PCI-Express バス対応型
ハードウェアセキュリティモジュール
セキュリティポリシ

Ver 1.00

2013 年 8 月 9 日

NTT エレクトロニクス株式会社

改訂履歴

2013/08/09　　Ver 1.00

- 新規作成

目次

1. 概要

本書は、NTT エレクトロニクス(株)が製造する「PCI-Express バス対応型ハードウェアセキュリティモジュール」（以下、本装置と記す）の公開セキュリティポリシを示すものである。

本装置が準拠するセキュリティ要求事項、セキュリティ試験要件、暗号モジュールの形態、及びセキュリティレベルは以下のとおりである。

セキュリティ要求事項、セキュリティ試験要件：

JIS X 19790　　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

JIX X 24759:2009　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

暗号モジュールの形態：

マルチチップ組込型

セキュリティレベル：

レベル 3

1.1 参考文献

(1) JIS X 19790 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) JIX X 24759:2009 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 JCMVP 承認されたセキュリティ機能に関する仕様(ASF-01) 平成 25 年 2 月 13 日
(4) IPA JCMVP 暗号アルゴリズム実装試験要件(ATR-01) 平成 21 年 1 月 8 日
(5) IPA JCMVP 運用ガイダンス(JIG-01) 平成 25 年 2 月 13 日

別紙の一覧を以下に示す。

別紙 1：PCI-Express バス対応型 HSM コマンド I/F 仕様書
別紙 2：PCI-Express バス対応型 HSM 状態遷移図

1.2 用語、略語定義

AC
追加クリプトオフィサ(Additional Crypt Officer)役割
クリプトオフィサ役割によって付与された権限に従い、暗号モジュールの管理機能を実行する個人。

API
応用プログラムインタフェース（Application Program Interface)

CO
クリプトオフィサ(Crypt Officer)役割
暗号モジュールが機能するように、暗号関連の初期化又は管理機能を実行する個人。

CSP
クリティカルセキュリティパラメタ(Critical Security Parameter)
秘密又はプライベートセキュリティに関する情報であって、その開示又は変更が暗号モジュールのセキュリティを危殆化しうるもの。

FROM
Flash memory

HSM
Hardware Security Module

PKCS
Public-Key Cryptography Standards

PKCS#11
Cryptographic Token Interface Standard

PSP
公開セキュリティパラメタ(Public Security Parameter)
セキュリティに関連する公開情報であって、その変更が暗号モジュールのセキュリティを危殆化しうるもの。

RTC
Real Time Clock

SDRAM
Synchronous Dynamic Random Access Memory

SO
Security Officer。PKCS#11 の SO のことを示す。

SRAM
Static Random Access Memory

User
暗号サービスを受けるために暗号モジュールにアクセスする人。
PKCS#11 の normal user のことを示す。

2. 暗号モジュールの仕様

2.1 システム概要

本装置は、高度なセキュリティ鍵管理と、高速・安全な暗号処理を行う PCI Express ボード形態の製品である。

2.2 ハードウェア構成

本装置の概観図と暗号境界を図 2-1 及び図 2-2 に示す。

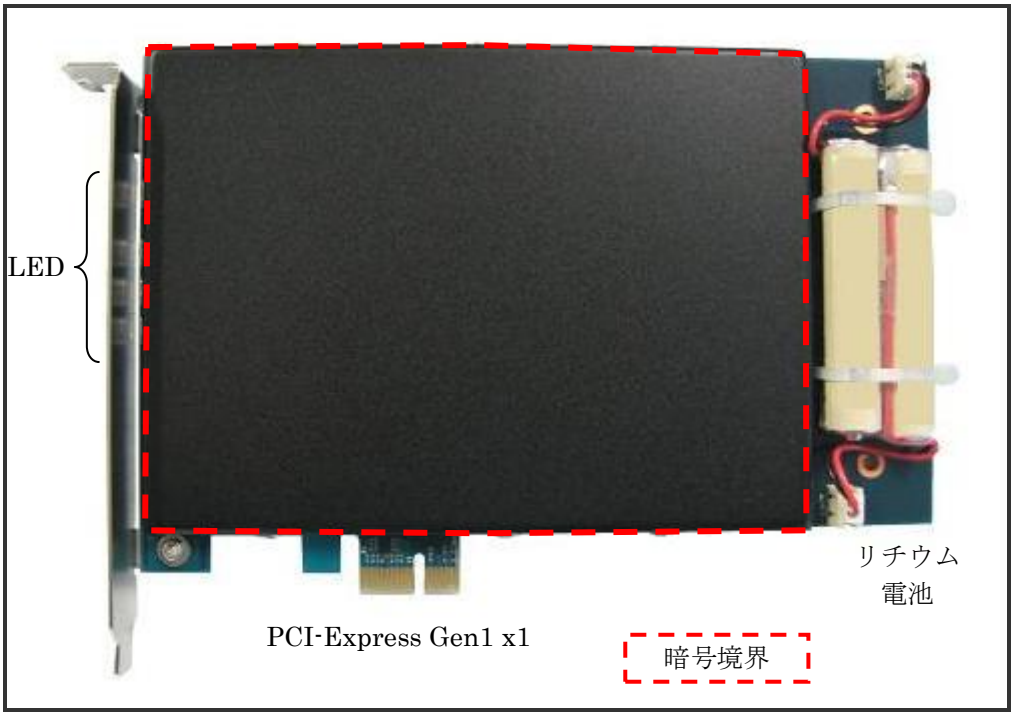

図 2-1 概観図（表）

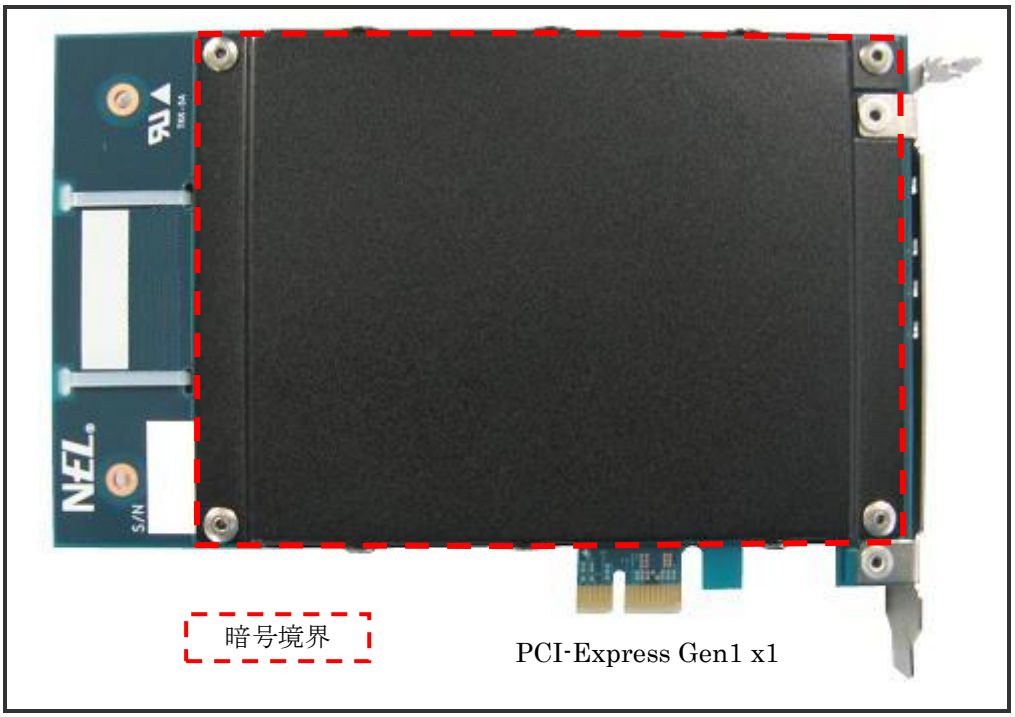

図 2-2 概観図（裏）

本装置のハードウェア構成図、および物理的暗号境界と外部との物理的ポートを図 2-3 に示す。物理的ポート（図中、網掛け部分）を以下に示す。

- PCI Express バス　　：データ入力、データ出力、制御入力、状態出力、電源
- LED 表示　　：状態出力
- バッテリーコネクタ　：電源（リチウム電池）

