暗号化ストレージの
プロテクションプロファイルと
FIPS140認定の動向

JNSA 第2回 鍵管理勉強会
2012.07.03

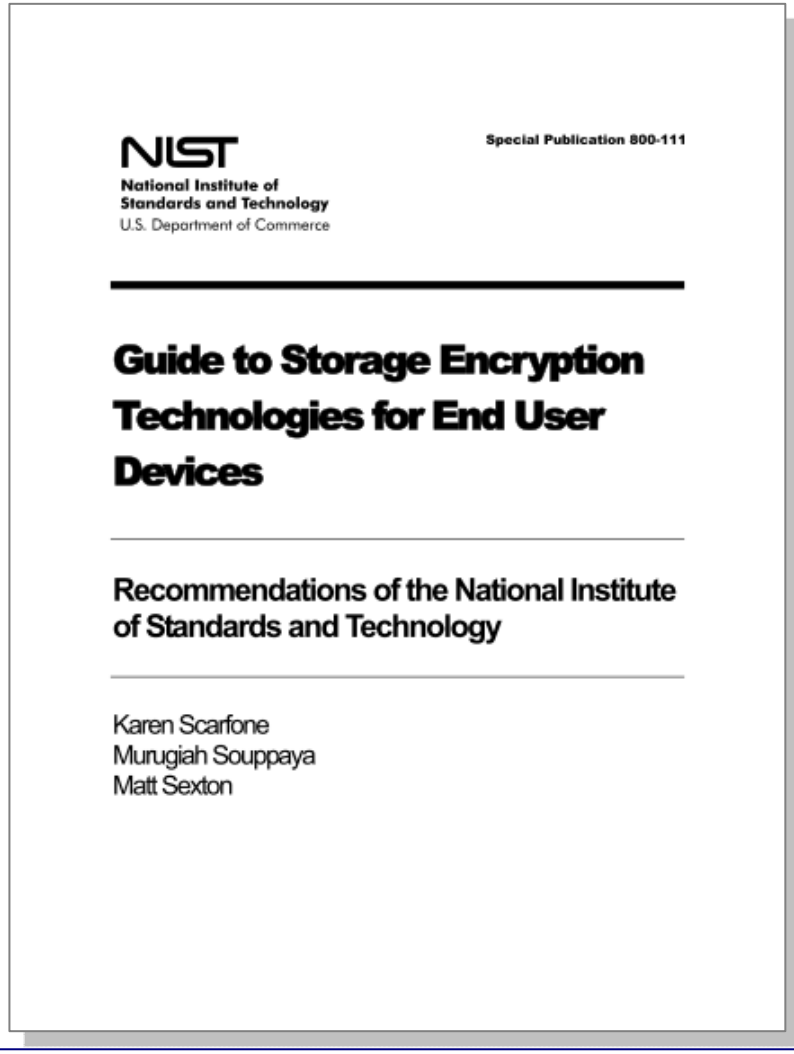
小川　博久

みずほ情報総研

内容

1. NIST SP800-111の概要（暗号関連部分）
2. 第三者評価制度と認証スキーム
   CMVP（FIPS140-1/2）とCC（ISO/IEC 15408）
3. CMVPの要件
4. CCの要件（CPP）
5. まとめ

NIST SP 800-111



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-111

Guide to Storage Encryption Technologies for End User Devices

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Murugiah Souppaya
Matt Sexton

Table of Contents

SP800-111のセキュリティ要件に関連する記述

- 2.2 The Need for Storage Security
  - Federal Information Security Management Act of 2002 (FISMA)
    - NIST SP 800-53
  - OMB Memorandum M-06-16
  - Privacy Act of 1974
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - NIST SP 800-66
    - Electronic Protected Health Information (EPHI)

- 4.2.1 Cryptography
  - Federal agencies must use FIPS-approved algorithms contained in validated cryptographic modules.

米国の政府調達の動向

- SP800-111で示されたセキュリティ要件は、FIPS140-2認証取得（CMVP）である。

- 一方、政府調達用のセキュリティ要件には、他の動き（CCの利用）もある。

- はじめに、この動向について説明します。

何故、ふたつの制度によるセキュリティ要求が存在するのか？

- CMVPは・・・
  - セキュリティ要件をレベルごとに定義。
  - 例えば、ディスク内のデータの暗号をAESに限定することは示せない。

- CCは・・・
  - セキュリティ要求仕様は、Protection Profile（PP）で任意に設定することが可能。
  - 例えば、ディスク内のデータの暗号をAESに限定することを示せる。

