暗号モジュール試験及び認証制度に関する Q&A

平成 30 年 7 月 2 日

QAJ-01

Questions and Answers for JCMVP beginners

IPA

独立行政法人情報処理推進機

新しい Q&A

追加日	内　容
2009/4/3	新規発行

改正された Q&A

改正日	内　容
2018/7/2	1.「概要」「JIS X19790」の解説を更新。 3.2 「適用性」「JCMVP 認証は政府機関の情報セキュリティ対策にどのように活用されますか」の解説を更新。 4.2 「暗号アルゴリズムの規格」「承認されたハッシュアルゴリズム」から RIPEMD-160 を削除、SHA-512/224 及び SHA-512/256 を追加。 4.2「暗号アルゴリズムの規格」「承認された守秘用公開鍵暗号アルゴリズム」から RSAES-PKCS1-v1_5 を削除。 1,及び 3.3 の認証機関の組織の情報を更新。 2.2.1,及び 3.5 の問い合わせ先を更新。

目次

JCMVP の Q&A

制定　平成 21 年 4 月 3 日
最終改正　平成 30 年 7 月 2 日

1. 概要

この文書は、暗号モジュール試験及び認証制度(JCMVP[1])に関する質問及び、暗号モジュール試験要件に関係する質問への回答（以下、「Q&A」という。）を提供することを意図しています。この文書が提示する Q&A は、試験機関、ベンダ及び他の関心がある団体から寄せられた質問に対して、暗号モジュール認証機関（以下、「認証機関」という。）が行った回答などに基づいています。

・JCMVP とは何ですか。

暗号モジュール試験及び認証制度（JCMVP： Japan Cryptographic Module Validation Program）は、暗号モジュールに暗号アルゴリズムが適切に実装され、その鍵やパスワードといった重要情報が攻撃者から保護されるとともに、許可された者がいつでもその機能を確実に利用できることを、暗号モジュールのユーザが客観的に把握できるように設けられた第三者適合性認証制度です。

CRYPTREC[2]が作成した電子政府推奨暗号リストに記載された暗号アルゴリズムを中心に本制度が承認した暗号アルゴリズム（以下、「承認されたセキュリティ機能」という。）を実装している暗号モジュール製品を対象に、暗号モジュールセキュリティ要件を規定した ISO/IEC 19790 (又は JIS X19790) に基づく試験・認証を実施します。

本制度は、IPA（独立行政法人情報処理推進機構）セキュリティセンター セキュリティ技術評価部を認証機関として運用されています。

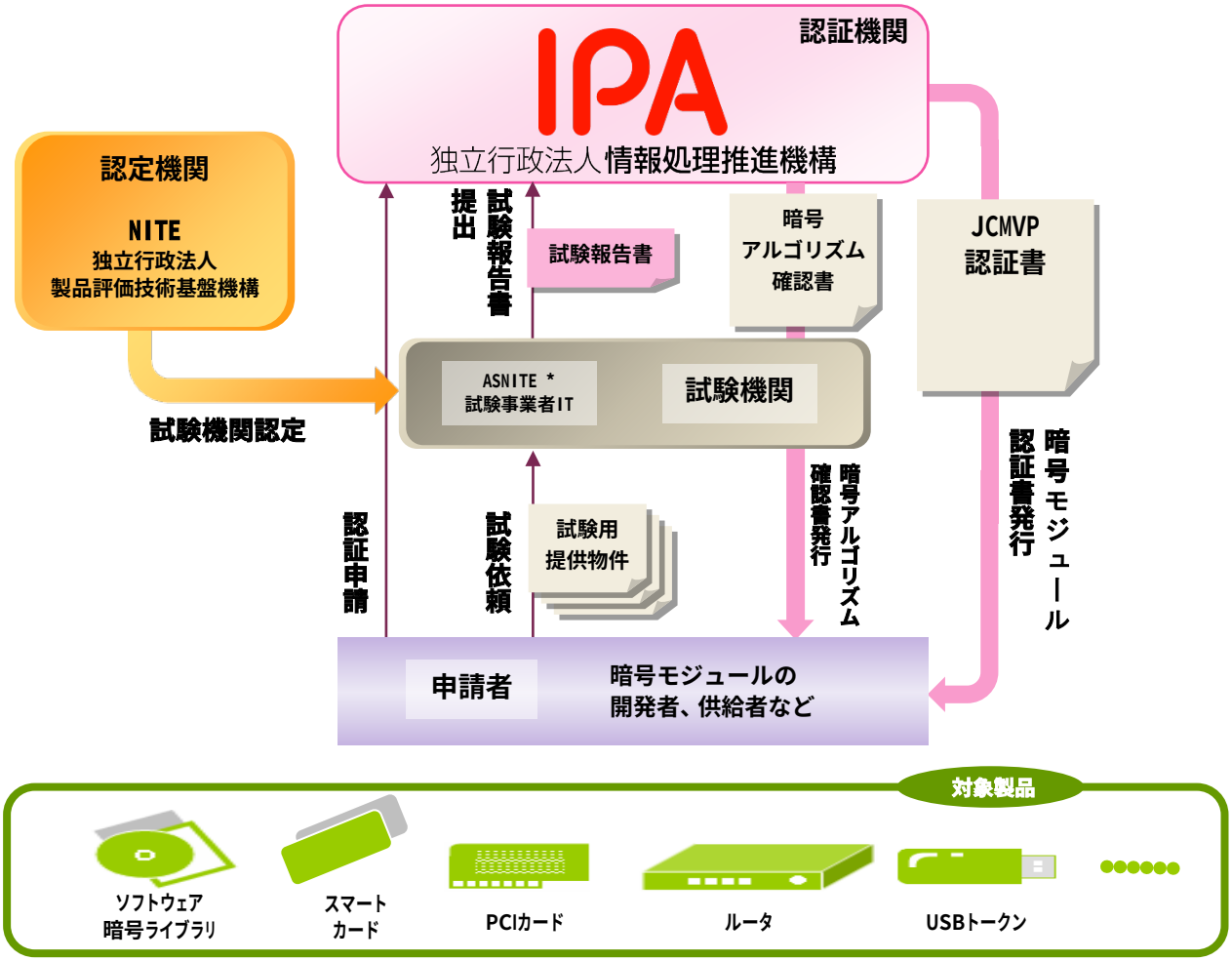
JCMVP に適用可能な規格、注記及び告示、試験機関の窓口、認証機関の窓口、暗号モジュールの認証製品リストについては、JCMVP のホームページから入手できます。

JCMVP のホームページ　https://www.ipa.go.jp/security/jcmvp/

[1] Japan Cryptographic Module Validation Program

[2] CRYPTREC :Cryptography Research and Evaluation Committees
電子政府推奨暗号の安全性を認証・監視し、暗号技術の適切な実装法・運用法を調査・検討する。経済産業省及び総務省が共同で開催する暗号技術検討会と、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構が共同で開催する暗号技術評価委員会及び暗号技術活用委員会で構成。
CRYPTREC URL:　http://www.cryptrec.go.jp/

図1に、JCMVPの仕組みを示します。



＊　ASNITE 試験事業者 IT:独立行政法人製品評価技術基盤機構認定センターが JIS Q 17025 を基準として、コモンクライテリア評価、暗号モジュール試験又はシステム LSI 侵入テストを行う試験事業者を認定する認定制度。

図1：JCMVPの仕組み

暗号モジュールは、承認されたセキュリティ機能を実装しなければなりません。JCMVP で承認されたセキュリティ機能のリストについては、以下を参照して下さい。

https://www.ipa.go.jp/security/jcmvp/algorithm.html

• ISO/IEC 19790 とは何ですか。

米国及びカナダが運営する暗号モジュール試験及び認証制度（CMVP: Cryptographic Module Validation Program）で認証基準として採用されている FIPS 140-2 を基に、暗号モジュールのセキュリティを確保するための要求事項を定めた国際規格として ISO/IEC 19790:2006 が作成されました。なお、JIS X19790:2007 は ISO/IEC 19790:2006 と一致する国内規格です。
なお、ここで FIPS とは、米国連邦政府情報処理規格(Federal Information Processing Standards)のことです。

その後、米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が策定を検討中の FIPS 140-3 のドラフトの内容をベースに、ISO/IEC JTC1/SC27 での議論を経て ISO/IEC 19790:2012 が発行されています。JIS X19790:2015 は、ISO/IEC 19790:2012 と一致する国内規格です。

ISO/IEC 19790 については、その後も Corrected version が発行される等変更がありますので、規格の動向については関連のウェブページを参照してください。