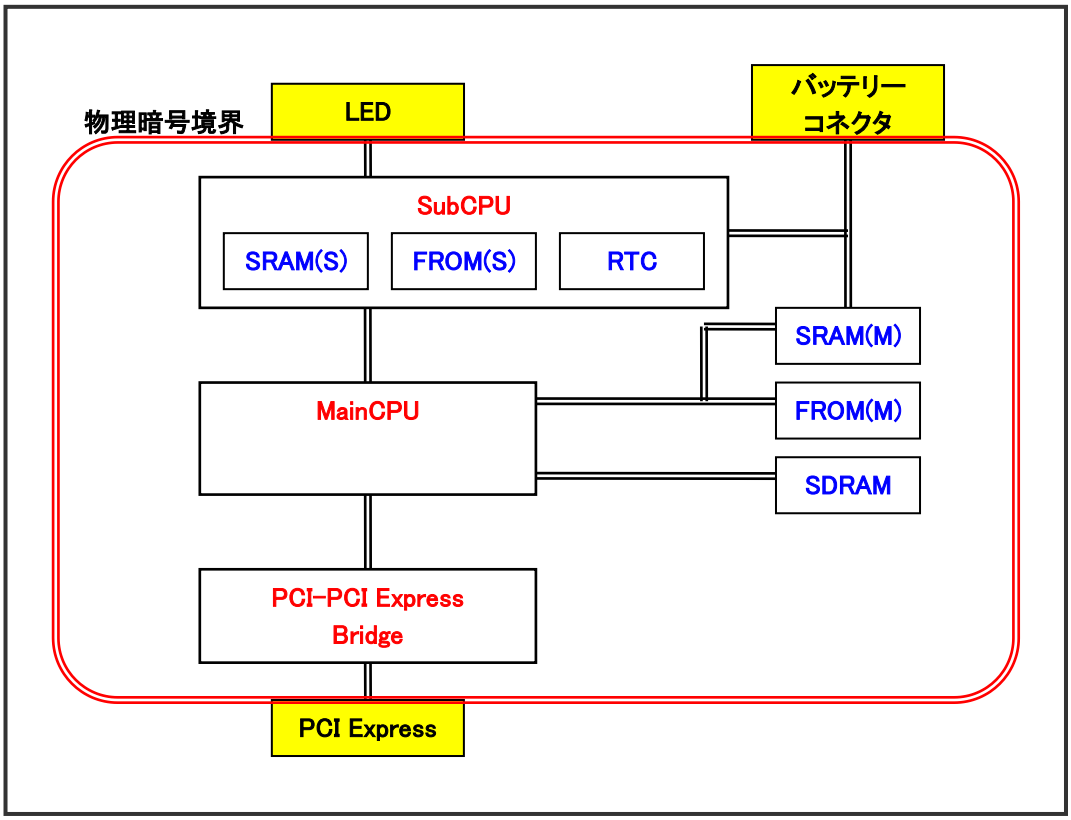

図 2-3 ハードウェア構成図

物理暗号境界内の役割を以下に示す。

- MainCPU　　：主プロセッサ。
- SubCPU　　：副プロセッサ。PCI Express バスから電源が供給されていない場合は、リチウム電池で動作し、タンパ応答を行う。
- PCI-PCI Express Bridge　：バス変換（PCI バス⇔PCI Express バス）
- SDRAM　　：大容量揮発性メモリ
- SRAM　　：暗号鍵、ログを格納。リチウム電池によりバックアップされる。（以下、MainCPU と接続されている SRAM を SRAM(M)、SubCPU 内の SRAM を SRAM(S)と記す。）
- FROM　　：不揮発性メモリ（ファームウェアを格納）（以下､MainCPU と接続されている FROM を FROM(M) 、SubCPU 内の FROM を FROM(S)と記す。）
- RTC　　：Real Time Clock（日付／時間）

2.3 ファームウェア構成

本装置に搭載されるファームウェアの機能概要を表 2-1 に示す。

表 2-1 ファームウェア機能概要

#	機能名	概要
1	管理機能	パスワードによるログイン、装置の設定、ログ管理等
2	監視機能	装置状態を監視
3	タンパ応答機能	タンパ検出時の秘密情報消去
4	自己診断機能	パワーアップ自己テスト、条件自己テスト
5	状態表示機能	LED 表示
6	暗号機能	鍵の生成／保存、鍵の削除、鍵のリスト取得、公開鍵の取得、暗号化／復号、署名生成等

2.4 動作モード

本装置は、以下に示す動作モードを有する。

(1) 承認動作モード

承認動作モードでは、表 2-3 に示す承認されたセキュリティ機能のみが動作し、表 2-4 に示す承認動作モードで使用できない承認されたセキュリティ機能、及び表 2-5 に示す承認されていないセキュリティ機能は動作しない。

(2) 非承認動作モード

非承認動作モードでは、表 2-3 に示す承認されたセキュリティ機能、表 2-4 に示す承認動作モードで使用できない承認されたセキュリティ機能、及び表 2-5 に示す承認されていないセキュリティ機能が動作する。

動作モードは、本装置の初期化時（InitHSM サービス実行時）にクリプトオフィサ役割のみが設定することができる。動作モードの切り替えは、再度初期化を行う必要がある。なお、初期化を行うと、本装置内のすべての秘密情報は初期化され、マスタ鍵、乱数シード、HSM Key Pair、及びクリプトオフィサ役割の初期 ID と初期パスワード（4 章参照）が再度生成・格納される。ただし、非承認動作モードから承認動作モードへ切り替える場合、InitHSM サービスを 2 回実行する必要がある。1 回目の InitHSM サービス完了後は機能制限の付いた承認動作モードとなり、2 回目の InitHSM サービス完了後に 4.1.1 章に記載のサービスが使用可能となる（別紙 2 参照）。

設定されている動作モードは、GetHSMInfo サービス、及び PCI コンフィグレーションレジスタに格納されているバージョン情報によって確認することができる。GetHSMInfo サービスの出力データのうち、171 バイト目が 0xC0（機能制限の付いた承認動作モード）又は 0x00 であること、かつ 176 バイト目が 0x00 であること。及び PCI コンフィグレーションレジスタの BAR1 領域のうち、バージョン情報が下記の値である場合に、承認動作モードにて動作中である。

表 2-2 バージョン情報

オフセット(Byte)	値
8～11	0x01, 0x1C, 0x14, 0xC7
12～15	0x01, 0x00, 0x00, 0x00
16～19	0x01, 0x22, 0x00, 0x00
20～23	0x01, 0x01, 0x3A, 0xDA
28～31	0x01, 0x03, 0x13, 0x17

※ オフセットは BAR1 領域の先頭からのオフセット値である。

2.5 セキュリティ機能

本装置が提供する、承認されたセキュリティ機能を表 2-3 に、承認動作モードで使用できない承認されたセキュリティ機能を表 2-4 に、承認されていないセキュリティ機能を表 2-5 に示す。

表 2-3 承認されたセキュリティ機能

カテゴリ	アルゴリズム
公開鍵＜署名：署名生成、署名検証＞	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)
公開鍵＜守秘：暗号化、復号＞	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)
共通鍵＜64 ビットブロック暗号：暗号化、復号＞	3-key Triple Des (SP800-67) 暗号利用モード：ECB, CBC
共通鍵＜128 ビットブロック暗号：暗号化、復号＞	AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB, CBC
ハッシュ	Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4)
メッセージ認証	HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1)
乱数生成器	HASH-DRBG (SP800-90A, SHA-256)

表 2-4 承認動作モードで使用できない承認されたセキュリティ機能

カテゴリ	アルゴリズム
公開鍵＜守秘：暗号化、復号＞	RSA-OAEP (PKCS#1 v2.1) (2,048～4,096bit)

表 2-5 承認されていないセキュリティ機能

カテゴリ	アルゴリズム
公開鍵＜署名：署名生成、署名検証＞	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (1,024bit) RSA (No Padding) (1,024～4,096bit)
公開鍵＜守秘：暗号化、復号＞	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (1,024bit) RSA-OAEP (PKCS#1 v2.1) (1,024bit) RSA (No Padding) (1,024～4,096bit)
共通鍵＜64 ビットブロック暗号：暗号化、復号＞	DES, 2-key Triple Des (SP800-67) 暗号利用モード：ECB, CBC
ハッシュ	Secure Hash Standard (SHA-1) (FIPS PUB 180-4) MD5 (RFC1321)
メッセージ認証	HMAC-SHA-1 (FIPS PUB 198-1) HMAC-MD5 (RFC2403)

2.6 セキュリティレベル

JIS X 19790 の各セキュリティ要求事項に対する本装置の実装されたセキュリティレベルを表 2-6 に示す。全体としてレベル 3 のセキュリティを満たす。

表 2-6 セキュリティ要求事項と実装レベル

#	分類	実装された セキュリティレベル
1	暗号モジュールの仕様	3
2	暗号モジュールのポート及びインタフェース	3
3	役割、サービス及び認証	3
4	有限状態モデル	3
5	物理的セキュリティ	3
6	動作環境	適用除外
7	暗号鍵管理	3
8	自己テスト	3
9	設計保証	3
10	その他の攻撃への対処	適用除外

