Joint Interpretation Library

Certification of “open” smart card products

平成 26 年 8 月翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

Version 1.1 (for trial use)
4 February 2013

IPA まえがき

はじめに

本文書は、コモンクライテリアにおいて、SOG-IS が CC 補助文書として公開している *Joint Interpretation Library – Certification of “open” smart card products* を翻訳した文書である。

原文

Joint Interpretation Library - Certification of “open” smart card products

Version 1.1 (for trial use)
February 2013

謝辞

本文書の日本語版の公開を許可して頂いた JIWG 議長、フランス ANSSI の Julie Chuzel 氏に感謝する。

謝辞：

以下に示される組織、及びJoint Interpretation Working Group（JIWG）の下部組織は、SOG-IS評価と認証スキームとの間の基準及び方法の一貫性のある適用を支援するために、JIWG関係文書を提供しています。

フランス : Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
ドイツ : Bundesamt für Sicherheit in der Informationstechnik (BSI)
イタリア : Organismo di Certificazione della Sicurezza Informatica (OCSI)
オランダ : Netherlands National Communications Security Agency (NLNCSA)
スペイン : Centro Criptológico Nacional (CCN)
英国 : Communications-Electronics Security Group (CESG)

目次

1 本書の適用範囲及び目的

1.1 定義

1 ここでの用語「製品」は、環境に関連付けられているTOEに対応する一般名称を意味する。

2 用語「プラットフォーム」は、評価結果プロセスのコンポジションに関する注釈[コンポ]で使用される用語を意味し、「プラットフォーム上のアプリケーション」のコンポジット評価の場合に適用される。このため、ここで「プラットフォーム」として指定される製品は、ソフトウェアオペレーティングシステムを備えているICであり、場合によってはネイティブアプリケーションコードを備えていることもある。

3 「オープンプラットフォーム」は、新しいアプリケーションを、最終ユーザに配付した後（つまり、従来のスマートカードライフサイクルの7番目のフェーズ中）に搭載するプラットフォームである。 このようなローディングは「発行後」ローディング（最終ユーザへのスマートカード配付後のアプリケーションローディング）と呼ばれる。

4 アプリケーションが7番目のフェーズ前にインストールされる場合は、「発行前」ローディングと呼ばれる。

5 「クローズドプラットフォーム」は、新しいアプリケーションを、最終ユーザへの配付後に搭載できないプラットフォームである。

6 「隔離プラットフォーム」は、プラットフォーム自体の場合と同様に、プラットフォーム上にある組込みアプリケーションすべての実行ドメインの分離を維持するプラットフォームである。ここで「分離」とは、アプリケーションのドメイン分離、及びアプリケーションのデータの保護を意味する。

7 「アーキテクチャ」は、製品の最上位構造、すなわち、すべてのアプリケーションが製品に含まれている「オープンプラットフォーム」に対応する。（発行前、発行後でロードされた、どちらのものでも）。

8 新しいアプリケーションローディングは評価プロセスの前または後で検討される場合があるため、既知のアプリケーションと未知のアプリケーションと呼ぶことで、評価プロセス時に検討されるアプリケーションを他のものから区別する。

9 「既知のアプリケーション」は、認証済み製品の元のアーキテクチャに対応する。これらのアプリケーションはすべて、評価プロセス時にITSEFによって検討される[1]。

10 「未知のアプリケーション」は、評価時に未知であったアプリケーションである。未知のアプリケーションは、評価済み製品のアーキテクチャの、認証報告書で述べられているものからのアップグレードに対応する。

1.2 適用範囲

11 本書の目的は、オープン製品の認証手続きを識別し、それらの製品の変更されたアーキテクチャが、この製品の異なるアーキテクチャにすでに発行された認証書の認証済みセキュリティ機能の有効性に影響を及ぼさないことを保証することである。ここで、変更されたアーキテクチャとは、元の認証済み製品のアーキテクチャに対するアプリケーションの追加（TOE環境の変更）を表す。