※1：セキュリティ機能に対する（保証）要件を意味します。

CCの新しい動き

- **各国共通の政府調達のセキュリティ要件を策定：**
  Collaborative Protection Profile（CPP）※2
  a. **ひとつの技術分野にひとつの要件**
  b. **ミニマムなベースライン要件**
  c. **詳細なテスト方法をセキュリティ要件に明記**
  d. **開発文書中心の評価から脆弱性テストに重点を置いた評価へ**

**CCでは暗号利用に関するセキュリティ要件の詳細な記述（特に、上記のc等の調査なテスト）はない。
そのため、NIST SP 800-53によるサポートが必須。**

※2：情報セキュリティ製品における政府調達の動向から抜粋 http://www.ipa.go.jp/security/event/2012/ist-expo/documents/preso_15.pdf

日本国を含む各国の動き

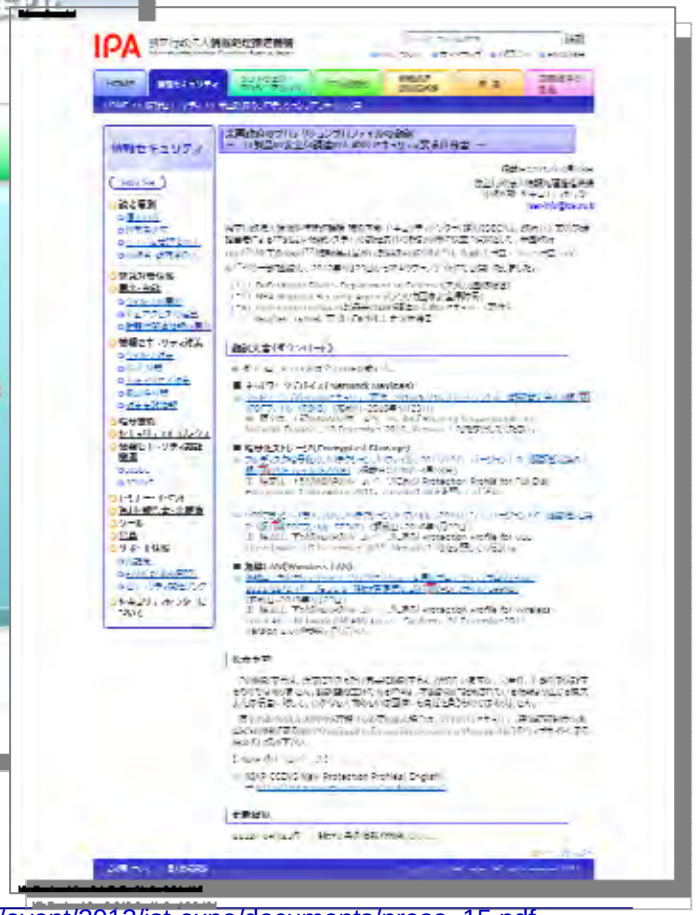
IPA

海外の政府調達の動向

日本発の適合製品がさまざまな技術分野に

今後、海外の政府調達の対象となる製品分野

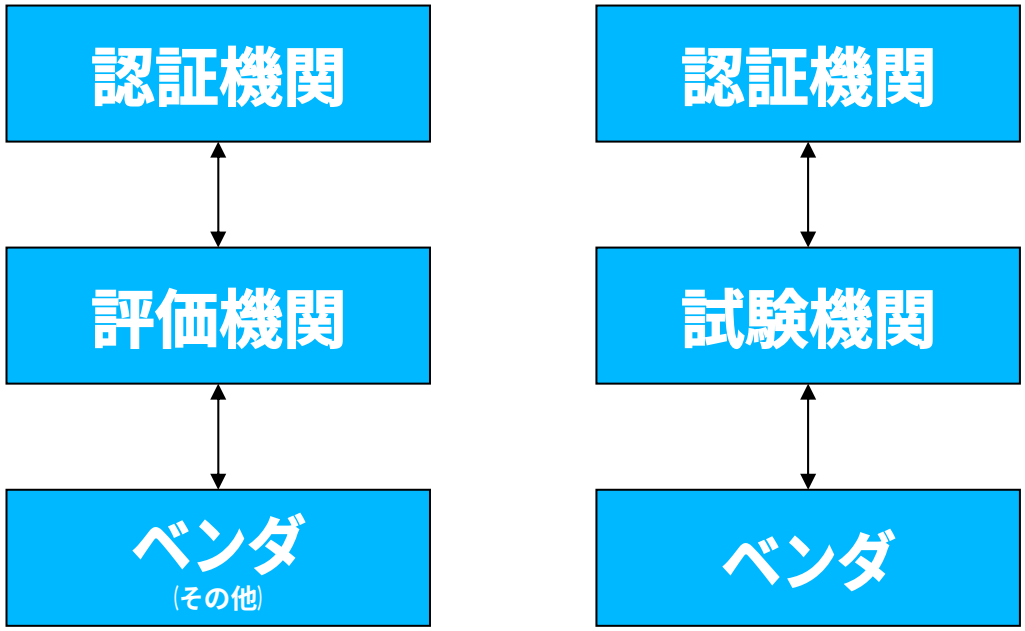
- ネットワーク関連製品
  - 無線LANアクセスシステム、IPsec VPNゲートウェイ、認証サーバー、仮想化製品、企業向けセキュリティ管理製品（北米、欧州、アジア各国）
- 暗号化製品（USBドライブ等）
  - USB暗号化製品、ハードディスク暗号化製品、ファイル暗号化製品（米国、欧州）
- モバイル関連製品
  - SIPサーバー、VoIPアプリケーション、モバイル端末、MDM（北米、欧州、豪州）
- その他
  - Smart Meter ゲートウェイ（欧州）