3. ポート及びインタフェース

本装置は以下の物理的ポートを有する。

- PCI Express バス
- LED
- バッテリーコネクタ

物理的ポートは、表 3-1 に示す論理的インタフェースに分けられる。

表 3-1 論理的インタフェースと物理的ポートのマッピング

論理的インタフェース	物理的ポート
データ入力インタフェース	PCI Express バス（PIN：Side-B 14, 15）
データ出力インタフェース	PCI Express バス（PIN：Side-A 16, 17）
制御入力インタフェース	PCI Express バス（PIN：Side-B 14, 15）
状態出力インタフェース	PCI Express バス（PIN：Side-A 16, 17）、 LED
電源インタフェース	PCI Express バス（PIN：Side-B 1, 2, 3, 8, 10, Side-A 2, 3, 9, 10）、 バッテリーコネクタ

本装置はメンテナンスインタフェースを有していない。また、外部入力デバイス、及び外部出力デバイスは使用せず、ボタンやスイッチなどの手動制御機器を有していない。

本装置は 4 つの LED を有する。各 LED の概要を表 3-2 に示す。なお、LED は PCI Express バスから電源供給されている場合にのみ点灯する。

表 3-2 LED

色	略称	概要
緑	PWR	本装置が PCI Express バスとのリンクが確立している場合に点灯する。
赤	ERR	本装置においてエラーが発生した場合に点灯する。
緑	ID	GetHSMInfo サービスにて、LED 点灯を指定された場合に点灯する。
黄	EJT	SetControlFlag サービスにより本装置の取り外し許可が指定され、PCI Express バスから取り外せる場合に点灯する。

4. 役割、サービス、及び認証

本装置は ID ベース認証をサポートする。アカウント名とパスワードによってオペレータを個別に識別し、オペレータが担う役割の認可を認証する。以後、クリプトオフィサの役割を担うオペレータ（アカウント）をクリプトオフィサ役割(CO)、クリプトオフィサによって権限付与されるオペレータ（アカウント）を追加クリプトオフィサ役割(AC)、ユーザの役割を担うオペレータ（アカウント）をユーザ役割(User)と記す。メンテナンス役割は存在しない。

本装置内にマスタ鍵が格納されていない状態（InitHSM サービスを一度も実行していない状態等）において、PCI-Express バスから電源が供給されると、CO の初期 ID と初期パスワードに固定値を割り当てる。CO の初期 ID と初期パスワードは固定値であるが、InitHSM サービスにて指定された ID とパスワードに変更される。また、ChangeAccount サービスによって ID を変更でき、ChangePassword サービスによってパスワードを変更できる。ただし、本装置内からマスタ鍵が消去される（8.6 章参照）と、CO の ID とパスワードは固定値である初期 ID と初期パスワードに戻る。

4.1 サービス

各サービスの入力、及び出力の情報は別紙 1 を参照のこと。本装置はバイパス機能を有していない。

4.1.1 承認動作モードにおけるサービス

承認動作モードにおける、本装置の提供するサービスと役割の対応を表 4-1 に示す。

表 4-1 サービスと役割の対応

#	サービス	概要	役割			
			CO	AC	User	No Role
1	SecretKey Algorithm	オブジェクト内の鍵を用いて、共通鍵暗号アルゴリズム(3-key Triple Des / AES)による暗号化／復号を行う。 また、本装置内に格納済みのオブジェクト（鍵も含む）を暗号化して出力することができ、暗号化して入力されたオブジェクト（鍵も含む）を復号して格納することができる。 CO、AC 及び User は本人のオブジェクトのみを使用、出力、格納することができる。	○	○	○	
2	PublicKey Algorithm	オブジェクト内の鍵を用いて、公開鍵暗号アルゴリズム(RSAES-PKCS1-v1.5)による暗号化／復号を行う。 また、本装置内に格納済みのオブジェクト（鍵を含む）を暗号化して出力することができ、暗号化して入力されたオブジェクト（鍵を含む）を復号して格納することができる。 CO、AC 及び User は本人のオブジェクトのみを使用、出力、格納することができる。	○	○	○	

CO：クリプトオフィサ、AC：追加クリプトオフィサ、User：ユーザ、No Role：未認証の状態

#	サービス	概要	役割			
			CO	AC	User	No Role
3	MessageDigest	ハッシュ値を生成する。または、オブジェクト内の鍵を用いて HMAC 値の算出を行う。 CO、AC 及び User は本人のオブジェクトのみを使用することができる。	○	○	○	
4	GenerateKey	本装置内で共通鍵を生成し、オブジェクトに格納する。 トークンオブジェクトの鍵の場合、マスタ鍵を用いて暗号化し、SRAM(M)に格納する。 セッションオブジェクトの鍵の場合、SDRAM に平文の状態で格納する。 本サービスでは、生成した共通鍵を本装置外に出力しない。 CO、AC 及び User は本人のオブジェクト（鍵）のみを生成することができる。	○	○	○	
5	GenerateKeyPair	本装置内で鍵ペアを生成し、オブジェクトに格納する。ただし、公開鍵 e を外部から指定することが可能である。 トークンオブジェクトの鍵ペアの場合、マスタ鍵を用いて暗号化し、SRAM(M)に格納する。 セッションオブジェクトの鍵ペアの場合、SDRAM に平文の状態で格納する。 本サービスでは、生成した鍵ペアを本装置外に出力しない。 CO、AC 及び User は本人のオブジェクト（鍵ペア）のみを生成することができる。	○	○	○	
6	SetRandomSeed	乱数シードを生成する際の、PersonalizationString を設定する。 EntropyInput などの他のパラメータを設定することはできない。 本サービスを実行すると、シード値を再計算する。	○	○	○	
7	Generate Random	乱数を出力する。	○	○	○	
8	Sign	オブジェクト内の鍵を用いて、公開鍵暗号アルゴリズム(RSASSA-PKCS1-v1.5)による署名生成／署名検証を行う。 CO、AC 及び User は本人のオブジェクトのみを使用することができる。	○	○	○	

#	サービス	概要	役割			
			CO	AC	User	No Role
9	CreateObject	トークンオブジェクト、又はセッションオブジェクトを生成する。 トークンオブジェクトはマスタ鍵を用いて暗号化し、SRAM(M)に格納する。 セッションオブジェクトは平文の状態でSDRAMに格納する。 オブジェクト（鍵を含む）は、本装置の外部から暗号化された状態で入力される。 CO、AC及びUserは本人のオブジェクトのみを生成することができる。	○	○	○	
10	FindObject	オブジェクトを検索する。 オブジェクト内の鍵にはアクセスしない。 CO、AC及びUserは本人が使用可能なオブジェクトのみを検索することができる。	○	○	○	
11	UpdateObject	オブジェクトの属性を変更する。 オブジェクト内のデータ（鍵を含む）は更新できない。 CO、AC及びUserは本人のオブジェクトのみを変更することができる。	○	○	○	
12	GetObjectState	オブジェクトの状態を出力する。 オブジェクト内のデータ（鍵を含む）は出力しない。 CO、AC及びUserは本人のオブジェクトの情報のみを取得することができる。	○	○	○	
13	GetObjectData	オブジェクトの内容を出力する。ただし、秘密鍵、及びプライベート鍵は出力しない。 CO、AC及びUserは本人のオブジェクトの情報のみを取得することができる。	○	○	○	
14	DestroyObject	オブジェクトを削除する。 CO、AC及びUserは本人のオブジェクトのみを削除することができる。	○	○	○	
15	OpenSession	セッションをオープンする。 オープンしたセッション上では実行できない。				○ (※1)
16	CloseSession	セッションをクローズする。 クローズするセッション上で生成したセッションオブジェクトを削除する。（ゼロ化されるのは全セッションがクローズされた際）				○ (※2)
17	GetSessionState	セッションの情報を出力する。 オープンしたセッション上でのみ実行でき、そのセッションの情報のみ出力する。	○	○	○	○ (※2)

#	サービス	概要	役割			
			CO	AC	User	No Role
18	GetPk (※3)	HSM Key Pair を出力する。 また、下記のサービスにおける CO、AC 及び User の認証に使用するチャレンジデータも出力する。 ・ InitHSM ・ Login ・ CloseAllSession				○
19	CloseAllSession	全てのセッションをクローズする。 また、全てのセッションオブジェクトを削除する。 本サービスは、未認証の状態でのみ実行可能であるが、CO 又は AC の ID とパスワードの入力を必要とし（本装置内で、入力された ID、パスワード、及び GetPk サービスで取得したチャレンジデータによる認証を実施する）、オープンしたセッション上では実行できない。また、サービスの実行後、本サービスを実行したオペレータは未認証の状態のままである。	○ (※1)	○ (※1)		
20	Login	ID 認証によって、CO、AC 又は User へログインする。 オープンしたセッション上でのみ実行できる。 本サービスの実行に成功した場合、認証失敗回数がクリアされる。				○ (※2)
21	ChangePassword	CO、AC 又は User へログインする際のパスワードを変更する。 CO、AC 及び User は、本人のパスワードのみを変更できる。 変更したパスワードは、マスタ鍵を用いて暗号化し、SRAM(M)に格納する。 変更するパスワードは本装置の外部から暗号化された状態で入力される。	○	○	○	
22	Logout	CO、AC 又は User へログインしている状態からログアウトする。	○	○	○	
23	GetHSMInfo (※3)	動作モード、シリアル番号等の装置情報を出力する。 オープンしたセッション上では実行できない。				○ (※1)

