

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、下記のとおり認証する。

平成 29 年 9 月 8 日

(初回発行日：平成 20 年 10 月 27 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 J0006

日本語名：暗号化機能搭載2.5型ハードディスクドライブ
「MHZ2 CJ」シリーズ

英語名：MHZ2 CJ Series of 2.5inch hard disk drive
with automatic hardware-based encryption

ハードウェアバージョン： 別紙参照
ファームウェアバージョン： 0000801F
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： JIS X 19790：2007 平成 19 年 3 月 20 日
試験要件： JIS X 5091：2007 平成 19 年 3 月 20 日
JCMVP 暗号アルゴリズム実装試験要件 平成 19 年 10 月 29 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 1-1-1
特記事項： なし

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。

<暗号化機能搭載 2.5 型ハードディスクドライブ「MHZ2 CJ」シリーズ 暗号モジュール認証書：別紙>

● 暗号モジュールハードウェアバージョン :

CA07062-B901 A1, CA07062-B218 A1, CA07062-B903 A1, CA07062-B222 A1,
CA07062-B904 A1, CA07062-B226 A1, CA07062-B906 A1, CA07062-B230 A1,
CA07062-B908 A1, CA07062-B245 A1, CA07062-B909 A1, CA07062-B242 A1,
CA07062-B911 A1, CA07062-B248 A1, CA07062-B913 A1, CA07062-B252 A1,
CA07062-B914 A1, CA07062-B256 A1, CA07062-B916 A1, CA07062-B260 A1,
CA07062-B918 A1, CA07062-B275 A1, CA07062-B919 A1, CA07062-B272 A1,
CA07062-B901 A2, CA07062-B218 A2, CA07062-B903 A2, CA07062-B222 A2,
CA07062-B904 A2, CA07062-B226 A2, CA07062-B906 A2, CA07062-B230 A2,
CA07062-B908 A2, CA07062-B245 A2, CA07062-B909 A2, CA07062-B242 A2,
CA07062-B911 A2, CA07062-B248 A2, CA07062-B913 A2, CA07062-B252 A2,
CA07062-B914 A2, CA07062-B256 A2, CA07062-B916 A2, CA07062-B260 A2,
CA07062-B918 A2, CA07062-B275 A2, CA07062-B919 A2, CA07062-B272 A2

【変更履歴】

平成 20 年 10 月 27 日	申請者： 富士通株式会社 所在地： 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
平成 22 年 1 月 29 日	(再発行理由) 事業譲渡に伴って申請者及び所在地を変更する。 変更前： 申請者： 富士通株式会社 所在地： 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 変更後： 申請者： 株式会社東芝 所在地： 東京都港区芝浦 1-1-1
平成 29 年 9 月 8 日	(再発行理由) 事業承継に伴って申請者を変更する。 変更前：株式会社東芝 変更後：東芝デバイス&ストレージ株式会社

以上

暗号モジュール認証報告書

認証対象の暗号モジュールについて、以下の通り認証したことを報告する。

平成 20年 10月 27日

独立行政法人 情報処理推進機構

理事長 西垣 浩司

押印済

記

暗号モジュール名：暗号化機能搭載 2.5 型ハードディスクドライブ「MHZ2 CJ」シリーズ
バージョン：別紙参照

暗号モジュール試験機関名：独立行政法人 情報処理推進機構 セキュリティセンター
暗号モジュール試験報告書

作成支援ツールバージョン：1.1.0

暗号モジュールの仕様：	1	暗号モジュールのポートとインタフェース：	1
役割、サービス、及び認証：	1	有限状態モデル：	1
物理的セキュリティ：	1	動作環境：	N/A
暗号鍵管理：	1	電磁妨害/電磁両立性：	N/A
自己テスト：	1	設計保証：	1
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：1

暗号モジュール試験時の構成：

OS: Microsoft Windows 98 [Version 4.10.2222]、マザーボード: Intel DG33FB

CPU: Intel Core2 Duo E6550@2.33GHz、FDD: 1.4MB、Memory: 2GB

暗号モジュール：FUJITSU MHZ2080CJ G1(CA07062-B901 A1) 及び

FUJITSU MHZ2320CJ G2(CA07062-B272 A1)

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(#6)、SHS(#6)、Hash_DRBG in NIST SP800-90(ベンダ自己確認)

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：なし

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

< 暗号化機能搭載 2.5 型ハードディスクドライブ「MHZ2CJ」シリーズ暗号モジュール認証報告書：別紙 >

- 暗号モジュールハードウェアバージョン :
CA07062-B901 A1, CA07062-B218 A1, CA07062-B903 A1, CA07062-B222 A1,
CA07062-B904 A1, CA07062-B226 A1, CA07062-B906 A1, CA07062-B230 A1,
CA07062-B908 A1, CA07062-B245 A1, CA07062-B909 A1, CA07062-B242 A1,
CA07062-B911 A1, CA07062-B248 A1, CA07062-B913 A1, CA07062-B252 A1,
CA07062-B914 A1, CA07062-B256 A1, CA07062-B916 A1, CA07062-B260 A1,
CA07062-B918 A1, CA07062-B275 A1, CA07062-B919 A1, CA07062-B272 A1,
CA07062-B901 A2, CA07062-B218 A2, CA07062-B903 A2, CA07062-B222 A2,
CA07062-B904 A2, CA07062-B226 A2, CA07062-B906 A2, CA07062-B230 A2,
CA07062-B908 A2, CA07062-B245 A2, CA07062-B909 A2, CA07062-B242 A2,
CA07062-B911 A2, CA07062-B248 A2, CA07062-B913 A2, CA07062-B252 A2,
CA07062-B914 A2, CA07062-B256 A2, CA07062-B916 A2, CA07062-B260 A2,
CA07062-B918 A2, CA07062-B275 A2, CA07062-B919 A2, CA07062-B272 A2
- 暗号モジュールファームウェアバージョン : 0000801F

以上