※情報セキュリティ製品における政府調達の動向から抜粋 http://www.ipa.go.jp/security/event/2012/ist-expo/documents/preso_15.pdf

CCとCMVPの認証スキーム

- CC(左)とCMVP(右)の認証スキーム
- 評価と試験の違いのみ。



国際的な総合認証の動きは異なる。CCにはCCRAというアレンジメントがあるが、CMVPには日本(IPA)と米(NIST)の共同認証のみ。カナダ(CSEC)等は別。

※IPA と米国 NIST との合意に基づく初の暗号モジュール共同認証を完了 http://www.ipa.go.jp/about/press/pdf/120412press.pdf

※共同認証の流れ http://www.ipa.go.jp/about/press/pdf/120227press2.pdf

各セキュリティ要件の調査方法について

- CMVPは、事例を調査する。

- CCは、CPPのセキュリティ要件を調査する。
（CPPは要求仕様なので事例は無し）

はじめに、CMVPから説明。

CMVPの認証取得モジュールについて

■HDDのFDE

- レベル2：有
- レベル3：有

■USBメモリ（フラッシュのみTokenを除く）

- レベル2：有
- レベル3：有

FIPS140-1/2　FDEの認定取得情報（抜粋）

Cert#	Vendor / CST Lab	Cryptographic Module	Module Type	Val. Date	Level / Description
1626	ViaSat UK Ltd.	**FlagStone Core**	Hardware	10/31/2011	***Overall Level:* 2** -Physical Security: Level 3 *-FIPS-approved algorithms:* AES (Certs. #922 and #923); RNG (Cert. #531) *-Other algorithms:* N/A Multi-chip embedded
1133	ViaSat UK Ltd.	**FlagStone Core** *(When operated in FIPS mode)* Security Policy Certificate	Hardware	05/22/2009;	***Overall Level:* 2** -Physical Security: Level 3 *-FIPS-approved algorithms:* AES (Certs. #922 and #923); RNG (Cert. #531) *-Other algorithms:* N/A Multi-chip embedded
779	ViaSat UK Ltd.	**FlagStone Core**	Hardware	05/18/2007;	***Overall Level:* 2** -Physical Security: Level 3 *-FIPS-approved algorithms:* AES (Certs. #403 and #630); RNG (Certs. #198 and #361) *-Other algorithms:* Multi-chip embedded
477	Secure Systems Limited	**Silicon Data Vault® (SDV®)**	Hardware	11/04/2004	***Overall Level:* 1** *-FIPS-approved algorithms:* AES (Cert. #136); SHS (Cert. *-Other algorithms:* CRC-32 Multi-chip embedded
1601	McAfee, Inc.	**McAfee Endpoint Encryption for PCs**	Software	09/08/2011;	***Overall Level:* 1** -Operational Environment: Tested as meeting Level 1 with Windows XP 32-bit; Windows Vista 64-bit (single-user mode) *-FIPS-approved algorithms:* AES (Cert. #1366); DSA (Cert. #446); SHS (Cert. #1247); RNG (Cert. #752) *-Other algorithms:* Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength); NDRNG Multi-chip standalone
1364	Marvell Semiconductor, Inc.	**Solaris 2**	Hardware	07/21/2010	***Overall Level:* 2** *-FIPS-approved algorithms:* AES (Certs. #1153 and #723); SHS (Cert. #1067); HMAC (Cert. #656); RSA (Cert. #545); RNG (Cert. #638) *-Other algorithms:* AES (Cert. #1153, key wrapping; key establishment methodology provides 128 bits of encryption strength); Single-chip