#	サービス	概要	役割			
			CO	AC	User	No Role
24	AddAccount	オペレータのアカウントを生成する。 入力されたパスワードを、生成したアカウントの初期パスワードとして設定する。 指定されたパスワードは、マスタ鍵を用いて暗号化し、SRAM(M)に格納する。 パスワードは本装置の外部から暗号化された状態で入力される。	○	○		
25	InitPassword	CO、AC 又は User へログインする際のパスワードを変更する。 本サービスは CO、及び AC のみが実行でき、全てのアカウントのパスワードを変更できる。 指定されたパスワードは、マスタ鍵を用いて暗号化し、SRAM(M)に格納する。 パスワードは本装置の外部から暗号化された状態で入力される。本サービスの実行によって、アカウントのロック状態は解除されず、認証失敗回数もクリアされない。	○	○		
26	GetAccountInfo	アカウントの情報（所有オブジェクト数など）を出力する。 アカウントのオブジェクト内の鍵にはアクセスしない。 CO、及び AC は全てのアカウント情報を取得することができる。 User は本人のアカウント情報のみを取得することができる。	○	○	○	
27	GetAccountList	アカウント名の一覧を出力する。 CO、及び AC は全てのアカウントのアカウント名を取得することができる。	○	○		
28	ChangeAccount	アカウント名を変更する。 CO、及び AC は全てのアカウントのアカウント名を変更することができる。	○	○		
29	Unlock	ロックされたオペレータのアカウントをアンロックする。 本サービスの実行に成功した場合、認証失敗回数がクリアされる。 CO、及び AC は全てのアカウントをアンロックすることができる。	○	○		
30	SetMaxObject Count	アカウントが所有可能な最大オブジェクト数を設定する。 CO、及び AC は全てのアカウントに対して設定することができる。	○	○		

#	サービス	概要	役割			
			CO	AC	User	No Role
31	DeleteAccount	オペレータのアカウントを削除する。 削除するアカウントのオブジェクト（鍵を含む）も削除される。	○	○		
32	GetLog	ログを出力する。 ログには鍵やパスワードなどの CSP/PSP の情報は含まれない。	○	○		
33	SetLogLevel	ログの出力レベル（詳細度）を設定する。	○	○		
34	GetLogInfo	ログの情報（行数や出力レベルなど）を出力する。	○	○		
35	ClearLog	ログを消去する。	○	○		
36	SetDateTime	本装置の時刻設定を行う。	○	○		
37	GetFirmware List	ファームウェアのバージョン等の情報を出力する。 また、非承認動作モードにおける、ファームウェアアップデート機能の実行の有無を出力する。	○	○		
38	SetControlFlag	PCI Express バスからの、本装置の取り外し許可設定を行う。	○	○		
39	SetLockCount	Login サービスなどの CO、AC 又は User の認証が、連続して失敗した場合にロックする回数を設定する。 InitHSM サービスによる初期化後に 1 回のみ実行可能である。	○	○		
40	SetLabel	本装置のラベルを設定する。 InitHSM サービスによる初期化後に 1 回のみ実行可能である。	○	○		
41	SetSOCommand	AC が実行可能なサービスを設定する。 本サービスは CO のみ実行可能であり、AC は実行できない。	○			
42	SelfTest	自己テストを実行する。	○	○		

#	サービス	概要	役割			
			CO	AC	User	No Role
43	InitHSM (※3)	本装置を初期化する。 全ての CSP、PSP を消去する。 マスタ鍵、乱数シード、HSM Key Pair、及び CO の初期 ID と初期パスワードを新規に作成し設定する。 本サービスは、未認証の状態でのみ実行可能であるが、CO の ID とパスワードの入力を必要とし（本装置内で、入力された ID、パスワード、及び GetPk サービスで取得したチャレンジデータによる認証を実施する）、オープンしたセッション上では実行できない。また、サービスの実行後、本サービスを実行したオペレータは未認証の状態のままである。 セッションがオープンしている状態では実行できない（つまり、SO Session Object、User Session Object、及び Bus Key が存在しない状態において、実行可能である。）。	○			

※1：オープンしたセッション上では実行できない。
※2：オープンしたセッション上でのみ実行できる。
※3：機能制限の付いた承認動作モードにおいて実行可能なサービス。

4.1.2 非承認動作モードにおける機能

非承認動作モードにおける、本装置の提供する機能を以下に示す。

(1) 承認動作モードと同等の機能
- 「2.4 動作モード」を参照のこと。

(2) オブジェクト バックアップ／リストア機能
- CO、又は AC が他のアカウントのオブジェクトをバックアップ、リストアする機能。

(3) ファームウェアアップデート機能
- ファームウェアを更新、削除する機能。
- 起動するファームウェアを選択する機能。

(4) サービス使用状況取得機能
- 各サービスを実行した回数を取得する機能。承認動作モードにおいて実行した情報は取得できない。

(5) ホスト情報格納機能
- ホスト PC の情報を格納する機能。

4.2 役割

4.2.1 クリプトオフィサ役割 (CO)

本装置の初期化・設定、アカウント設定、AC への実行権限付与などの管理、及び CO のデータにアクセスする役割。CO は本装置に 1 アカウントのみである。

CO の状態において、本装置に入力及び本装置から出力されるデータは、Bus Key（8.1.9 章参照）によって暗号化される。ただし、SecretKeyAlgorithm、PublicKeyAlgorithm、MessageDigest、及び Sign サービスの入出力データは暗号化されない。（サービスのヘッダ情報の一部のみ暗号化される。）

CO のログインに関する制限事項を以下に示す。

- AC、又は User がログインしている場合、CO はログインできない。

CO に与えられたサービス、及びサービスにおいて使用する承認されたセキュリティ機能を表 4-2 に示す。

表 4-2 CO のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	SecretKeyAlgorithm	3-key Triple Des (SP800-67) 暗号利用モード：ECB/CBC AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB/CBC
2	PublicKeyAlgorithm	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
3	MessageDigest	Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
4	GenerateKey	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
5	GenerateKeyPair	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
6	SetRandomSeed	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
7	GenerateRandom	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
8	Sign	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
9	CreateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
10	FindObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
11	UpdateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
12	GetObjectState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
13	GetObjectData	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
14	DestroyObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
15	GetSessionState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC

#	サービス	セキュリティ機能
16	CloseAllSession	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (3,072bit) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
17	ChangePassword	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
18	Logout	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
19	AddAccount	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
20	InitPassword	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
21	GetAccountInfo	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
22	GetAccountList	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
23	ChangeAccount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
24	Unlock	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
25	SetMaxObjectCount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
26	DeleteAccount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
27	GetLog	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
28	SetLogLevel	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
29	GetLogInfo	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
30	ClearLog	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
31	SetDateTime	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
32	GetFirmwareList	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
33	SetControlFlag	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
34	SetLockCount	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
35	SetLabel	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
36	SetSOCommand	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
37	SelfTest	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) 3-key Triple Des (SP800-67) 暗号利用モード：ECB/CBC AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB/CBC Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1) HASH-DRBG (SP800-90A, SHA-256)
38	InitHSM	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (3,072bit) Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC

4.2.2 追加クリプトオフィサ役割 (AC)

CO によって付与された権限に従い、本装置の設定やアカウント設定などの管理、及び AC のデータにアクセスする役割。生成された直後の AC は CloseAllSession サービスのみが実行可能であり、CO によって他のサービスの実行権限が付与される。AC は本装置に複数生成することができる。

AC の状態において、本装置に入力及び本装置から出力されるデータは、Bus Key（8.1.9 章参照）によって暗号化される。ただし、SecretKeyAlgorithm、PublicKeyAlgorithm、MessageDigest、及び Sign サービスの入出力データは暗号化されない。（サービスのヘッダ情報の一部のみ暗号化される。）

AC のログインに関する制限事項を以下に示す。

- CO、他の AC、又は User がログインしている場合、AC はログインできない。

AC に与えられたサービス、及びサービスにおいて使用する承認されたセキュリティ機能を表 4-3 に示す。

表 4-3 AC のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	SecretKeyAlgorithm	3-key Triple Des (SP800-67) 暗号利用モード：ECB/CBC AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB/CBC
2	PublicKeyAlgorithm	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
3	MessageDigest	Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
4	GenerateKey	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
5	GenerateKeyPair	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
6	SetRandomSeed	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
7	GenerateRandom	HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
8	Sign	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
9	CreateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
10	FindObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
11	UpdateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
12	GetObjectState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
13	GetObjectData	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
14	DestroyObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
15	GetSessionState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC

#	サービス	セキュリティ機能
16	CloseAllSession	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (3,072bit) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
17	ChangePassword	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
18	Logout	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
19	AddAccount	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
20	InitPassword	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
21	GetAccountInfo	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
22	GetAccountList	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
23	ChangeAccount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
24	Unlock	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
25	SetMaxObjectCount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
26	DeleteAccount	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
27	GetLog	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
28	SetLogLevel	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
29	GetLogInfo	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
30	ClearLog	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
31	SetDateTime	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
32	GetFirmwareList	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
33	SetControlFlag	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
34	SetLockCount	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
35	SetLabel	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
36	SelfTest	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) 3-key Triple Des (SP800-67) 暗号利用モード：ECB/CBC AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB/CBC Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1) HASH-DRBG (SP800-90A , SHA-256)

4.2.3 ユーザ役割 (User)

User のデータにアクセスする役割。

User の状態において、本装置に入力及び本装置から出力されるデータは、Bus Key（8.1.9 章参照）によって暗号化される。ただし、SecretKeyAlgorithm、PublicKeyAlgorithm、MessageDigest、及び Sign サービスの入出力データは暗号化されない。（サービスのヘッダ情報の一部のみ暗号化される。）

User のログインに関する制限事項を以下に示す。

- CO、又は AC がログインしている場合、User はログインできない。

User に与えられたサービス、及びサービスにおいて使用する承認されたセキュリティ機能を表 4-4 に示す。

表 4-4 User のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	SecretKeyAlgorithm	3-key Triple Des (SP800-67) 暗号利用モード：ECB/CBC AES-128, 192, 256 (FIPS PUB 197) 暗号利用モード：ECB/CBC
2	PublicKeyAlgorithm	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A , SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
3	MessageDigest	Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (FIPS PUB 198-1) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
4	GenerateKey	HASH-DRBG (SP800-90A , SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
5	GenerateKeyPair	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) HASH-DRBG (SP800-90A , SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
6	SetRandomSeed	HASH-DRBG (SP800-90A , SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
7	GenerateRandom	HASH-DRBG (SP800-90A , SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
8	Sign	RSASSA-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit) Secure Hash Standard (SHA-224, SHA-256, SHA-384, SHA-512) (FIPS PUB 180-4) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
9	CreateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
10	FindObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
11	UpdateObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
12	GetObjectState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
13	GetObjectData	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
14	DestroyObject	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
15	GetSessionState	AES-256 (FIPS PUB 197) 暗号利用モード：CBC

#	サービス	セキュリティ機能
16	ChangePassword	Secure Hash Standard (SHA-256) (FIPS PUB 180-4) HASH-DRBG (SP800-90A, SHA-256) AES-256 (FIPS PUB 197) 暗号利用モード：CBC
17	Logout	AES-256 (FIPS PUB 197) 暗号利用モード：CBC
18	GetAccountInfo	AES-256 (FIPS PUB 197) 暗号利用モード：CBC

4.2.4 未認証の状態 (No Role)

CO、AC 又は User へログインしていない状態。

No Role の状態で使用できるサービス、及びサービスにおいて使用する承認されたセキュリティ機能を表 4-5 に示す。

表 4-5 No Role のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	OpenSession	HASH-DRBG (SP800-90A, SHA-256)
2	CloseSession	なし
3	GetSessionState	なし
4	GetPk	HASH-DRBG (SP800-90A, SHA-256)
5	Login	RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (3,072bit)
6	GetHSMInfo	なし

4.3 認証

本装置は ID ベース認証をサポートする。アカウント名とパスワードによってオペレータを個別に識別し、オペレータが担う役割の認可を認証する。CO、AC 又は User の状態では Login サービスを実行できないため、他のアカウントにログインする場合には、Logout サービスにてログアウトし、未認証の状態(NoRole)へ戻る必要がある。

本装置が許容する最小パスワード長は 8 文字である。また、92 種類の文字が使用可能である。

1 回のランダムな試行が成功する確率は、1,000,000 分の 1 以下である(1/ 5,132,188,731,375,616)。

1 回の試行に必要な時間は 4 マイクロ秒であり、1 分間に 15,000,000 回の試行が可能とすると、1 分間のランダムな試行が成功する確率は、1,000,000 分の 1 以下である(1/ 342,145,916)。

認証に失敗した場合、認証失敗の結果のみを出力する。(「指定されたアカウント名がない」、「パスワードが不正」などの詳細な情報は出力しない。) また、SetLockCount サービスにて設定されているロック規定回数 (5～15 回)、連続で認証に失敗した場合、そのアカウントはロックされ、認証を行えなくなる。アカウントのアンロックは、CO 又は AC が行える。

5. 有限状態モデル

別紙 2 参照。

6. 物理的セキュリティ

本装置は、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セキュリティレベル 3 を満たす。

セキュリティレベル 3 を満たすために、本装置の暗号境界は硬く不透明な囲いに覆われ、内部構造が見えない構造になっている。また、この囲いは、通気口・スリット、及びドア・除去可能なカバーを有していない。

本装置は、秘密情報保護のためのタンパ応答機能を有している。タンパ応答により、SRAM(S)に格納されている平文の秘密情報をゼロ化する。タンパ応答は囲いのこじ開けを検知した際に動作する。

7. 動作環境

本装置は、限定された動作環境でのみ動作する。したがって、動作環境のセキュリティ要件は適用除外とする。

8. 暗号鍵管理

8.1 CSP, PSP

本装置の CSP、PSP を以下に示す。

8.1.1 SO Token Object

概要

CO 又は AC が生成したオブジェクト（秘密鍵、プライベート鍵、又は公開鍵を含む）。

CSP/PSP 種別

CSP/PSP

鍵の種別（暗号アルゴリズム等）

オペレータによって指定された暗号アルゴリズム：

- RSASSA-PKCS1-v1_5 (2,048～4,096bit)：署名生成・署名検証
- RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)：暗号化・復号
- 3-key Triple Des (192bit)：暗号化・復号、暗号利用モード：ECB, CBC
- AES (128,192,256bit)：暗号化・復号、暗号利用モード：ECB, CBC
- HMAC-SHA-224 (14～8,191Byte)：メッセージ認証、
  HMAC-SHA-256 (16～8,191Byte)：メッセージ認証、
  HMAC-SHA-384 (24～8,191Byte)：メッセージ認証、
  HMAC-SHA-512 (32～8,191Byte)：メッセージ認証

RSASSA-PKCS-v1.5、及び RSAES-PKCS1-v1_5 の鍵には、プライベート鍵のみ、公開鍵のみ、又はプライベート鍵と公開鍵の両方（鍵ペア）のいずれかが格納される。

鍵の生成

GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成する。
ただし、GenerateKeyPair サービスでは、公開鍵 e を外部から指定することが可能である。

鍵の格納

下記の鍵を、マスタ鍵で暗号化された状態で SRAM(M)に格納する。公開鍵のみを格納する場合、暗号化して格納するか、平文で格納するかは、オペレータの指定に従う。ただし、プライベート鍵と共に格納される場合は、暗号化して格納する。

- CreateObject サービスによって外部から入力された鍵、又は SecretKeyAlgorithm、PublicKeyAlgorithm サービスの演算結果を鍵として格納
- GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成した鍵
  （GenerateKeyPair サービスにて、外部から指定された公開鍵 e を含む）

鍵をゼロ化するサービス

- InitHSM
- DestroyObject
- DeleteAccount（AC のみ。CO のアカウントは削除できない。）

8.1.2 SO Session Object

概要

CO 又は AC が生成したオブジェクト（秘密鍵、プライベート鍵、又は公開鍵を含む)。

CSP/PSP 種別

CSP/PSP

鍵の種別（暗号アルゴリズム等）

オペレータによって指定された暗号アルゴリズム：

- RSASSA-PKCS1-v1_5 (2,048～4,096bit)：署名生成・署名検証
- RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)：暗号化・復号
- 3-key Triple Des (192bit)：暗号化・復号、暗号利用モード：ECB, CBC
- AES (128,192,256bit)：暗号化・復号、暗号利用モード：ECB, CBC
- HMAC-SHA-224 (14～8,191Byte)：メッセージ認証、
  HMAC-SHA-256 (16～8,191Byte)：メッセージ認証、
  HMAC-SHA-384 (24～8,191Byte)：メッセージ認証、
  HMAC-SHA-512 (32～8,191Byte)：メッセージ認証

RSASSA-PKCS-v1.5、及び RSAES-PKCS1-v1_5 の鍵には、プライベート鍵のみ、公開鍵のみ、又はプライベート鍵と公開鍵の両方（鍵ペア）のいずれかが格納される。

鍵の生成

GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成する。
ただし、GenerateKeyPair サービスでは、公開鍵 e を外部から指定することが可能である。

鍵の格納

下記の鍵を、平文の状態で SDRAM に格納する。

- CreateObject サービスによって外部から入力された鍵、又は SecretKeyAlgorithm、PublicKeyAlgorithm サービスの演算結果を鍵として格納
- GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成した鍵（GenerateKeyPair サービスにて、外部から指定された公開鍵 e を含む）