[1] これらのアプリケーションは、必ずしも TOE に含まれない。

12 （上記の状況と対照的に）プラットフォーム自体の変更には、プラットフォーム、ひいては製品全体の認証書更新または保証継続が必要になることに注意すること。

13 認証書でこれらの製品のアーキテクチャ変更を考慮に入れるために、プラットフォームにはいくつかの特性、特に、製品上で起動されたアプリケーションの顕著な隔離特性がなければならない。実際に、これらの隔離特性を提供する製品だけが、新しいアプリケーションの起動が認証済み機能の保証に影響を及ぼさないことを確実にする、それらの製品が上記の保証を（特定の制約下で）提供することを実証することを評価されたプラットフォームを、本書では「オープンな隔離プラットフォーム」と呼ぶ。

14 このようなオープン製品に新しいアプリケーションがロードされた場合、評価済み製品（TOE）が、期待された拡張IT環境で目指されるAVA_VANレベルに到達することを保証するために、それらの新しいアプリケーションによるプラットフォームセキュリティ制約の達成の検証が要求される。

15 アプリケーションの隔離を保証しないオープンプラットフォームは、クローズドプラットフォームとして認証される。発行後のローディングを認可しないクローズドプラットフォームは、本書の適用範囲外となる。

1.3 注釈の計画

16 第2章では、プラットフォームに対するこれらの保証及び制約を定義し、評価用の入力ならびに「オープンな隔離プラットフォーム」の認証を提示する。

17 第3章では、アプリケーションに対するこれらの保証及び制約を定義し、認証済み「オープンな隔離プラットフォーム」上にあるアプリケーションの評価用の入力を提示する。

2 オープンな隔離プラットフォーム

2.1 評価

18 本書では、以下に示されるエレメントに従って評価されたプラットフォームについては、オープンな隔離プラットフォームを参照する。

2.1.1 目的

2.1.1.1 解析機能

19 「*オープンな隔離プラットフォーム*」は、評価される必要がある以下の機能を提供しなければならない

- O1：考慮されるプラットフォームに格納されるすべてのアプリケーション間の隔離、及び敵対する可能性のあるアプリケーションに対する、このような保護。

  ならびに

- O2：以下の OE2 で定義される証拠によるアプリケーションの起動 [2]前に、各アプリケーションの検証 [3]における完全性及び真正性の検証によって考慮されるプラットフォームへのアプリケーションの発行後ローディングの保護。

20 O1及びO2は、プラットフォームのセキュリティターゲットにおけるTOEの目的でなければならない。

2.1.1.2 評価環境

21 「*オープンな隔離プラットフォーム*」は、プラットフォームにロードされたすべてのアプリケーションに関する、以下の要件を規定する評価プロセスを受けるプラットフォームである。

- OE1：プラットフォームにロードされるすべてのアプリケーションは、隔離特性に関連する対象のプラットフォームに課せられる制約に従って、アクティベートされる前に、検証される必要がある。

  ならびに

- OE2：（OE1 の検証以降にロードされたアプリケーションが変更されていないことを確実にするために）プラットフォームにロードされる各アプリケーションの完全性証拠の可用性、及びこれらの検証の真正性証拠の可用性。

22 OE1及びOE2は、プラットフォームのセキュリティターゲットにおける環境の目的でなければならない。

23 OE1及びOE2は、評価で認証されるかどうかにかかわらず、すべてのアプリケーションに適用できる。そのように、OE1及びOE2は、すべての既知または未知のアプリケーションに適用できる。

24 既知のアプリケーションの場合、OE1及びOE2の達成はITSEFによって検証される。それ

[2] つまり、ロードされたファイルが最終ユーザに使用可能なアプリケーションになる前。
[3] ロードされているものは、検証されたものである

でも、OE1を検証するだけで、OE2が達成されなければならない方法を記述することは可能である[4]。その後、ITSEFはOEIの達成を検証し、OE2を達成するために使用されるガイダンス証拠資料を評価する。そのような場合、認証書では、これらのアプリケーションを曖昧さなく識別し、OE2を達成するためにガイダンス証拠資料を最終ユーザが適用することを要求する使用制限を示す。

