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
セキュリティポリシー

２００８年８月

富士通株式会社

目次

更新履歴

版数	日付	更新内容
01	2008 年 8 月 18 日	公開用新規作成

1. 概要

この文書は、以下に示す富士通株式会社の暗号化機能搭載 2.5 型ハードディスクドライブのセキュリティポリシーを定義する。

表 1 暗号化機能搭載 2.5 型 ハードディスクドライブ

装置		ファームウェア		装置仕様	
Parts Number	版数	モデル名	版数	容量	SATA 転送レート
CA07062-B901	A1、A2	MHZ2080CJ G1	0000801F	80GB	1.5Gbps
CA07062-B218	A1、A2				
CA07062-B903	A1、A2	MHZ2120CJ G1	0000801F	120GB	1.5Gbps
CA07062-B222	A1、A2				
CA07062-B904	A1、A2	MHZ2160CJ G1	0000801F	160GB	1.5Gbps
CA07062-B226	A1、A2				
CA07062-B906	A1、A2	MHZ2200CJ G1	0000801F	200GB	1.5Gbps
CA07062-B230	A1、A2				
CA07062-B908	A1、A2	MHZ2250CJ G1	0000801F	250GB	1.5Gbps
CA07062-B245	A1、A2				
CA07062-B909	A1、A2	MHZ2320CJ G1	0000801F	320GB	1.5Gbps
CA07062-B242	A1、A2				
CA07062-B911	A1、A2	MHZ2080CJ G2	0000801F	80GB	3.0Gbps.
CA07062-B248	A1、A2				
CA07062-B913	A1、A2	MHZ2120CJ G2	0000801F	120GB	3.0Gbps.
CA07062-B252	A1、A2				
CA07062-B914	A1、A2	MHZ2160CJ G2	0000801F	160GB	3.0Gbps.
CA07062-B256	A1、A2				
CA07062-B916	A1、A2	MHZ2200CJ G2	0000801F	200GB	3.0Gbps.
CA07062-B260	A1、A2				
CA07062-B918	A1、A2	MHZ2250CJ G2	0000801F	250GB	3.0Gbps.
CA07062-B275	A1、A2				
CA07062-B919	A1、A2	MHZ2320CJ G2	0000801F	320GB	3.0Gbps.
CA07062-B272	A1、A2				