鍵をゼロ化するサービス

- DestroyObject
- CloseSession（全セッションがクローズされた時点で削除される。）
- CloseAllSession
- DeleteAccount（AC のアカウントのみ）

8.1.3 User Token Object

概要

User が生成したオブジェクト（秘密鍵、プライベート鍵、又は公開鍵を含む）。

CSP/PSP 種別

CSP/PSP

鍵の種別（暗号アルゴリズム等）

オペレータによって指定された暗号アルゴリズム：

- RSASSA-PKCS1-v1_5 (2,048～4,096bit)：署名生成・署名検証
- RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)：暗号化・復号
- 3-key Triple Des (192bit)：暗号化・復号、暗号利用モード：ECB, CBC
- AES (128,192,256bit)：暗号化・復号、暗号利用モード：ECB, CBC
- HMAC-SHA-224 (14～8,191Byte)：メッセージ認証、
  HMAC-SHA-256 (16～8,191Byte)：メッセージ認証、
  HMAC-SHA-384 (24～8,191Byte)：メッセージ認証、
  HMAC-SHA-512 (32～8,191Byte)：メッセージ認証

RSASSA-PKCS-v1.5、及び RSAES-PKCS1-v1_5 の鍵には、プライベート鍵のみ、公開鍵のみ、又はプライベート鍵と公開鍵の両方（鍵ペア）のいずれかが格納される。

鍵の生成

GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成する。
ただし、GenerateKeyPair サービスでは、公開鍵 e を外部から指定することが可能である。

鍵の格納

下記の鍵を、マスタ鍵で暗号化された状態で SRAM(M)に格納する。公開鍵のみを格納する場合、暗号化して格納するか、平文で格納するかは、オペレータの指定に従う。ただし、プライベート鍵と共に格納される場合は、暗号化して格納する。

- CreateObject サービスによって外部から入力された鍵、又は SecretKeyAlgorithm、PublicKeyAlgorithm サービスの演算結果を鍵として格納
- GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成した鍵
  （GenerateKeyPair サービスにて、外部から指定された公開鍵 e を含む）

鍵をゼロ化するサービス

- InitHSM
- DestroyObject
- DeleteAccount

8.1.4 User Session Object

概要

User が生成したオブジェクト（秘密鍵、プライベート鍵、又は公開鍵を含む）。

CSP/PSP 種別

CSP/PSP

鍵の種別（暗号アルゴリズム等）

オペレータによって指定された暗号アルゴリズム：

- RSASSA-PKCS1-v1_5 (2,048～4,096bit)：署名生成・署名検証
- RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (2,048～4,096bit)：暗号化・復号
- 3-key Triple Des (192bit)：暗号化・復号、暗号利用モード：ECB, CBC
- AES (128,192,256bit)：暗号化・復号、暗号利用モード：ECB, CBC
- HMAC-SHA-224 (14～8,191Byte)：メッセージ認証、
  HMAC-SHA-256 (16～8,191Byte)：メッセージ認証、
  HMAC-SHA-384 (24～8,191Byte)：メッセージ認証、
  HMAC-SHA-512 (32～8,191Byte)：メッセージ認証

RSASSA-PKCS-v1.5、及び RSAES-PKCS1-v1_5 の鍵には、プライベート鍵のみ、公開鍵のみ、又はプライベート鍵と公開鍵の両方（鍵ペア）のいずれかが格納される。

鍵の生成

GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成する。
ただし、GenerateKeyPair サービスでは、公開鍵 e を外部から指定することが可能である。

鍵の格納

下記の鍵を、平文の状態で SDRAM に格納する。

- CreateObject サービスによって外部から入力された鍵、又は SecretKeyAlgorithm、PublicKeyAlgorithm サービスの演算結果を鍵として格納
- GenerateKey、又は GenerateKeyPair サービスによって本装置内で生成した鍵（GenerateKeyPair サービスにて、外部から指定された公開鍵 e を含む）

鍵をゼロ化するサービス

- DestroyObject
- CloseSession（全セッションがクローズされた時点で削除される。）
- CloseAllSession
- DeleteAccount

8.1.5 SO Password

概要

CO 又は AC のパスワード。

CSP/PSP 種別

CSP

鍵の種別（暗号アルゴリズム等）

8～32 文字の文字列

鍵の生成

CO の初期パスワードは、本装置内で生成する（固定値）。

CO の初期パスワード以外の SO Password は本装置内では生成しない。

鍵の格納

下記のサービスにて入力されたパスワードを、SHA-256 を用いてハッシュ値を生成し、本装置内で生成した乱数と連結し、マスタ鍵で暗号化して SRAM(M)に格納する（平文のパスワードは保持しない）。

- InitHSM（CO のパスワードのみ）
- AddAccount
- ChangePassword
- InitPassword

鍵をゼロ化するサービス

- InitHSM（AC のみ。CO のパスワードは InitHSM サービスによって更新される。）
- DeleteAccount（AC のみ。CO のアカウントは削除できない。）

8.1.6 User Password

概要

User のパスワード

CSP/PSP 種別

CSP

鍵の種別（暗号アルゴリズム等）

8～32 文字の文字列

鍵の生成

User Password は本装置内では生成しない。

鍵の格納

下記のサービスにて入力されたパスワードを、SHA-256 を用いてハッシュ値を生成し、本装置内で生成した乱数と連結し、マスタ鍵で暗号化して SRAM(M)に格納する（平文のパスワードは保持しない）。

- AddAccount
- ChangePassword
- InitPassword

鍵をゼロ化するサービス

- InitHSM
- DeleteAccount

8.1.7 Master Key

概要

マスタ鍵。CSP/PSP を暗号化して格納する際に用いる秘密鍵。

CSP/PSP 種別

CSP

鍵の種別（暗号アルゴリズム等）

AES-256、暗号利用モード：CBC

鍵の生成

InitHSM サービスによって本装置内で生成する。

鍵の格納

InitHSM サービスによって本装置内で生成した鍵を、SubCPU 内の SRAM(S)に平文の状態で格納する。

鍵をゼロ化するサービス

- InitHSM（ゼロ化後、再度生成・格納する）。

8.1.8 Random Seed

概要

乱数シード。（SP800-90A における V と C）

CSP/PSP 種別

CSP

鍵の種別（暗号アルゴリズム等）

HASH-DRBG(SP800-90A, SHA-256)

鍵の生成

電源投入後に本装置内で生成する。

鍵の格納

本装置内で生成した乱数シードを、平文の状態で SDRAM に格納する。

鍵をゼロ化するサービス

- InitHSM（ゼロ化後、再度生成・格納する）
- SetRandomSeed（ゼロ化後、入力された PersonalizationString を用いて再度生成・格納する）

8.1.9 Bus Key

概要

CO、AC、又は User にログインしている状態において、入出力されるデータを暗号化／復号するための秘密鍵。

CSP/PSP 種別

CSP

鍵の種別（暗号アルゴリズム等）

AES-256、暗号利用モード：CBC

鍵の生成

Login サービスによって、CO、AC、又は User にログインする際に、本装置外から入力される。
入力する鍵は 256bit のエントロピーを持つこと。

鍵の格納

Login サービスによって入力された鍵を、平文の状態で SDRAM に格納する。

鍵をゼロ化するサービス

- Logout
- CloseAllSession

8.1.10 HSM KeyPair

概要

HSM の鍵ペア。InitHSM、Login、CloseAllSession サービスにおいて、入力データを暗号化／復号するための、本装置の鍵ペア。2 つの異なる鍵ペアから構成される。

CSP/PSP 種別

CSP/PSP

鍵の種別（暗号アルゴリズム等）

RSAES-PKCS1-v1_5 (PKCS#1 v2.1) (3,072bit)

鍵の生成

本装置内にマスタ鍵が格納されていない状態（InitHSM サービスを一度も実行していない状態等）では、固定値の初期 HSM Key Pair を使用する。
また、InitHSM サービスによって本装置内で生成する。