25 未知のアプリケーションの場合、OE1及びOE2の達成の検証は可能ではない。プラットフォーム認証は認証書の使用制限で構成され、最終ユーザがOE1及びOE2を達成するためにガイダンス証拠資料を適用することを要求している。

2.1.2 識別

26 一般的に、オープンプラットフォームの認証によって、ITSEFに評価された製品の識別ができるようになるべきである。 この識別は、以下の識別からなる。

- 評価のために提出された（ITSEF に提供された）状態にある製品の識別。これには、発行前でロードされたすべての既知のアプリケーションが含まれる。
- 発行後でロードできる既知の全アプリケーションの識別。

27 製品による要求に応じて返される識別子によって、プラットフォームの識別及び格納された全アプリケーションの一覧表示を行うことでTOEと製品を区別できなければならない。

28 評価では、TOEがどのようなものであっても、製品全体を検討しなければならない。このため、プラットフォームコンポーネント及び既知のアプリケーションは、セキュリティターゲットにより提供された識別情報において識別されなければならない。これらの識別情報は、プラットフォームの認証報告書で明白に指定される。

29 開発者は、ITSEFに対して利用可能な製品識別子がITSEFに既知の一連のコンポーネントに対応していることを検証する手段をITSEFに与えなければならない。（これらのコンポーネントがTOEに属しているかどうかにかかわらず）。

30 これらの要件によって、プラットフォーム制約を遵守しない、つまり、製品上で起動している他のアプリケーションに敵対することがあるアプリケーションを含む製品を認証するリスクを回避することができる。

2.1.3 ライフサイクル

31 下図は、オープンプラットフォームのライフサイクルのフェーズモデルを示している。これは、そのようなライフサイクルの単なる例であり、プラットフォーム評価に関連するALC配付時点は、ここで識別されるものと異なる場合がある。

32 サイト認証の証拠または同等の監査結果が提供される場合、配付の考慮すべき点が実際の評価で考慮されるものから拡張される可能性があることにも注意すること。

[4] これは、認証ライフサイクルフェーズで可能な組織的手段によって OE2 を満たすことができる場合に適用できる。2.1.3 節を参照。

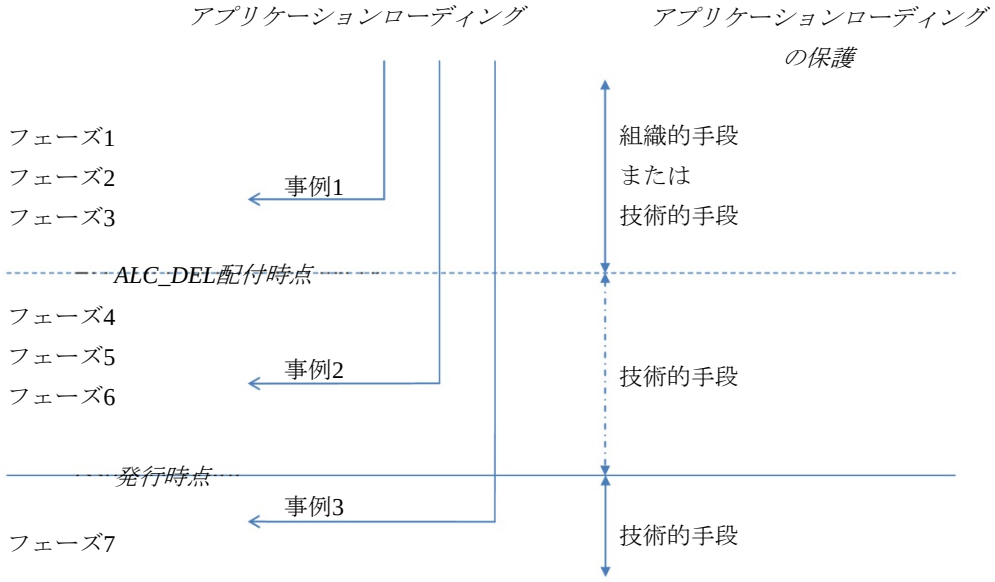

図 1　オープンな隔離プラットフォームのライフサイクル [5]

