

暗号モジュール認証書

暗号モジュール試験及び認証制度に基づき、下記のとおり認証する。

平成 21 年 1 月 20 日
 独立行政法人 情報処理推進機構
 理事長 西垣 浩司

認証番号 J0008

日本語名：「SecureWare/開発キット Ver5.0」および
 「SecureWare/開発キット Ver5.0 CIPHERUNICORN オプション」

英語名：

ハードウェアバージョン： N/A
 ファームウェアバージョン： N/A
 ソフトウェアバージョン： Ver5.0

(型番：UL1123-401 (Windows 版)、
 UQ3042-000C1, UQ3042-H000C1, UQ3042-G000C1 (HP-UX 版))

物理形態： マルチチップスタンドアロン型

適合規格： JIS X 19790 : 2007 平成 19年 3月 20日

試験要件： JIS X 5091 : 2007 平成 19年 3月 20日

JCMVP暗号アルゴリズム実装試験要件 平成 19年 10月 29日

申請者： 日本電気株式会社 第一システムソフトウェア事業部

所在地： 東京都港区芝浦四丁目14 番22 号

特記事項： なし

注意事項：本暗号モジュール認証書で識別される暗号モジュールは、「暗号モジュール試験及び認証制度」で承認された試験機関による、暗号モジュール試験要件に基づく暗号モジュール試験結果が、適合していることを示す。本暗号モジュール認証書は、暗号モジュール試験を受けた構成及び動作環境に関して、暗号モジュールの特定のバージョンのみに適用される。暗号モジュール試験は「暗号モジュール試験及び認証制度」の規定に従って実施され、暗号モジュール試験報告書の試験機関による結論は、暗号モジュール試験に用いた提供物件にのみ対応している。この暗号モジュール認証書は独立行政法人 情報処理推進機構による暗号モジュール製品等の保証書ではない。また、独立行政法人 情報処理推進機構は、明示、黙示を問わず、本暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない。なお、本認証書を、不正にしようとした場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

暗号モジュール認証報告書

認証対象の暗号モジュールについて、以下の通り認証したことを報告する。

平成 21 年 1 月 20 日
独立行政法人 情報処理推進機構
理事長 西垣 浩司

記

暗号モジュール名：「SecureWare/開発キットVer5.0」及び
「SecureWare/開発キット Ver5.0 CIPHERUNICORN オプション」
バージョン： Ver5.0
(型番：UL1123-401 (Windows 版)、
UQ3042-000C1, UQ3042-H000C1, UQ3042-G000C1 (HP-UX 版))

暗号モジュール試験機関名：独立行政法人 情報処理推進機構 セキュリティセンター
暗号モジュール試験報告書

作成支援ツールバージョン：1.1.0

暗号モジュールの仕様：	1	暗号モジュールのポートとインタフェース：	1
役割、サービス、及び認証：	1	有限状態モデル：	1
物理的セキュリティ：	N/A	動作環境：	1
暗号鍵管理：	1	自己テスト：	1
設計保証：	1	その他の攻撃への対処：	N/A

全体的なセキュリティレベル：1

暗号モジュール試験時の構成：別紙の通り

暗号モジュールに搭載されている承認暗号アルゴリズム：
RSA(#5)、CIPHERUNICORN-E(#1)、3-key Triple DES(#4)、AES(#7)、CIPHERUNICORN-A(#1)、SHS(#7)、
HMAC(#5)、DH(#3)、Hash_DRBG in NIST SP800-90(ベンダ自己確認)

暗号モジュールに搭載されている非承認暗号アルゴリズム：
RSA-raw、Triple DES (2Key)、DES、RC2、RC5、MD2、MD4、MD5、HMAC-MD2、HMAC-MD5

結果：合格

試験に用いた試験対象の暗号モジュールは、暗号モジュール試験及び認証制度が定める所定の基準に基づく試験の結果、所定の暗号モジュールセキュリティ要件を満たした。

以上

< 「SecureWare/開発キット Ver5.0」 および 「SecureWare/開発キット Ver5.0 CIPHERUNICORN オプション」

暗号モジュール認証報告書：別紙>

暗号モジュール試験時の構成：

- | | |
|------------|--|
| ハードウェア環境 1 | NEC VJ21A/W-4
(CPU: Intel Core2Duo T7400 2.16GHz,
Memory: 2048MB, HDD: 80GB) |
| ソフトウェア環境 1 | OS Microsoft Windows XP Professional Version 2002
Service Pack 3 (バージョン 5.1.2600) |
| ハードウェア環境 2 | NEC VJ21A/W-4
(CPU: Intel Core2Duo T7400 2.16GHz,
Memory: 2048MB, HDD: 80GB) |
| ソフトウェア環境 2 | OS Microsoft Windows Vista Business Service Pack 1
(バージョン 6.0.6001) |
| ハードウェア環境 3 | NEC Express 5800/120Rj-2
(CPU: クアッドコア Intel Xeon X5460 3.16GHz ×2,
Memory: 16GB, HDD: 73.2GB ×4) |
| ソフトウェア環境 3 | OS Microsoft Windows Server 2003 R2 Enterprise Edition
Service Pack 2 (バージョン 5.2.3790) |
| ハードウェア環境 4 | NEC NX7700i/5012L-8
(CPU: デュアルコア Intel Itanium 9140N 1.6GHz ×4,
Memory: 16GB, HDD: 73GB ×4) |
| ソフトウェア環境 4 | OS HP-UX 11i v2 Mission Critical Operating Environment
(バージョン B.11.23.0712) |

以上