鍵の格納

InitHSM サービスによって本装置内で生成した HSM Key Piar を、マスタ鍵で暗号化された状態で SRAM(M)に格納する。

鍵をゼロ化するサービス

- InitHSM（ゼロ化後、再度生成・格納する）

CSP/PSP とサービスの対応を表 8-1 に示す。

【凡例】
C　：消去
R　：読み出し
W　：書き込み
X　：鍵の使用
－　：CSP/PSP を使用しない

表 8-1 CSP/PSP とサービスの対応

	CSP / PSP サービス	SO Token Object	SO Session Object	User Token Object	User Session Object	SO Password *7	User Password *7	Master Key	Random Seed	Bus Key	HSM KeyPair
1	SecretKeyAlgorithm	X R*1 W*2	X R*1 W*2	X R*1 W*2	X R*1 W*2	－	－	X*2	－	X*6	－
2	PublicKeyAlgorithm	X R*1 W*2	X R*1 W*2	X R*1 W*2	X R*1 W*2	－	－	X*2	X	X*6	－
3	MessageDigest	X R*1 W*2	X R*1 W*2	X R*1 W*2	X R*1 W*2	－	－	X*2	－	X*6	－
4	GenerateKey	W	W	W	W	－	－	X	X	X	－
5	GenerateKeyPair	W	W	W	W	－	－	X	X	X	－
6	SetRandomSeed	R*3	R*3	R*3	R*3	－	－	－	WX	X	－
7	GenerateRandom	－	－	－	－	－	－	－	－	X	－
8	Sign	X R*1	X R*1	X R*1	X R*1	－	－	X*2	－	X*6	－
9	CreateObject	W	W	W	W	－	－	X	－	X	－
10	FindObject	R	R	R	R	－	－	－	－	X	－
11	UpdateObject	W	W	W	W	－	－	－	－	X	－
12	GetObjectState	R	R	R	R	－	－	－	－	X	－
13	GetObjectData	R	R	R	R	－	－	－	－	X	－
14	DestroyObject	C	C	C	C	－	－	－	－	X	－
15	OpenSession	－	－	－	－	－	－	－	X	－	－
16	CloseSession	－	C*4	－	C*4	－	－	－	－	－	－

*1　対象データにオブジェクトを指定された場合
*2　出力先にオブジェクトを指定された場合
*3　シード値(PersonalizationString)にオブジェクトを指定された場合
*4　全セッションがクローズされる際
*5　CO、AC 又は User にログインしている状態で実行した場合
*6　入出力データは暗号化されず、ヘッダ情報の一部のみ暗号化される。（4.2.1,4.2.2,4.2.3 章参照）
*7　SO Password、及び User Password は、平文ではなくハッシュ値で管理する

	CSP / PSP サービス	SO Token Object	SO Session Object	User Token Object	User Session Object	SO Password *7	User Password *7	Master Key	Random Seed	Bus Key	HSM KeyPair
17	GetSessionState	–	–	–	–	–	–	–	–	X*5	–
18	GetPk	–	–	–	–	–	–	–	X	–	R
19	CloseAllSession	–	C	–	C	R	–	–	–	C	X
20	Login	–	–	–	–	R	R	–	–	W	X
21	ChangePassword	–	–	–	–	RW	RW	X	X	X	–
22	Logout	–	–	–	–	–	–	–	–	CX	–
23	GetHSMInfo	–	–	–	–	–	–	–	–	–	–
24	AddAccount	–	–	–	–	W	W	X	X	X	–
25	InitPassword	–	–	–	–	W	W	X	X	X	–
26	GetAccountInfo	–	–	–	–	–	–	–	–	X	–
27	GetAccountList	–	–	–	–	–	–	–	–	X	–
28	ChangeAccount	–	–	–	–	–	–	–	–	X	–
29	Unlock	–	–	–	–	–	–	–	–	X	–
30	SetMaxObjectCount	–	–	–	–	–	–	–	–	X	–
31	DeleteAccount	C	C	C	C	C	C	X	–	X	–
32	GetLog	–	–	–	–	–	–	–	–	X	–
33	SetLogLevel	–	–	–	–	–	–	–	–	X	–
34	GetLogInfo	–	–	–	–	–	–	–	–	X	–
35	ClearLog	–	–	–	–	–	–	–	–	X	–
36	SetDateTime	–	–	–	–	–	–	–	–	X	–
37	GetFirmwareList	–	–	–	–	–	–	–	–	X	–
38	SetControlFlag	–	–	–	–	–	–	–	–	X	–
39	SetLockCount	–	–	–	–	–	–	–	–	X	–
40	SetLabel	–	–	–	–	–	–	–	–	X	–
41	SetSOCommand	–	–	–	–	–	–	–	–	X	–
42	SelfTest	–	–	–	–	–	–	R	WX	X	–
43	InitHSM	C	–	C	–	CRW	C	CW	CWX	–	CWX

*5 CO、AC 又は User にログインしている状態で実行した場合

*7 SO Password、及び User Password は、平文ではなくハッシュ値で管理する

電源投入時に、暗号化された状態で SRAM(M)に格納されている CSP/PSP を、マスタ鍵を用いて復号して SDRAM に展開する。

8.2 乱数ビット列生成器(RBG)

HASH-DRBG (SP800-90A, SHA-256)を用いて乱数を生成する。乱数シードの入力及び出力は行わない。本装置内で暗号鍵を生成する場合に使用する。

また、GenerateRandom サービスにより乱数を生成し、出力する。

HASH-DRBG (SP800-90A, SHA-256)における Entropy Input、及び Nonce は、常に変化するハードウェア情報（乱数生成器による乱数）を使用する。また、Entropy Input と Nonce の長さは 320bit 固定とする。PersonalizationString は、SetRandomSeed サービスにて、本装置へ入力することができる。

8.3 鍵生成

SO Token Object, SO Session Object, User Token Object, User Session Object の鍵（RSA 鍵ペア、秘密鍵）は、GenerateKey サービス、又は GenerateKeyPair サービスにて、本装置内で承認された RBG を用いて生成することができる。

Master Key、HSM KeyPair は、本装置内で承認された RBG を用いて生成する。

8.4 鍵の入力及び出力

CO、AC、又は User にログインしている場合、本装置への入力又は本装置から出力される鍵は、Bus Key で暗号化される。未認証の状態では、鍵の入出力は行わない。

- SO Token Object 及び SO Session Object の鍵：
  入力： BusKey で暗号化されて入力される。平文では入力されない。
  出力： BusKey で暗号化して出力する。平文では出力しない。
  鍵に関連付けられた ID の CO、又は AC のみが出力できる。

- User Token Object 及び User Session Object の鍵：
  入力： BusKey で暗号化されて入力される。平文では入力されない。
  出力： BusKey で暗号化して出力する。平文では出力しない。
  鍵に関連付けられた ID の User のみが出力できる。

- SO Password 及び User Password
  入力： BusKey で暗号化されて入力される。平文では入力されない。
  出力： 出力しない。

- Master Key
  入力： 本装置内で生成し、外部からは入力されない。
  出力： 出力しない。

- Random Seed
  入力： PersonalizationString は BusKey で暗号化されて入力される。乱数シード本体は本装置内で生成し、外部からは入力されない。
  出力： 出力しない。

・ BusKey
　　入力： Login サービスにて HSM KeyPair の公開鍵で暗号化されて入力される。
　　出力： 出力しない。

・ HSM KeyPair
　　入力： 本装置内で生成し、外部からは入力されない。
　　出力： 公開鍵(PSP)は GetPk サービスの出力データとして平文で出力する。
　　プライベート鍵(CSP)は出力しない。

本装置は、平文による鍵の入力、及び手動による鍵の入力を用いていない。

8.5 鍵の格納

鍵の格納先と、マスタ鍵によって暗号化された状態／平文の状態での格納を表 8-2 に示す。

表 8-2 鍵の格納先と暗号化

CSP / PSP	鍵の種別	格納先	暗号化 / 平文
SO Token Object	秘密鍵／プライベート鍵／公開鍵	SRAM(M)	暗号化／平文 ※
SO Session Object	秘密鍵／プライベート鍵／公開鍵	SDRAM	平文
User Token Object	秘密鍵／プライベート鍵／公開鍵	SRAM(M)	暗号化／平文 ※
User Session Object	秘密鍵／プライベート鍵／公開鍵	SDRAM	平文
SO Password	パスワード	SRAM(M)	暗号化
User Password	パスワード	SRAM(M)	暗号化
Master Key	秘密鍵	SRAM(S)	平文
Random Seed	乱数シード	SDRAM	平文
Bus Key	秘密鍵	SDRAM	平文
HSM KeyPair	プライベート鍵／公開鍵	SRAM(M)	暗号化

※ 公開鍵のみを格納する場合、暗号化して格納するか、平文で格納するかは、オペレータの指定に従う。プライベート鍵と共に格納される場合は、暗号化して格納する。

8.6 鍵のゼロ化

本装置の初期化時に、全ての CSP/PSP は消去され、マスタ鍵、乱数シード、HSM Key Pair、及び CO の初期 ID と初期パスワードが再度生成・格納される。

タンパ応答時に、SDRAM 及び SRAM(S)に格納されている平文の CSP/PSP をゼロ化する。

PCI Express バスから電源供給されていない場合において、バッテリーの電圧低下を検知するとマスタ鍵を消去する。

PCI Express バスからの取り外しを検知すると、マスタ鍵を消去する。ただし、PCI Express バスのスロットからの取り外しの検知は、CO、又は AC によって無効化することが可能である。

