SecureWare/開発キット Ver5.1

セキュリティポリシ

２０１６年１１月１５日

Version 1.97

日本電気株式会社

NEC

— 目 次 —

1 概要

SecureWare/開発キット Ver5.1（以下、開発キット Ver5.1）は、日本電気株式会社の提供するソフトウェアの暗号モジュールである。

本セキュリティポリシでは、開発キット Ver5.1 セキュリティポリシについて述べる。

認証対象の暗号モジュールの正式バージョンは Ver5.1.0.0 であるが本書では便宜上 Ver5.1 と記す。

2 モジュール概要

開発キット Ver5.1 は、一般用途のコンピュータのオペレーティングシステム上で動作するマルチチップスタンドアロン型暗号モジュールであり、ダイナミックリンクライブラリとして他アプリケーションへ API を提供する。

開発キット Ver5.1 は JIS X19790 のセキュリティレベル 1 に必要な条件を満たす。

3 暗号モジュールの仕様

3.1　暗号境界

3.1.1 物理的暗号境界

開発キット Ver5.1 はソフトウェア製品であり、暗号モジュールが動作するハードウェア構成はマルチチップスタンドアロン型のパーソナルコンピュータ（以下、PC）またはワークステーション（以下、WS）である。

物理的な暗号境界は、ＣＰＵ、メモリ、システムバス、ハードディスク等のストレージデバイス、ネットワークポート、コントローラ、電源、LED、FibreChannel、スピーカ･イヤホン・マイクロホン端子、プリンタポートや USB ポートなどの外部デバイスを接続するポート、DVD・DAT・FD のドライブなどを含む一般用途のＰＣまたは WS と規定する。

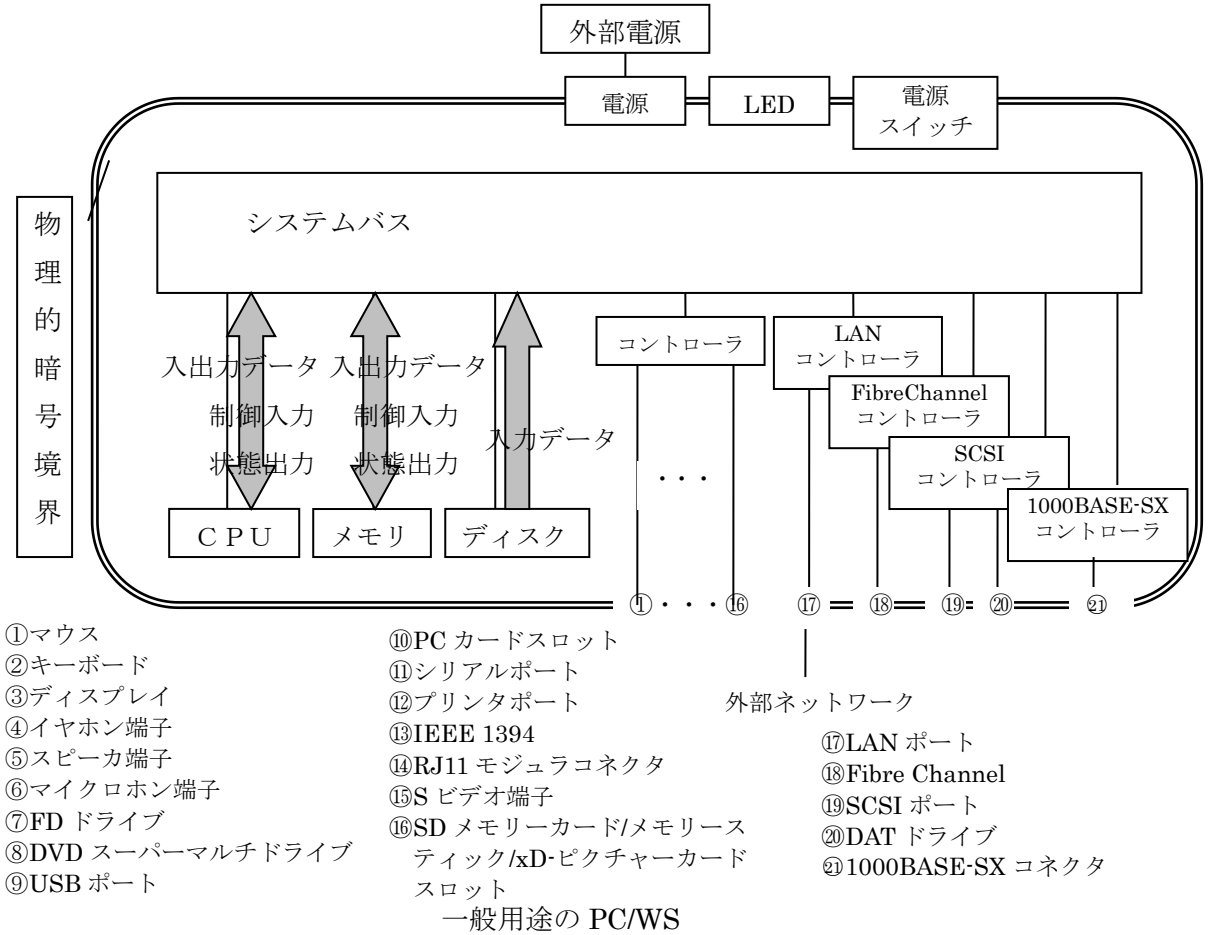

図 3.1　暗号モジュールの物理的境界

なお、開発キット Ver5.0 を試験した環境は以下の通りである。

①

ソフトウェア：Microsoft Windows XP Professional Version 2002 Service Pack 3

ハードウェア：VersaPro VY16F/HB-R

[CPU] Intel PentiumM 1.6GHz

[メモリ] 1024MB

[HDD] 60GB

②

ソフトウェア：Microsoft Windows Vista Business Service Pack 1

ハードウェア：VersaPro VJ21A/W-4

[CPU] Intel Core2Duo T7400 2.16GHz

[メモリ] 2048MB

[HDD]80GB

③

ソフトウェア：Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 2

ハードウェア：Express5800/R120b-2

[CPU] ヘキサコア Intel Xeon X5690 3.46GHz ×2

[メモリ] 24GB

[HDD] 73.2GB ×6

④

ソフトウェア：HP-UX 11i v2 Mission Critical Operating Environment

ハードウェア：NX7700i/5012L-8

[CPU]デュアルコア Intel Itanium9140N 1.6GHz ×4

[メモリ] 16GB

[HDD] 73 GB× 4

3.1.2 論理的暗号境界

開発キット Ver5.1 は、上位アプリケーションプログラムに API でセキュリティ機能を提供する。暗号モジュールの論理的な暗号境界を「図 3.2」に示す。

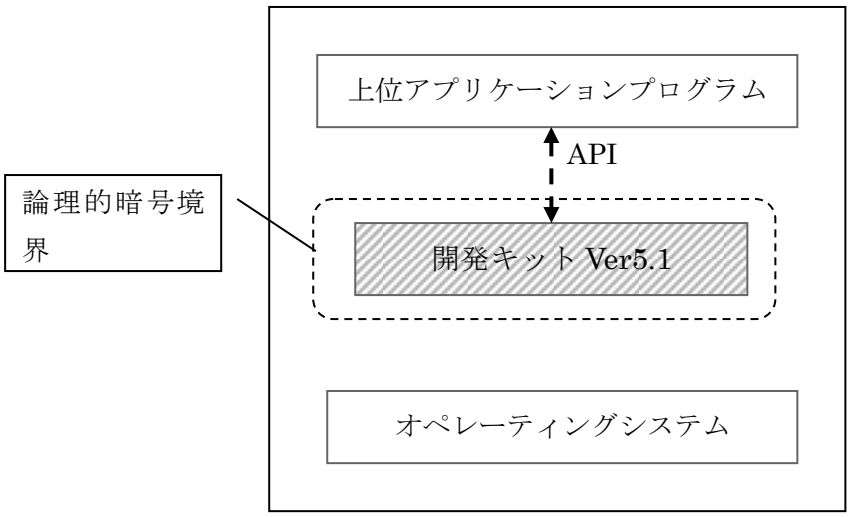

図 3.2　暗号モジュールの論理的境界

3.2　動作モードとアルゴリズム

開発キット Ver5.1 では暗号モジュール試験及び認証制度（以下、JCMVP）で認証を受けたモジュールと、JCMVP 認証を受けていないモジュールを論理的に分離して提供する。

開発キット Ver5.1 が実装するセキュリティ機能の一覧および JCMVP で認証を受けたモジュール(表中[JCMVP 認証モジュール)と記載)と、JCMVP で承認されたセキュリティ機能が動作するが、JCMVP 認証を受けていないモジュール(表内[推奨暗号モジュール)と、JCMVP 認証を受けていないモジュール(表中[従来モジュール]と記載)のそれぞれが使用可能なセキュリティ機能の対応を「表 3.1」に示す。

表 3.1 暗号モジュールセキュリティ機能一覧

分類	アルゴリズム	JCMVP 認証モジュール/推奨暗号モジュール	従来モジュール
署名	RSASSA-PKCS1-v1_5 (注 1)	○	○
	RSASSA-PSS (注 1)	○	○
守秘	RSAES-PKCS1-v1_5 (注 4)	○	○
	RSA-OAEP (注 5)	○	○
	RSA-raw		○

64 ビットブロック暗号	CIPHERUNICORN-E (注 3) (注 4)	○	○
	Triple DES (注 2)	○	○
	DES		○
ストリーム暗号	RC2		○
	RC5		○
128 ビットブロック暗号	CIPHERUNICORN-A (注 3) (注 4)	○	○
	AES（注 6）	○	○
ハッシュ	SHA-1	○	○
	SHA-224	○	○
	SHA-256	○	○
	SHA-384	○	○
	SHA-512	○	○
	MD2		○
	MD4		○
	MD5		○
メッセージ認証	HMAC-SHA-1(注 7)	○	○
	HMAC-SHA-224	○	○
	HMAC-SHA-256	○	○
	HMAC-SHA-384	○	○
	HMAC-SHA-512	○	○
	HMAC-MD2		○
	HMAC-MD5		○
乱数生成	Hash_DRBG（ベンダ自己確認：NIST SP800-90)	○	○
鍵確立	DH	○	○
自己テスト実行	-	○	
モジュール状態取得	-	○	

(注 1) 署名生成について、JCMVP の承認されたセキュリティ機能の条件は、モジュラスとなる合成数が 2048 ビット以上、かつ、使用するハッシュ関数の出力長が 224 ビット以上。

(注 2) 3-key Triple DES のみ

(注 3)SecureWare/開発キット Ver5.1 のオプション製品「SecureWare/開発キット Ver5.1 CIPHERUNICORN オプション」で提供。

(注 4) 2014/4/1 を以て、JCMVP で承認されたセキュリティ機能から取り消された。

(注 5) 暗号化について、JCMVP の承認されたセキュリティ機能の条件は、モジュラスとなる合成数が 2048 ビット以上、かつ、使用するハッシュ関数の出力長が 224 ビット以上。

(注 6) 承認されたモードで AES を動作させるための方法については、6 動作環境 3. AES 暗号/復号 に記載している。
(注 7) MAC 生成について、JCMVP の承認されたセキュリティ機能の条件は、暗号鍵の鍵長が 112 ビット以上。

3.3　ポートとインタフェース

セキュリティに関係する情報は、コンポーネントの提供する API の引数で、入力データ及び出力データとして上位アプリケーションと暗号モジュールの間を受け渡しされる。

論理的インタフェースを「表 3.2」に定義する。

表 3.2　論理インタフェース一覧

インタフェース種別	情報
データ入力インタフェース	API 呼び出しの入力パラメータ ・暗号化/署名の入力となる平文 ・復号の入力となる暗号文 ・検証の入力となる署名データ ・暗号化/復号/署名/検証の入力となる鍵(共通鍵、プライベート鍵、公開鍵、HMAC 鍵) ・暗号化/復号の入力となる初期化用データ ・乱数生成評価の入力となるシード ・鍵確立(鍵生成)の入力となるドメインパラメータ ・鍵確立の入力となる鍵(秘密鍵/公開鍵)
データ出力インタフェース	API 呼び出しの出力パラメータ ・復号の出力となる平文 ・暗号の出力となる暗号文 ・署名の出力となる署名データ ・検証の出力となる検証結果 ・鍵生成の出力となる鍵(共通鍵、プライベート鍵、公開鍵) ・鍵確立(ドメインパラメータ生成)の出力となるドメインパラメータ ・鍵確立(鍵生成)の出力となる鍵(秘密鍵/公開鍵) ・鍵確立の出力となる鍵(共有秘密鍵)
制御入力インタフェース	入力パラメータ ・暗号の動作モード ・暗号に必要なパラメータ API 呼び出しのアクション ・API の呼出し ファイルシステム ・暗号（AES）の動作モード
状態出力インタフェース	API 呼び出しの戻り値及び出力パラメータ

	・処理結果及び状態情報 ・エラー詳細コード

4 暗号モジュールのセキュリティルール

開発キット Ver5.1 は以下のセキュリティルールに従って動作する。

1. 暗号モジュールは、以下の自己テストを実施する。
   (1) パワーアップ自己テスト
      (a) ソフトウェア/ファームウェア完全性テスト（HMAC 検証）
      (b) 暗号アルゴリズムテスト
         - AES 既知解テスト
         - CIPHERUNICORN-A 既知解テスト
         - CIPHERUNICORN-E 既知解テスト
         - 3-Key Triple DES 既知解テスト
         - HMAC-SHA-1、HMAC-SHA-224/256/384/512 既知解テスト
         - RSAES-PKCS1-v1_5 既知解テスト
         - RSA-OAEP 既知解テスト
         - RSASSA-PKCS1-v1_5 既知解テスト
         - RSASSA-PSS 既知解テスト
         - SHA-1、SHA-224/256/384/512 既知解テスト
         - 乱数生成器既知解テスト
         - DH 検証テスト
      (c) RBG エントロピーテスト
      (d) エントロピー取得エラーテスト
   (2) 条件自己テスト
      (a) 鍵ペア整合性テスト
         - RSA 鍵整合性テスト
      (b) 連続乱数生成器テスト
      (c) リシードテスト
2. 暗号モジュールは、エラー状態では暗号演算及びデータの出力を行わない。
3. 暗号モジュールが動作するプロセスのアドレス空間は、オペレーティングシステムによって他プロセスのアクセスから保護される。
4. 暗号モジュール、及び暗号モジュールのコンポーネントの置換や改変は許可されない。
5. 暗号モジュールが自己テストで異常を検出しエラー状態になった場合、暗号モジュールの再ロード、あるいは安全に保管されたインストール媒体からの再インストールによって回復される。
6. 鍵確立では、Diffie-Hellman パラメータの作成において、L=1024～15360 の鍵をサポートし、セキュリティビット 80～256 に対応することで、暗号モジュールで取り扱う、最

大長の鍵（AES-256）の確立を行う場合においてもセキュリティ強度を保つ。(NIST SP800-57 part1 より参照)

5 暗号モジュールのセキュリティポリシ

5.1 識別と認証ポリシ

開発キット Ver5.1 では、以下の役割を定義する。

(1) ユーザ役割

ユーザは、暗号モジュールの承認されたセキュリティ機能及び承認されていないセキュリティ機能のすべての API を実行する。

(2) クリプトオフィサ役割

クリプトオフィサは、暗号モジュールのインストールを行う。この場合、クリプトオフィサはオペレーティングシステムによって PC またはＷＳのソフトウェアの更新を許可されている。

開発キット Ver5.1 ではメンテナンス機能を提供しないため、メンテナンス役割は定義しない。

役割は、暗号モジュールが利用者を識別して割り当てるものではない。利用者が該当する API を利用すること、インストール作業を行うことが、その役割の遂行とみなし、役割は暗黙的に変更される。

開発キット Ver5.1 は、役割の認証を行わない。よって「表 5.1」及び「表 5.2」に示すように、認証のタイプ、認証データ、認証メカニズム、及びメカニズムの強度は規定しない。

表 5.1 役割並びに必要な識別及び認証

役割	認証のタイプ	認証データ
ユーザ	無し	無し
クリプトオフィサ	無し	無し

表 5.2 認証メカニズムの強度

認証メカニズム	メカニズムの強度
なし	なし

5.2 アクセス制御ポリシ

役割として規定されたユーザは、「表 5.3」に示すサービスを提供される。

さらに、役割の提供されたサービスにおける CSP、PSP への許可されたアクセスを以下に定義し、「表 5.3」のアクセス欄に略号で記載する。

・ 生成(g): CSP、PSP が暗号モジュール内で生成される。

- 入力(i): CSP、PSP が暗号モジュールに論理インタフェースのデータ入力インタフェースで入力される。
- 使用(u): CSP、PSP がサービス実行のため暗号モジュール内で使用される。
- 出力(o): CSP、PSP が暗号モジュールから論理インタフェースのデータ出力インタフェースで出力される。

表 5.3　役割に許可されたサービスと CSP、PSP へのアクセス

サービス	CSP	PSP	アルゴリズム	API	アクセス	
					CSP	PSP
対称鍵 暗号	共通鍵		AES	SwSealAesBlock	i,u	
				SwUnsealAesBlock	i,u	
			Triple DES	SwGenerateDesKey	g,o	
				SwSealDesBlock	i,u	
				SwUnsealDesBlock	i,u	
			CIPHERUNICORN-E	SwSealCUEBlock	i,u	
				SwUnsealCUEBlock	i,u	
			CIPHERUNICORN-A	SwSealCipherUnicornBlock	i,u	
				SwUnsealCipherUnicornBlock	i,u	
公開鍵 署名、守秘	プライベート鍵, prime1, prime2 , exponent1, exponent2, coefficient	公開鍵	下記４つに共通	SwGenerateRsaKey	g,o	g,o
			RSAES-PKCS1-v1_5 RSAES-OAEP	SwSealRsaBlockPKCS		i,u
				SwUnsealRsaBlockPKCS	i,u	
			RSASSA-PKCS1-v1_5 RSASSA-PSS	SwSignRsaBlockPKCS	i,u	
				SwVerifyRsaBlockPKCS		i,u
ハッシュ	-		SHA-1	SwDigestSHA1Block		
			SHA-224	SwDigestSHA224Block		
			SHA-256	SwDigestSHA256Block		
			SHA-384	SwDigestSHA384Block		
			SHA-512	SwDigestSHA512Block		-
メッセージ認証	HMAC 鍵		HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	SwHMACBlock	i,u	
乱数生成	シード		Hash_DRBG (ベンダ自己確	SwGenerateRandom	g,u	

			認 : NIST SP800-90)			
鍵確立 (注 1)		ドメインパラメータ	DH	SwKEDomainParameterGeneration		g,o
		ドメインパラメータ		SwKEDomainParameterValidation		i,u
	秘密値	ドメインパラメータ, 公開値		SwKEKeyGeneration	g,o	i,u g,o
		ドメインパラメータ, 公開値		SwKEPublicKeyValidation		i,u i,u
	秘密値, 共有秘密鍵	ドメインパラメータ, 公開値		SwKEKeySharing	i,u g,o	i,u i,u
		ドメインパラメータ		SwKEDomainParameterFree		i
	秘密値, 共有秘密鍵	公開値		SwKEDataFree	i i	i
モジュール状態取得	-		-	SwFipsGetStatus		-
自己テスト	-		-	SwFipsPowerUpSelfTest		
モジュール状態取得 (注 1)				SwKEFipsGetStatus		
自己テスト (注 1)				SwKEFipsPowerUpSelfTest		-

(注 1) swsdkdhv50j.dll で提供される関数。

5.3 物理的セキュリティポリシ

開発キット Ver5.1 はソフトウェアによって実装されるため、物理的セキュリティの要求事項の対象外である。よって「表 5.4」に示すように、物理的セキュリティメカニズムの検査/試験について規定しない。

表 5.4　物理的セキュリティメカニズムの検査/試験

物理的セキュリティメカニズム	推奨する検査/試験の繰り返し数	検査/試験のガイダンス詳細
なし	なし	なし

5.4　その他の攻撃への対処のためのセキュリティポリシ

その他の攻撃への対処は規定しない。

6 動作環境

開発キット Ver5.1 をインストールし動作させるためには「表 6.1」または「表 6.2」に示す環境が必要である。なお、Linux 向け開発キット Ver5.1 は JCMVP の試験、認証はされていない。

表 6.1 動作環境(Windows 版)

オペレーティングシステム (注 1)	Windows Vista/7/8.1/10（日本語版）(32bit 版) Windows Server 2008（日本語版）(32bit 版) Windows 7/8.1/10（日本語版）(64bit 版) Windows Server 2008 R2/2012/2012R2/2016（日本語版）(64bit 版)
マシン環境	PC/AT 互換機
メモリ	32MB（OS や他のソフトウェアが必要とするメモリサイズは含んでいない。）
ハードディスク空き容量	開発キット Ver5.1 のインストールするドライブには 2MB 以上の空き容量が必要。 インストールの際にはセットアップを展開するためにさらに 5MB 以上の空き容量が必要。空き容量が必要なディスクはシステム環境変数 TEMP が設定されているドライブとなる。（通常 Windows のインストールされているディレクトリ。）

（注 1） 32bit 版/64bit 版共に動作環境に記載されているオペレーティングシステムにインストール可能。ただし、64bit 版開発キットは 64bit アプリケーションからしか使用できないため、32bitOS 上で動作しない。

表 6.2 動作環境(Linux 版)

オペレーティングシステム (注 2)	Red Hat Enterprise Linux 6.8(32bit 版) Red Hat Enterprise Linux 6.8/7.2(64bit 版)
マシン環境	PC/AT 互換機

メモリ	32MB（OS や他のソフトウェアが必要とするメモリサイズは含んでいない。）
ハードディスク空き容量	開発キット Ver5.1 をインストールするドライブには 2MB 以上の空き容量が必要。

（注 2） 32bit 版/64bit 版共に動作環境に記載されているオペレーティングシステムにインストール可能。ただし、64bit 版開発キットは 64bit アプリケーションからしか使用できないため、32bitOS 上で動作しない。

「表 6.1」に示すオペレーティングシステムは、プロセスごとに独立した仮想アドレス空間を割り当て、プロセス間の独立を確保する。動的リンクライブラリである暗号モジュールの使用する領域は呼び出しプロセスのアドレス空間内に確保される。オペレーティングシステム内で複数のプロセスが同時に暗号モジュールをロードし使用したとしても、１つのプロセスインスタンスごとに暗号モジュールが個々にロードされ実行される。よって実行中の暗号モジュールにとっては制御を受けるのは常に１つのプロセスインスタンスからのみであり、他プロセスインスタンスから動作中の暗号モジュール内の CSP、PSP へのアクセス、処理への割り込みが行われることはない。この意味で暗号モジュールは単一オペレータモードで動作するものである。

なお、開発キット Ver5.1 では JCMVP 認証を受けたモジュールと、JCMVP 認証を受けていないモジュールを論理的に分離して提供する。

そのため、開発キット Ver5.1 インストール後、JCMVP 認証を受けた暗号モジュールを使用する場合、以下の点に注意する必要がある。

１．使用するモジュールの選択

開発キットをインストールするとインストールディレクトリ配下に sdk,sdkJCMVP の２つのディレクトリが作成される。それぞれのディレクトリ配下にインストールされるモジュールは下記の通りである。なお、JCMVP 認証を受けたモードで動作させる場合、sdkJCMVP ディレクトリ配下に格納されている DLL を使用する必要がある。

sdk ディレクトリ配下にインストールされるモジュール：

従来製品の互換用として使用可能なモジュール。MD5 や DES など JCMVP 認証を受けていない暗号モジュールがインストールされる。

sdkJCMVP ディレクトリ配下にインストールされるモジュール：

JCMVP 認証を受けた暗号モジュールがインストールされる。

Windows 版の開発キットは、32bit 版と 64bit 版の暗号モジュールを別のインストーラで提供している。32bit 版、64bit 版共にインストールディレクトリ配下に sdk,sdkJCMVP の２つのディレクトリが作成され、暗号モジュールがインストールされるが、JCMVP 認証を受

けた暗号モジュールは 32bit 版の sdkJCMVP ディレクトリにインストールされた暗号モジュールである。

なお、各ディレクトリに含まれるライブラリ名と提供するサービスは、下記「暗号モジュールのコンポーネント」に示すとおり。

表 6.3　暗号モジュールコンポーネント一覧(Windows)

	ライブラリ名		提供するサービス
	32bit モジュール	64bit モジュール	
JCMVP 認証モジュール	swsdkv50j.dll swsdkv50j.hmac		RSA 暗号化/復号/署名/検証/鍵生成 TripleDES 暗号化/復号/鍵生成 AES 暗号化/復号(注 2) SHA-224/256/384/512 ハッシュ SHA-1 ハッシュ 乱数生成 HMAC メッセージ認証 CIPHERUNICORN-A 暗号化/復号(注 1) CIPHERUNICORN-E 暗号化/復号(注 1) モジュール状態取得 自己テスト実行
	swsdkdhv50j.dll swsdkdhv50j.hmac		Diffie-Hellman 鍵確立 モジュール状態取得 自己テスト実行
推奨暗号モジュール		swsdkv50j_64.dll swsdkv50j_64.hmac	RSA 暗号化/復号/署名/検証/鍵生成 TripleDES 暗号化/復号/鍵生成 AES 暗号化/復号(注 2) SHA-224/256/384/512 ハッシュ SHA-1 ハッシュ 乱数生成 HMAC メッセージ認証 CIPHERUNICORN-A 暗号化/復号(注 1) CIPHERUNICORN-E 暗号化/復号(注 1) モジュール状態取得 自己テスト実行
		swsdkdhv50j_64.dll swsdkdhv50j_64.hmac	Diffie-Hellman 鍵確立 モジュール状態取得 自己テスト実行
従来のモジュール	swrsa.dll	swrsa64.dll	RSA 暗号化/復号/署名/検証/鍵生成
	swkdes.dll	swkdes64.dll	TripleDES 暗号化/復号/鍵生成
	swkaes.dll	swkaes64.dll	AES 暗号化/復号(注 2)
	swksha.dll	swksha64.dll	SHA-224/256/384/512 ハッシュ
	swsha1.dll	swsha1_64.dll	SHA-1 ハッシュ
	swkhmac.dll	swkhmac64.dll	HMAC メッセージ認証
	swkcu.dll	swkcu64.dll	CIPHERUNICORN-A 暗号化/復号(注 1)
	swkcue.dll	swkcue64.dll	CIPHERUNICORN-E 暗号化/復号(注 1)
	swkrc2.dll	swkrc2_64.dll	RC2 暗号化/復号
	swkrc5.dll	swkrc5_64.dll	RC5 暗号化/復号
	swkrng.dll	swkrng64.dll	乱数生成
	swkcrypt.dll	swkcrypt64.dll	DES 暗号化/復号

	swcry20.dll	swcry20_64.dll	MD2 MD4 MD5 ハッシュ
	swDH.dll	swDH64.dll	Diffie-Hellman 鍵確立

（注１）SecureWare/開発キット Ver5.1 のオプション製品「SecureWare/ 開発キット Ver5.1 CIPHERUNICORN オプション」でライセンス提供。

（注 2）CPU がインテル プロセッサで AES-NI 対応の場合、AES-NI の命令セットを使用。この場合、推奨暗号モジュールとなる。

表 6.4　暗号モジュールコンポーネント一覧(Linux)

	ライブラリ名		提供するサービス
	32bit モジュール	64bit モジュール	
推奨暗号モジュール	libswsdkv50j.sol libswsdkv50j.hmac	libswsdkv50j_64.dll libswsdkv50j_64.hmac	RSA 暗号化/復号/署名/検証/鍵生成 TripleDES 暗号化/復号/鍵生成 AES 暗号化/復号(注 2) SHA-224/256/384/512 ハッシュ SHA-1 ハッシュ 乱数生成 HMAC メッセージ認証 CIPHERUNICORN-A 暗号化/復号(注 1) CIPHERUNICORN-E 暗号化/復号(注 1) モジュール状態取得 自己テスト実行
	libswsdkdhv50j.dll libswsdkdhv50j.hmac	libswsdkdhv50j_64.dll libswsdkdhv50j_64.hmac	Diffie-Hellman 鍵確立 モジュール状態取得 自己テスト実行

（注１）SecureWare/開発キット Ver5.1 のオプション製品「SecureWare/ 開発キット Ver5.1 CIPHERUNICORN オプション」でライセンス提供。

（注 2）CPU がインテル プロセッサで AES-NI 対応の場合、AES-NI の命令セットを使用。

２．認証データファイルの使用

JCMVP 認証モジュールを使用する場合、暗号モジュール(swsdkv50j.dll、swsdkdhv50j.dll)と同じ場所に認証データファイル(swsdkv50j.hmac、swsdkdhv50j.hmac)を配置する必要がある。認証データファイルがない場合、ライブラリロード時にエラーとなる。

swsdkv50j.dll を使用する場合は swsdkv50j.hmac が、swsdkdhv50j.dll を使用する場合は swsdkdhv50j.hmac が必要となる。

３．AES 暗号/復号

. 暗号モジュールを動作させる環境の CPU がインテル プロセッサで AES-NI 対応の場合、AES 暗号/復号は AES-NI の命令セットを使用して動作する。この場合、暗号モジュールは JCMVP で承認されてないモードで動作する。

JCMVP で承認されたモードで動作させるためには、暗号モジュールを実行するアプリケーションと同じ場所に以下のファイルを配置する必要がある。

ファイル名：「SecureWareAES」

※ファイル属性は特に問わない。