• JCMVP 認証を取得するメリットは何でしょうか。

暗号モジュール試験及び認証制度（JCMVP）認証取得のメリットには、次のことが挙げられます。

（１）承認されたセキュリティ機能が適正に実装されていることが、第３者によって確認されていることを示すことができます。
承認されたセキュリティ機能を使用しても、正しく実装されていなければ意味がありません。また、適正に実装されているか否かをベンダがユーザに証明すること及びユーザが自身で確認することは容易ではありません。
承認されたセキュリティ機能を適正に実装することによって、以下の機能が確保されます。

① 不正な操作又は利用から暗号モジュールを保護する。
② 暗号モジュールの内部情報の不正な開示を防止する。
③ 暗号モジュール及び暗号アルゴリズムに対する不正な改変を防止する。
④ 暗号モジュールにエラーが発生した場合に、これを検出し、このエラーによる重要情報の漏洩を防止する。

（２）JCMVP 認証を取得することで政府機関向けセキュリティシステムに、承認されたセキュリティ機能が適正に実装され、暗号鍵等の重要情報のセキュリティが確保された暗号モジュールであることを主張できます。

2. JCMVP の導入

2.1 ユーザのための情報

・暗号モジュール認証製品リストはどこで入手できますか。

認証済み暗号モジュールの認証製品リストは、JCMVP の Web サイト https://www.ipa.go.jp/security/jcmvp/val.html で入手できます。

・全ての IT セキュリティ機能が試験機関でテストされるのでしょうか。

いいえ。JCMVP では暗号モジュールが ISO/IEC 19790(又は JIS X19790)の暗号モジュールセキュリティ要件に適合しているかどうかテストします。

・暗号モジュールの認証書に有効期限はありますか。

いいえ。暗号モジュール認証は、暗号モジュールが変更されない限り、少なくとも１つの承認されたセキュリティ機能を実装している場合に有効です。

・暗号モジュールの認証を確認する方法はありますか。

暗号モジュールの認証書を確認するには、https://www.ipa.go.jp/security/jcmvp/val.html を参照してください。

・次に示す例で暗号モジュールが認証されていると言えますか。

ベンダが、JCMVP 認証を次のように主張していますが、それらは受け入れられますか？

· モジュールは、ISO/IEC 19790（又は JIS X19790）に準拠するように設計されました。	<いいえ>
· モジュールは試験のため提供されました。	<いいえ>
· ISO/IEC 19790（又は JIS X19790）に準拠するため、モジュールは第三者によりレビューされ、テストされました。	<いいえ>
· モジュールは ISO/IEC 19790（又は JIS X19790）の要件全てを満たします。	<いいえ>
· モジュールは承認されたセキュリティ機能を実装しています。	<いいえ>
· モジュールは ISO/IEC 19790（又は JIS X19790）の詳細なガイドラインに従っています。	<いいえ>
· モジュールは認証され、認証番号 Jxxxx を受けました。 認証番号を参照できない場合、暗号モジュールは要件を満たしません。また、ISO/IEC 19790（又は JIS X19790）規格にも準拠しません。モジュールは、バージョンも含めて認証書の記載内容と同じである必要があります。その他の主張は意味がありません。	<はい>

・認証番号の先頭文字に「J」と「F」があるのは、なぜですか。

「J」は暗号モジュールが ISO/IEC 19790（又は JIS X19790）の暗号モジュールセキュリティ要件に適合し、「F」は JCMVP 暗号モジュールセキュリティ要件（FIPS 140-2 ベース）に適合することを表しています。

2.2 ベンダのための情報

2.2.1 要件情報を探す場合

・必ず実装しなければならない機能についての具体的な要件はどうしたら入手できますか。

暗号モジュールセキュリティ要件、暗号モジュールセキュリティ試験要件はそれぞれ ISO/IEC 19790 (又は JIS X19790)、ISO/IEC 24759 (又は JIS X24759) に記載されていますので、それらの規格を参照して下さい。暗号モジュールのセキュリティ試験要件である ISO/IEC 24759 (又は JIS X 24759) には、暗号モジュールの個別要件（AS)、AS に関連したベンダ情報要件(VE)、試験手順要件(TE)が記述されています。AS は ISO/IEC 19790 から抽出されたセキュリティ要件で、VE がベンダに対する要求事項です。TE は暗号モジュールの試験者に対する要求事項です。これらの規格は、一般財団法人日本規格協会から購入できます。購入方法の詳細は一般財団法人日本規格協会のホームページ（http://www.jsa.or.jp/）を参照してください。

・セキュリティ要件又はセキュリティ試験要件の解釈に迷う場合、どうすればよいですか。

暗号モジュール試験について試験機関と契約を交わしているベンダは、セキュリティ要件・セキュリティ試験要件についての質問及びそのセキュリティ要件・セキュリティ試験要件が、どのように実装の試験に影響を及ぼすか、試験機関と相談して下さい。

試験機関との契約を交わしていないベンダが、暗号モジュール試験の試験要件などに具体的な疑問が生じた場合には、次の認証機関の連絡先まで連絡して下さい。

認証機関連絡先：独立行政法人情報処理推進機構
セキュリティセンター セキュリティ技術評価部 JCMVP 担当
E-mail： jcmvp-info@ipa.go.jp

・他社の認証済み暗号モジュールを組み込むことができますか。

はい。JCMVP の認証書を既に取得した暗号モジュールは、別の製品に組み込むことができます。新製品が元の認証済み暗号モジュールを変更しない限り、新製品は認証済み暗号モジュールの認証書を参照します。組み込まれた認証済み暗号モジュールを使用する製品は、製品全体が認証されていると主張はできません。組み込まれた認証済み暗号モジュールを使用していることのみを主張できます。

・認証された暗号モジュールに、認証されていない追加アプリケーションを組み込んだ場合、認証状態は維持されますか。

認証された暗号モジュールに、認証されていないアプリケーションを後で組み込んだり、実行した

りした場合、当初行われた認証内容は無効になります。

・JIS X19790 はハードウェア暗号モジュールにのみ適用されますか。

いいえ。JIS X19790 は、ハードウェア、ソフトウェア、ファームウェア又はそれらの組合せで実装されている全ての暗号モジュールに適用されます。

・暗号モジュールに関する機密情報は保護されますか。

はい。暗号モジュールの機密情報は試験機関及び認証機関内で全て保護されます。通常、試験機関は製品のベンダと秘密保持契約（Non-Disclosure Agreement：NDA）を締結します。

また、認証機関は、試験機関と秘密保持契約を締結していますので、試験機関より提出された試験報告書に掲載されている情報を開示しないで保護します。 認証機関はベンダの要望により、ベンダと秘密保持契約を締結することもあります。

2.2.2 試験機関に関する情報

・暗号モジュール試験機関はどこか教えてください。

JCMVP で承認している試験機関のリストは JCMVP の Web ページ（https://www.ipa.go.jp/security/jcmvp/lablist.html）を参照して下さい。

・暗号モジュール試験の期間と費用を教えてください。

暗号モジュール試験の料金は試験機関から請求されます。試験期間は、暗号モジュールの複雑さ、全体的なセキュリティ･レベルと各セキュリティレベル及びベンダの提出書類の完成度に応じて変わってきます。試験期間は以下の要因により左右されます。

a) 暗号モジュールのタイプ – ソフトウェア、ファームウェア、ハードウェア、単機能か多機能か、など
b) 暗号モジュールの全体的なセキュリティレベル - 1、2、3 又は 4
c) 提出書類の正確さと完成度
d) 適合性試験中に試験機関により特定された不具合の数

再認証の場合や、前に認証された暗号モジュールのバージョンアップ版の試験の場合には、通常、期間と費用は少なくなります。認証機関は、ベンダと試験機関間の契約交渉に関与しません。見積価格又は概算は試験機関から入手できます。

尚、試験費用の他に認証申請手数料が別途必要です。認証申請料金は、本制度の「暗号モジュール認証申請手続等 に関する規程」(https://www.ipa.go.jp/security/jcmvp/documents/cbm02.pdf)の申請手数料料金表に記載されています。

・試験機関が競合するベンダの暗号モジュールを試験した場合、機密情報が漏れることはありませんか。

試験機関は、企業の機密情報を保護するのに細心の注意を払います。一般的に、試験機関はベンダごとに秘密保持契約(NDA)を締結し、認証機関以外の外部組織に暗号モジュールに関する情報を決して開示しません。

・社内の試験機関で自社の暗号モジュールを試験できますか。

いいえ、できません。JCMVP では承認された第 3 者試験所のみが試験を実施します。

・暗号モジュール試験に必要な文書を試験機関が作成することはできますか。

証拠文書をベンダが作成しない場合、試験機関とコンサルティング会社がこの作業を代わりに行うことができます。ただし、試験機関は文書の編集のみ可能で、オリジナル文書を作成できないという制限があります。

