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、以下のとおり認証する。

平成24年3月27日
独立行政法人 情報処理推進機構
理事長 藤江 一正

原紙 押印済

認証番号 J0014

日本語名：SASEBO-GII-AES暗号FPGAボード

英語名：SASEBO-GII-AES Cryptographic FPGA Board

暗号モジュールバージョン：SASEBO-GII-AES-1.0
ハードウェアバージョン：TD-BD-SASEBOG2-31, TD-BD-SASEBOG2-32
ファームウェアバージョン：SASEBO-FPGA1(1.0), SASEBO-FPGA2(1.0)
ソフトウェアバージョン：N/A
物理形態：マルチチップ組込型

適合規格：JIS X 19790	平成 21 年 10 月 20 日 改正
試験要件：JIS X 24759:2009	平成 21 年 10 月 20 日
JCMVP暗号アルゴリズム実装試験要件	平成 21 年 1 月 8 日

申請者：独立行政法人 産業技術総合研究所 情報セキュリティ研究センター
所在地：〒305-8568 茨城県つくば市梅園1-1-1
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、不正に使用した場合、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

平成24年3月27日
独立行政法人 情報処理推進機構
理事長 藤江 一正

原紙押印済

記

暗号モジュール名： SASEBO-GII-AES暗号FPGAボード
バージョン： SASEBO-GII-AES-1.0
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： 1.2.2

暗号モジュール試験の結果、上記の暗号モジュールは、以下の暗号モジュールセキュリティ要件を満足することを認証したので報告します。
平成24年3月27日

セキュリティセンター　情報セキュリティ認証室
技術管理者　近藤 潤一

暗号モジュールセキュリティ要件：JIS X 19790　平成 21 年 10 月 20 日 改正
暗号モジュール試験要件：JIS X 24759:2009　平成 21 年 10 月 20 日

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：	1	動作環境：	N/A
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：別紙のとおり

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：AES(#25)

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：なし

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

<SASEBO-GII-AES 暗号 FPGA ボード 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	Dynabook SS RX1/T7E
	(CPU：Intel Core2 Duo CPU U7600, Memory 2GB, HDD 80GB)
ソフトウェア環境	OS Microsoft Windows Vista
	(Version 6.0, build 6001; Service Pack 1)
	Microsoft .NET Framework 3.5SP1
	SASEBO-GII-AES 1.0.0.0 rev625

以上