FIPS140-1/2　FDEの認定取得情報（抜粋）-2

Seagate Technology LLC	1299 - Seagate Secure® Enterprise Self-Encrypting Drives FIPS 140 Module 1388 - Momentus® FDE Drives FIPS 140 Module 1451 - Seagate® Momentus® Thin Self-Encrypting Drives TCG Opal FIPS 140 Module 1635 - Seagate Secure Constellation® ES.2, Savvio® 10K.5 and Savvio® 15K.3 Self-Encrypting Drives FIPS 140 Module 1636 - Seagate Secure Constellation® ES and Constellation®.2 Self-Encrypting Drives FIPS 140 Module 1688 - Momentus® FDE Attached Storage Drives FIPS 140 Module

FIPS 140-1 and FIPS 140-2 Vendor Listから抜粋

FIPS140-1/2　USB Flashの認定取得情報（抜粋）

Cert#	Vendor / CST Lab	Cryptographic Module	Module Type	Val. Date	Level / Description
1712	Kanguru Solutions	**Kanguru Defender 2000**	Hardware	05/03/2012	***Overall Level:* 2** -Cryptographic Module Specification: Level 3 *-FIPS-approved algorithms:* HMAC (Cert. #954); AES (Cert. #1623); SHS (Cert. #1432); RSA (Cert. #801); DRBG (Cert. #86); PBKDF (vendor affirmed) *-Other algorithms:* NDRNG; RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength) Multi-chip standalone
1570	SanDisk Corporation	**Cruzer Enterprise FIPS Edition**	Hardware	08/12/2011	***Overall Level:* 2** *-FIPS-approved algorithms:* AES (Certs. #1432 and #1433); RSA (Cert. #702); SHS (Cert. #1295); RNG (Cert. #779) *-Other algorithms:* RSA (encrypt/decrypt) Multi-chip embedded
1555	BlockMaster AB	**BM-C1000**	Hardware	06/07/2011	***Overall Level:* 2** -Mitigation of Other Attacks: Level 3 *-FIPS-approved algorithms:* AES (Cert. #1236); SHS (Cert. #1134); RNG (Cert. #683), RSA (Cert. #617) *-Other algorithms:* NDRNG; RSA-512 (non-compliant) Multi-chip embedded
1527	Systematic Development Group, LLC	**LOK-IT™ 10 KEY (Series SDG003FM) and LOK-IT™ 5 KEY (Series SDG004FP)**	Hardware	03/28/2011;	***Overall Level:* 3** *-FIPS-approved algorithms:* AES (Cert. #1514) *-Other algorithms:* N/A Multi-chip standalone
1438	Kingston Technology, Inc.	**DataTraveler 6000**	Hardware	11/03/2010	***Overall Level:* 3** *-FIPS-approved algorithms: AES (Certs. #1259, #1260, #1261, #1262, #1263 and #1264); SHS (Certs. #1155, #1156, #1157, #1158, #1159, #1160, #1161, #1162 and #1163); ECDSA (Certs. #147, #148 and #149); DRBG (Certs. #29, #30 and #31); RNG (Certs. #703, #704* *-Other algorithms:* EC Diffie-Hellman (key agreement; key establishment methodology provides 128, 192 or 256 bits of encryption strength) Multi-chip standalone

Module Validation Listsから抜粋

FIPS140-1/2 USB Flashの認定取得情報(抜粋)-2

Kingston Technology Company, Inc.	929 - Kingston S2 CM 1227 - DataTraveler 5000 (DT5000) 1306 - Kingston DataTraveler DT4000 Series USB Flash Drive 1316 - DataTraveler 5000 1438 - DataTraveler 6000
Spyrus, Inc.	5 - FORTEZZA Crypto Card, v0.2 22 - LYNKS Metering Device (LMD) 46 - LYNKS Metering Device (LMD) 48 - FORTEZZA Crypto Card and Jumbo FORTEZZA Crypto Card 78 - LYNKS Privacy Card 95 - Rosetta Smart Card 144 - Rosetta USB 157 - Rosetta USB 166 - Rosetta USB 167 - Rosetta Smart Card 369 - Rosetta CSI sToken 561 - LYNKS Privacy Card 679 - LYNKS Series II 1179 - Hydra PC Personal Edition FIPS Module 1215 - Hydra PC FIPS Sector-based Encryption Module 1255 - Hydra PC FIPS Sector-based Encryption Module 1302 - SPYCOS® Module 1394 - Hydra PC FIPS Sector-based Encryption Module
Imation Corp.	748 - Stealth MXP 777 - Stealth MXP Passport 937 - MXI Cryptographic NAND Controller (CNC) 938 - Imation Secure Flash Drive Cryptographic Module 987 - Stealth MXP 988 - Stealth MXP Passport 1022 - Outbacker MXP 1149 - Imation S200/D200 1269 - Bluefly Processor 1397 - Imation Secure Flash Drive 1442 - Imation S200/D200 1479 - Imation S200/D200

FIPS 140-1 and FIPS 140-2 Vendor Listから抜粋

CMVPの認証取得モジュールの実装例(１)

Stealth MXP and Stealth MXP Passport (#988) Memory Experts International Inc.