3. JCMVP の一般的な情報

3.1 規格概要

・JCMVP では、暗号モジュール認証と暗号アルゴリズム確認に適用する規格は何ですか。

JCMVP は、ISO/IEC 19790（又は JIS X19790）に基づいて、暗号モジュール認証書を発行します。

また、「JCMVP 暗号アルゴリズム実装試験要件（ATR-01)」に基づいて、暗号アルゴリズム確認書を発行します。

3.2 適用性

・JCMVP 認証は政府機関の情報セキュリティ対策にどのように活用されますか。

情報セキュリティ政策会議による「府省庁対策基準策定のためのガイドライン（平成 28 年度版)」に基づき、政府機関向けセキュリティシステムの調達に際して、供給者は、本制度に基づく認証を取得することにより、選択された暗号アルゴリズムが適切に実装され、鍵等の重要情報のセキュリティが確保された暗号モジュールであることをアピールできます。

府省庁対策基準策定のためのガイドライン（平成 28 年度版抜粋）

平成 28 年 8 月 31 日　内閣官房　内閣サイバーセキュリティセンター

【基本対策事項】	選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 （6．1．5．（1）(a)関連）

・JCMVP は北米 CMVP と相互承認を行っていますか。

いいえ、相互承認を行っていません。ただし、JCMVP と CMVP 両方の試験機関を兼ねている試験機関があり、その試験機関で試験を行うと１回の試験で、JCMVP と CMVP 両方の認証を取得可能です。

3.3 役割

・JCMVP にはどのような関係者がいますか。

JCMVP 関係者は次のとおりです。

a) ユーザ
b) 暗号モジュールベンダ
c) （承認された）試験機関
d) 認証機関

図 3.3 のフローチャートは、関係者と JCMVP 内での役割を示します。

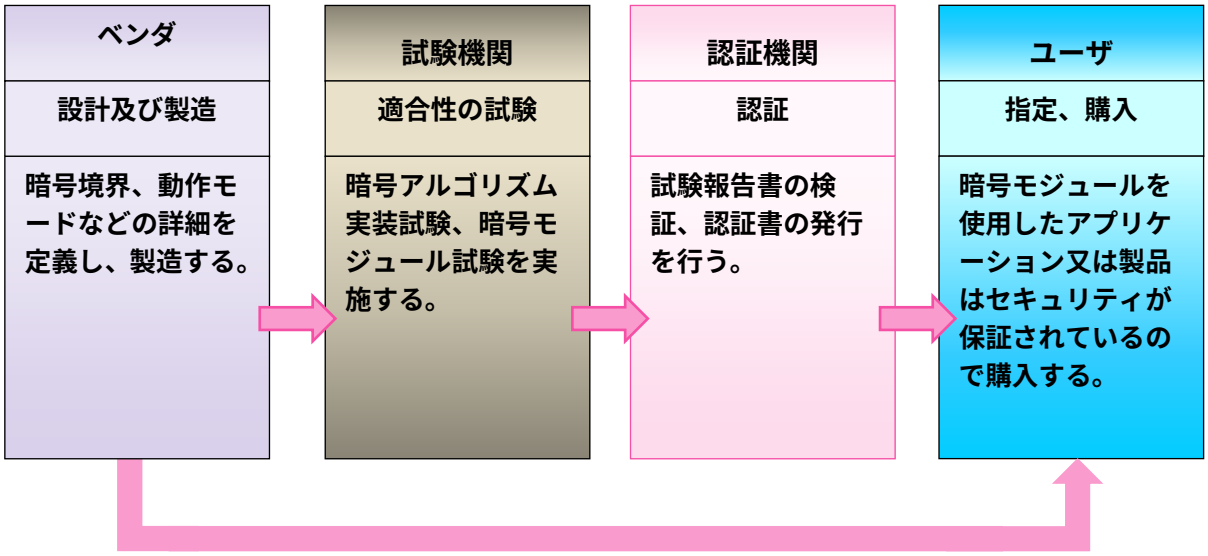


図3.3：JCMVPの関係者と役割

・認証機関はどこですか、また、その役割は何ですか。

認証機関は次のとおりです。

· IPA（独立行政法人情報処理推進機構）セキュリティセンター セキュリティ技術評価部

JCMVP は IPA により運用されています。認証機関の役割は、暗号モジュールごとに試験結果を検証することです。試験結果は、試験機関が作成した試験報告書です。暗号モジュールが暗号モジュールセキュリティ要件に準拠していると判断した場合、暗号モジュール認証書を発行して、暗号モジュール認証製品リストを更新します。認証レビュー中、認証機関は試験機関に所見報告書を提出します。所見報告書は技術的な内容に焦点を当て、特に、暗号モジュールが規格の要件を満たし、情報が正確で完全であるか確認します。試験機関は所見報告書に通常、1 つ以上の文書（所見報告書の回答、試験報告書、セキュリティポリシなど）を再提出することになります。認証レビュー中、試験機関はベンダと協力して、認証機関が提起した問題を解決します。

認証機関は、暗号アルゴリズム実装の試験結果も検証します。暗号アルゴリズム実装試験結果が正

しいと判断した場合、暗号アルゴリズム確認書を発行します。

・試験機関の役割は何ですか。

承認された試験機関の役割とは、ISO/IEC 19790 (又は JIS X19790) の暗号モジュールセキュリティ要件の該当要件に則して、暗号モジュールを試験し、結果を記録することです。暗号モジュールが暗号モジュールセキュリティ試験要件に記述された該当する個別要件（AS）を全て満足する場合、試験機関は暗号モジュール試験報告書を認証機関に提出します。暗号モジュールが 1 つ以上の個別要件を満たさない場合、試験機関は試験報告書等の書類を認証機関に再提出する前に、ベンダと協力して全ての相違を解決します。

暗号アルゴリズム実装試験の場合、一般的に試験機関はベンダが提供した情報をもとに暗号アルゴリズム実装試験ツールを使って、テストベクター（質問ファイル）を生成します。試験機関とベンダは、質問ファイルを使用して、暗号アルゴリズム実装試験を行います。ベンダは質問ファイルに対する回答を回答ファイルとして試験機関に提出します。試験機関はその回答ファイルの内容を暗号アルゴリズム実装試験ツールで検証します。検証結果に問題がなければ、試験機関は暗号アルゴリズム実装試験報告書を認証機関に提出します。

・ベンダの役割は何ですか。

ベンダの役割は、当該規格のセキュリティ要件に準拠するよう、暗号モジュールを設計し、製造することです。暗号モジュール試験の準備が整った場合、ベンダは試験のため、モジュール及びそれに関連した文書を試験機関に提出します。

暗号アルゴリズム確認の場合、ベンダは当該規格に準拠するように暗号アルゴリズムを実装します。暗号アルゴリズム実装の試験準備が整ったら、ベンダは、試験機関が質問ファイルを生成するのに必要な情報を提供し、試験機関が生成した質問ファイルに対する回答ファイルを作成し、試験機関に提出します。

・ユーザの役割は何ですか。

ユーザは、購入を考えている暗号モジュールが認証されているかを確認します。それは暗号モジュール認証製品リストで確認できます。ユーザは、JCMVP 認証済み暗号モジュールの要件を含めてアプリケーションまたは製品の仕様を作成します。また、ユーザが必要とするセキュリティ機能を暗号モジュールが提供しているかどうか、暗号モジュールのセキュリティポリシを確認する必要があります。