装置のハードウェアバージョンは、Parts Number と装置版数の組合せで特定される。

このセキュリティポリシーは、暗号モジュールが JIS X 19790 のセキュリティレベル 1 の要件を満たしていることを述べる。

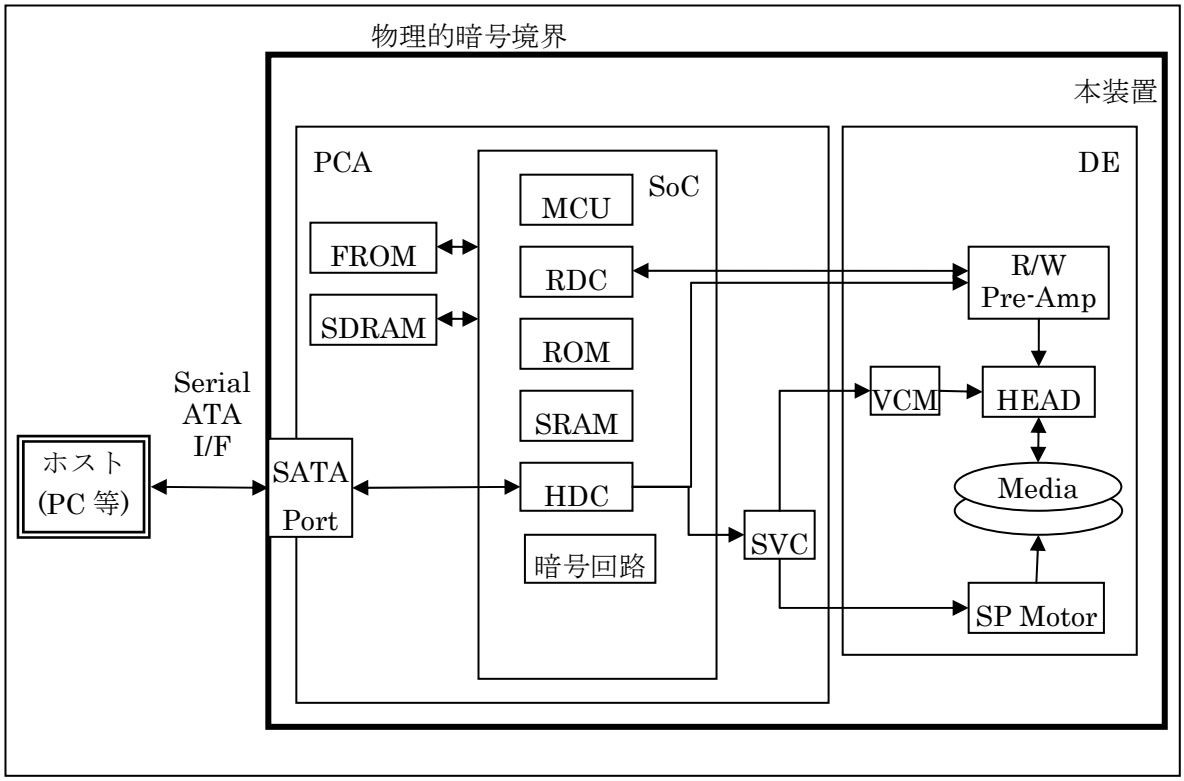
2. 暗号モジュールの仕様

(1) 概要

本暗号モジュールは、AT Attachment 8、Serial ATA R2.6 に準拠した Serial ATA インタフェースを持ち、暗号化機能を搭載した 2.5 型の内蔵磁気ディスク装置である。ハードウェアとファームウェアから構成され、マルチチップ組込型暗号モジュールに分類される。

(2) ハードウェア構成

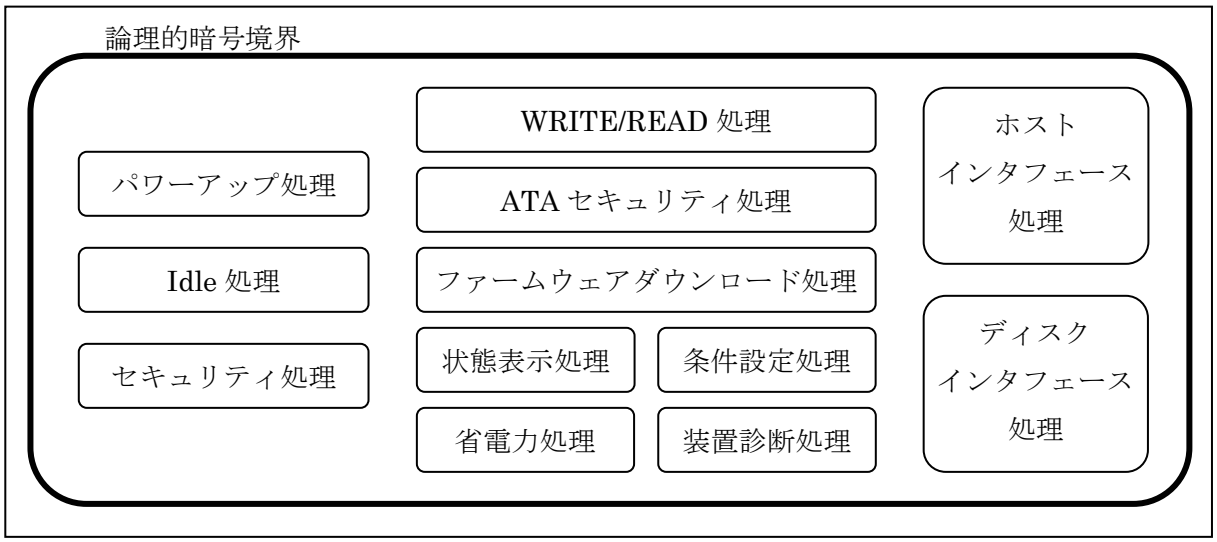
図 1 ハードウェア構成図



- PCA：Printed circuit assembly
- DE：Disk Enclosure
- SVC：Servo Combo
- HDC：Hard Disk Controller
- RDC：Read Channel
- SP Motor：Spindle Motor
- VCM：Voice Coil Motor

(3) ファームウェア構成

図 2 ファームウェア構成図



(4) セキュリティ機能と動作モード

本暗号モジュールは、以下のセキュリティ機能を実装している。

表 2 セキュリティ機能一覧

機能	アルゴリズム	規格
暗号化・復号	AES-256	FIPS PUB 197
ハッシュ	SHA-256	FIPS PUB 180-2 with Change Notice 1
メッセージ認証	CMAC(AES-256)	NIST Special Publication 800-38B
乱数生成	Hash_DRBG(SHA-256)	NIST Special Publication 800-90

- 本暗号モジュールは、起動後、常に承認された動作モードとして動作する。
- PSP は持たない。
- 乱数生成アルゴリズムは、ベンダー自己確認による。

(5) セキュリティレベル

本暗号モジュールは、各セキュリティ要求事項に対して下記のレベルを満たし、全体としてレベル 1 のセキュリティを満たす。

表 3 セキュリティレベル

セキュリティ要求事項	レベル
暗号モジュールの仕様	1
ポート及びインタフェース	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
自己テスト	1
設計保証	1
その他の攻撃への対処	N/A