- Random number generation
- Key generation with internal or external entropy
- Symmetric encryption/decryption (AES)
- Asymmetric signing and verification (RSA)
- Asymmetric encryption and decryption (RSA)
  Note: RSA encryption and decryption are non-FIPS approved services.
- Open Authentication HMAC (keyed-hash message authentication code)
- One Time Password (OATH HOTP)
- Secure hash (SHA-1 and SHA-256) and
- Compliance with industry standards such as ANSI X9.31, PKCS #1
- (Public-Key Cryptography Standards) and SAML 1.1.

CMVPの認証取得モジュールの実装例(1)

Stealth MXP and Stealth MXP Passport (#988) Memory Experts International Inc.

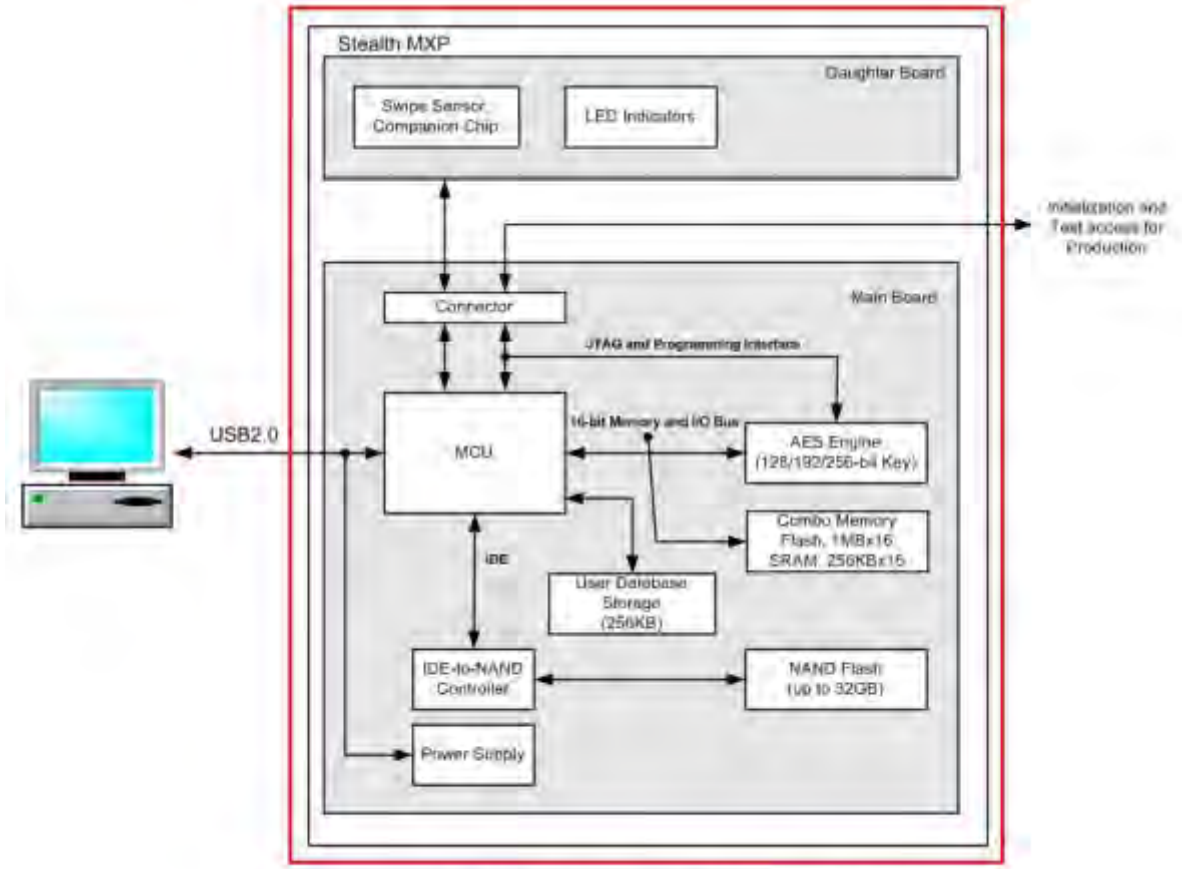


Figure 7: Block Diagram of Stealth MXP

CMVPの認証取得モジュールの実装例(２)

JumpDrive SAFE S3000（#1205）Lexar Media, Inc.

