2003 年 3 月.
[8]ISO/IEC 19790:2006, Information technology－Security techniques－Security requirements for cryptographic modules, 2006 年 3 月.
[9]JIS X 19790 セキュリティ技術－暗号モジュールのセキュリティ要求事項, 2007 年 3 月.
[10] JIS X 5091 セキュリティ技術－暗号モジュールのセキュリティ試験要件, 2007 年 3 月.
[11] JCMVP 暗号モジュールセキュリティ要件 (MSR-01), 独立行政法人情報処理推進機構, 平成 19 年 10 月.