PCI Express バスからの電源供給が断たれた場合、SDRAM に格納されている CSP/PSP は消去される。

【凡例】

C ：消去

X ：PCI Express バスから電源が供給されていないため、SDRAM に存在しない

－ ：何もしない

表 8-3 CSP/PSP のゼロ化ケース

ケース / CSP / PSP	格納場所	PCI Express バスから電源が供給されている場合			PCI Express バスから電源が供給されていない場合		
		サービス	タンパ応答	PCI-Express バスからの電源供給断 *3	タンパ応答	バッテリー電圧低下	PCI-Express バスからの取り外し *4
SO Token Object *1	SRAM(M)	（表 8-4 参照）	C	－	－	－	－
	SDRAM		C	C	X	X	X
SO Session Object	SDRAM		C	C	X	X	X
User Token Object *1	SRAM(M)		C	－	－	－	－
	SDRAM		C	C	X	X	X
User Session Object	SDRAM		C	C	X	X	X
SO Password *1	SRAM(M)		C	－	－	－	－
	SDRAM		C	C	X	X	X
User Password *1	SRAM(M)		C	－	－	－	－
	SDRAM		C	C	X	X	X
Master Key *2	SRAM(S)		C	－	C	C	C
	SDRAM		C	C	X	X	X
Random Seed	SDRAM		C	C	X	X	X
Bus Key	SDRAM		C	C	X	X	X
HSM KeyPair *1	SRAM(M)		C	－	－	－	－
	SDRAM		C	C	X	X	X

*1　電源投入時に、マスタ鍵を用いて復号され、平文の状態で SDRAM に展開される。

*2　電源投入時に、SRAM(S)から読出し、平文の状態で SDRAM に展開される。

*3,*4　PCI-Express バスから電源が供給されている場合に、PCI バスから取り外した場合には、*3 列と *4 列の両方の動作が実行される。（*4 列の X の欄は*3 列の動作によって消去される。）

表 8-4 CSP/PSP をゼロ化するサービス

CSP / PSP	CSP/PSP をゼロ化するサービス
SO Token Object (SRAM(M)/SDRAM)	InitHSM DestroyObject DeleteAccount
SO Session Object (SDRAM)	DestroyObject CloseSession CloseAllSession DeleteAccount
User Token Object (SRAM(M)/SDRAM)	InitHSM DestroyObject DeleteAccount
User Session Object (SDRAM)	DestroyObject CloseSession CloseAllSession DeleteAccount
SO Password (SRAM(M)/SDRAM)	InitHSM（ゼロ化後、CO の初期パスワードを生成・格納する） DeleteAccount
User Password (SRAM(M)/SDRAM)	InitHSM DeleteAccount
Master Key (SRAM(S)/SDRAM)	InitHSM（ゼロ化後、再度生成・格納する）
Random Seed (SDRAM)	InitHSM（ゼロ化後、再度生成・格納する） SetRandomSeed（ゼロ化後、入力された PersonalizationString を用いて再度生成・格納する）
Bus Key (SDRAM)	Logout CloseAllSession
HSM KeyPair (SRAM(M)/SDRAM)	InitHSM（ゼロ化後、再度生成・格納する）

9. 自己テスト

9.1 パワーアップ自己テスト

本装置は、PCI Express バスからの電源投入時にパワーアップ自己テストを実行する。暗号アルゴリズムテスト、RBG エントロピーテスト、ファームウェア完全性テスト、及び重要機能テストを実行する。いずれかのテストに失敗した場合、本装置はエラー状態となり、状態出力インタフェースを介して状態を通知する。

9.1.1 暗号アルゴリズムテスト

暗号アルゴリズムテストでは、既知解テスト(Known Answer Test)を実行する。既知解テストで実行するアルゴリズムを表 9-1 に示す。

表 9-1 アルゴリズムとテスト方法

アルゴリズム	テスト方法
RSA	RSASSA-PKCS1-v1_5 の既知解テスト
	RSAES-PKCS1-v1_5 の鍵ペア整合性テスト
AES	128,192,256 ビットの鍵長による CBC モード暗号化、復号
	128,192,256 ビットの鍵長による ECB モード暗号化、復号
3-key Triple Des	3-key Triple Des による CBC モード暗号化、復号
	3-key Triple Des による ECB モード暗号化、復号
SHA	SHA-256, SHA-512 によるメッセージダイジェスト生成
HMAC	HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 によるメッセージダイジェスト生成
乱数生成	既存入力値による擬似乱数生成（正常終了、異常終了の両方をテストする。）

9.1.2 RBG エントロピーテスト

Random Seed 生成時に使用するエントロピーソース(Entropy Input)は、64 ビットの構成要素を 5 個連結して作成する。64 ビットの 5 個の構成要素がそれぞれ異なることを検証する。エントロピーソース（64 ビット×5）を 2 つ作成し、異なることを検証する。このテストは電源投入時の他に、Random Seed を更新する（エントロピーソースを使用する）際にも実行する。また、ISO/IEC 18031 に記載されている RBG エントロピーソースの暗号ヘルステストを実行する。

9.1.3 ファームウェア完全性テスト

ファームウェア完全性テストでは、CRC32 又は SHA-256 を用いたハッシュ値を用いてファームウェアの完全性を保証する。

9.1.4 重要機能テスト

ファームウェアを SDRAM に展開する前に、SDRAM の書き込み／読み出し機能が正しく動作することを確認する。

9.2 条件自己テスト

本装置は、特定の機能（鍵ペア生成／乱数生成等）が実行される前に、条件自己テストを実行する。鍵ペア整合性テスト、及び連続乱数生成テストを実行する。

9.2.1 鍵ペア整合性テスト

鍵ペア整合性テストでは、鍵ペアを生成した際に、任意の値の署名生成・署名検証、及び暗号化・復号を行うことで、鍵ペアが正しいことを保証する。署名生成・署名検証、又は暗号化・復号に失敗した場合、本装置はエラー状態となり、状態出力インタフェースを介して状態を通知する。

9.2.2 連続乱数ビット列生成器テスト

乱数は 32 バイトの倍数のサイズを生成し、必要なサイズを使用する。

連続乱数ビット列生成器テストでは、生成した乱数を 32 バイト単位で検証する。乱数生成時、最初に 32 バイトの乱数生成を 1 回実行する。生成した乱数と、前回生成した乱数の最終 32 バイトと比較し異なることを検証する。以後、32 バイト単位で直前の乱数と比較検証する（図 9-1 参照）。今回生成した乱数の最終 32 バイトを前回生成した乱数として保存する。

最初に生成した 32 バイトの乱数は、連続乱数ビット列生成器テストにのみ使用する。

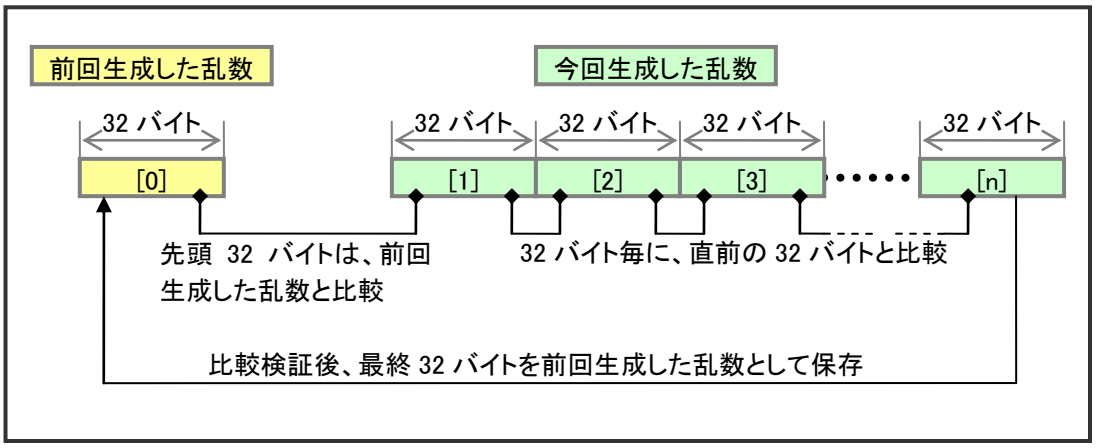

図 9-1 連続乱数ビット列生成器テスト

10. 設計保証

10.1 構成管理及び開発

本装置の構成管理、及び開発は「PCI-Express バス対応型ハードウェアセキュリティモジュール開発手順書」に則り実施される。

10.2 配付及び運用

本装置は PC などの機器の PCI Express バスに接続されて動作するものである。本装置の設置方法、初期化方法等は下記の文書に記載されている。

- PCI-Express バス対応型ハードウェアセキュリティモジュール 取扱説明書

10.3 ガイダンス文書

クリプトオフィサガイダンス、及びユーザガイダンス文書は、下記の文書に記載されている。

- PCI-Express バス対応型ハードウェアセキュリティモジュール クリプトオフィサガイダンス
- PCI-Express バス対応型ハードウェアセキュリティモジュール ユーザガイダンス

11. その他の攻撃への対処

本装置において、その他の攻撃（DPA／SPA／タイミング攻撃／故障解析等）への対策は行わない。従って、その他の攻撃に対するセキュリティ要件は適用除外とする。