3.4 暗号アルゴリズム確認及び暗号モジュール認証の手順

・暗号アルゴリズム確認の手順はどうなっていますか。

暗号アルゴリズム確認は、次の図 3.4.1 に示すように、いくつかのステップを実行する必要があります。

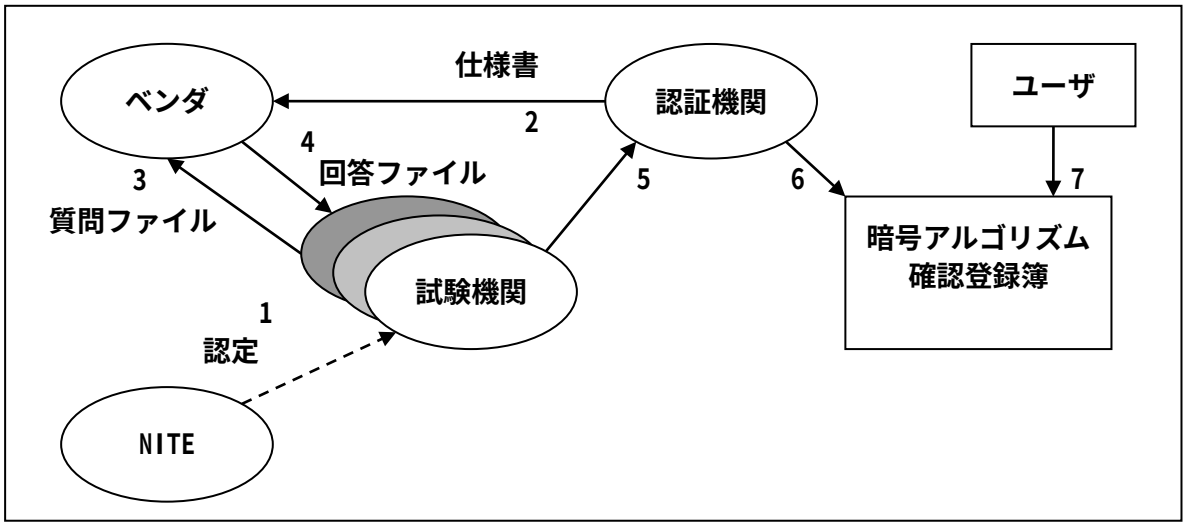


図3.4.1：暗号アルゴリズム確認の手順

以下に、暗号アルゴリズム実装試験のステップを説明します。

1. 暗号アルゴリズム実装試験を受けるには、ベンダは NITE から認定された試験機関と契約します。
2. 認証機関が作成した暗号アルゴリズム実装試験仕様書、JCATT ファイルフォーマットが公開されています。（https://www.ipa.go.jp/security/jcmvp/open_documents.html）ベンダは、それらの文書を参考に試験機関に暗号アルゴリズム実装試験のパラメータを提出します。
3. 試験機関はベンダの要望に応じて、各試験対象の暗号アルゴリズムに対して試験条件の異なる複数の質問ファイルを暗号アルゴリズム実装試験ツールで生成し、ベンダに送付します。
4. ベンダは質問ファイルのデータと暗号モジュールを使用して、回答ファイルを作成します。そして、回答ファイルを試験機関に送付します。尚、回答ファイル作成の際に、試験機関が立会う場合があります。
5. 試験機関は、ベンダが提出した回答ファイルを暗号アルゴリズム実装試験ツールで検証します。検証結果が正しくない場合、試験機関はその情報をベンダに提供します。ベンダは暗号アルゴリズム（又は試験インタフェース）を修正し、回答ファイルを試験機関に再提出します。回答ファイルが正しいと試験機関が確認した場合、試験機関は暗号アルゴリズム実装試験報告書を認証機関に提出します。
6. 認証機関は暗号アルゴリズム実装試報告書を確認し、暗号アルゴリズム確認書を発行します。また、認証機関は、暗号アルゴリズム確認登録簿にその情報を掲載します。
（https://www.ipa.go.jp/security/jcmvp/avallists.html）

7．ユーザ（政府機関、民間企業）は、暗号アルゴリズム確認登録簿を閲覧することによって、暗号アルゴリズムの実装が正しいことを確認できます。

・暗号モジュール認証の手順はどうなっていますか。

暗号モジュール認証は、次の図 3.4.2 に示すように、いくつかのステップを実行する必要があります。

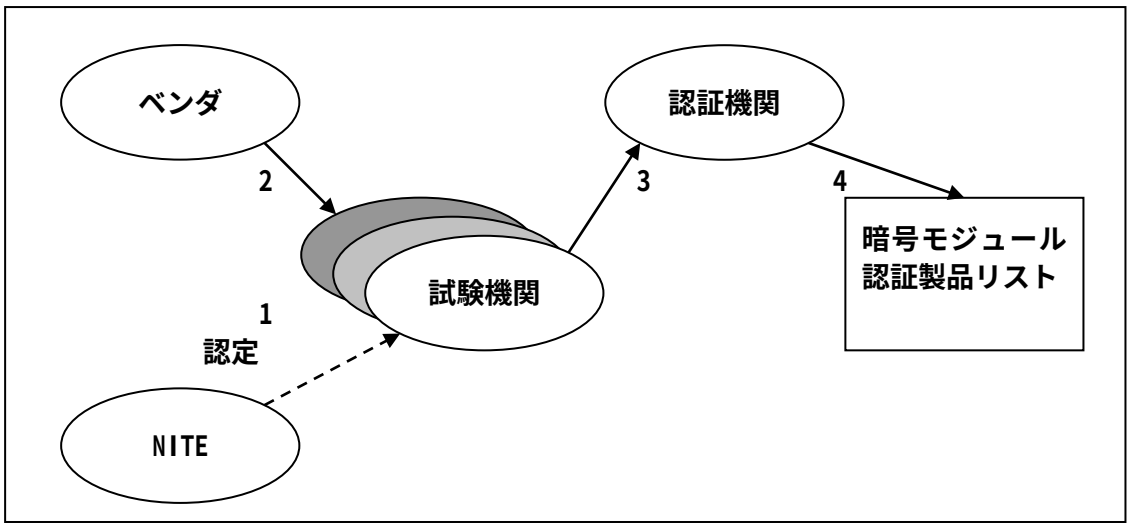


図3.4.2：暗号モジュール認証の手順

以下に、暗号モジュール認証を受けるためにベンダが実行するステップを説明します。

1．暗号モジュール試験を受けるには、ベンダは NITE から認定された試験機関と契約します。

2．ベンダは暗号モジュールと証拠書類一式を試験機関に提出します。試験機関はまず、ベンダが提供した証拠書類一式を精査し、暗号モジュールを理解します。疑問がある場合、試験機関がベンダに質問することがあります。（必要に応じて、試験機関の担当者は、ベンダの施設内で暗号モジュールを試験することがあります）。

3．試験機関は、暗号モジュールセキュリティ要件への適合性を確認するため、関連する暗号モジュールのセキュリティ試験要件を使用して、暗号モジュール試験を実施します。試験機関は暗号モジュール試験を完了すると、その結果を暗号モジュール試験報告書として認証機関に提出します。

4．認証機関は、試験報告書を審査します。その際、認証機関は疑問点があれば、それを解消するための質問を試験機関へ提出します。（全ての問題を解決するのに何回も繰り返す必要がある場合もあります。）認証機関は試験報告書の結果により、暗号モジュールがセキュリティ要件に適合していると判断した場合、暗号モジュール認証書を発行し、暗号モジュール認証製品リスト（https://www.ipa.go.jp/security/jcmvp/val.html）を更新します。

ユーザ（政府機関、民間企業）は、暗号モジュール認証製品リストを閲覧することによって、暗号モジュールが認証済みであるか確認します。

・一般的な暗号モジュール試験期間はどのくらいですか。

試験期間は、試験する暗号モジュールによって異なります。その要因には、暗号モジュールの複雑さ、全体のセキュリティレベル、個別のセキュリティレベル（全体のセキュリティレベルよりも高い場合）、現在の試験機関の作業量、及びベンダが提出した暗号モジュールに関する文書の内容と完成度などがあります。

・一般的な認証期間はどれくらいですか。

一般的に 2～4 週間の期間が必要ですが、暗号モジュールの複雑さや試験報告書の完成度によっても異なります。

・暗号モジュールがセキュリティ要件（ISO/IEC 19790）に適合していないという問題を第三者が通知した場合、JCMVP では何を行いますか。

JCMVP は、提供された情報を精査します。その情報の中に、認証済みモジュールの適合性を疑問視する特定の技術的な指摘が含まれていた場合、JCMVP は、モジュールの適合性試験を担当した暗号モジュール試験機関にその情報の本質的な部分を通知します。試験機関は、その情報を確認します。提供された情報が規格適合性を疑問視させる場合、試験機関と認証機関はその問題を再調査して確認します。不適合であると確認した場合、JCMVP は、試験機関に再試験を指示します。再試験の結果によっては、認証書が取り消される場合があります。

3.5 連絡先

・JCMVP の詳細についての問い合わせ先

認証機関の連絡先については、以下を参照してください。

認証機関連絡先：独立行政法人情報処理推進機構
セキュリティセンター セキュリティ技術評価部 JCMVP 担当
E-mail： jcmvp-info@ipa.go.jp

・暗号モジュール試験の詳細についての問い合わせ先

各試験機関の連絡先リストについては、https://www.ipa.go.jp/security/jcmvp/lablist.html を参照してください。

4. 規格

4.1 暗号モジュールの規格

・ISO/IEC 19790, JIS X19790 とはどんな規格ですか。

ISO/IEC 19790 及び JIS X19790 は、コンピュータの中の取扱いに慎重さを要する情報を保護するセキュリティシステム及び通信システムの中で使用される暗号モジュールに対するセキュリティ要求事項を規定します。暗号モジュールには、その幅広い潜在用途やその動作環境に応じて、要求されるセキュリティの強度は異なります。この規格では、セキュリティの要求程度を、レベル 1、レベル 2、レベル 3、及びレベル 4 の 4 段階で定義しています。セキュリティ要件は、暗号モジュールのセキュアな設計と実装に関連した分野を扱います。これらの分野には、暗号モジュールの仕様、暗号モジュールインタフェース、役割、サービス、オペレータ認証、ソフトウェア・ファームウェアセキュリティ、動作環境、物理セキュリティ、非侵襲セキュリティ、センシティブセキュリティパラメタ管理、自己テスト、ライフサイクル保証、及びその他の攻撃への対処が含まれます。

