JIS

セキュリティ技術ー
暗号モジュールのセキュリティ要求事項

JIS X 19790：2023

（ISO/IEC 19790：2012）

（IPA/JSA）

令和 5 年 1 月 20 日 改正

日本産業標準調査会 審議

（日本規格協会 発行）

日本産業標準調査会標準第二部会 構成表

	氏名	所属
（部会長）	古 関 隆 章	東京大学
（委員）	青 木 真 理	川崎市地域女性連絡協議会
	青 柳 恵美子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
	岩 渕 幸 吾	一般社団法人電子情報技術産業協会
	上 野 貴 由	一般社団法人日本電機工業会
	岡 本 正 英	株式会社日立製作所
	上参郷 龍 哉	一般財団法人電気安全環境研究所
	河 合 和 哉	国立研究開発法人産業技術総合研究所
	熊 田 亜紀子	東京大学
	髙 橋 弘	IEC/CAB 委員（富士電機株式会社）
	田 中 博 敏	一般社団法人ビジネス機械・情報システム産業協会
	田 辺 恵 子	主婦連合会
	野 田 耕 一	一般財団法人日本規格協会
	林 泰 弘	早稲田大学
	平 本 俊 郎	東京大学
	藤 原 昇	一般社団法人電気学会

主 務 大 臣：経済産業大臣　　制定：平成 19.3.20　　改正：令和 5.1.20
官 報 掲 載 日：令和 5.1.20
原 案 作 成 者：独立行政法人情報処理推進機構
（〒113-6591　東京都文京区本駒込 2-28-8 文京グリーンコートセンターオフィス　TEL 03-5978-7507）
一般財団法人日本規格協会
（〒108-0073　東京都港区三田 3-13-12 三田 MT ビル　TEL 050-1742-6017）
審 議 部 会：日本産業標準調査会　標準第二部会（部会長　古関　隆章）

この規格についての意見又は質問は，上記原案作成者又は経済産業省産業技術環境局 国際電気標準課（〒100-8901 東京都千代田区霞が関 1-3-1）にご連絡ください。

なお，日本産業規格は，産業標準化法の規定によって，少なくとも 5 年を経過する日までに日本産業標準調査会の審議に付され，速やかに，確認，改正又は廃止されます。

目　次

まえがき

この規格は，産業標準化法第 16 条において準用する同法第 12 条第 1 項の規定に基づき，独立行政法人情報処理推進機構（IPA）及び一般財団法人日本規格協会（JSA）から，産業標準原案を添えて日本産業規格を改正すべきとの申出があり，日本産業標準調査会の審議を経て，経済産業大臣が改正した日本産業規格である。これによって，**JIS X 19790**:2015 は改正され，この規格に置き換えられた。

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本産業標準調査会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

日本産業規格　　JIS
X 19790：2023
(ISO/IEC 19790：2012)

セキュリティ技術ー
暗号モジュールのセキュリティ要求事項

Security techniques—Security requirements for cryptographic modules

序文

この規格は，2012 年に第 2 版として発行された **ISO/IEC 19790**（Corrected version:2015）を基に，技術的内容及び構成を変更することなく作成した日本産業規格である。

なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。

情報技術分野において，エンティティ認証のため及び否認防止のために，また，許可されていない開示又は操作からのデータ保護の仕組みとして,暗号メカニズムを利用する必要性は益々高くなってきている。そのようなメカニズムのセキュリティ及び信頼性は，それらが実装されている暗号モジュールに依存している。

この規格は，内容が段階的に深まる四つのレベルのセキュリティ要求事項を規定しているが，これは，様々なものが考えられる応用業務及び環境に広く対応できるよう考慮したからである。対象の暗号技術群は，四つのセキュリティレベルにわたり同一である。このセキュリティ要求事項は，暗号モジュールの設計及び実装に関係した分野を取り上げている。その分野には，次のものがある。

- 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，サービス及びオペレータ認証
- 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
- その他の攻撃への対処

暗号モジュールの全体的なセキュリティレベル付けは，暗号モジュールを利用する応用業務及び環境からのセキュリティ要求事項，並びに暗号モジュールの提供するセキュリティサービスに応じた適切なレベルを提供するように選ぶ必要がある。それぞれの組織の責任者は，暗号モジュールを利用するコンピュータシステム及び通信システムが，所与の応用業務及び環境からみて受容し得るセキュリティレベルを提供することを確実にすることが望ましい。承認されたセキュリティ機能のどれが所与の応用業務に対して適