33　「オープンな隔離プラットフォーム」の製品には、発行前及び発行後のアプリケーションが含まれる場合がある。

34　OE2オブジェクトに到達する手段の特性がローディングの時点に応じて異なる場合があることを明確化することは有用である。

35　以下の3つの異なる事例が区別される。

- 事例 1：アプリケーションは、発行前（配付前）にロードされ、OE2 オブジェクトは、組織的手段または技術的手段によって実施される場合がある。
- 事例 2：アプリケーションは、発行前（配付後）にロードされ、組織的手段は許可されず、技術的手段が使用されなければならない。
- 事例 3：アプリケーションは発行後（製品の発行後）にロードされ、OE2 に関連付けられている技術的手段が使用されなければならない。

36　定義により、考慮されるすべてのプラットフォームでは事例3では（少なくともフェーズ7での）ローディングが可能である。

37　OE1及びOE2が実現される方法を明確化するために、セキュリティターゲットは、アプリケーションの開発、検証、及び配付において示されるプロセス、ならびに様々な役割を説明しなければならない。セキュリティターゲットは、この詳細なライフサイクルに関する評価範囲も記述しなければならない。

38　既知のアプリケーションが評価済み製品に含まれる場合、ライフサイクルの以下の詳細もセキュリティターゲットで記述されなければならない。

- アプリケーション検証に示されるプロセスの管理における役割に関連するアクターの識別。

[5] BSI-CC-PP-0035-2007 に基づき認証されるプロテクションプロファイルで定義されている通りにフェーズ 1～7 が使用されることに注意すること。

- 検証からローディングまでのアプリケーションの完全性及び真正性の保護に示されるプロセスの管理における役割に関連するアクターの識別。

39 さらに、認証済みプラットフォームと、認証済みプラットフォームの最上層にあるアプリケーションの後続のコンポジット認証ではALC配付時点が異なる（第3章を参照）。代表的な使用事例として、ALC配付時点が後期に移動する場合がある。その結果、コンポジット認証では、事例1に属するか事例2に属するかに関するフェーズの分類が変更される場合がある。事例2のプラットフォーム認証フェーズは、配付時点が延期されるに伴ってコンポジット認証の事例1フェーズになり、その後、技術的対策を要求しない。このような再分類は、受入れられ、プラットフォーム認証に対して矛盾することも、影響を及ぼすこともない。

2.1.4 製品ガイダンス

40 第2.1.1.2章で特定されている評価環境に関連して、以下の特定のガイダンスを開発者が提供しなければならない。

- アプリケーション開発ガイダンス（OE1 に関連する）。このガイダンスは、プラットフォームの隔離特性を維持するためにアプリケーションに課せられる制約を記述する検証ガイダンスから導かれる。[ISO_VERIF]
- 以下の事項に対応するアプリケーションローディング保護ガイダンス（OE2 に関連する）
  - アプリケーションローディングの組織的手段[ORG_LOAD][6]。
  - 検証の真正性（例えば、鍵保護）を保証するために必要な手段に関連する、プラットフォームの関連機能（O2 に関連する）を起動する方法を記述しなければならないアプリケーションローディングの技術的手段[TECH_LOAD]。

41 「オープンな隔離プラットフォーム」では常に、事例3のアプリケーションローディングが可能であるため、必ず[ISO_VERIF]及び[TECH_LOAD]を開発者が提供する必要がある。

42 開発者が組織的手段で事例1を実装しない場合、[ORG_LOAD]を提供することは不要である。

43 [ISO_VERIF]が、AGD_OPEによって要求されるガイダンス（セキュアなアプリケーションのコーディング用のガイダンス証拠文書）に対応しないことに注意すること。[ISO_VERIF]では、アプリケーション間のプラットフォームの隔離特性の保守に関連するすべての開発規則が示される。アプリケーション開発専用のAGD_OPEガイダンスの部分では、特定のセキュリティ特性を提供する必要があるアプリケーションに関連するすべての開発規則が示される。