Approved mode of operation

The cryptographic module supports FIPS Approved algorithms as follows:

Security Functions	Cert #.	Description
AES	990, 877	CBC/ECB Encryption and Decryption
TDES	719	CBC/ECB Encryption and Decryption
RNG	503	ASNI X9.31 RNG
SHA-1	869	Hashing algorithm
SHA-256	957, 869	Hashing algorithm
HMAC-SHA-1	491	Keyed hashing algorithm
RSA(1024 and 2048)	424	Sign\Verify (PKCS #1.5) with SHA-1

CMVPの認証取得モジュールの実装例(３)

Approved Algorithms
- AES 256 bit (CBC), NIST certification #1514

Non-Approved Algorithms
- There are no non-approved algorithms.

CMVPのセキュリティ要件

	セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
暗号モジュールの仕様	暗号モジュール，暗号境界，承認されたアルゴリズム，承認された動作モードの仕様。すべてのハードウェア，ソフトウェア，ファームウェアの構成要素を含む暗号モジュールの記述。暗号モジュールのセキュリティポリシの宣言。			
暗号モジュールのポート及びインタフェース	必す(須)のインタフェース及び選択可能なインタフェース。すべてのインタフェースの仕様及びすべての入出力データパスの仕様。		他のデータポートから論理的に分離された，CSPのためのデータポート。	
役割，サービス，及び認証	必す(須)の役割及びサービスと選択可能な役割及びサービスとの論理的な分離。	役割ベースのオペレータ認証又はIDベースのオペレータ認証。	IDベースのオペレータ認証。	
有限状態モデル	有限状態モデルの仕様。必す(須)の状態及び選択可能な状態。状態遷移図及び状態遷移の仕様。			
物理的セキュリティ	製品グレードの装置。	錠又はタンパー証跡。	カバー及びドアに対してのタンパー検出及びタンパー応答。	タンパー検出及びタンパー応答が可能な包被。EFP又はEFT。
動作環境	単一のオペレータ。実行可能なコード。承認された完全性技術。	参照PPに適合し，EAL2の条件で評価を受けた環境。EAL2の条件で評価を受け，任意アクセス制御機構及び監査機構をもつ環境。	参照PPに加え，高信頼パスに適合し，EAL3に加え，セキュリティポリシのモデル化の条件で評価を受けた環境。	参照PPに加え，高信頼パスに適合し，EAL4の条件で評価を受けた環境。
暗号鍵管理	鍵管理機構：乱数生成及び鍵生成，鍵確立，鍵配送，鍵入出力，鍵の保管，並びに鍵のゼロ化。			
	手動の転送方法を用いて転送された秘密鍵及びプライベート鍵は，平文の形式で入力又は出力してもよい。		手動の転送方法を用いて転送された秘密鍵及びプライベート鍵は，暗号化又は知識分散処理を用いて，入力又は出力されなければならない。	
自己テスト	パワーアップ自己テスト：暗号アルゴリズムテスト，ソフトウェア/ファームウェア完全性テスト及び重要機能テスト。条件自己テスト。			
設計保証	構成管理。セキュアな設置及び生成。設計とポリシとの対応。ガイダンス文書。	構成管理システム。セキュアな配送。機能仕様。	高級言語による実装。	セキュリティポリシのセキュリティルール、特徴を記述する形式的モデルの規定
その他の攻撃への対処	攻撃への対処の仕様。 現在は，試験可能な要求事項は用意されていない。			試験可能な要求事項を備えた，攻撃への対処の仕様。

※引用）IPA 暗号モジュール試験及び認証制度のご紹介
http://www.ipa.go.jp/security/jcmvp/documents/open/jcmvp_seminar_090325.pdf

FDEの実装例（Seagate Level2 #1299,1388）

6 Physical Security

6.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation,
- Exterior of the drive is opaque,
- Opaque, tamper-evident security labels which cannot be penetrated or tamper-evidence.
- Security labels cannot be easily replicated with a low attack time.
- Security label on the exposed (back) side of the PCBA protects physic board removal,

- Security labels on side of drive to provide tamper-evidence of HDA c

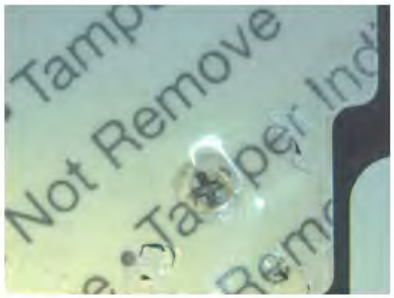
Momentus FDE Drives, FIPS 140 Module Security Policy Rev. 2.1

6.2 Operator Requirements

The operator is required to inspect the CM periodically for one or more of the following tamper evidence:

- Checkerboard pattern on security label or substrate,

- Security label over screws at indicated locations is missing or penetrated,



- Text (including size, font, orientation) on security label does not match original,
- Security label cutouts do not match original.

Upon discovery of tamper evidence, the module should be removed from service.