・この規格のセキュリティ目標は何ですか。

ISO/IEC 19790 及び JIS X19790 のセキュリティ要件は、暗号モジュールのセキュアな設計と実装に関連します。要件は、暗号モジュールに対する以下の大きなセキュリティ目標から導かれています。

- 取扱いに慎重さを要する情報を保護するために、承認されたセキュリティ機能を採用し、正しく実装する。
- 許可されていない操作又は許可されていない利用から暗号モジュールを保護する。
- その暗号モジュールの内容（CSP を含む。）の許可されていない開示を防ぐ。
- その暗号モジュール及び暗号アルゴリズムに対する、許可されていない変更及び検出不能な変更（CSP 及び／又は PSP に対する、許可されていない変更、置換、挿入、及び消去を含む。）を防ぐ。
- その暗号モジュールの動作状態を表示する。
- 承認された動作モードで動作するときに、その暗号モジュールが適切に実行することを保証する。
- モジュールの動作においてエラーを検出し、かつ、これらのエラーによる CSP 及び／又は PSP の危たい化を防ぐ。

4.2 暗号アルゴリズムの規格

・暗号アルゴリズム確認は暗号モジュール認証と、どのように関係していますか。

暗号モジュールが JCMVP 認証を取得するためには、承認された動作モードで使用する承認されたセキュリティ機能を 1 つ以上、実装する必要があります。それらの承認されたセキュリティ機能が、正しく実装されていることを確認するために、暗号アルゴリズム実装試験を受けて、暗号アルゴリズム確認書を取得する必要があります。暗号アルゴリズム確認書がない場合、暗号モジュール認証書は発行されません。

単に承認されたセキュリティ機能を実装し、暗号アルゴリズム確認書を取得しただけでは、製品又はモジュールが暗号モジュールのセキュリティ要件を満たしているとは言えません。

・承認されたセキュリティ機能の分類には何がありますか。

現在、承認されたセキュリティ機能の分類には、公開鍵、共通鍵、ハッシュ、メッセージ認証、乱数生成器、及び鍵確立手法があります。

・承認された共通鍵暗号アルゴリズムには何がありますか。

共通鍵（又は対称）暗号アルゴリズムは、暗号化と復号の両方に単一の秘密鍵を使用します。暗号アルゴリズム実装試験は現在、AES などの共通鍵暗号アルゴリズムについて実施できます。承認された共通鍵暗号アルゴリズムの一覧は、https://www.ipa.go.jp/security/jcmvp/algorithm.html を参照してください。

・承認されたハッシュアルゴリズムには何がありますか。

承認されたハッシュアルゴリズムは、SHA-1、SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256、SHA3-256、SHA3-384、及び SHA3-512 です。

・承認された署名用公開鍵暗号アルゴリズムには何がありますか。

公開鍵（又は非対称）暗号アルゴリズム は、公開鍵とプライベート鍵の鍵ペアを使用します。2 つの鍵には、公開鍵からのプライベート鍵を取得することは計算上、困難であるという特性があります。現在の承認された公開鍵暗号アルゴリズム（署名）は、DSA、ECDSA、RSASSA-PKCS1-v1_5、RSASSA-PSS、です。一般的に、公開鍵暗号アルゴリズム（署名）は以下に使用されます。

- データの不正又は偶発的な変更に対処するデータ整合性。これには、データの挿入、削除、変更が含まれます。データ整合性を確実にするため、システムは不正なデータ変更を検出する必要があります。目標は、データが変更されていないことをデータの受信者が確認することです。
- 送信、メッセージ、又は発信元の有効性を確立する検証。（認証サーバは、特定の情報カテゴリを受信する個人の権限も確認します。上記のサービスは暗号化に固有のものではありません。）従って、このサービスは個人と情報の両方に適用されます。目標は、データの受信者が発信元を特定することです。
- 個人が以前発信した文書を否定できないようにする否認防止。目標は、データの受信者が送信者の ID を確認することです。

承認されたセキュリティ機能については、https://www.ipa.go.jp/security/jcmvp/algorithm.html を参照してください。

・承認された守秘用公開鍵暗号アルゴリズムには何がありますか。

公開鍵（又は非対称）暗号アルゴリズム は、公開鍵とプライベート鍵の鍵ペアを使用します。2 つの鍵には、公開鍵からのプライベート鍵を取得することは計算上、困難であるという特性があります。現在の承認された公開鍵暗号アルゴリズム（守秘）は、RSA-OAEP です。

5. 暗号モジュールの認証

5.1 暗号モジュールのセキュリティレベル

・セキュリティレベルの種類 には何がありますか。

セキュリティレベルの種類は、1、2、3 及び 4 があります。

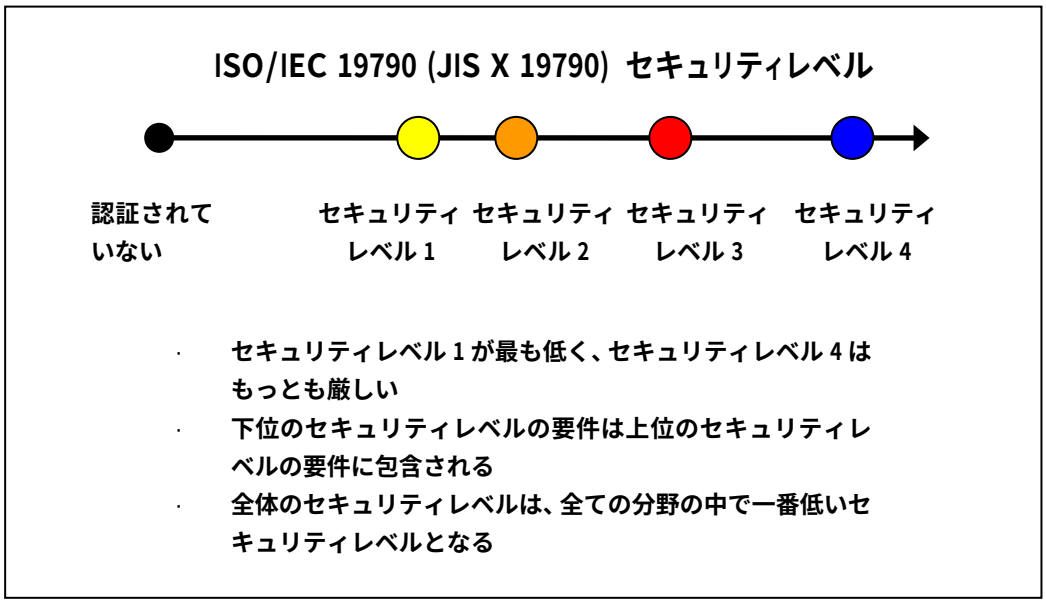


図5：ISO/IEC 19790 及び JIS X19790のセキュリティレベル

4 つのセキュリティレベルは、10 の要件の分野にそれぞれ指定されます。各セキュリティレベルは、下のセキュリティレベルのセキュリティ要件が蓄積されていきます。これらの 4 つのセキュリティレベルにより、機密データの異なる度合いと異なるアプリケーション環境に適した費用効果の高いソリューションが可能になります。

・セキュリティレベル 1 で提供するセキュリティ機能は何ですか。

セキュリティレベル 1 は、セキュリティの最も低いレベルです。暗号モジュールとしての基本的なセキュリティ要求事項（例えば、少なくとも一つの承認されたアルゴリズム、又は承認されたセキュリティ機能が使用されていなければならないこと。）がここで規定されています。セキュリティレベル 1 では、製品グレードとしての基本的な要求事項を超える特別な物理セキュリティのメカニズムは要求されません。セキュリティレベル 1 では、評価されていないオペレーティングシステムを使用している汎用コンピュータシステム上で実行される暗号モジュールのソフトウェア構成要素及びファームウェア構成要素を許可しています。セキュリティレベル 1 の暗号モジュールの例として、パーソナルコンピュータ（PC）に搭載されたソフトウェア暗号ライブラリがあります。