44 これらのガイダンスは、開発者が考慮するローディング事例に応じて、AGDまたはALCに従って評価される必要がある。

[6] このガイダンスは、ALC セキュリティ保証要件に含まれる

2.1.5 評価構成

45 考慮される製品の実際のライフサイクルに応じて、OE1及びOE2は、ITSEFによって以下の方法で扱われる必要がある。

1. ITSEFは、すべての既知のアプリケーションがOE1の制約を満たすことを系統的にチェックする必要がある。ITSEFは、アプリケーションの検証が行われたことをチェックするために開発者証拠に頼る場合がある。この検証は既知のアプリケーションではチェックできないため、[ISO_VERIF]の規則遵守は認証書の制限事項となる。
2. 配付時点前に組織的手段が使用される場合、アプリケーションローディングは開発者の責任下となり、OE2を実装している関連保護は、ALCセキュリティ保護要件で対処される。このため、組織的手段は監査される必要がある。
3. 本書の適用範囲内では、少なくとも事例3の、OE2を実施する技術的手段が常に使用される。関連する要件は[TECH_LOAD]に記載されている。これらの要件の一部またはすべてはALCセキュリティ保証要件によって実施できるため、対応する組織的手段が監査される必要がある。チェックできない[TECH_LOAD]の規則遵守は、認証制限で構成される。

46 こうして、OE1及びOE2は、すべての既知のアプリケーションについてチェックされる必要がある。

2.2 オープンな隔離プラットフォームの認証

47 オープンな隔離プラットフォームの認証報告書には、以下の特異性がある。

- 報告書では、このプラットフォームが「オープンな隔離プラットフォーム」の概念に適合していることを識別するために、アプリケーションの隔離、及び発行後のアプリケーションローディング保護が調べられたことを明確化する。「評価構成の章」では、評価構成が「オープンな隔離プラットフォーム」であることを明確化する。
- 報告書では、「アーキテクチャ」及び「評価構成」の章で、評価プロセス中に ITSEF によってチェックされたすべての既知のアプリケーションを識別する [7]。また、認証報告書のすべてのアプリケーションが OE1 及び OE2 オブジェクトに従ってチェックされたことも明らかにする。
- また、「評価構成」の章では、既知のアプリケーションのサブセットで構成される製品も認証されることを明確化する。
- 「使用上の制限事項」の章では、制約 OE1 及び OE2、ならびに[ISO_VERIF]、[ORG_LOAD]、[TECH_LOAD]のガイダンスへの参照を述べている。これは、製品のロードされたアプリケーション、特に評価時に未知である新しいアプリケーションに適用される。この章には、プラットフォームのオープンな隔離プロパティにリンクされていない使用上の制限事項も記載される場合があることにも注意すること。
- 報告書では、「製品ライフサイクル」の章で、製品に適用でき、かつ、開発者によっ

[7] これらの既知のアプリケーションは、ITSEF に対して利用可能な製品バージョンに含まれるプラットフォームによってすでに搭載されているアプリケーション（発行後でのアプリケーション）、または発行後でロードされることを意図されている、開発者が ITSEF に提供するアプリケーションに対応する。

て検討される様々な種類のアプリケーションローディングを記述する。

- 報告書では、さらに、OE1 だけが検証された既知のアプリケーションのリストが記載される場合がある。 そのような場合、認証書では、これらのアプリケーションを曖昧さなく識別し、OE2 を満たすためにガイダンス証拠資料を最終ユーザが適用することを要求する使用上の制限を示す。

48 Bi（i ∈ [l,l])のような未知のアプリケーションのローディングは、製品がもはや、オープンな隔離プラットフォーム認証書で述べられている製品のアーキテクチャに完全に適合していないことを示している。評価結果は、プラットフォームにロードされている他のすべてのアプリケーションがプラットフォーム認証の制約を遵守する場合だけに有効である。したがって、関連付けられている認証書のセキュリティ制約を遵守する派生製品アーキテクチャは、認証済みと見なすことができる。これは、これらのアプリケーションの展開を担当するアクターが提供するOE1及びOE2の検証の保証に依存するか、またはスキームに依存するかは、リスクマネージャ次第である。この最後の場合（CCスキーム解決策が選択される場合）、スポンサーは今後、第2、3章に述べられている保守を要求する。

