

パート2の主な変更内容 注:エディトリアルに近い内容の変更(TSP SFR, system TOEなど)は無視してある。 ×は変更が無いことを示す。

クラス	V2	V3.1
FAU:Audit	Security audit automatic response (FAU_ARP)	×
	Security audit data generation (FAU_GEN)	Annexに、「サブジェクトが利用者の場合、利用者認証が完了/実施されていない場合には、入力された利用者IDがログイン時のサブジェクトIDとして記録される。」ことが説明追加。
	Security audit analysis (FAU_SAA)	Annexの、「PP/ST作成者は、TSFによって表される特徴的事象及び事象シーケンスの基本セットを定義すべきである。システム開発者は、特徴的事象及び事象シーケンスの定義を追加することができる。」削除
	Security audit review (FAU_SAR)	Annexに、「入手可能な監査情報を指定する際、FAU_GEN.1で指定の監査情報を繰り返し記述する必要はない」ことが説明追加。
	Security audit event selection (FAU_SEL)	×
	Security audit event storage (FAU_STG)	保護しなければならない監査レコードとは監査証跡のレコードであり、一時ファイル上の監査レコードではないことを明確化。Annexに、「監査証跡として保管されている監査レコード」が対象である旨が説明追加。
FCO: Communication	Non-repudiation of origin (FCO_NRO)	×
	Non-repudiation of receipt (FCO_NRR)	×
FCS: Cryptographic support	Cryptographic key management (FCS_CKM)	×
	Cryptographic operation (FCS_COP)	×
FDP: User data protection	Access control policy (FDP_ACC)	subject in the TSC subject controlled by the TSF
	Access control functions (FDP_ACF)	×
	Data authentication (FDP_DAU)	×
	Export to outside TSF control (FDP_ETC)	Export from the TOE (FDP_ETC) TSC TOE Annexで「利用者データのエクスポート」「TSFが介在する利用者データのエクスポート」
	Information flow control policy (FDP_IFC)	TSC TOE Annexで、満足するセキュリティポリシーモデルとして例示されていた”Bell and LaPadula security model”を削除
	Information flow control functions (FDP_IFF)	AVA_CCA.1 Covert channel analysisへの依存性削除 Annexで、ポリシーモデルとして例示されていた”Bell and LaPadula security model”を削除
	Import from outside TSF control (FDP_ITC)	Import from outside of the TOE (FDP_ITC) TSC TOE Annexで「利用者データのインポート」「TSFが介在する利用者データのインポート」
	Internal TOE transfer (FDP_ITT)	×
	Residual information protection (FDP_RIP)	TSC TSF Annexで、administrative guidance operational user guidance Annexで、「このファミリーは、論理的に削除または解放された情報(その利用者には利用できないが、システム内にまだ存在し、回復可能かもしれない)に対する保護を要求する。」の()内を削除
	Rollback (FDP_ROL)	×
	Stored data integrity (FDP_SDI)	user data stored within the TSC user data stored in containers controlled by the TSF
	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	×
	Inter-TSF user data integrity transfer protection (FDP_UIT)	×