このような暗号モジュールの実装は、例えば、物理セキュリティ、ネットワークセキュリティ、管理手続のような他の管理手段が限られているか又は存在しないときの、低いレベルのセキュリティのアプリケーションに適しています。暗号のソフトウェア実装は、ハードウェア実装よりも費用対効果

が高いため、低いレベルのセキュリティ要求事項を満たすための、ハードウェアメカニズムに代わる暗号での解決策として選択できます。

・セキュリティレベル 2 で提供するセキュリティ機能は何ですか。

セキュリティレベル 2 は、タンパー証跡をもつコーティング若しくはシール、又は除去可能なカバー若しくはドアに対してこじ開け耐性のある錠を含むタンパー証跡に関する要求事項を追加することで、セキュリティレベル 1 の物理セキュリティのメカニズムを強化したものです。

タンパー証跡をもつコーティング又はシールは、暗号モジュールに塗布又は貼付され、暗号モジュール内のクリティカルセキュリティパラメタ（以下、CSP と記します。）及び／又は公開セキュリティパラメタ（以下、PSP と記します。）への物理的なアクセスがあった場合、そのコーティング又はシールは必ず破壊されなければなりません。タンパー証跡を残すシール又はこじ開け耐性のある錠は、許可されていない物理的なアクセスから保護するために、カバー又はドアに添付又は設置されます。

セキュリティレベル 2 は、役割ベースの認証を最低限必要とします。この認証では、オペレータが特定の役割を担い、その役割に対応したサービスを実行する権限があることを、暗号モジュールが認証します。

セキュリティレベル 2 では、ソフトウェアの暗号モジュールが，(a) 役割ベースのアクセス制御，又は (b) 最低限，新しいグループを定義しアクセス制御リスト（例えば，ACL）を通じて制限付きの許可を規定する堅ろう（牢）なメカニズムをもち，かつ，一つ以上のグループに各ユーザを割り当てる能力を備えた任意アクセス制御を実装し，無許可の実行，変更及び暗号のソフトウェアを読み取ることを防止する，変更可能な環境で実行されることを許可しています。

・セキュリティレベル 3 で提供するセキュリティ機能は何ですか。

セキュリティレベル 2 で要求されるタンパー証跡を残す物理セキュリティのメカニズムに加えて、セキュリティレベル 3 は、侵入者が暗号モジュール内の CSP 及び／又は PSP に対してアクセスすることを防止することを意図しています。セキュリティレベル 3 で要求される物理セキュリティのメカニズムは、物理アクセスの試み、暗号モジュールの利用又は変更及び通気口又はスリットを通したプロービングに対して、高い確率で検出及び応答することを目的としています。この物理セキュリティのメカニズムには、暗号モジュールの除去可能なカバー・ドアが開けられたときに、CSP を全てゼロ化するタンパー検出・タンパー応答をもつ回路、及び頑丈な囲いの使用を含むことができます。

セキュリティレベル 3 は、ID ベースの認証メカニズムを要求します。これは、セキュリティレベル 2 で規定される役割ベースの認証メカニズムが提供するセキュリティを更に強化します。暗号モジュールは、オペレータの ID を認証し、かつ、識別されたオペレータが特定の役割を担って、その役割に応じたサービスを実行する権限が与えられていることを検証します。

セキュリティレベル 3 は、手動で確立される CSP の入出力が、暗号化されるか、トラステッドチャネルを利用するか、又は知識分散処理を用いて行われることを要求します。

セキュリティレベル 3 は，暗号モジュールが正常に動作する電圧及び温度の範囲を超えた環境条件によるセキュリティの危たい（殆）化からも暗号モジュールを保護します。攻撃者は，暗号モジュールの防御を妨害するために，通常動作範囲を意図的に逸脱させるかもしれません。暗号モジュールは，電圧及び温度の境界を超えたことを検出し CSP をゼロ化するよう設計された特別な環境故障保護機構

をもつか，又は暗号モジュールのセキュリティを危たい（殆）化するような形で通常動作範囲から外れたときに暗号モジュールが影響を受けない妥当な保証を提供する，厳しい環境故障試験を受けることが要求されます。

・セキュリティレベル 4 で提供するセキュリティ機能は何ですか。

セキュリティレベル 4 は、この規格の中で定義される最も高いセキュリティレベルのセキュリティを提供します。このセキュリティレベルでの物理セキュリティのメカニズムは、外部電源を用いるかどうかにかかわらず、CSP 及び／又は PSP がモジュールに含まれる場合、全ての許可されていない物理的なアクセスに対して検出及び応答するための、暗号モジュールの周りを完全に囲んだ包被での保護を提供します。あらゆる方向からの暗号モジュールの囲いへの侵入は、非常に高い確率で検出され、その結果、即座に全ての保護されていない SSP がゼロ化されます。セキュリティレベル 4 の暗号モジュールは、物理的に保護されていない環境下での使用に役立ちます。

セキュリティレベル 4 は，オペレータの認証に多要素認証の要求事項を導入している。最低でも，これは，次の三つの属性のうちの二つを要求する。

a) 秘密のパスワードのような，知識
b) 物理鍵又はトークンのような，所持物
c) 生体情報

セキュリティレベル 4 での暗号モジュールは，暗号モジュールのセキュリティを危たい（殆）化し得るような形で通常動作範囲を超える場合に影響を受けない妥当な保証をもたらすために，電圧及び温度の境界を検出し，全ての保護されていない SSP をゼロ化するよう設計された，特別な環境故障保護機構をもつことが要求されている。

5.2 ISO/IEC 19790:2012 (JIS X19790:2015)

・セキュリティレベル 1～4 のセキュリティ要件の相違点は何ですか。

次の表では、4つのセキュリティレベル要件の相違を示します。

表5.2.1 セキュリティ要件

	セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
暗号モジュールの仕様	暗号モジュール，暗号境界，承認されたセキュリティ機能，並びに通常動作モード及び縮退動作モードの仕様。全てのハードウェア，ソフトウェア及びファームウェアの構成要素を含む暗号モジュールの記述。全てのサービスは，そのサービスが承認された暗号アルゴリズム，セキュリティ機能又はプロセスを承認された方法で利用していることを示す状態情報を提供する。			
暗号モジュールのインタフェース	必須のインタフェース及び選択可能なインタフェース。全てのインタフェースの仕様及び全ての入出力データパスの仕様。		トラステッドチャネル。	
役割、サービス、及び認証	必須の役割と選択可能な役割との論理的な分離，及び必須のサービスと選択可能なサービスとの論理的な分離。	役割ベース又はIDベースのオペレータ認証。	IDベースのオペレータ認証。	多要素認証。

		セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
ソフトウェア・ファームウェアセキュリティ		承認された完全性技術，又はEDCに基づく完全性テスト。定義されたSFMI，HFMI及びHSMI。 実行可能コード。	承認されたディジタル署名又は鍵付きメッセージ認証コードに基づく完全性テスト。	承認されたディジタル署名に基づく完全性テスト。	
動作環境		変更不可能な動作環境，限定動作環境又は変更可能な動作環境。 SSPの制御。	変更可能な動作環境。 役割ベースの，又は任意アクセス制御。 監査メカニズム。		
物理セキュリティ		製品グレードの部品。	タンパー証跡。 不透明なカバー又は囲い。	カバー及びドアに対してのタンパー検出・応答。強固な囲い又はコーティング。直接的なプロービングからの保護。EFP又はEFT。	タンパー検出・応答が可能な包被。EFP。故障注入への対処。
非侵襲セキュリティ		暗号モジュールは，附属書Fで規定されている非侵襲攻撃に対処するよう設計されている。			
		JIS X 19790 附属書 F で規定されている対処技術の文書化及び有効性。		対処法試験。	対処法試験。
センシティブセキュリティパラメタ管理		乱数ビット生成器，SSP生成，確立，入出力，格納及びゼロ化。			
		承認された方法を利用した，自動化されたSSP配送又はSSP共有。			
		手動で確立されたSSPは，平文の形式で入力又は出力されてもよい。		手動で確立されたSSPは，暗号化された形式か，トラステッドチャネル経由で知識分散処理を利用して入力又は出力されてもよい。	
自己テスト		動作前自己テスト：ソフトウェア・ファームウェア完全性テスト，バイパステスト，又は重要機能テスト。			
		条件自己テスト：暗号アルゴリズムテスト，鍵ペア整合性テスト，ソフトウェア・ファームウェアのロードテスト，手動入力テスト，条件バイパステスト及び重要機能テスト。			
ライフサイクル保証	構成管理	暗号モジュール，部品，及び文書用の構成管理システム。ライフサイクルを通じて，各々一意に識別及び追跡される。		自動化された構成管理システム。	
	設計	提供する全てのセキュリティ関連サービスの試験を許すよう設計された暗号モジュール。			
	FSM	有限状態モデル。			
	開発	注釈付きソースコード，回路図又はHDL。	ソフトウェアの高級言語。ハードウェアの上位記述言語。		暗号モジュールの構成要素への入力時の事前条件，及び構成要素が完了した場合に真であると期待される事後条件を伴う注釈付き文書。
	テスト	機能試験。		下位レベル試験。	

		セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
	配付及び運用	初期化手順。	配付手順。		ベンダから提供された認証情報を用いたオペレータ認証。
	ガイダンス	管理者ガイダンス及び非管理者ガイダンス。			
その他の攻撃への対処		試験可能な要求事項は用意されていない攻撃への対処の仕様。			試験可能な要求事項を備えた、攻撃への対処仕様。

・暗号モジュールとは何ですか。

暗号モジュールは、セキュリティ機能を実装した、暗号境界内のハードウェア、ソフトウェア及び／又はファームウェアの集合です。

3 種類の物理的な形態（シングルチップ暗号モジュール、マルチチップ組込み型暗号モジュール、マルチチップスタンドアロン型暗号モジュール）があります。

・暗号境界とは何ですか。

暗号モジュールの境界を確定し，かつ，暗号モジュールの全ての構成要素（すなわち，ハードウェア，ソフトウェア，及び／又はファームウェア）をその内側に含む，明確に定義された連続する境界線です。

・モジュールインタフェースとは何ですか。

モジュールインタフェースは、情報が暗号モジュールを出入りする物理的又は論理的な入出力ポイントです。少なくとも、暗号モジュールの設計には以下のインタフェースを含める必要があります。

a)**データ入力インタフェース**　暗号モジュールに入力され処理される全てのデータ（制御入力インタフェースを介して入力される制御データを除く）は、データ入力インタフェースを介して入力されなければなりません。これらのデータには、平文データ、暗号文データ、CSP、PSP 及び別の暗号モジュールからの状態情報を含みます。

b)**データ出力インタフェース**　暗号モジュールから出力される全てのデータ（状態出力インタフェースを介して出力される状態データ及び制御出力インタフェースを介しての制御データ出力を除く）は、データ出力インタフェースから出力されなければなりません。これらのデータには、平文データ、暗号文データ、CSP、PSP を含みます。手動入力、動作前自己テスト、ソフトウェア・ファームウェアのロード、及びゼロ化を実行している間、又は暗号モジュールがエラー状態にある場合には、データ出力インタフェースからの全てのデータ出力は禁止されなければなりません。

c)**制御入力インタフェース**　暗号モジュールの動作を制御するために使用される全ての入力コマンド、信号及び制御データ（関数呼出し及びスイッチ、ボタン、並びにキーボードのような手動制御を含みます。）は、制御入力インタフェースから入力されなければなりません。

d)**制御出力インタフェース**　暗号モジュールの動作の状態を制御又は伝えるために使用される全ての出力コマンド、信号及び制御データ（例えば、他の暗号モジュールに対する制御コマンド）は、“ 制

御出力”インタフェースを介して出力されなければなりません。暗号モジュールがエラー状態にあるときには，セキュリティポリシに、例外が規定されており、かつ、文書化されている場合を除き、“制御出力”インタフェースを介する全ての制御出力は禁止されなければなりません。

e)状態出力インタフェース　暗号モジュールの状態を示すために使用される全ての出力信号、インジケータ及び状態データ（戻り値、並びに発光ダイオード及びディスプレイのような物理的なインジケータを含みます。）は、状態出力インタフェースから出力されなければなりません。

・役割とサービスには、何がありますか。

暗号モジュールは、オペレータに対し、許可された次の役割をサポートするものとします。

a)クリプトオフィサ役割　暗号関連の初期化又は管理機能、及び一般的なセキュリティサービス（例えば、暗号モジュールの初期化、CSP・PSP の管理、監査機能）を行うことを担う役割。

暗号モジュールは、次の役割をサポートすることができます。

b)ユーザ役割　暗号操作及びその他の承認されたセキュリティ機能を含む、一般的なセキュリティサービスを行うことを担う役割。

サービスは、暗号モジュールが実行できるサービス、動作、又は機能を示します。

認証メカニズムは、モジュールにアクセスするオペレータを認証し、オペレータが要求された役割を担い、役割のサービス実行が許可されているか検証するために、暗号モジュール内で必要とされます。暗号モジュールは、セキュリティレベルに応じて、モジュールへのアクセスを制御するために、次のメカニズムの 1 つ以上をサポートしなければなりません。

a)役割ベースの認証

暗号モジュールに役割ベースの認証メカニズムがサポートされている場合には、暗号モジュールは、オペレータが一つ以上の役割を選択することを要求しなければなりません。暗号モジュールは、オペレータが選択された役割（又は役割の集合）を担っていることを認証しなければなりません。暗号モジュールは、オペレータ個人の ID を認証することは要求されません。役割の選択及び選択された役割を担うことの認証は、同時に行うことができます。暗号モジュールが、オペレータの役割変更を許可する場合には、暗号モジュールは、オペレータが以前に認証されていないいかなる役割を担うことに対しても認証をしなければなりません。

b)ID ベースの認証

暗号モジュールにおいて ID ベースの認証メカニズムがサポートされている場合には、暗号モジュールはオペレータが一意に識別されることを要求し、オペレータによって暗黙的又は明示的に一つ以上の役割が選択されることを要求し、並びにオペレータの ID 及びオペレータが選択された役割（又は役割の集合）を担うことが許可されていることを検証しなければなりません。オペレータの ID、役割の選択及び選択された役割を担うことの許可は、同時に行うことができます。暗号モジュールがオペレータに役割を変更することを許可する場合には、暗号モジュールは、以前に許可されていない役割を担うために、識別されたオペレータの許可を検証しなければなりません。

・オペレータ認証するための最小のセキュリティ要件は何ですか。

セキュリティレベル 1 の場合、暗号モジュールは、モジュールへのアクセスを制御する認証メカニズムを採用する必要はありません。認証メカニズムが暗号モジュールによってサポートされない場合、モジュールは、オペレータに 1 つ以上の役割を暗黙的又は明示的に選択させる必要があります。セキュリティレベル 1 の認証は、役割ベースか ID ベースのいずれでもかまいません（単独の役割又は ID

ベースのアカウントを含みます)。セキュリティレベル 2 は少なくとも役割ベースのオペレータ認証である必要があるのに対し、セキュリティレベル 3 とセキュリティレベル 4 は ID ベースのオペレータ認証である必要があります。

サポートされた認証メカニズムを実行するため、暗号モジュールは様々なタイプの認証データを必要とします。認証データには、パスワード、PIN、暗号鍵、及び同等なものの知識や所有、物理鍵、トークン、及び同等のものの所有、あるいは個人的特徴の照合（バイオメトリクスなど）が含まれますが、これらに限定するものではありません。暗号モジュール内の認証データは、不正な開示、変更、及び置き換えから保護されるものとします。

・有限状態モデルとは何ですか。

有限状態モデルは、暗号モジュールの機能と動作シーケンスを一般的に説明するものです。

・暗号モジュールに含まれなければならない状態には何がありますか。

暗号モジュールには、次の動作状態及びエラー状態を含める必要があります。

a)**電源オン・オフ状態**　主電源、副電源、又はバックアップ電源が供給されており、電源オフ、スタンバイモード（揮発性メモリは維持されている)、又は（休止モードのように）不揮発性メモリに動作状態が保持されている状態。暗号モジュールに供給されている電源によってこの状態を分類しても良い。

b) **一般初期化状態**　暗号モジュールが，承認された状態へ遷移する前に初期化を実行している状態。

c)**クリプトオフィサ状態**　クリプトオフィサのサービスが実行されている状態（例えば、暗号関連の初期化及び鍵管理)。

d)**CSP 入力状態**　CSP を暗号モジュールへ入力している状態。

e)**ユーザ状態**　（ユーザ役割が実装されている場合,）許可されたユーザに対してセキュリティサービスを提供している，暗号操作を実行している，又は他の承認されたセキュリティ機能を実行している状態。

f)**承認された状態**　承認されたセキュリティ機能を実行している状態。

g)**自己テスト状態**　暗号モジュールが自己テストを実行している状態。

h)**エラー状態**　暗号モジュールがエラーとなったときの状態　エラー状態は、装置故障を指し示し、かつ、暗号モジュールのメンテナンス、サービス、若しくは修理を必要とするかもしれない“ハード”エラー又は暗号モジュールの初期化若しくはリセットを必要とするかもしれない復旧可能な“ソフト”エラーを含もこともできます。エラー状態からの復旧は、そのエラー状態が暗号モジュールのメンテナンス、サービス、又は修理を必要とするハードエラーによって引き起こされたものでない限りは、可能でなくてはなりません。