FDEの実装例（ Zyt Cryptographic Module Level3）

Figure 1 – Image of the Cryptographic Module

CMVP事例調査のまとめ

1. AES256bit及びTDESが実装されている。
2. 「暗号化鍵」をアクティベートする「認証」がある。
3. 「認証」に、様々なレパートリがある。
（公開鍵暗号、バイオメトリクス暗号、PIN／パスワード等）
4. 認証後に、フラッシュメモリの書き込み時に暗号化、読み出し時に復号される。
5. フラッシュメモリ自体には、セキュリティ機能は実装されていない。（フラッシュメモリとは別にセキュリティ機能が実装されている）
6. 「暗号化鍵」「暗号化」チップに耐タンパー性がある場合（Level3）と、モジュール自体のタンパ証跡のみの場合（Level2）がある。

CCのセキュリティ要件

ここからは、CCのセキュリティ要件

- PP for FDE
  (Protection Profile for Full Disk Encryption)

- PP for USB Flash
  (Protection Profile for USB Flash Drives)

※暗号利用（CCの用語では、暗号サポートクラス）に関するセキュリティ要件は同じ。

PP-USB Flash(機能クラス)

機能クラス	機能コンポーネント
暗号サポートクラス(FCS)	FCS_CKM.1(1) 暗号鍵生成(DEK)
暗号サポートクラス(FCS)	FCS_CKM.1(2) 暗号鍵生成(KEK)
暗号サポートクラス(FCS)	FCS_CKM.1(3) 暗号鍵生成(パスフレーズ条件付け)
暗号サポートクラス(FCS)	FCS_CKM_EXT.4 暗号鍵とする材料の破棄
暗号サポートクラス(FCS)	FCS_COP.1(1) ディスク暗号化
暗号サポートクラス(FCS)	FCS_COP.1(2) 署名検証
暗号サポートクラス(FCS)	FCS_COP.1(3) 暗号技術的ハッシュ
暗号サポートクラス(FCS)	FCS_COP.1(4) 鍵のマスキング
暗号サポートクラス(FCS)	FCS_RBG_EXT.1 拡張:ランダムビット生成
利用者データ保護クラス(FDP)	FDP_DSK_EXT.1 拡張:ディスク上のデータの保護
識別及び認証のクラス(FIA)	FIA_AUT_EXT.1 拡張:FDE利用者認証
セキュリティ管理クラス(FMT)	FMT_SMF.1 管理機能の特定
TSFクラスの保護	FPT_TUD_EXT.1 高信頼更新
TSFクラスの保護	FPT_TST_EXT.1 TSFのテスト

PP-USB Flash(主な暗号サポートクラスの記述)

FCS_COP.1 (1)	暗号操作(ディスク暗号化)
FCS_COP.1.1 (1)	詳細化:TSFは、FIPS PUB 197「Advanced Encryption Standard (AES)」及び[選択:NIST SP 800-38A、NIST SP 800-38C、NIST SP800-38E]を満たす[選択:CBC、CCM、CFB128、CTR、OFB、XTS]モード及び暗号鍵サイズ[選択:128ビット、256ビット]で使用される、特定された暗号アルゴリズムAESに従って、暗号化と復号を実行しなければならない。

FCS_COP.1 (2)	暗号操作(署名検証)
FCS_COP.1.1 (2)	詳細化:TSFは、以下に従ってTOE更新の暗号署名検証を実施しなければならない。[選択: (1) 2048ビット以上の鍵サイズ(係数)のデジタル署名アルゴリズム(DSA) (2) 2048ビット以上の鍵サイズ(係数)のRSAデジタル署名アルゴリズム(rDSA)、または (3) 256ビット以上の鍵サイズの楕円曲線デジタル署名アルゴリズム(ECDSA)]

FCS_COP.1 (3)	暗号操作(暗号ハッシュ)
FCS_COP.1.1 (3)	詳細化:TSFは、以下のFIPS Pub 180-3「Secure Hash Standard」を満たす[選択:SHA-1、SHA 224、SHA 256、SHA 384、SHA 512]及びメッセージダイジェストサイズ[選択:160、224、256、384、及び512]ビットに従って、暗号ハッシュサービスを実行しなければならない。

FCS_COP.1 (4)	暗号操作(鍵のマスキング)
FCS_COP.1.1 (4)	詳細化:TSFは、[選択:XORの場合、「なし」;AESの場合、「FIPS PUB 197, Advanced Encryption Standard (AES)及び NIST SP 800-38A」]を満たす、指定された暗号アルゴリズム[選択:XOR;ECBモードで使用されるAES]及び暗号鍵サイズ[選択:128ビット、256ビット]に従って、鍵のマスキングを実行しなければならない。