パート2の主な変更内容 注:エディトリアルに近い内容の変更(TSP SFR, system TOEなど)は無視してある。 ×は変更が無いことを示す。

クラス	V2	V3.1
FIA: Identification and authentication	Authentication failures (FIA AFL)	×
	User attribute definition (FIA ATD)	×
	Specification of secrets (FIA SOS)	×
	User authentication (FIA UAU)	×
	User identification (FIA UID)	×
	User-subject binding (FIA USB)	×
FMT: Security management	Management of functions in TSF (FMT MOF)	×
	Management of security attributes (FMT_MSA)	ADV_SPM.1: Informal TOE security policy modelへの依存性削除 Annexで、「セキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を開発者が提供すれば、FMT_MSA.2のADV_SPM.1への依存性を、論証し取り除くことができる。」の記述削除
	Management of TSF data (FMT_MTD)	ADV_SPM.1: Informal TOE security policy modelへの依存性削除 Annexで、「TSFデータを消去する」の意味を判りやすく言うと、TSFデータの内容が除去されるが、エンティティ自身はシステムの中に残るとのことである。」「TSFデータを消去する」の意味を判りやすく言うと、TSFデータの内容が除去されるが、TSFデータを保管するエンティティはTOEの中に残るとのことである。 Annexで、「セキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を開発者が提供すれば、FMT_MSA.2のADV_SPM.1への依存性を、論証し取り除くことができる。」の記述削除
	Revocation (FMT_REV)	within the TSC under the control of the TSF
	Security attribute expiration (FMT_SAE)	×
	Specification of Management Functions (FMT_SMF)	security management functions management functions
	Security management roles (FMT_SMR)	×
FPR: Privacy	Anonymity (FPR_ANO)	Annexで、「PP/ST作成者は、どれくらいの厳密さが適用されるべきかを示すのに、機能強度を使用したいと考えるかもしれない。」を削除
	Pseudonymity (FPR_PSE)	Annexで、「そのため、FPR_PSE偽名性ファミリは、機能強度要件の対象になる。」を削除
	Unlinkability (FPR_UNL)	×
	Unobservability (FPR_UNO)	Annexで、「論理的分離では、FPT_SEPが関係するかもしれない。」を削除 Annexで、「このコンポーネントに加え、PP/ST作成者は、隠れチャンネル分析と一緒に使用したいと思うかもしれない。」を削除
FPT: Protection of the TSF	Underlying abstract machine test (FPT_AMT)	AnnexのFPTの解説の中で、「c) FPT_SEP(ドメイン分離)とFPT_RVM(リファレンス調停)、これらは、動作中のTSFを保護し、TSFがバイパスされ得ないことを保証する。これらのファミリの適切なコンポーネントがDV_INT(TSF内部構造)の適切なコンポーネントと組み合わせられたとき、TOEは、従来「リファレンスモニタ」と呼ばれていたものを持つと言えるようになる。」を削除
	Fail secure (FPT_FLS)	ADV_SPM.1: Informal TOE security policy modelへの依存性削除 Annexで、「「セキュアな状態」は、TSPモデルで定義される。もし開発者が、セキュアな状態の明確な定義と、なぜそれがセキュアと考えられるべきかの理由を提供すれば、FPT_FLS.1からADV_SPM.1への依存性は、論証し取り除くことができる。」を削除
	Availability of exported TSF data (FPT_ITA)	×
	Confidentiality of exported TSF data (FPT_ITC)	×
	Integrity of exported TSF data (FPT_ITI)	×
	Internal TOE TSF data transfer (FPT_ITT)	×
	TSF physical protection (FPT_PHP)	TSP is not violated SFRs are always enforced

パート2の主な変更内容 注:エディトリアルに近い内容の変更(TSP SFR, system TOEなど)は無視してある。 ×は変更が無いことを示す。

クラス	V2	V3.1
FPT: Protection of the TSF (続き)	Trusted recovery (FPT_RCV)	failure of a security function failure of the TSF 依存性: AGD_ADM AGD_OPE Operational user guidance ADV_SPM.1: Informal TOE security policy modelへの依存性削除 Annexで、”「セキュアな状態」は、TSP モデルで定義する。開発者が、セキュアな状態の明確な定義と、なぜそれがセキュアとみなせるべきかの理由を提供すれば、FPT_RCV における各コンポーネントからADV_SPM.1 への依存性は、論証し取り除くことができる。”を削除 Annexで、"within the TSC" "under the control of TSF"
	Replay detection (FPT_RPL)	×
	Reference mediation (FPT_RVM)	ファミリー削除
	Domain separation (FPT_SEP)	ファミリー削除
	State synchrony protocol (FPT_SSP)	×
	Time stamps (FPT_STM)	"for its own use"削除
	Inter-TSF TSF data consistency (FPT_TDC)	×
	Internal TOE TSF data replication consistency (FPT_TRC)	×
	TSF self test (FPT_TST)	×
FRU: Resource utilisation	Fault tolerance (FRU_FLT)	×
	Priority of service (FRU_PRS)	within the TSC under the control of the TSF Annexで、"within the TSC" "under the control of TSF"
	Resource allocation (FRU_RSA)	FRU_RSA.2.1 のselectionに subjectsを追加 Annexで、"within the TSC" "under the control of TSF"
FTA: TOE access	Limitation on scope of selectable attributes (FTA_LSA)	×
	Limitation on multiple concurrent sessions (FTA_MCS)	×
	Session locking (FTA_SSL)	×
	TOE access banners (FTA_TAB)	×
	TOE access history (FTA_TAH)	×
	TOE session establishment (FTA_TSE)	×
FTP: Trusted path/channels	Inter-TSF trusted channel (FTP_ITC)	×
	Trusted path (FTP_TRP)	×