3. ポート及びインタフェース

(1) 物理ポート

本暗号モジュールは、Serial ATA ポートのみを有す。

(2) 論理インタフェース

各論理インタフェースは、すべて Serial ATA ポートに対応する。

表 4 論理インタフェース

論理インタフェース	物理ポート
データ入力	Serial ATA ポート
データ出力	Serial ATA ポート
制御入力	Serial ATA ポート
状態出力	Serial ATA ポート
電源	Serial ATA ポート

(3) ATA コマンド

本暗号モジュールと外界との転送プロトコルは、AT Attachment 8、Serial ATA R2.6 に準拠する。本暗号モジュールは、ホストからの ATA コマンドを受付・実行する従属デバイスとして働く。

4. 役割、サービス、及び認証

(1) 役割

本暗号モジュールは、ユーザ役割とクリプトオフィサ役割をサポートする。

a) ユーザ役割 (User 役割)

本暗号モジュールのユーザデータにアクセスする役割。データ暗号鍵の初期化、ファームウェアダウンロード以外のサービスを利用する時は、暗黙的にユーザ役割を担う。

b) クリプトオフィサ役割 (CO 役割)

データ暗号鍵の初期化、あるいはファームウェアダウンロードを行う役割。データ暗号鍵の初期化、あるいはファームウェアダウンロード時は、暗黙的にクリプトオフィサ役割を担う。

(2) サービス

本暗号モジュールは、AT Attachment 8、Serial ATA R2.6 で規定された必須機能、一部のオプション機能、およびベンダー固有の条件設定/装置診断機能をサポートする。次の表に、本暗号モジュールがサポートするサービス、各サービスのセキュリティ機能、CSP アクセス状態と、各サービスが有効となる役割とを示す。

表 5 サービス一覧

分類	サービス	セキュリティ機能	CSP アクセス	User 役割	CO 役割
ユーザコマンド	WRITE 系コマンド	AES 暗号化	データ暗号鍵参照	有効	無効
	READ 系コマンド	AES 復号	データ暗号鍵参照		
	ATA セキュリティパスワード制御系コマンド	SHA ハッシュ AES 暗号化	データパスワード入力 データパスワードの設定又は照合 データ暗号鍵の参照		
	状態表示系コマンド	—	—		
	条件設定系コマンド	—	—		
	装置診断系コマンド	—	—		
	省電力系コマンド	—	—		
クリプトオフィサコマンド	データ暗号鍵初期化コマンド	SHA ハッシュ AES 暗号化 乱数生成	データパスワード入力 データパスワードの照合 乱数データの生成と参照 データ暗号鍵の再設定	無効	有効
	ファームウェアダウンロードコマンド	CMAC メッセージ認証 SHA ハッシュ AES 復号	ダウンロードパスワード入力 CMAC 鍵参照 ファームウェア復号鍵参照		

(3) 認証

本暗号モジュールは、ユーザ役割とクリプトオフィサ役割に対して認証のメカニズムを持たない。ユーザ役割、及びクリプトオフィサ役割は暗黙的に選択される。ただし、ATA セキュリティ機能を有効にした場合、ATA セキュリティ機能の範囲内においてパスワードによりユーザデータを保護する。

5. 物理的セキュリティ

本製品は、マルチチップ組込型暗号モジュールであり、JIS X 19790 物理的セキュリティ要求事項のレベル 1 を満たす。

6. 動作環境

本暗号モジュールは、限定動作環境をサポートする。従って、動作環境のセキュリティ要件は、適用除外とされる。

7. 暗号鍵管理

(1) 乱数ビット列生成器(RBG)

本暗号モジュールは、RBG を単体で採用し、データ暗号鍵の生成／初期化に使用する。RBG 及びその動作モードは JCMVP 運用ガイダンス(JIG-01 2008 年 8 月 7 日版)を適用し、NIST Special Publication 800-90 に適合している。

