

ADV_ARC における指摘内容

指摘者

一般社団法人 IT セキュリティセンター 評価部

1	2	3	4	5
番号	章・節	パラグラフ・図表	コメント内容	修正案
1	3	3	初期化プロセスの説明はあるが、TSF の初期化プロセスのセキュリティがどのように確保されているかの記述がない。	どのようなセキュリティ上の脅威があるが、いかにしてその脅威を抑止しているか、設計書に則し記述する。
2	4	4	自己保護に対して、個々の機能の説明があるが、自分（護るべきもの）がどこに存在するか？が不明確であるためか、護っていることを実証できていない。	自分がどこに存在し、それにどのような脅威があり、いかにしてその脅威を抑止しているか、設計書に則し記述する。
3	5	5	鍵の生成・導入、パスワードや暗号アルゴリズムの処理の記述はあるが、TSF が SFR 実施機能性のバイパスをいかに防いでいるかの実証は一切ない。	SFR 機能の関連を明記し、いかにバイパスされないか、設計書に則し、または IT 環境の機能を提示しながら実証する。
4	5	5	バイパスを防いでいることを実証することが目的の資料に「TrueCrypt ではこのメカニズムのバイパス防止を保証することはできない。」と記述されている。	バイパス防止をオペレーションシステムなどに依存しているなら、「オペレーションシステムのこの機能をこのようにしているからバイパスは抑止される」など、バイパスされないことを実証する。