暗号モジュール認証書

暗号モジュール試験及び認証制度に基づき、以下のとおり認証する。

平成30年3月19日
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

認証番号　F0022

日本語名：Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)

英語名：　Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)

ハードウェアバージョン：　AA
ファームウェアバージョン：　FN001S, FN002S
ソフトウェアバージョン：　N/A
物理形態：　マルチチップ組込型

適合規格：Federal Information Processing Standards (FIPS) PUB 140-2
Security Requirements for Cryptographic Modules
Change Notices (12-03-2002)
試験要件：Derived Test Requirements for FIPS PUB 140-2, January 04, 2011
JCMVP暗号アルゴリズム実装試験要件　平成21年1月8日

申請者：　東芝デバイス＆ストレージ株式会社
所在地：　東京都港区芝浦一丁目1番1号
特記事項：　本暗号モジュール認証書の対象は、暗号モジュールを承認された動作モードで動作させた場合に限る。

注意事項：本暗号モジュール認証書で識別される暗号モジュールは、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号モジュール試験要件に基づく暗号モジュール試験結果が、適合していることを示す。本暗号モジュール認証書は、暗号モジュール試験を受けた構成及び動作環境に関して、暗号モジュールの特定のバージョンのみに適用される。暗号モジュール試験は「暗号モジュール試験及び認証制度」の規定に従って実施され、暗号モジュール試験報告書の試験機関による結論は、暗号モジュール試験に用いた提供物件にのみ対応している。この暗号モジュール認証書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない。なお、本認証書を、不正に使用した場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

暗号モジュール認証報告書

平成30年3月19日
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

記

暗号モジュール名：　Toshiba Secure TCG Opal SSC and Wipe technology
Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)
バージョン：
ハードウェアバージョン：　AA
ファームウェアバージョン：　FN001S, FN002S
ソフトウェアバージョン：　N/A
暗号モジュール試験機関名：　一般社団法人 ITセキュリティセンター 評価部
暗号モジュール試験報告書
作成支援ツールバージョン：　1.2.2

暗号モジュール試験の結果、上記の暗号モジュールは、以下の暗号モジュールセキュリティ要件を満足することを認証したので報告します。
平成30年3月16日

技術本部セキュリティセンター　情報セキュリティ認証室
技術管理者　佐藤　眞司

暗号モジュールセキュリティ要件：FIPS PUB 140-2 Security Requirements for Cryptographic Modules (Change Notice 2, 12/3/2002)
暗号モジュール試験要件：Derived Test Requirements for FIPS PUB 140-2 (Change Notice 8, 01/04/2011)
JCMVP運用ガイダンス(平成26年1月17日)

暗号モジュールの仕様：	2	暗号モジュールのポートとインタフェース：2	
役割、サービス、及び認証：	2	有限状態モデル：	2
物理的セキュリティ：	2	動作環境：	N/A
暗号鍵管理：	2	自己テスト：	2
設計保証：	2	その他の攻撃への対処：	N/A

全体的なセキュリティレベル：2

暗号モジュール試験時の構成：

暗号モジュールに搭載されている承認暗号アルゴリズム：
AES(#36, #37), SHS(#26), HMAC(#17), DRBG(#5)

暗号モジュールに搭載されている非承認暗号アルゴリズム：
NDRNG

結果：　合格
試験に用いた試験対象の暗号モジュールは、暗号モジュール試験及び認証制度が定める所定の基準に基づく試験の結果、所定の暗号モジュールセキュリティ要件を満たした。

以上