PP-USB Flash(暗号鍵管理の概要)

暗号鍵管理;

適合する実装には、鍵暗号鍵(KEK)及びデータ暗号鍵(DEK)の少なくとも 2 個の鍵が含まれる。以下の要件は、鍵の生成方法を規定する。DEK の生成は、FCS_CKM.1(1) に規定されている。KEK は、FCS_CKM.1(2) で説明されているように 1 つまたは複数の認証要素から導出したサブマスクから作成される。認証要素は、必要なパスワードベースの認証要素(サブマスクを生成するための条件付けは FCS_CKM.1(3) に規定されている)及び(オプションで)ホスト分割認証要素(FCS_CKM.1(X1))及び / または PIN 保護方式のサブマスク(FCS_CKM.1(X2))から構成される。KEK の形成に寄付するサブマスクが導出される他の認証要素は、前述の認証要素から導出されるサブマスクと(XOR 関数を使用して)組み合わされる限り許される。

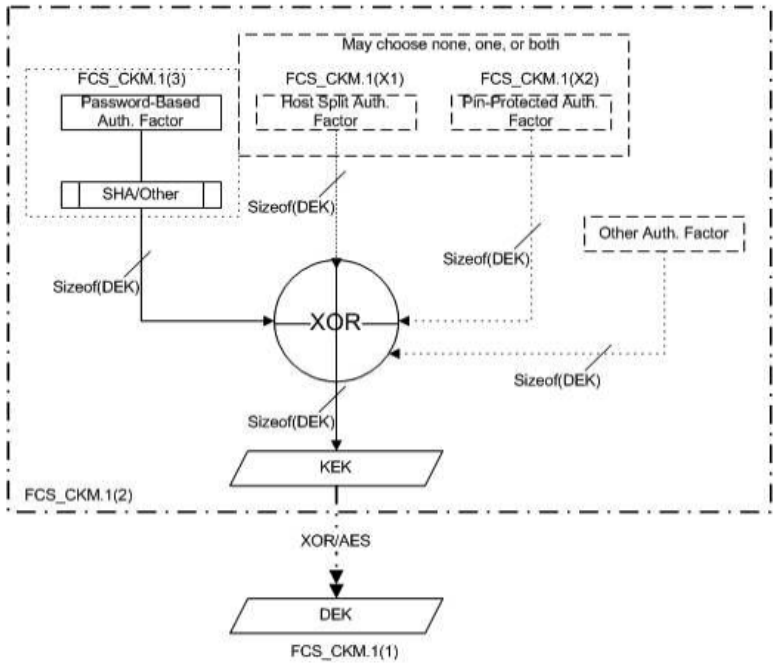


図 1 : KEK 導出オプション

CPP調査のまとめ

1. CMVPの事例調査と比べ、以下のアルゴリズムが指定された。
   - ディスク暗号化
   - 署名検証
   - 暗号ハッシュ
   - 鍵のマスキング
   - （ホスト分割認証要素：オプションによる）
2. 鍵暗号鍵（KEK）及びデータ暗号鍵（DEK）が明確に分離された。
3. 各種のテストは、CMVPを流用（参照）している。
   - AES／利用モード：The Advanced Encryption Standard Algorithm Validation Suite（AESAVS）［AESAVS］、The CCM Validation System（CCMVS）［CCMVS］、モンテカルロ、AESCCMの可変関連データテスト、可変ペイロードテスト、可変ナンステスト、可変タグテスト、The XTS-AES Validation System（XTSVS）［XTSVS］
   - RSA、DSA、ECDSAのテストベクターによるテスト
   - 暗号ハッシュ：The Secure Hash Algorithm Validation System（SHAVS）［SHAVS］
   - DRBGのThe Random Number Generator Validation System（RNGVS）［RNGVS］

本調査のまとめ(Data at Restの観点から)

	CMVP	CC
データ保護	要件 有	要件 有(詳細化)
鍵消去	要件 有	要件 有(詳細化)
耐タンパ (鍵の保護等)	要件 有	FIPS140-2参照※

※　FIPS140-2の参照以外には、明確に示されていないが、暗号鍵の利用や機能などから類推することはできる。

CMVPのPhysical Security のLevel2(タンパ証跡等)とLevel3(耐タンパ応答)では要件が大きく異なる。
本当に(Level3)ではなく、(Level2)でセキュリティを担保できる製品(技術分野)は何か？を明確にする必要があると考えられる。
(タンパ証跡の基本は、CO (Crypto Officer Role) 又はCU (Crypto User Role) が 証跡を確認する作業が求められる。つまり、FDEの場合は、PCを開けて、モジュール (HDDやSSD等) を確認する必要がある。)
((そんな確認作業を要求しますか？))