暗号モジュール試験及び認証制度(JCMVP)

～国際規格ISO/IEC19790に基づく試験・認証～

意外と身近な暗号製品とそのセキュリティ

・スマートカードや、スマートフォンなどの身近な製品の中にも暗号機能が組み込まれて、セキュリティを支えています

・暗号製品は、さまざまなリスク・脅威・攻撃にさらされています。

実際の報告事例 1
ECBの多用

実際の報告事例 2
固定の暗号鍵の使用

実際の報告事例 3
鍵管理の不備を突かれて暗号鍵が暴露

暗号製品のセキュリティを第三者が試験及び認証

メリット

専門家による試験及び認証を通じて、国際規格に基づいた、暗号製品としての最低限のセキュリティを確認することができます。

国際標準

ISO/IEC 19790
暗号モジュールのセキュリティ要求事項

ISO/IEC 24759
暗号モジュールのセキュリティ試験要件

暗号の実装が適切で、それが確実に実行され、かつ、
暗号鍵などの重要情報が適切に保護されているかを試験

ISO/IEC 19790の適用分野

- スマートカード
- ストレージセキュリティ
- モバイルバンキング
- 通信暗号化
- ホーム エレクトロニクス システム
- その他

試験項目

- 文書・ソースコードレビュー
- 物理セキュリティ試験
- 乱数の試験
- 暗号が正確に実装されているか試験
- 動作の確実性を確認する試験
- サイドチャネル攻撃の耐性試験

開発証拠資料
- 機能仕様書
- ソースコード
- ガイダンス文書

認証

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan