

# 国内で入手可能な暗号関連製品リスト

※平成14年度に調査した最新の結果はこちらを参照願います。

※平成11年度10月時点での調査をベースに、平成13年12月現在での情報をもとに更新したものです。

情報処理振興事業協会（IPA）が調査した国内で入手可能な暗号関連製品の一覧表のドラフト版です。個人の提供による製品は掲載していません。

本リストに掲載している各製品の詳細につきましては、それぞれの開発元あるいは国内販売窓口にお問い合わせください。

開発元あるいは国内販売窓口の方で内容の補記・追加・訂正がありましたら、セキュリティセンター 暗号技術グループ: isec-crypt@ipa.go.jp までお知らせください。

- 注1)本リストに掲載している製品について、IPAが保証あるいは推奨しているものではありません。
- 注2)本リストの各会社名及び各製品名はそれらの開発元あるいは国内販売窓口の商標もしくは登録商標です。

## 1. 暗号化製品

- [暗号メール](#)
- [暗号web/ブラウザ](#)
- [データ/ファイル暗号化、暗号化装置等](#)
- [暗号ライブラリ・暗号ツールキット](#)

## 2. VPN

## 3. 認証製品

- [PKI](#)
- [電子署名](#)
- [ワンタイムパスワード](#)

## 4. ICカード

## 5. 電子商取引

- [電子決済ツール](#)
- [不正コピー防止](#)

## 6. 電子認証サービス

### 1. 暗号化製品

#### (1) 暗号メール

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
CryptoPlug for EUDORA for MS Exchange / Outlook	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		EUDORA PRO のプラグイン
Entrust/Express	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム セコム サイバーセキュリティ事業部 ネットマークス	共通鍵 公開鍵、鍵配送 ハッシュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11	・ Entrust/ Entelligence が必要 ・ Microsoft Outlook、 Microdoft Exchangeのプ ラグインとして動作 ・ 鍵管理機能により、復号 鍵を紛失した場合でも復旧 可能

Entrust/Web Connector	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム セコムサイバーセキュリティ事業部 ネットマークス		S/MIMEを使用するメーラーに依存(S/MIME暗号)	S/MIME, SSL X.509	<ul style="list-style-type: none"> <li>Webサーバー、ブラウザ、S/MIME対応メーラーに対してSLL、S/MIME証明書を発行するコンポーネント</li> <li>WebCAの構築が可能</li> </ul>
F*ENCRY	富士通ビー・エス・シー	富士通ビー・エス・シー	共通鍵	DES (56bit)		セキュア活性化方式 (自動暗号復号) ※ソフトウェアのみ
FEAL for EUDORA PRO	NTTアドバンステクノロジー	NTTアドバンステクノロジー	共通鍵 公開鍵 署名	FEAL(128bit) 楕円DH(256bit) ESIGN(768bit)	MOSS PERSEUS	EUDORA PRO のプラグイン
FJPEM	WIDE プロジェクト	-	共通鍵 公開鍵	DES (56bit) RSA	PEM	暗号メール ソフトウェア 無償ダウンロード可
MAIL guardian	Vanguard Security Technologies	Vanguard Security Technologies	共通鍵 ハッシュ	DES(56bit) , TripleDES, Blowfish MD5, SHA-1	S/MIME	暗号メール ソフトウェア
MailSecure	Baltimore Technologies	日本バルチモアテクノロジーズ	共通鍵 公開鍵	TripleDES RSA(512,768,1028,2048bit)	PKCS S/MIME X.509 LDAP	暗号メール ソフトウェア
MailSecure Enterprise	Baltimore Technologies	日本バルチモアテクノロジーズ	共通鍵 公開鍵	TripleDES(112bit) RSA(2048bit)	S/MIME X.509 LDAP	暗号メール ソフトウェア
Misty Guard/ CryptoSign	三菱電機	三菱電機	共通鍵 公開鍵 ハッシュ	MISTY (128bit) , DES (64bit), TripleDES (192bit) , RC2 (40bit) RSA (鍵長は認証書に依存) SHA-1, MD5	S/MIME X.509	暗号メール ソフトウェア 魔法便IIと相互通信可能
Netscape Messenger	Netscape Communications	日本ネットスケープコミュニケーションズ	共通鍵 公開鍵	RC2, RC4, RC5(各40bit) RSA(512bit)	S/MIME	ブラウザのメール機能として普及
Outlook Express	Microsoft	マイクロソフト	共通鍵 公開鍵	RC2(40bit) RSA(512bit)	S/MIME	メールソフトとして普及
PGP for Business Security	Network Associates	日本ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120~168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4096bit)	PGP	メール/ファイル暗号化ソフトウェア EUDORA PRO、Outlook、Outlook Express、Lotus Notesへプラグイン可能
PGP Policy Management Agent for SMTP	Network Associates	日本ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120~168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit)	PGP	企業内メールのポリシー設定

				Diffie-Hellman(最大4096bit)		
Secure Messenger	Tumbleweed Communications	アイフォア	共通鍵 公開鍵 署名 ハッシュ	RC2(40bit), DES(56bit) RSA(512bit) RSA(512/2048bit) SHA-1, MD5	S/MIME	MS Exchange, EUDOEAPRO, Lotus Notes等へのプラグイン、スタンドアロン使用及びファイル暗号
SecureWare/電子メール SecureWare Plugin for EUDORA PRO	NEC	NEC	共通鍵 公開鍵	DES RSA	PEM X.509	EUDORA PRO のプラグイン
Tumbleweed MMS 4.6J	Tumbleweed Communications	タンブルウィード・コミュニケーションズ	共通鍵 公開鍵	RC2(40/255bit), DES(56bit), TripleDES(112bit) RSA(512/1024/2048bit)	S/MIME X.509 LDAP PKCS PKI	電子メール総合管理支援ソフトウェア
WorldSecure Serever	Tumbleweed Communications	アイフォア	共通鍵 公開鍵 署名 ハッシュ	RC2(40bit), DES(56bit) RSA(512bit) RSA(512/2048bit) SHA-1, MD5	S/MIME	電子メール総合管理支援ツール ソフトウェア
あやとり	キヤノン	キヤノン販売			MOSS	暗号メール ソフトウェア
インターネット安心便システム	トランスコスモス	トランスコスモス	共通鍵 鍵共有	(128bit) 動的鍵共有アルゴリズム (1024bit)		メール/ファイル暗号化ソフトウェア
カオスメールv2.3	国際情報科学研究所	国際情報科学研究所	共通鍵	GCCカオス暗号 (320bit)		暗号メール ソフトウェア
セキュア電子メール	NTTアドバンステクノロジー	NTTアドバンステクノロジー	共通鍵 署名	FEAL ESIGN	MOSS	暗号メール ソフトウェア
秘文/メール	日立ソフトウェアエンジニアリング	日立ソフトウェアエンジニアリング	共通鍵	顧客の要望に応じて対応		暗号メール ソフトウェア
封印PGP (For Consumer)	Network Associates	ソースネクスト	共通鍵 公開鍵 鍵配送	TripleDES(120~168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4096bit)	PGP	メール/ファイル暗号化ソフトウェア

(2) 暗号web/ブラウザ

製品名	開発元	国内販売窓口		暗号アルゴリズム・鍵長	標準化対応	製品概要
Entrust/Direct	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム	共通鍵 公開鍵、 鍵配送 ハッシュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11	・ Entrust/ Directoryは下記の2製品で構成 Entrust/Direct Client Proxy Entrust/Direct Server Proxy

		セコム サイバーセキュリティ事業部 ネットマークス				<ul style="list-style-type: none"> <li>・ Entrust/ Entelligenceが必要</li> <li>・ Webサーバー、ブラウザ間での、http上の、証明書を用いた双方向認証、暗号化、デジタル署名</li> <li>・ SSLとの併用を可能</li> </ul>
Entrust/Web Connector	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム セコム サイバーセキュリティ事業部 ネットマークス		SSLを使用するブラウザに依存(SSL暗号)	S/MIME, SSL X.509	<ul style="list-style-type: none"> <li>・ Webサーバー、ブラウザ、S/MIME対応メーラーに対してSLL、S/MIME証明書を発行するコンポーネント</li> <li>・ WebCAの構築が可能</li> </ul>
InfoProxy	富士通	富士通	公開鍵 ハッシュ	RSA(512,768,1024,2048bit) MD5,SHA-1	X.509 SSL HTTP LDAP	SSL対応プロキシサーバ
Internet Explore	Microsoft	マイクロソフト	共通鍵 公開鍵 鍵配送	RC2, RC4, DES(40bit) RSA Diffie-Hellman	SSL PCT PKCS	無償ダウンロード可
MistyGuard/ TRUSTWEB	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)	HTTP X.509	セキュアWebアクセスソフトウェア
Netscape Navigator	Netscape Communications	日本ネットスケープコミュニケーションズ	共通鍵 公開鍵 鍵配送	RC2 (40bit), RC4 (128bit), DES, TripleDES RSA Diffie-Hellman	SSL PKCS	無償ダウンロード可
InfoProxy	富士通	富士通	公開鍵 ハッシュ	RSA(512,768,1024,2048bit) MD5,SHA-1	X.509 SSL HTTP LDAP	SSL対応プロキシサーバ
Stronghold Secure Web Server	C2NET	C2NET	共通鍵 公開鍵 ハッシュ	DES(56bit) , TripleDES(168bit), RC4, RC2, IDEA RSA SHA,MD5		暗号機能対応Web
WebSecure	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵	RC4(40bit) RSA(512,768,1024bit)	PKCS SSL	webセキュリティ

			公開鍵 ハッシュ	MD5		
--	--	--	-------------	-----	--	--

(3) データ/ファイル暗号化、暗号化装置等

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
4758-001,013 PCI 暗号化コプロセッサ	IBM	日本IBM	共通鍵 公開鍵、署名	DES(56bit) RSA(512,768,1024bit)		暗号化PCIバス・アダプターカード
4758-002,023 PCI 暗号化コプロセッサ	IBM	日本IBM	共通鍵 公開鍵、署名	DES(56bit) RSA(512,768,1024,2048bit)		暗号化PCIバス・アダプターカード
AsgentIt!	アズジェント	アズジェント	共通鍵 公開鍵	DES(56bit) RSA(1024bit)		ファイル暗号ソフトウェア 無償ダウンロード可
Atalla A1000E NSP	Compaq Computer	コンパックコンピュータ	共通鍵	DES(56bit)		暗号化プロセッサ
Atalla TrustMaster CSP	Compaq Computer	コンパックコンピュータ	共通鍵 公開鍵、鍵配送 署名 ハッシュ	DES, RC2, RC4(各40bit) RSA(公開鍵256~2048bit, 鍵配送256~512bit) DSA MD2, MD5, SHA-1	FIPS140-1 Level3, UL, CSA, TUV	CryptoAPI用 暗号化ハードウェア
BOS	ビーオーエス・ネットワーク研究所	ビーオーエス・ネットワーク研究所	共通鍵	TripleDES		暗号、認証、署名システム
Choas InforGuard v4.02a	国際情報科学研究所	国際情報科学研究所	共通鍵	GCCカオス暗号 (320bit)		ファイル暗号化ソフトウェア
CKガード	NEC	NEC	共通鍵 公開鍵	DES(56bit) RSA (512~4096bit)		秘密鍵装置
CPロック (パソコン用)	シーアイシーシステムズ (他社と共同)	シーアイシーシステムズ	共通鍵	独自暗号方式(128bit) ・テキスト暗号 ・ファイル暗号		暗号化ソフトウェア
CryptoSwift	RAINBOW Technologies	RAINBOW Technologies	公開鍵 鍵配送 署名	RSA(384~1024bit) DSA Diffie-Hellman	SSL, X.509, S/MIME, PKCS, SET, SSH, IKE,	暗号PCIバスボード

					IPSec, TLS, SWAN, FIPS	
D-RANS	KENWOOD ローレルインテリ ジェントシステム ズ	ローレルインテリ ジェントシステム ズ	共通 鍵 公開 鍵 鍵共 有	DES, SXAL/MBAL, MISTY, MULTI, FEAL RSA KPS		暗号化ソフトウ ェア
Entrust/ICE	Entrust Technologies	エントラストジャ パン NTTデータ(SIパ ートナー) セコム情報システ ム セコム サイバー セキュリティ事業 部 ネットマークス	共通 鍵 公開 鍵、 鍵配 送 ハッ シュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140- 1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11	・ Entrust/ Entelligenceが 必要 ・ 任意のフォル ダをセキュア・ フォルダとして 設定し、自動的 な暗号化を行な う ・ 削除ファイル の復旧を防ぐ、 完全削除機能 (True Delete)を サポート ・ 鍵管理機能に より、復号鍵を 紛失した場合で も復旧可能
e-Parcel	e-Parcel	東芝情報システム		SSL		データ転送
FastMAP	RAINBOW Technologies	RAINBOW Technologies	公開 鍵 鍵配 送 署名	RSA(4~4096bit) Diffie-Hellman DSA	IPSec, IKE, ISAKMP, SSL, SET	暗号LSI
FEAL・ESIGN・ 楯円DH	NTTアドバンステ クノロジ	NTTアドバンステ クノロジ	共通 鍵 公開 鍵 署名	FEAL(128bit) 楯円DH(256bit) ESIGN(768bit)	ISO/IEC 9979	暗号化ソフトウ ェア (関数)
FILE LOCK with FEAL	NTTアドバンステ クノロジ	NTTアドバンステ クノロジ	共通 鍵 公開 鍵 署名	FEAL(128bit) 楯円DH(256bit) ESIGN(768bit)	MOSS	フォルダ・ファ イルの暗号化 ソフトウェア
F-Secure Desktop	F-Secure	山田洋行	共通 鍵	TripleDES(168bit), Blowfish(256bit)	-	ファイル暗号ソ フトウェア (On- Demand)
F-Secure File Crypto	F-Secure	山田洋行	共通 鍵	TripleDES(168bit), Blowfish(256bit)	-	ファイル暗号ソ フトウェア (On-the-Fly)
F-Secure SSH2	F-Secure	山田洋行	共通 鍵	TripleDES(168bit), オプション(IDEA(128bit)), Blowfish(128bit), Twofish(128), ARC4(128bit)	SSH2	ソフトウェア

/Server for UNIX  /Client for Windows, Macintosh, UNIX			公開鍵	DSA(512-1024bit) , RSA(512-4096bit)		
IKEVIEW	松下電工	松下電工	共通鍵	DES(40,56bit), TripleDES(112,168bit)	IPsec ISAKMP/Oakley	リアルタイムIPSec, ISAKMP解析ソフトウェア
InstaGate	Technologic	Technologic	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ハードウェア
Interceptor	Technologic	Technologic	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ハードウェア
KPS Cipher PC Guard	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		KPS対応暗号通信用PCカード
KPS CipherPRO	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		ファイル暗号ソフトウェア
KPSAGS	アドバンス	アドバンス	鍵共有	KPS		KPS鍵配送方式のIDを生成するソフトウェア
MELWALL A3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号アダプタ ハードウェア
MELWALL H3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		集線型暗号装置 ハードウェア
MELWALL Mgr	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(512bit)		鍵管理ソフトウェア
MELWALL P3000	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ドライバソフトウェア (WAN対応)
MELWALL P3000CL	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ドライバソフトウェア(LAN対応)
MistyGuard/ CRYPTOFILE	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)		ファイル暗号化ソフトウェア
MistyGuard/ DIGICAPSULE	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)	X.509	暗号化コンテンツ配布
nCipher KeySafe	nCipher	東京エレクトロン	公開鍵	RSA, El Gamal	X.509	・鍵管理GUIソフトウェア

			署名 鍵配送	DSA Diffie-Hellman	SSL v2/v3 TLS PKCS#11	・ K of NIによる 秘密鍵分散管理 機能
NE-Secure	ソリトンシステムズ	ソリトンシステムズ	共通鍵 公開鍵	FEAL, DES RSA		LAN間接続の暗号ルータ
NetSwift 1000 PCI Card	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, RC4 RSA(384~1024bit) DSA Diffie-Hellman MD5, SHA-1, HMAC	IPSec DMA ISO	暗号PCIカード
nFast PCI Crypto Accelerator	nCipher	東京エレクトロン	公開鍵 署名 鍵配送	RSA DSA Diffie-Hellman	SSL v2/v3 TLS SET S/MIME	・ SSL暗号化アクセラレータ (PCI接続) ・ 各種Webサーバ対応API(MS CryptoAPI、 OpenSSL他対応)
nFast SCSI Crypto Accelerator	nCipher	東京エレクトロン	公開鍵 署名 鍵配送	RSA DSA Diffie-Hellman	SSL v2/v3 TLS SET S/MIME	・ SSL暗号化アクセラレータ (SCSI接続) ・ 各種Webサーバ対応API(MS CryptoAPI、 OpenSSL他対応)
nForce Hardware Security Modules	nCipher	東京エレクトロン	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11	・ SSL暗号化アクセラレータ (PCI接続) ・ 各種Webサーバ対応 API(PKCS#11、 MS CryptoAPI、 OpenSSL他対応)
nForce SCSI Hardware Security Modules	nCipher	東京エレクトロン	共通鍵 公開鍵 署名 鍵配送	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11	・ SSL暗号化アクセラレータ (SCSI接続) ・ ハードウェアセキュリティモジュール(HSM) ・ FIPS140-1 レベル2認定 ・ 各種Webサーバ/PKIアプリケーション対応



			ハッシュ		FIPS140-1レベル2認定	API(PKCS#11、MS CryptoAPI、OpenSSL他対応)
NLC0268A	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵	DES(56bit), TripleDES(112bit,168bit)		各種暗号製品
nShield Hardware Security Modules	nCipher	東京エレクトロン	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11 FIPS140-1レベル3認定	・ハードウェアセキュリティモジュール(HSM) ・FIPS140-1レベル3認定 ・各種PKIアプリケーション対応 API(PKCS#11、MS CryptoAPI他対応) ・nCipher KeySafeソフトウェアによる鍵管理 ・K of Nによる秘密鍵分散管理機能
NSOC3	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送	DES(56bit), TripleDES, RC4 RSA DSA, 楕円DSA Diffie-Hellman, 楕円Diffie-Hellman	IPSec IKE	暗号PCIカード
NX7000 暗号ボード	NEC	NEC	共通鍵 公開鍵	DES(56bit), TripleDES RSA (512~1024bit)	FIPS140-1	暗号ボード
Page Vault	Authentica Security	ディアアイティ	共通鍵	RC4(128bit)		暗号化ソフトウェア
PGP Certificate Server	Network Associates	日本ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120~168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4096bit)	PGP	鍵管理サーバソフトウェア
PGP for SDK	Network Associates	日本ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120~168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4096bit)	PGP	PGPシステム開発モジュール
PointSec!	ProtectData	メトロ NECソフト	共通鍵	BlowFish(56,256bit), CAST(56,128bit)	ANSI X9.9	企業向けハードディスク丸ごと暗号化ソフトウェア
Private Internet Exchange	Cisco Systems	日本シスコシステムズ	共通鍵	DES(56bit)	NAT	ハードウェア
Protect Plus	DECROS	東芝情報システム	共通鍵	WinCros(80 or 160bit), WinCros II (80 or 160bit), CAST		ファイル暗号化ソフトウェア

SecureBOX (セキュアボックス)	富士通北陸システムズ	富士通北陸システムズ	共通鍵	DES(56bit), TripleDES(168bit), RC2(40, 64, 128, 256bit)	PKCS#5	ファイル暗号化 /圧縮ソフトウェア  自動暗号化が可能  管理者による緊急時データリカバリが可能
SECURE PC CARD	富士通ビー・エス・シー	富士通ビー・エス・シー	共通鍵	DES(56bit)		セキュア活性化方式 (自動暗号復号)  ・指紋認証版  ・ハードウェア版 (PCカード)  ・ソフトウェア版
SecureExplorer 防人	ローレル インテリジェント システムズ	ローレル インテリジェント システムズ	共通鍵	SXAL/MBAL		暗号化ソフトウェア
SecureWare/ ICカード発行キット	NEC	NEC	公開鍵 ハッシュ	RSA (1024bit) MD5, SHA-1		ソフトウェア
SecureWare/ 暗号ボードマネージャ	NEC	NEC	共通鍵 公開鍵	DES(56bit), TripleDES RSA (512~1024bit)		暗号ボードの制御ソフトウェア
SecureWare/ 秘密鍵マネージャ	NEC	NEC	共通鍵 公開鍵	DES(56bit) RSA (512~4096bit)		秘密鍵管理ソフトウェア
SecurityPack'98	システムニーズ	システムニーズ	共通鍵	カオス量子化多値暗号(56bit)		ICカード対応セキュリティシステム
SmartCipher (スマートサイファー)	ローレルインテリジェントシステムズ	ノア・ビジネス	共通鍵	SXAL/MBAL		ファイル・データ暗号化
SmartSafe for Notes	BIGベスト情報システム	ノア・ビジネス	共通鍵	SXAL/MBAL		Lotus Notes対応  ソフトウェア
Soliton IPSec	ソリトンシステムズ	ソリトンシステムズ	共通鍵	DES, TripleDES, FEAL	IPSec	暗号化ソフトウェア
SSH Internet Key Exchange	SSH Communications Security	SSH Communications Security	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES(168bit), Blowfish(40~4467bit), CAST(80bit以上) RSA SHA-1, MD5	X.509, IKE, ISKAMP, PKCS	鍵管理ソフトウェア
Tripwire	Tripwire	東芝情報システム		El Gamal(128bit)、RSA相当		不正アクセス検知ソフトウェア

Tumbleweed IME 4.0	Tumbleweed Communications	タンブルウィー ド・コミュニケー ションズ	共通 鍵 ハッ シユ 鍵配 送	RC4 MD5,SHA-1 Deiffie-Hellman(512bit)	SSL PKI	セキュアパッケ ージ配信ソフト ウェア
VerSecure	Hewlett Packard	日本HP	共通 鍵 公開 鍵 鍵配 送	DES(56bit), TripleDES(128bit), RC2(40~128bit), RC4(40~128bit) RSA(256~2048bit) Deiffie-Hellman(512~2048bit)	IPSec	ハードウェアベ ース 暗号フレームワ ーク
WinSafe Lite	システムニーズ	システムニーズ	共通 鍵	カオス量子化多値暗号(56bit),DES(56bit)		データ暗号化ソ フトウェア
あい言葉	システムニーズ	システムニーズ	共通 鍵	カオス量子化多値暗号(56bit)		ICカード対応デ ータ暗号化ソフ トウェア
暗号プロセッサ	富士通	富士通	共通 鍵 公開 鍵	DES(56bit),TripleDES(168bit) RSA(最大2048bit)		暗号化PCIポート
暗号プロセッサ	富士通	富士通	共通 鍵	DES(56bit),TripleDES(168bit)		GS8000向け暗 号プロセッサ
安心金庫PRO Group Edition	トランスコスモス	トランスコスモス	共通 鍵	TEE128(128bit), GOST, DES(56bit), TripleDES(168bit), Blowfish(128/160bit)		動的鍵共有アル ゴリズム (1024bit)使用 ソフトウェア
回線暗号装置 T- Cypher	NTTエレクトロニ クス	NTTエレクトロニ クス	共通 鍵	FEAL、DES及びTripleDES		ハードウェア
カオスリモコン v2.02	国際情報科学研 究所	国際情報科学研 究所	共通 鍵	GCCカオス暗号 (320bit)		メール暗号化リ モコン ソフトウェア
カオスリモコン v2.2	国際情報科学研 究所	国際情報科学研 究所	共通 鍵	GCCカオス暗号 (320bit)	S/MIME PGP	暗号リモコン ソフトウェア
スマートセデッ ク	大日本印刷	大日本印刷	共通 鍵 公開 鍵	DES(56bit) RSA(512/576bit)		データ分割&暗 号システム
セキュアサービ スプラットフォーム	NTTアドバンス テクノロジー	NTTアドバンス テクノロジー	共通 鍵	FEAL, DES		認証、権限、暗 号化のプラット フォーム
ノキアIPシリー ズ	NOKIA	NOKIA ネットワーク インテック KDD 東芝情報システム	共通 鍵	DES(56bit) , RC4(40bit) , FWZ-1		統合型ファイ アウォール、ルー タ
秘文/Enterprise	日立ソフトウェア エンジニアリング	日立ソフトウェア エンジニアリング	共通 鍵	IDEA		ネットワーク対 応自動ファイル 暗号ソフト
秘文/SAFE	日立ソフトウェア エンジニアリング	日立ソフトウェア エンジニアリング	共通 鍵	IDEA		自動ファイル暗 号ソフト

盗聴防止電話機	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵	鍵長128bit使用		ハードウェア
---------	-------------	-------------	-----	------------	--	--------

(4) 暗号ライブラリ・暗号ツールキット

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
C/SSL	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵 公開鍵 ハッシュ	DES(40,56bit), TripleDES, RC4(40,128bit) RSA(1024bit) MD5, SHA	PKCS#7, #12 TLS	暗号化 クラスライブラリ ソフトウェア
Certicom Security Builder SDK	Certicom	Certicom	共通鍵 公開鍵 鍵配送 署名 ハッシュ	DES(56bit), TripleDES(112bit), RC4 楕円曲線暗号 Diffie-Hellman, 楕円Diffie-Hellman DSA, 楕円DSA SHA-1	ANSI X9.62, ANSI X9.63, S/MIME, TLS, PKIX, IIEEEP1363	暗号ツールキット
Certicom SSL Plus Toolkit	Certicom	Certicom	共通鍵 公開鍵 鍵配送 署名 ハッシュ	DES(56bit), TripleDES, RC4 RSA, 楕円曲線暗号 Diffie-Hellman DSA MD5, SHA-1	X.509, SSL, TLS, PKIX, ANSI X9.62, ANSI X9.63, IIEEEP1363	SSL対応暗号ツールキット
CICロック (汎用コンピュータ用)	シーアイシーシステムズ (他社と共同)	シーアイシーシステムズ 富士通エフ・アイ・ピー	共通鍵・ハッシュ	独自暗号方式(128bit) ・ブロック暗号 ・ストリーム暗号 ・圧縮 ・SHA		暗号・圧縮化ソフトウェア
Crypto System Toolkit for Visual Basic	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵 公開鍵 署名 ハッシュ	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4, BSA4, BSA5 RSA DSA SHA-1, MD2, MD5, BHF, BSAH, RIPEMD, RIPED-160, MDC2, HMAC	PKCS#1, #3, #5, #8, #12	暗号化クラスライブラリ
Crypto System Toolkit v7.2	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵 公開鍵 署名 ハッシュ	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4, BSA4, BSA5 RSA DSA	PKCS#1, #3, #5, #8, #12	暗号化クラスライブラリ

				SHA-1, MD2, MD5, BHF, BSAH, RIPEMD, RIPPED-160, MDC2, HMAC		
CryptoWsift SoftWare Developer's Kit	RAINBOW Technologies	RAINBOW Technologies	公開 鍵 署名 鍵配 送	RSA(384~1024bit) DSA Diffie-Hellman	SSL, X.509, S/MIME, PKCS, SET, SSH, IKE, IPSec, TLS, S/WAN, FIPS	暗号ツールキット
Entrust/Toolkit	Entrust Technologies	エントラストジャ パン NTTデータ(SIパ ートナー) セコム情報システ ム セコム サイバーセ キュリティ事業部 ネットマークス	共通 鍵 公開 鍵 署名 ハッ シュ 鍵配 送	DES(56bit), TripleDES, CAST(40,64,80,128bit), RC2(40,128bit) RSA DSA MD5, SHA-1 Diffie-Hellman	PKCS FIPS140-1 RFC LDAP IKE, IPSec PEM GSS-API	<ul style="list-style-type: none"> <li>・ S/MIME、SSLアプリケーションから、Managed-PKI対応アプリケーションまで、様々なレベルに応じたアプリケーションを構築可能</li> <li>・ 既存で動作しているシステム/アプリケーションを、Entrust/PKIが提供するManaged-PKI対応にカスタマイズ可能(CMS Toolkit)</li> <li>・ 多くの開発言語をサポート(C/C++、Java、COM)</li> <li>・ 輸出規制対象製品(カナダ)</li> </ul>
FlexCrypto	ドゥイット	ドゥイット	共通 鍵	MES[Multi-methods Encryption Scheme](最大 60bit)		Java暗号化ライ ブラリソフトウエア (開発キットとし て提供)
FSEcParamGen V1.0L10 (WindowsNT)	富士通	富士通	公開 鍵	楕円曲線暗号 (50bitから 600bitまで)	ANSI X9.62, IEEE P1363, SECG	楕円曲線パラメタ 生成ツール
IAIK-JCE	IAIK	IAIK	共通 鍵 公開 鍵 署名 鍵配 送 ハッ シュ	DES(56bit), TripleDES112bit), IDEA(64bit), Blowfish(64~ 448bit), GOST(64~256bit), CAST128(64~128bit), RC2(64bit), RC4 RSA DSA Diffie-Hellman MD2, MD5, SHA-1	PKCS ANSI X.509 FIPS PUB	Javaアプリケーシ ョン用暗号ツール キット
J/CRYPTO	Baltimore Technologies	日本パルチモアテ クノロジーズ	共通 鍵	DES(56bit), TripleDES(112bit), RC2,	PKCS X.509	Javaアプリケーシ ョン用暗号化クラ

			公開鍵 署名 鍵配送	RC4(128bit) RSA(512,1024bit) DSA(512,768,1024bit) Diffie-Hellman(256,512,768,1024bit)	HMAC FIPS-186	スライブラリ
J/SSL	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵 公開鍵 ハッシュ	DES(40,56bit), TripleDES, RC4(40,128bit) RSA(1024bit) MD5, SHA	PKCS TLS	暗号化クラスライブラリ
Keymate/Crypto	日立製作所	日立製作所	共通鍵 公開鍵	MULTI2(256bit), DES(56bits), TripleDES(168bits) 楢円曲線, RSA		暗号ライブラリソフトウェア
Keymate/Multi Ver2	日立製作所	日立製作所	共通鍵	MULTI2(256bit)	GSS-API	暗号ライブラリ&ユーティリティソフトウェア
KPSSDK	アドバンス	アドバンス	共通鍵 鍵配送	TripleDES(112bit), DES(56bit) KPS		KPSソフトウェア開発キット
nCipher Software Developer Kit	nCipher	東京エレクトロン	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	PKCS#11 MSCAPI OpenSSL FIPS140-1 レベル3認定	・アプリケーション開発用暗号ツールキット ・PKCS#11、MSCAPI、OpenSSL、nCipher Native API(C、Java)対応 ・FIPS140-1 レベル3認定 ・鍵管理・秘密鍵分散管理機能
PKCS暗号ソフトウェア標準キット	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC2(5~128byte), RC5(5~255byte), MISTY1(128bit) RSA相当(512~4096bit), DSA(512~1024bit) MD2(128bit), MD5(128bit), SHA-1(160bit)	X.509 PKCS	暗号ソフトウェア
Policy Director for SECOM3.0 (旧名称 InterVerse)	US IBM社	日本ダスコム(販売元) セコム情報システム	共通鍵 公開鍵	DES(56bit) ※SSL認証、ケロベロス認証 RSA	X.509, ケロベロス LDAPサーバ(ユーザ管理情報サーバ用、製品にバンドル)	3階層型Webアプリ用統合管理製品 (認証、シングルサインオン、アクセスコントロール、負荷分散)
PowerMISTY for Windows/HP-UX	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit), DES(56,112,168bit), RC2 RSA, 楢円ELGamal MD5, MD2, SHA-1, SHA		暗号ライブラリソフトウェア

			ハッシュ署名	RSA, DSA, 楕円DSA		
RSA BSAFE Cert-C	RSA Security	RSAセキュリティ	公開鍵 ハッシュ	RSA MD2, MD5, SHA-1	PKCS X.509	PKIアプリケーション開発用暗号化ツールキット
RSA BSAFE Cert-J	RSA Security	RSAセキュリティ	公開鍵 ハッシュ	RSA MD2, MD5, SHA-1	PKCS X.509	PKIアプリケーション開発用暗号化ツールキット (Java用)
RSA BSAFE Crypto-C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES, TripleDES, RC2, RC4, RC5, RC6 RSA RSA, DSA/DSS MD2, MD5, SHA-1 Diffie-Hellman	ANSI NIST (FIPS) PKCS IEEE	C言語用汎用暗号化ツールキット
RSA BSAFE Crypto-J	RSA Security	RSAセキュリティ	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES, RC2, RC4, RC5, RC6 RSA RSA, DSA/DSS MD2, MD5, SHA-1 Diffie-Hellman	NIST (FIPS) PKCS	Java用汎用暗号化ツールキット
RSA BSAFE S/MIME -C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 ハッシュ	DES, RC2, RC5 RSA MD5, SHA-1	IETF (S/MIME) PKCS X.509	S/MIME対応アプリケーション開発用暗号化ツールキット
RSA BSAFE SSL-C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 鍵配送 ハッシュ 署名	DES, TripleDES, RC2, RC4 RSA Diffie-Hellman MD5, SHA-1 RSA, DSA, DSS	SSL IETF (TLS) PKCS X.509	C言語用SSL対応アプリケーション開発用暗号化ツールキット
RSA BSAFE SSL-J	RSA Security	RSAセキュリティ	共通鍵 公開鍵 鍵配送	DES, RC4 RSA Diffie-Hellman MD5, SHA-1	SSL IETF (TLS) PKCS X.509	SSL対応アプリケーション開発用暗号化ツールキット

			ハッシュ			
RSA BSAFE WTLS-C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES, TripleDES, RC5 RSA RSA MD5, SHA-1 Diffie-Hellman	ANSI X.509 v3 WTLS v1.1 PKCS	C言語用WAP対応 アプリケーション 開発ツールキット
S/MIME暗号ソフトウェア標準キット	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵 ハッシュ	DES (56bit), TripleDES (56×3bit), RC2 (40,128,256bit), RC4 (40,128,256bit), MISTY (128bit) RSA相当(512~4096bit) MD2(128bit), MD5(128bit), SHA-1(160bit)	S/MIME PKCS X.509v3	S/MIMEをベースとする暗号通信ツールキット (開発中)
Secure Messaging Toolkit	Baltimore Technologies	日本バルチモアテクノロジー	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC2(40,64,128bit) RSA(512~2048bit) MD5, SHA-1	S/MIME X.509 PKCS#1,#5,#7	S/MIMEをベースとする暗号通信ツールキット
Securecryptoライブラリ 1.1 Solaris用	富士通	富士通	公開鍵 共通鍵 ハッシュ	RSA(2048bit), ECDSA DES, TripleDES, RC2 MD5,SHA-1	PKCS	暗号ライブラリ (アプリケーション開発)
Securecryptoライブラリ V1.0L30 Windows用	富士通	富士通	公開鍵 共通鍵 ハッシュ	RSA(2048bit), ECDSA DES, TripleDES, RC2 MD5, SHA-1	PKCS	暗号ライブラリ (アプリケーション開発)
Securecryptoライブラリ ランタイム for 暗号プロセッサ 1.0 Solaris用	富士通	富士通	公開鍵 共通鍵 ハッシュ	RSA(2048bit) DES, TripleDES MD5, SHA-1	PKCS	暗号ライブラリ (ランタイムライブラリ)
Securecryptoライブラリ ランタイム for 暗号プロセッサ V1.0L10 WindowsNT4.0 Server用	富士通	富士通	公開鍵 共通鍵 ハッシュ	RSA(2048bit) DES, TripleDES MD5, SHA-1	PKCS	暗号ライブラリ (ランタイムライブラリ)
SecureWare/ 開発キット	NEC	NEC	共通鍵	DES(56bit), TripleDES RSA (512~1024bit)		ソフトウェア



			公開鍵 ハッシュ	MD5, MD2, SHA-1		
Soliton IPSEC	ソリトンシステムズ	ソリトンシステムズ	共通鍵	DES(56bit), TripleDES(168bit), FEAL(64bit)	IPSEC	IPレベルの暗号ツール
SSH IPSEC Express Tollkit	SSH	SSH			ISKAMP IPSec IKE X.509	暗号ツールキット
SunScreenSKIP エクスポータブル版 グローバル版	Sun Microsystems	サン・マイクロシステムズ	共通鍵 ハッシュ	RC2(40bit), DES(56bit), RC4(40bit) KeyedMD5	SKIP	暗号ソフトウェア モジュール
暗号ライブラリ (カオス量子化多値暗号方式)	システムニーズ	システムニーズ	共通鍵	カオス量子化多値(56bit以上)		プログラム組込型 暗号/復号モジュール (Windows版)
セキュリティライブラリ	日立製作所	日立製作所	共通鍵 公開鍵	DES(56bit), MULTI2(256bit) RSA(1024bit)	X.509 PKCS#7	セキュリティライブラリ ソフトウェア
セキュリティライブラリ開発環境	日立製作所	日立製作所		暗号エンジン無し。前提プログラムとしてKeymate/Crypto要		セキュリティライブラリ開発ツール ソフトウェア
認証サーバ/セキュリティライブラリ	日立製作所	日立製作所	共通鍵 公開鍵	DES3 (128bit) RSA (1024,2048bit)	X.509 PKCS#7 PKCS#10	セキュリティライブラリ ソフトウェア
法人認証/公証ライブラリ	日立製作所	日立製作所	共通鍵 公開鍵	DES3 (128bit) RSA (1024,2048bit)	X.509 CMP (rfc2510) OCSP (rfc2560)	法人認証/公証システム ソフトウェア

## 2. VPN

製品名	開発元	国内販売窓口		暗号アルゴリズム・鍵長	標準化対応	製品概要
Access Point 450/1000	Lucent Technologies	<a href="#">販売代理店</a>	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit) MD5(128bit), SHA-1(160bit)	IPSec L2TP(LNS)	VPN構築
AccessMaster RemoteAccess Security	Bull	ブル	共通鍵	DES/TripleDES (40bit,56bit,128bit)	SOCKS v5 SSL v3	統合セキュリティ 管理ソフトウェア
AccessMaster VPN	Bull	ブル	共通鍵	DES(56bit), TripleDES(168bit) RSA(2048bit)		統合セキュリティ 管理ソフトウェア

			公開鍵			
AltaVista Tunnel 98	AltaVista Software	アクセントテクノロジー	共通鍵 公開鍵 ハッシュ	RC4(40,56,128bit) RSA(512bit) MD5		ソフトウェア
Altiga C50,C20,C10	Altiga Networks	Altiga Networks	共通鍵 公開鍵 鍵配送 ハッシュ	DES(56bit) , TripleDES(168bit) , RC4(40,128bit) Deiffie-Hellman MD5, SHA-1, HMAC	X.509 IPSec IKE LDAP	VPNハードウェア
cIPro-VPNシリーズ	RADGUARD	千代田情報機器	共通鍵 鍵配送 署名	DES(56bit), TripleDES(112bits) RSA(256bit), IKE DES-MAC	IPSec IKE	VPN構築 ハードウェア
Cisco IOS Firewall	Cisco Systems	日本シスコシステムズ	共通鍵	DES(56bit) , TripleDES(168bit)	IPSec	VPN対応ファイアウォールシステム ソフトウェア
CiscoPIX FireWall 500	Cisco Systems	日本シスコシステムズ	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit) MD5	IPSec	暗号化 ファイアウォール
CyberGuard Firewall	CyberGuard	日立ソフトウェアエンジニアリング			NCSC-B2準拠	ファイアウォール VPN機能をオプションでサポート
Encryptor	Cylink Company	アズジェント	共通鍵 公開鍵	DES(56bit) ,TripleDES(168bit) Diffie-Hellman(1024bit) MD5,SHA-1		専用線・フレームリレー・ATM用VPN装置

			ハ ッ シ ユ			
Entrust/VPN Connector	Entrust Technologies	エントラスト ジャパン NTTデータ(SI パートナー) セコム情報シ ステム セコム サイバ ーセキュリティ 事業部 ネットマーク ス		各VPNデバイスに依存	X.509v3, IPSec CEP PKCS #7, #10 PEM/BASE64 ASN.1, LDAP,	・ IPSec標準をサポ ートするVPNデバ イス、VPNアプリ ケーションに対し て、証明書を発行 ・ 広範囲なVPNネ ットワークを構築 可能
Fireless FL-50A/FL-80A	コンテック	コンテック	共 通 鍵	DES(56bit), RC5		ハードウェア,ソフ トウェア一体型 F W
FireWall Plus V4.0	Network-1 Security Solutions	三井物産	共 通 鍵 ハ ッ シ ユ	DES(56bit) MD4,MD5	CAPI	
FireWall-1	Check Point Software Technologies	フォーバルク リエーティブ ENICOM ART ソフトバンク 富士通	共 通 鍵 公 開 鍵 ハ ッ シ ユ	RC4(40bit), RC2(40bit), DES(56bit), TripleDES(128bit), CAST(128bit), FWZ-1(48bit) RSA(1024bit), Diffie- Hellman(1024bit) MD5,SHA-1	X.509 IPSec SKIP I K E	VPN,PKI対応 ソフトウェア
FortKnox F-3000/F- 5000	Alcatel	日本アルカテ ル クボタシステ ム開発	共 通 鍵	RC4 (40bit) , DES(56bit), TripleDES (128bit)	IPsec,ISAKMP	VPNハードウェア (ファイアウォール)
F-Secure VPN	F-Secure	山田洋行	共 通 鍵 公 開 鍵	TripleDES(168bit), Blowfish(128bit) RSA(1024bit)	SSH	VPN構築ソフトウ ェア
F-Secure VPN + /Enterprise Gateway for WindowsNT4.0 /Gateway Windows NT4.0 /Solaris, Linux 等 (β版)	F-Secure	山田洋行	共 通 鍵 認 証 方 式	TripleDES(168bit), IDEA(128bit), Blowfish(40- 446bit), CAST128(40-128bit), DES(56bit) HMAC-MD5-96, HMAC-SHA-96	IPSec ISAKMP/Oakley	VPN構築ソフトウ ェア
F-Secure VPN + /Server for	F-Secure	山田洋行	共 通	TripleDES(168bit), IDEA(128bit), Blowfish(40-	IPSec ISAKMP/Oakley	VPN構築ソフトウ ェア

WindowsNT4.0 /Client for Windows95, 98, NT4.0			鍵 認 証 方 式	446bit), CAST128(40-128bit), DES(56bit) HMAC-MD5-96, HMAC-SHA-96		
Guardian IPsec Client	NetGuard	NetGuard	共 通 鍵 ハ ッ シ ユ	DES(40,56bit), TripleDES(168bit) SHA	X.509 IPSec IKE	VPNソフトウェア
Guardian IPsec VPN soft	NetGuard	NetGuard	共 通 鍵	DES(40,56bit), TripleDES(168bit)	X.509 IPSec IKE	VPNソフトウェア
Guardian IPsec VPNNodeManager	NetGuard	NetGuard	共 通 鍵 ハ ッ シ ユ	DES(40,56bit), TripleDES(168bit) SHA	X.509 IPSec	VPNソフトウェア
IBM SecureWay Firewall V4.1 AIX/ WindowsNT	IBM	日本IBM	共 通 鍵	DES(56bit) CDMF(40bit)	IPSec	VPN対応 ファイアーウォール
Infonet VP-100	Alcatel	クボタシステム 開発	共 通 鍵	DES(56bit)	IPsec, IKE/ISAKMP	VPNハードウェア
interConclave	Internet Dynamics	アズジェント	共 通 鍵 公 開 鍵 ハ ッ シ ユ	RC4(40bit), RC2(40bit), DES(56bit), TripleDES(128bit) RSA(1024bit), Diffie- Hellman(2048bit) SHA-1	X.509 IPSec SKIP I K E	統合セキュリティ ソフトウェア
LANBASE SX20	日新電機	日新電機	共 通 鍵 ハ ッ シ ユ	IDEA(128bit), DES(56bit : 対応 予定) 鍵付きMD5	IPSec準拠	VPN対応暗号装置 ハードウェア
Mucho-EV	Alcatel	クボタシステム 開発	共 通 鍵	DES(56bit)	IPsec, IKE/ISAKMP	VPNハードウェア (ルータ)
net GUARDIAN	Net Guard	日立ソフトウ ェアエンジニア リング	共 通 鍵 公 開 鍵	RC2, RC4(各40bit) RSA	IPSec	VPN対応FireWall ソフトウェア

NetCocoon Client/Server	松下電工	松下電工	共通鍵 鍵配送	DES(40,56bit), TripleDES(112,168bit)  Diffie-Hellman	IPSec	VPN対応  ソフトウェア
NetDefender	Technologic	ダイナラブ・ ジャパン			IPSec X.509	ファイヤーウォール
NetGuard Control Center	Net Guard	日立ソフトウ ェアエンジニア リング	共通鍵 公開鍵	RC2, RC4(各40bit)  RSA	IPSec	VPN対応FireWall  ソフトウェア
Network CryptoGate	東芝	東芝情報シス テム	共通鍵	DES(56bit), TripleDES(168bit)	IPSec Mobile-IP	VPNソフトウェア
NOKIA IPセキュリティ シリーズ	NOKIA	アズジェント	共通鍵 公開鍵 ハッシュ ユ	RC4(40bit), RC2(40bit), DES(56bit), TripleDES(128bit), CAST(128bit), FWZ-1(48bit)  RSA(1024bit), Diffie- Hellman(1024bit)  MD5,SHA-1	X.509 IPSec SKIP  I K E	ファイアウォール 内臓型ルータ X.509
OmniGuard/ PowerVPN	Axent Technologies	ソリトンシス テムズ  千代田情報機 器	共通鍵 鍵配送 ハッシュ ユ	DES(56bit), TripleDES(112,168bit)  Diffie-Hellman  MD5		ワンタイム  パスワード・暗号 化  VPN
PERMIT/Client	TimeStep	ディアイティ クボタシステ ム開発	共通鍵 公開鍵 ハッシュ ユ	DES(56bit), TripleDES(168bit),  RC5(40~2040bit), Blowfish(40 ~448bit), CAST(40~128bit), IDEA(128bit)  RSA  HMAC-MD5, HMAC-SHA1	IPSec (IKE, IKE- XAUTH)  X.509v3  PKCS#7, #10, #12  IPComp (LZS)	VPNソフトウェア
PERMIT/Gate1520 (2Mbps)  PERMIT/Gate2520 (4Mbps)	TimeStep	ディアイティ クボタシステ ム開発	共通鍵	DES(56bit), TripleDES(168bit),  RC5(40~2040bit), Blowfish(40 ~448bit), CAST(40~128bit), IDEA(128bit)	IPSec (IKE, IKE- XAUTH)  X.509v3	V P Nハードウェ ェア  ゲートウェイ

PERMIT/Gate4620 (10Mbps) PERMIT/Gate7520 (70Mbps)			公 開 鍵 ハ ッ シ ユ	RSA HMAC-MD5, HMAC-SHA1	PKCS#7, #10, #12 PKIX IPComp (LZS) FIPS-140-1 level 2 ISO 9000	
Pipeline 220	Lucent Technologies	<a href="#">販売代理店</a>	共 通 鍵 ハ ッ シ ユ	DES(56bit), TripleDES(168bit) MD5(128bit), SHA-1(160bit)	IPSec SSL	VPN構築
PowerVPN	AXENT Technoogies	日新電機	共 通 鍵	DES(56bit)		暗号通信ソフトウ ェア
PrivateWire	Algorithmic Rsearch/ Cylink Company	アズジェント	共 通 鍵 公 開 鍵 ハ ッ シ ユ	RC4(128bit), DES(56bit), TripleDES(128bit) RSA(1024bit) MD5,SHA-1	X.509	認証、暗号、ファ イアーウォール統 合 ソフトウェア
PusBuilder トンネルスイッチ	3com	3com	共 通 鍵 ハ ッ シ ユ	DES(56bit), TripleDES, RC4, RC5 MD5, SHA-1	IPSec	VPNハードウェア
Raptor FireWall RaptorRemote RaptorMobile	AXENT Technoogies	日立インフォ メーションテ クノロジー	共 通 鍵 ハ ッ シ ユ 鍵 配 送	DES(56bit), Triple DES(米国内 のみ), RC2(40bit) Keyed MD5, SHA-1, MD5 Deffie-Hellman	IPSec IKE swIPe X.509	VPN対応FireWall ソフトウェア
Safegate	富士通	富士通	共 通 鍵 公 開 鍵 ハ ッ シ ユ	DES(56bit),TripleDES(168bit) RSA(512,768,1024,2048bit) MD5(128bit),SHA-1(160bit) Deffie-Hellman	X.509 IPSec IKE	VPN対応ファイア ウォール ソフト ウェア

			鍵 配 送			
SC-W001	ステラクラフト	ステラクラフト		Odo2(56bit : 独自暗号)		VPN
Secure Connect Firewall + VPN	Lucent Technologies	<a href="#">販売代理店</a>	共 通 鍵 ハ ッ シ ユ	DES(56bit), TripleDES(168bit) MD5(128bit), SHA-1(160bit)	IPSec SSL	VPN構築
Secure Socket	日立製作所	日立製作所	共 通 鍵	MULTI2(256bit)	ISO/IEC9798 X.509	VPNシステム ソフトウェア
Sidewinder Security Server	Secure Computing	ネットワンシ ステムズ			IPSec (オプション)	VPN対応ファイア ウォール
SmartGate	V-ONE	V-ONE アスキーNT	共 通 鍵 公 開 鍵	DES(56bit) RSA		VPN アプリケーション
SOCKS VPN-E40 ver2.4	NEC	NEC	共 通 鍵 公 開 鍵 ハ ッ シ ユ	RC4(40bit), DES (56bit) RSA(512,768,1024bit) MD5	SSL	VPN構築ソフトウ ェア
SOCKSVPNver2.1 + SecureWare/認証キ ット	NEC	NEC	共 通 鍵 公 開 鍵	DES(56bit) RSA(512,768,1024bit)	ISO/IEC11770	VPN構築ソフトウ ェア
SonicWALLPro	SonicWALL Inc.	住友金属シス テム開発	共 通 鍵	DES(56bit), RC4	IPsec	VPN,FireWall対応 ハードウェア
VPN-1 Accelerator Card	Check Point Software Technologies	日本IBM NEC	共 通 鍵 ハ ッ シ ユ	DES(56bit), TripleDES(168bit) MD5, SHA-1	IKE IPSec	VPN対応 ハードウェアカー ド
VPN-1 SecuRemote	Check Point Software Technologies	日本IBM NEC	共 通 鍵 公 開 鍵 鍵 配	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512~1024bit) Diffie-Hellman(512~1024bit)	IKE SKIP IPSec X.509	リモートVPN ソフトウェア

			送			
VPN-1 Appliance	Check Point Software Technologies	日本IBM NEC	共通鍵 公開鍵 鍵 配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512~1024bit) Diffie-Hellman(512~1024bit)	IKE SKIP IPSec	VPNハードウェア
VPN-1 GatewaySolutions	Check Point Software Technologies	日本IBM NEC	共通鍵 公開鍵 鍵 配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512~1024bit) Diffie-Hellman(512~1024bit)	IKE SKIP IPSec X.509	VPN対応 ゲートウェイ ソフトウェア
VPN-1 SecureClient	Check Point Software Technologies	日本IBM NEC	共通鍵 公開鍵 鍵 配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512~1024bit) Diffie-Hellman(512~1024bit)	IKE SKIP IPSec X.509	VPNソフトウェア
VPN210 VPN220 VPN230 VPN240	NOKIA	NOKIA ネットワール ド インテック KDD 東芝情報シス テム	共通鍵	DES(56bit), RC4(40bit), FWZ-1	IPSec	VPNハードウェア
VSU-1010/ VSU-10	ネットワールド	ネットマーク ス	共通鍵 ハッ シユ	DES(56bit) MD5	SKIP IKE IPSec X.509	VPN対応 ハードウェア
WatchGuard Firebox- II シリーズ	WatchGuard	千代田情報機 器	共通鍵 鍵 配送 署名	DES(56bit), TripleDES(112bit) IKE DES-MAC	IPSec IKE	VPN対応 ファイアーウォー ル ソフトウェア
WebTrends for FierWall and VPNs	WebTrends	アズジェント				VPN,FireWall対応 ソフトウェア



仮想プライベートネットワーク支援機能 for Gauntlet	日立製作所	日立製作所	共通鍵	MULTI2(256bit)	ISO/IEC9798	VPNシステム ソフトウェア
秘文/SC	日立ソフトウェアエンジニアリング	日立ソフトウェアエンジニアリング	共通鍵 公開鍵	IDEA RSA	SSL X.509	VPN構築ソフト

### 3. 認証製品

#### (1) PKI

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
CAstation@白山	東芝情報システム	NTTエレクトロニクス 東芝情報システム 東洋情報システム	公開鍵	RSA相当(512~2048bit)	X.500 X.509v3 LDAPv2,v3 PKCS#10, PKCS#7	電子認証局システム
CertMISTY for Windows	三菱電機	三菱電機	共通鍵 ハッシュ 署名	MISTY(128bit), DES(56, 168bit), RC2(40bit) MD5, MD2, SHA-1 RSA	X.509 PKCS#7, #10, #12	認証ライブラリ ソフトウェア
Entrust/Entelligence	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム セコム サイバーセキュリティ事業部 ネットマークス	共通鍵 公開鍵、鍵配送 ハッシュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11 S/MIME IPSec ISAKMP	・クライアント側アプリケーションとして、自動的な鍵/証明書管理を実現 ・暗号エンジンとして、各アプリケーションに対し、暗号、デジタル署名サービスを提供 ・輸出規制対象製品(カナダ)
Entrust/PKI	Entrust Technologies	エントラストジャパン NTTデータ(SIパートナー) セコム情報システム セコム サイバーセキュリティ事業部 ネットマークス	共通鍵 公開鍵、鍵配送 ハッシュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11 S/MIME IPSec ISAKMP	・Entrust/PKIは下記の2製品で構成 Entrust/Authority(証明書発行サーバー) Entrust/Admin(証明書発行管理コンソール) ・輸出規制対象製品(カナダ)
FibeCrypt	日本発条	日本発条		非公開		機械認識ファイバ ハードウェア
iKey	RAINBOW Technologies	RAINBOW Technologies	公開鍵 ハッシュ	RSA MD5	IPSEC/IKE SET,SSL	認証デバイス

					PKCS MilliCent eWallet X.509 S/MIME	
InfoCA	富士通	富士通	公開鍵 ハッシュ	RSA(2048bit) MD5(128bit), SHA-1(160bit)	X.509 V1,V3 PKCS 7,10	電子証明書発行ソフトウェア。国際標準(X.509)準拠の電子証明書を発行する機能を有している。
KyberPASS	KyberPASS	丸文	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES(168bit), CAST(128bit) RSA(512-1024bit), Deffie-Hellman(1024bit) MD5	PKCS#10,#11,#12, LDAP,X.509, RADIUS, TACACS/TACACS+	PKIを利用したユーザ認証、セントラル・アクセス・コントロール機能を有し、ダイレクト・セッションVPNを構築するミドルウェア。
MistyGuard CERTMANAGER	三菱電機	三菱電機	公開鍵 署名 ハッシュ	RSA(512,1024,2048bit) RSA MD5,SHA-1	X.509, PKCS, SSL,S/MINE, LDAP	認証サーバシステム
nShield Hardware Security Modules	nCipher	東京エレクトロン	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA Diffie-Hellman MD2, MD5, SHA-1, HMAC	SSL v2/v3 TLS SET S/MIME PKCS#11 FIPS140-1 レベル3 認定	<ul style="list-style-type: none"> <li>PKIハードウェアセキュリティモジュール(HSM)</li> <li>FIPS140-1 レベル3認定</li> <li>各種PKIアプリケーション対応</li> <li>API(PKCS#11、MS CryptoAPI他対応)</li> <li>nCipher KeySafeソフトウェアによる鍵管理</li> <li>K of Nによる秘密鍵分散管理機能</li> </ul>
PERMIT/Detector suite	TimeStep	ディアイティクボタシステム開発	公開鍵	RSA (1024bit)	PKIX X.509v3 PKCS#7,#10,#12	認証局、 ポリシー管理 アプリケーション
PKI Manager V1.1	富士通	富士通	共通鍵 公開鍵 ハッシュ	DES(56bit), T-DES, RC2, RC4 RSA(512,1024,2048bit) MD2,MD5, SHA-1	X.509 V1,V3 PKCS 7,10,12	PKI構築ソフトウェア。証明書鍵ペアを集中作成して、配布する機能を有している。
PKI-Plus SDK	Baltimore Technologies	日本バルチモアテクノロジーズ	共通鍵 公開鍵 鍵配送 署名	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4 RSA(1024,2048bit) Diffie-Hellman DSA	PKCS X.509	PKIソフトウェア
PKIサーバ/Carassuit	NEC	NEC	共通鍵 公開鍵 ハッシュ	DES(56bit) RSA(512~1024bit) MD5,SHA-1	X509	ソフトウェア
RSA Keon Agent	RSA Security	<a href="#">販売代理店</a>				エージェント・ソフト

RSA Keon Certificate Server	RSA Security	<a href="#">販売代理店</a>					デジタル証明書発行/管理ソフト
RSA Keon Desktop	RSA Security	<a href="#">販売代理店</a>	共通鍵 公開鍵	DES, TripleDES, RC5 RSA	X.509 PKCS		PKIクライアント・ソフト
RSA Keon Security Server	RSA Security	<a href="#">販売代理店</a>					デジタル証明書管理ソフト
SecureWare/ 認証プラグイン	NEC	NEC	共通鍵 公開鍵	DES(56bit) RSA	GSS-API ISO-IEC		ソフトウェア
UniCERT	Baltimore Technologies	日本バルチモアテクノロジーズ	公開鍵 署名	RSA DSA, 楕円DSA	X.509 SET S/MIME SSL SEIS PKCS		PKI
イントラキーセンタ	NTTアドバンステクノロジー	NTTアドバンステクノロジー	共通鍵 公開鍵 署名	FEAL(128bit) 楕円Diffie-Hellman(256bit) ESIGN(768bit)	PERSEUS		プライベートCA ソフトウェア
プライベートCAビルダー	NTTエレクトロニクス	NTTエレクトロニクス	公開鍵、署名 ハッシュ 関数	RSA相当(512~2048bit) SHA-1,MD5(各160,128bit)	X.509 PKCS#7,#10,#12		証明書発行局 ソフトウェア
鬼刑事ver 2.1 2000年6月に、 SecureTicketに改名予定	ワイ・ディ・シー	ワイ・ディ・シー	ハッシュ	MD5	SSL Ver3.0		ワンタイムパスワード セキュリティシステム

## (2) 電子署名

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
Atalla SignMaster ISP Atalla SignMaster/PCI ISP	Compaq Computer	コンパックコンピュータ	署名 ハッシュ	RSA, MAC, DSA(各256~2048bit) MD2, MD5, SHA-1	FIPS140-1レベル3 UL CSA TUV	署名, 認証 暗号化ハードウェア BOX/PCI
ESIGN	NTT	NTT	署名	ESIGN		電子署名ソフトウェア
Keymate/Sign	日立製作所	日立製作所		暗号エンジン無し。 Keymate/Multiの署名機能を前提プログラムとして使用		電子署名ソフトウェア

## (3) ワンタイムパスワード

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
CRYPTOCARD	CRYPTOCARD	ニューテクノロジーコーポレーション	共通鍵	DES(56bit)		リモートからのアクセス時に強力な個人認証機能を提供
CrypToken for Web	アドバンス	アドバンス	鍵共有	KPS		Webへのアクセスを管理
Defender	AXENT	日新電機	共通鍵	DES(56bit)		ユーザ認証システムハード

	Technologies					ノソフト
OmniGuard/ Defender	AXENT Technologies	ソリトンシステムズ 千代田情報機器	共通鍵	DES(56bit)		
RSA SecurID	RSA Security	<a href="#">販売代理店</a>	共通鍵 公開鍵	DES,RC5,SDI RSA	X.509, SSL, PKCS #11	
SAFEWORD	Secure Computing	メトロ(H15.12 取 扱終了) 千代田情報機器	共通鍵	DES(56bit)	ANSI	ワンタイムパスワードの世界モデル。B2B、B2C、B2B2Cの認証を導入即稼動で実現。

#### 4. ICカード

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
ActivCard Gold	ActivCard	エヌ・シー・エル コミュニケーション	共通鍵 公開鍵	DES(56bit) RSA(512,768,1024bit)	PKCS#11 X.509 SSL S/MIME	ICカード
ARCACLAVIS for CIPHER,LOCK, NOTES,VPN	ネットタイム	ネットタイム セコム情報システム		SXAL/MBAL(Substitution Xor Algorithm/Multi Block Algorithm),鍵長64bit	ISO9979登録済 (1995年)	ICカード
Certicom Smart Card Evaluation Toolkit	Certicom	Certicom	署名	楯円DSA (163~1024bit), DSA(163~1024bit)	ANSI X9.62 PKCS IETF X.509 ISO IEEE FIPS140-1	電子署名 ICカード
Crypto Builder	Bull	ブル	共通鍵 公開鍵	TripleDES(128bit) DSA(512bit)、RSA(1024bit)	PC/SC, CAPI, PKCS#11	クリプトICカード 開発ツールキット
Crypto Safe	Bull	ブル	共通鍵 公開鍵	TripleDES(128bit) DSA(512bit)、RSA(1024bit)	PC/SC, CAPI, PKCS#11	クリプトICカード アプリケーション
DNP Standard-7	大日本印刷	大日本印刷	共通鍵	DES(56bit)、TripleDES(112bit)	ISO/IEC7816, JIS X 6303, JIS X 6304, JIS X 6306, JICSAP(Ver1.0)	ICカード
DNP Standard-9	大日本印刷	大日本印刷	共通鍵 公開鍵 ハッシュ ユ	DES(56bit)、TripleDES(112bit) RSA(512~1024bit) SHA-1	ISO/IEC7816, JIS X 6303, JIS X 6304, JIS X 6306, JICSAP(Ver1.1), PC/SC, PKCS#11	ICカード
GemSAFE	Gemplus	日本バルチモアテクノロジーズ	公開鍵	RSA(512,1024bit)	PKCS#11, X.509, SSL,	ICカード

					S/MIME, ISO7816	
KPS Cipher Card	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		KPS対応暗号IC カード
MULTOS4	大日本印刷	大日本印刷	共通鍵 公開鍵	DES(56bit)、TripleDES(112bit) RSA(最大1024bit)	ISO/IEC7816	ICカード
RSA SecurID 3100	RSA Security	<a href="#">販売代理店</a>	公開鍵	RSA(512/1024bit)	X.509 PKCS#11 PC/SC	デジタル証明 書を保管できる 暗号化スマート カード
SafePad	Bull	ブル	共通鍵 公開鍵	DES(56bit) RSA(1024bit)	SET C-SET	ICカード リーダー・ライター
SecureWare /ICカード発行キット	NEC	NEC	共通鍵	DES(56bit)	ISO7816 PKCS#11	ソフトウェア
SmartAuth	ローレルインテリジ ェンスシステムズ	ローレルインテリジ ェンスシステムズ		独自暗号		ICカード
TBC80	Bull	ブル	共通鍵 公開鍵	TripleDES(128bit) DSA(512bit)、RSA(1024bit)	ISO7816	クリプトICカー ド
WinSafe Standard スマートカード4 K タイプ	システムニーズ	システムニーズ	共通鍵	カオス量子化多値 (56bit),DES(56bit)		ICカード対応セ キュリティシス テム
WinSafe Standard スマートカードタイ プ (クリプトカー ド)	システムニーズ	システムニーズ	共通鍵 公開鍵	カオス量子化多値 (56bit),DES(56bit) RSA(512bit)		ICカード対応セ キュリティシス テム、指紋照合 対応タイプもあ る
WinSafe 2000	システムニーズ	システムニーズ	共通鍵 公開鍵	カオス量子化多値 (56bit),DES(56bit) RSA(512bit)		ICカード対応セ キュリティシス テム
Windows2000スマー トカードセキュリティ キット	システムニーズ	システムニーズ	共通鍵	カオス量子化多値 (56bit),DES(56bit)		ICカード対応セ キュリティシス テム
WinSafe Mobileスマ ートカードタイプ	システムニーズ	システムニーズ	共通鍵 公開鍵	カオス量子化多値 (56bit),DES(56bit) RSA(512bit)		ICカード対応セ キュリティシス テム、指紋照合 対応タイプもあ る
各種ICカード	凸版印刷	凸版印刷			ISO7816 JISSAP	ICカード
リゾナカード	大日本印刷	大日本印刷	共通鍵	DES(56bit),TripleDES(112bit)	ISO/IEC7816, JIS X 6303, JIS X 6304, JIS X 6306	ICカード

## 5. 電子商取引

### (1) 電子決済ツール

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
Atalla PayMaster ISP Atalla PayMaster/PCI ISP	Compaq Computer	コンパックコンピ ュータ	共通鍵 公開 鍵、署 名	DES(40~128bit) RSA(鍵配送：256~ 1024bit、署名：256~ 2048bit)	SET FIPS140-1 Level3	クレジットカード 決済 暗号化ハードウェ ア

			ハッシュ	MAC		BOX/PCI
Atalla WebSafe2 ISP Atalla WebSafe2/PCI ISP	Compaq Computer	コンパクトコンピューター	共通鍵 公開鍵、署名 ハッシュ	DES, RC2, RC4(各40~128bit) RSA(256~2048bit), DSA MD5, SHA-1 Diffie-Hellman(鍵共有)	FIPS140-1 Level3 SSL PEM S/MIME UL CSA TUV	電子商取引 暗号化ハードウェア BOX/PCI
Globeset Wallet	Globeset	Globeset			SET	WWWブラウザ等のプラグイン
IBM Consumer Wallet	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済 ソフトウェア
IBM Payment Gateway	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応ゲートウェイ ソフトウェア
IBM Payment Registry	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済 ソフトウェア
IBM WebSphere Commerce Suite	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応仮想モデル 構築ソフトウェア
IBM WebSphere Payment Manager	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済 ソフトウェア
Infomercer Mail	沖電気工業	沖電気工業			SET SSL	クレジットカードによるオンライン決済
Infomercer Store	沖電気工業	沖電気工業			SET	仮想店舗構築ソフトウェア
INTERSTAGE CollaborationRing PM	富士通	富士通	共通鍵 公開鍵 ハッシュ	SSL:DES(56bit), TripleDES(168bit), RC2(128bit), S/MINE(EDI-INT準拠):DES(56bit) SSL:RSA(2048bit), S/MINE(EDI-INT準拠):RSA(1024bit) MD5,SHA-1	SSL S/MINE(EDI-INT準拠)	ビジネスルールに基づいて業務プロセスを統合するインターネット環境でのEAI(Enterprise Application Integration) 基盤製品
Microsoft Wallet	Microsoft	マイクロソフト				WWWブラウザへのプラグイン 無償ダウンロード可
MilliCent Wallet	MilliCent	MilliCent				無償ダウンロード可
NetPay Marchant	Maithean	アルウス	共通鍵 公開鍵	DES(56bit) RSA	SET ISO SSL X.509 HTTP/MIME	SET/SSLハイブリッド マーチャント ソフトウェア

					CAPI/CSP VAP	
PayGateway	Trintesh	Trintesh	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応 ゲートウェイ ソフトウェア
PayPurse	Trintesh	Trintesh			SET	SET対応電子財布 ソフトウェア
PayWare	Trintesh	Trintesh	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応コマース サーバーソフトウ ェア
SecureWare/ 電子取引	NEC	NEC	共通鍵 公開鍵 ハッシュ	DES(56bit) RSA MD5	CII EDI	ソフトウェア
vGATE	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応 ゲートウェイ ソフトウェア
vPOS	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応 コマース・サーバ ー・ ソフトウェア
vWALLET	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応電子財布 ソフトウェア
WebWallet	SPYRUS	SPYRUS			SET	電子財布ソフトウ ェア
日立コマース・ ソリューション	日立製作所	日立製作所	共通鍵 公開鍵	DES(56bit) RSA(1024,2048ビット)	SET SECS	SET対応電子決済 ソフトウェア

(2) 不正コピー防止

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
CXD3201R	Sony Electronics	Sony Electronics	共通鍵 署名	M6(56/64bit), DES(56bit), Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	IEEE1394LSI
CXD3204R CXD3205R	Sony Electronics	Sony Electronics	共通鍵 署名	M6(56/64bit), DES(56bit), Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	1チップ i.LINC コントローラLSI
Internet secureEDI, secureEDI/WEB	日本バルチモアテク ノロジーズ	アドバンスシステム コンサルティング	共通鍵 公開鍵	RC4(128bit) RSA (1024,2048bit)		EDIソフトウェア・パッケージ
MN864501	松下電器産業	松下電器産業	共通鍵 署名	M6(56/64bit), DES(56bit), Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	IEEE1394LSI

6. 電子認証サービス

製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
Go Secure! for Microsoft Exchange	VeriSign	日本ベリサイン	公開鍵	RSA		企業向け電子認証ソリューション
Go Secure! for Web Applications	VeriSign	日本ベリサイン	公開鍵	RSA		企業向け電子認証ソリューション
Microsoft AuthenticodeTM対応デジタルID	VeriSign	日本ベリサイン	公開鍵	RSA		コードサイン用デジタル証明書
PaymentSign	日立/富士通/NEC	日本認証サービス	公開鍵	RSA(1024,2048bit)	SET/SECE	カード会員/銀行口座保有者向け証明書発行
SecureSign Private	日本認証サービス	日本認証サービス	公開鍵	RSA(512,1024,2048bit)	SSL,S/MIME	顧客専用CAによる証明書発行
SecureSign Public	日本認証サービス	日本認証サービス	公開鍵	RSA(512,1024,2048bit)	SSL,S/MIME	日本認証サービス(株)のルート傘下CAによる証明書発行
SecureSign Server	日本認証サービス	日本認証サービス	公開鍵	RSA(512,1024,2048bit)	SSL,S/MIME	サーバ用証明書発行
SET 対応証明書発行サービス・ソリューション	VeriSign	日本ベリサイン	公開鍵	RSA		企業向け電子認証ソリューション
グローバル・サーバID	VeriSign	日本ベリサイン	公開鍵	RSA	128bit SSL対応	ウェブサーバ用デジタル証明書
セキュア・サーバID	VeriSign	日本ベリサイン	公開鍵	RSA	40bit SSL対応	ウェブサーバ用デジタル証明書
ブラウザ用クラス1デジタルID	VeriSign	日本ベリサイン	公開鍵	RSA	SSL, S/MIME対応	個人ユーザー向けデジタル証明書
ベリサイン・オンサイト	VeriSign	日本ベリサイン	公開鍵	RSA		企業内認証局
電子メール用クラス1デジタルID	VeriSign	日本ベリサイン	公開鍵	RSA	S/MIME対応	個人ユーザー向けデジタル証明書