49 下図は、認証済み製品を示している。ここでは、TOEだけがプラットフォームに対応する。Ai（i ∈ [1,n]）アプリケーションは既知の発行前のアプリケーションに対応し、プラットフォーム認証報告書で識別される。

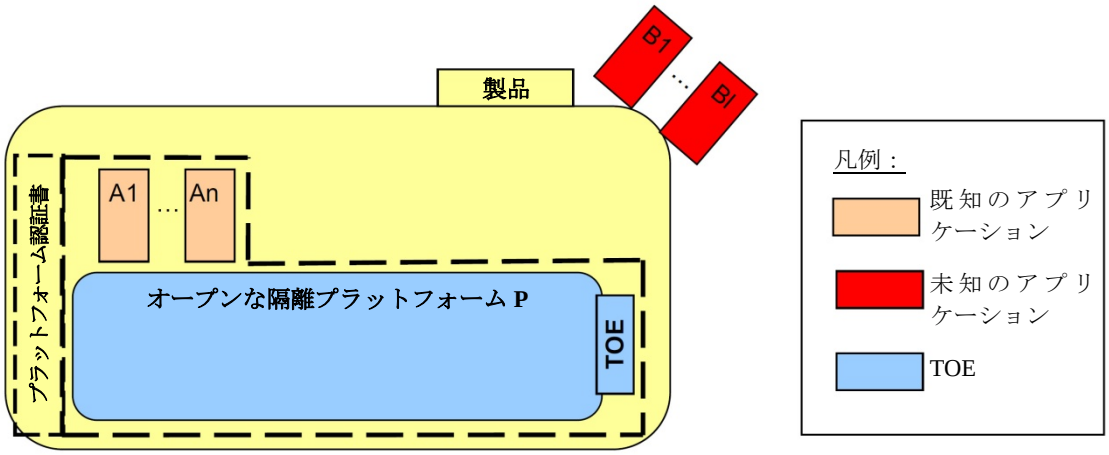

図2　オープンな隔離プラットフォームTOEに関連する製品

2.3 オープンな隔離プラットフォームの保守

50 保証継続プロセスは、その他の認証書と同様に、オープンな隔離プラットフォーム認証書に適用できる。本章では、プラットフォームの大きな変更が行われてない場合、及び初期評価中に未知であった一部のアプリケーションが認証済み製品に含まれることを開発者が希望する場合に、オープンな隔離プラットフォームの本プロセスの特異性のみを取り扱う。

51 これらの新しいアプリケーションに関係する認証書の制限事項は、チェックされなければならない。 これらの新しいアプリケーションの検証及びローディングが、既知のアプリケーションの場合と同じ以前に評価された方法で行われることによってOE1及びOE2に対応し、サイト訪問報告書がまだ有効であれば保守報告書を発行することができる。

52 開発者は、インパクト解析を持つそれらの新しいアプリケーションに関連する証拠を提供する必要がある（アプリケーションAi,（i ∈ [1,n]）の初期評価プロセス中に提供されたものと同じ種類の証拠)。 インパクト解析では、新しいアプリケーションの主要機能も記述しなければならない（アプリケーションBj,（j ∈ [1,l])）。