・暗号モジュールに含むことのできる状態には何がありますか。

暗号モジュールには、次の状態を含めることができます。ただし、これらに限定するものではありません。

a)**バイパス状態**　バイパス能力が作動し、暗号化処理がされない（例えば、暗号モジュールを通して平文を転送する）サービスが提供される状態。

b)**休眠状態**　暗号モジュールが休眠中の状態（例えば，低電力，サスペンド，休止状態)。

・物理セキュリティとは何ですか。

暗号モジュールは、物理セキュリティのメカニズムを用いて、実装後の暗号モジュールの内容への許可されていない物理的なアクセスを制限し、実装後の暗号モジュールの許可されていない使用又は変更（暗号モジュール全体の置き換えを含む。）を防がなければなりません。暗号境界内の全てのハードウェア、ソフトウェア、ファームウェア及びデータ構成要素は保護されなければなりません。
JIS X19790 の当該細分箇条では、暗号モジュールの物理セキュリティの全要件を詳しく説明しています。ソフトウェアの暗号モジュールについては、適用除外となります。

・物理形態の種類には何がありますか。

物理セキュリティの要求事項は、次の三つの定義された暗号モジュールの物理形態に対して規定されています。

a)**シングルチップ暗号モジュール**　これは、単一の集積回路(IC)チップがスタンドアロンのデバイスとして用いられているか、又は物理的に保護されていない囲い若しくは製品内に組込まれている物理形態である。シングルチップ暗号モジュールの例には、単一 IC チップ又は単一 IC チップの付いたスマートカードが含まれます。

b)**マルチチップ組込み型暗号モジュール**　これは、二つ又はそれ以上の IC チップが相互接続されて、物理的に保護されていない囲い又は製品内に組込まれている物理形態である。マルチチップ組込型暗号モジュールの例には、アダプタ及び拡張ボードが含まれます。

c)**マルチチップスタンドアロン型暗号モジュール**　これは、二つ又はそれ以上の IC チップが相互接続されて、囲い全体が物理的に保護されている物理形態である。マルチチップスタンドアロン型暗号モジュールの例には、暗号化ルータ又は HSM（Hardware Security Module）が含まれます。

・物理形態ごとの各レベルでの物理セキュリティ要件は何ですか。

次の表は、四つのセキュリティレベルそれぞれの物理セキュリティの要求事項（一般的な要求事項及び三つの形態に特有の要求事項）を要約しています。それぞれのセキュリティレベルにおける形態特有の物理セキュリティの要求事項は、同じセキュリティレベルの一般的要求事項を強化し、かつ、それよりも低いセキュリティレベルにおける形態特有の要求事項を包含しています。

表5.3.2 物理セキュリティ要求事項の要約

	全ての形態に対する一般的要求事項	シングルチップ	マルチチップ組込み型	マルチチップスタンドアロン型
セキュリティレベル 1	製品グレードの構成要素。標準的な表面安定化処理。メンテナンスアクセスインタフェースへのアクセス時の手続的又は自動ゼロ化。	追加要求事項なし。	製品グレードの囲い又は除去可能なカバー。	製品グレードの囲い又は除去可能なカバー。
セキュリティレベル 2	タンパー証跡。可視光領域内で不透明又は半透明。穴又はスリットを通しての直接の観察の防止。	タンパー証跡を残す，チップ上のコーティング又は囲い。	タンパー証跡を残す被覆材料，ドア若しくは除去可能なカバーに適用するタンパー証跡を残すシール，又はこじ開け耐性のある錠の付いた囲い。	タンパー証跡を残す被覆材料，ドア若しくは除去可能なカバーに適用するタンパー証跡を残すシール，又はこじ開け耐性のある錠の付いた囲い。
セキュリティレベ	タンパー応答及びゼロ化	硬くかつタンパー	硬くかつタンパー証跡を残	硬くかつタンパー証跡を残

ル 3	回路。メンテナンスアクセスインタフェースへのアクセス時の自動ゼロ化。穴又はスリットを通してのプロービングの防止。温度及び電圧に関する EFP 又は EFT。	証跡を残すチップ上のコーティング又は強固で除去耐性及び貫き耐性のある囲い。	す被覆材料又は強固な囲い。	す被覆材料又は強固な囲い。
セキュリティレベル 4	タンパー検出・タンパー応答包被。温度及び電圧に関する EFP。故障誘導からの保護。	硬く除去耐性のあるチップ上のコーティング。	ゼロ化機能の付いたタンパー検出・応答包被。	ゼロ化機能の付いたタンパー検出・応答包被。

・ライフサイクル保証とは何ですか。

ライフサイクル保証とは、暗号モジュールの設計、開発、運用及び使用終了におけるベストプラクティスの使用を指し、次の二つを保証します。

- 暗号モジュールの適切な設計、開発、試験、構成、配付、及び運用。
- 適切な操作ガイダンス文書の提供。

構成管理、設計、有限状態モデル、開発、試験、配付及び運用、並びにガイダンス文書についてセキュリティ要求事項を規定します。

・動作環境とは何ですか。

暗号モジュールの動作環境とは、暗号モジュールが動作するために必要なソフトウェア構成要素、ファームウェア構成要素及び／又はハードウェア構成要素の管理を指します。動作環境は、変更不可能（例えば、ROM に収められたファームウェア、入出力デバイスの機能を無効にしたコンピュータに収められたソフトウェア）であるか、又は変更可能（例えば、RAM に収められたファームウェア、汎用コンピュータで実行されるソフトウェア）です。オペレーティングシステムは、暗号モジュールの動作環境の重要な構成要素です。

汎用動作環境とは、次の機能をもつ市販の汎用オペレーティングシステムを利用していることを指します。

・暗号境界内のソフトウェア構成要素及びファームウェア構成要素の管理。
・汎用アプリケーションソフトウェアを含むシステム及びユーザプロセス／スレッドの管理。

6. 略語

CSP　critical security parameter

セキュリティに関する情報であって，その開示又は変更が，暗号モジュールのセキュリティを危たい（殆）化し得るもの。

([JIS X19790:2015, 定義 3.18]を参照)

EDC　error detection code

データから計算された冗長ビット及びデータで構成される値で，データの意図しない改変

を検出するためのもの。データの訂正はしない。

([JIS X19790:2015, **定義** 3.41]**を参照**)

EFP environmental failure protection

暗号モジュールの通常動作範囲外の環境条件によって，暗号モジュールのセキュリティが危たい（殆）化することを防止する機構を使用すること。

([JIS X19790:2015, **定義** 3.39]**を参照**)

EFT environmental failure testing

暗号モジュールの通常動作範囲外の環境条件によって，暗号モジュールのセキュリティが危たい（殆）化しないという妥当な保証を与えるために特定の方法を使用すること。

([JIS X19790:2015, **定義** 3.40]**を参照**)

HFMI hybrid firmware module interface

ハイブリッドファームウェアモジュールのサービスを要求するために使われるコマンドの全体。その暗号モジュールの暗号境界で，要求されたサービスの一部として，入出力されるパラメタを含む。

([JIS X19790:2015, **定義** 3.55]**を参照**)

HMI hardware module interface

ハードウェアモジュールのサービスを要求するために使われるコマンドの全体。そのハードウェアモジュールの暗号境界で，要求されたサービスの一部として，入出力されるパラメタを含む。

([JIS X19790:2015, **定義** 3.52]**を参照**)

HSMI hybrid software module interface

ハイブリッドソフトウェアモジュールのサービスを要求するために使われるコマンドの全体。その暗号モジュールの暗号境界で，要求されたサービスの一部として，入出力されるパラメタを含む。

([JIS X19790:2015, **定義** 3.56]**を参照**)

PSP public security parameter

セキュリティに関連する公開情報であって，その変更が，暗号モジュールのセキュリティを危たい（殆）化し得るもの。

([JIS X19790:2015, **定義** 3.99]**を参照**)

SFMI software/firmware module interface

ソフトウェア又はファームウェアモジュールのサービスを要求するために使用されるインタフェースの全体。その暗号モジュールの暗号境界で，要求されたサービスの一部として，

入出力されるパラメタを含む。

([JIS X19790:2015, **定義** 3.119]**を参照**)

SSP sensitive security parameter

クリティカルセキュリティパラメタ（CSP**）及び公開セキュリティパラメタ（**PSP**）の総称。**

([JIS X19790:2015, **定義** 3.110]**を参照**)

改訂履歴

識別番号	QAJ-01

改訂年月日	作成者・承認者	改訂内容
平成 21 年 4 月 3 日	井上・近藤	新規制定
平成 30 年 7 月 2 日	櫻井・塚元	一部改訂