(2) 鍵確立、及び鍵の出力

本暗号モジュールは、鍵確立を用いていない。また、鍵を外部に出力しない。

(3) 鍵生成、鍵の入力、鍵の格納、及び鍵のゼロ化

表 6 鍵管理一覧

CSP	用途、生成／入力、格納、ゼロ化
データ暗号鍵	ユーザデータの暗号化、復号に用いられる。 乱数ビット列生成器によって生成される。 暗号モジュール内でデータパスワードを用いて暗号化され、オペレータからはアクセスできない領域に格納される。 データ暗号鍵初期化コマンドでゼロ化され、再設定される。
データパスワード	ユーザデータアクセス権の確認、およびデータ暗号鍵の暗号化に用いられる。 ATA セキュリティ系コマンドでホストから平文で入力され､RAM 上に展開される。 データパスワードを伴うコマンド処理が完了すると RAM 上に展開された平文のデータパスワードは消去される。
データパスワード認証データ	ユーザデータアクセス権の確認に用いられる。 ATA の Security Set Password コマンドでホストから平文で入力されたデータパスワードはハッシュ化され、オペレータからはアクセスできない領域に格納される。 オペレータからは無効化できない。
ファームウェア MAC 鍵	ダウンロードされたファームウェアの認証に用いられる。 開発時に生成、ダウンロードパスワードを用いて暗号化され、オペレータからはアクセスできない領域に格納される。 オペレータからは無効化できない。
ダウンロードパスワード	ファームウェア MAC 鍵、ファームウェア復号鍵の暗号化に用いられる。 開発時に生成される。 ファームウェアダウンロード時にホストから平文で入力され、RAM 上に展開される。 ファームウェアダウンロードコマンド処理が完了すると RAM 上から消去される。
ファームウェア復号鍵	ダウンロードされたファームウェアの復号に用いられる。 開発時に生成、ダウンロードパスワードを用いて暗号化され、オペレータからはアクセスできない領域に格納される。 オペレータからは無効化できない。
乱数データ	乱数の生成に用いる内部データ。 エントロピーにより生成される。 RAM 上に格納される。 乱数の生成が終了するとゼロ化される。

8. 自己テスト

(1) パワーアップ自己テスト

本暗号モジュールは、電源投入時にパワーアップ自己テストを開始する。オペレータは、本暗号モジュールの電源切断・投入によって、パワーアップ自己テストをオンデマンドで開始することができる。

本暗号モジュールは、次のパワーアップ自己テストを実行する。

a) 暗号アルゴリズムテスト

表 7 暗号アルゴリズムテスト一覧

機能	アルゴリズム	テスト
暗号化・復号	AES-256	既知解テスト
ハッシュ	SHA-256	既知解テスト
メッセージ認証	CMAC	既知解テスト
乱数生成	Hash_DRBG	既知解テスト

b) RBG エントロピーテスト

最小エントロピーの評価を行う。

c) ファームウェア完全性テスト

ファームウェアは 32 ビットの CRC を持ち、格納先から RAM にロードされる時に完全性を確認する。

d) 重要機能テスト

MPU のバスのテスト、内部レジスタのライト／リードテスト、ワーク RAM のライト／リードテスト、及びデータバッファのライト／リードテストなどを実施する。

(2) 条件自己テスト

本暗号モジュールは、該当するセキュリティ機能がよびだされる時に次の条件自己テストを実行する。

a) ファームウェアロードテスト

ダウンロードされるファームウェアはメッセージ認証として CMAC が適用される。

b) 連続乱数ビット列生成器テスト(RBG テスト)

新たにブロックを生成し、直前に生成したブロックと等しくないことを確認する。NIST Special Publication 800-90 で要求しているヘルステストを実行する。

9. 設計保証

本暗号モジュールには次のドキュメントがある。

- MHZ2080 CJ, MHZ2120 CJ, MHZ2160 CJ, MHZ2200 CJ, MHZ2250 CJ, MHZ2320 CJ ハードディスクドライブ プロダクト／メンテナンスマニュアル

以下、上記ドキュメントを装置マニュアルと称する。

(1) 構成管理及び開発

本暗号モジュールの機能仕様は、装置マニュアルに記載されている。

本暗号モジュールの構成管理及び開発は、ISO9001:2000 認証取得済みの品質マネジメントシステムにのっとり実施される。

(2) 配布及び運用

本暗号モジュールは、PC などのホストに内蔵されて動作するものであり、以下の内容が装置マニュアルに記載されている。

- ドライブ(本暗号モジュール)の設置方法
- パワーオン(電源投入)時のホストの手順
- データパスワード設定などのホストコマンドインタフェース

(3) ガイダンス文書

ガイダンス文書は、装置マニュアルとして提供される。クリプトオフィサガイダンス及びユーザガイダンスは、同文書に記載されている。

10. その他の攻撃への対処

本暗号モジュールは、その他の攻撃へ対処しない。

11. 参考文献

(1) JIS X 19790：2007 セキュリティ技術－暗号モジュールのセキュリティ要求事項

(2) JIS X 5091：2007 セキュリティ技術－暗号モジュールのセキュリティ試験要件

(3) IPA 承認されたセキュリティ機能に関する仕様（ASF-01） 平成 20 年 4 月 7 日

(4) IPA JCMVP 暗号アルゴリズム実装試験要件（ATR-01） 平成 19 年 10 月 29 日

(5) IPA JCMVP 運用ガイダンス（JIG-01） 平成 20 年 8 月 7 日

(6) FIPS PUB 197, Advanced Encryption Standard (AES), November 26, 2001

(7) FIPS PUB 180-2 with Change Notice 1, Secure Hash Standard, February 25, 2004.

(8) Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology Special Publication 800-38B, May 2005.

(9) Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), National Institute of Standards and Technology Special Publication 800-90, March 2007.