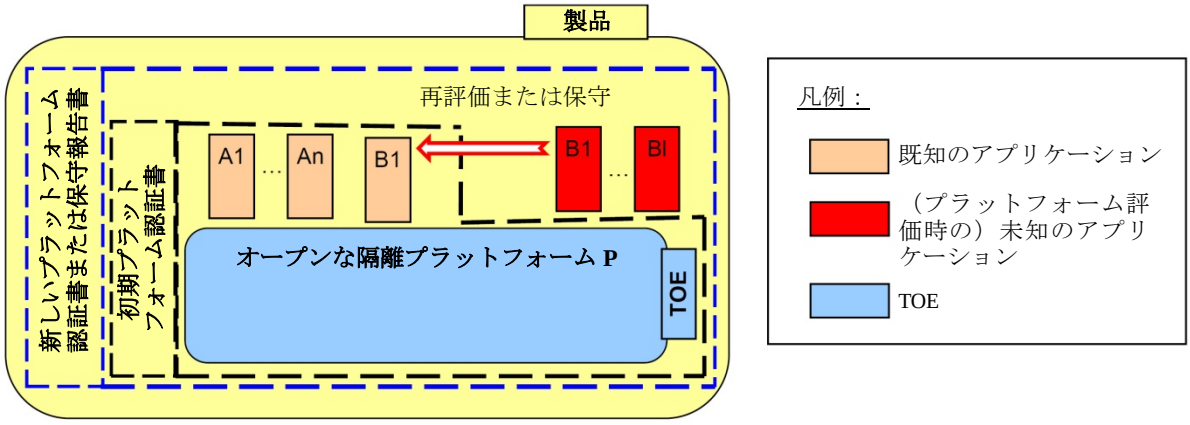

図3 オープンな隔離プラットフォームTOEに関連する保守製品

3 オープンな隔離プラットフォーム上のアプリケーション

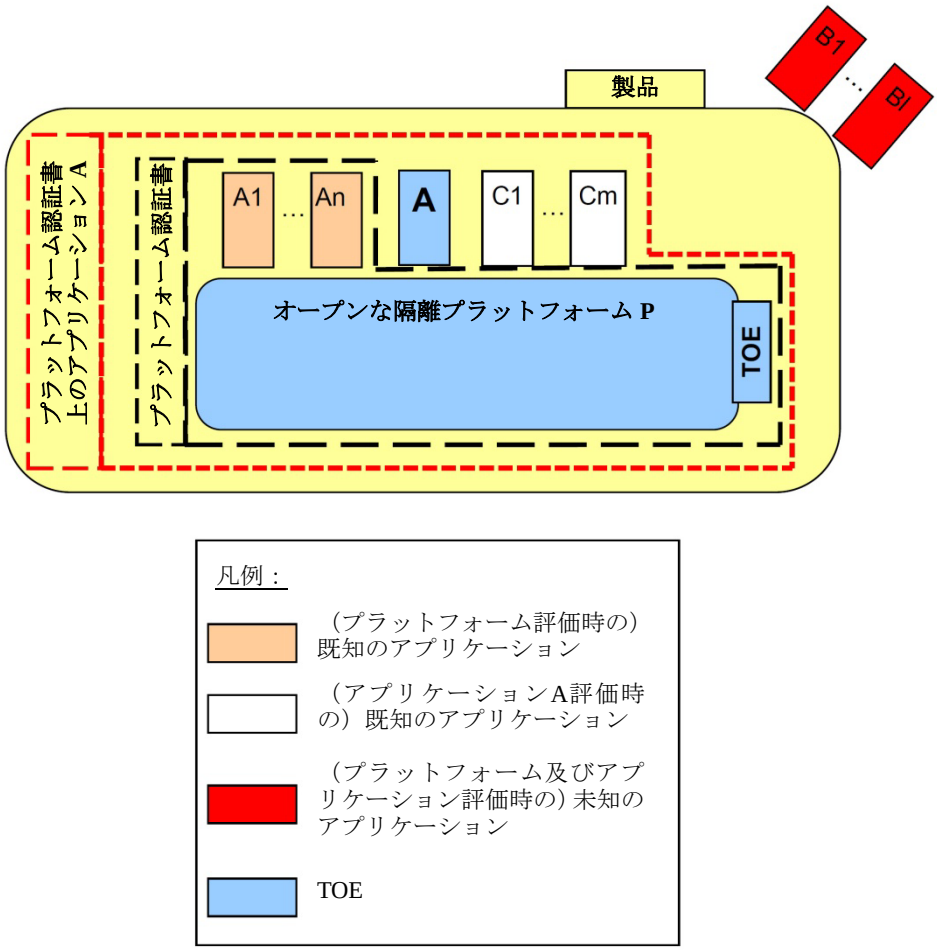

図4 標準認証書のTOE及び関連製品

53 この図では、プラットフォームP及びアプリケーションAi（I ∈ [1,n]）が評価され、オープンな隔離プラットフォーム認証書に至っている。プラットフォーム認証書では、すべてのAiアプリケーションが識別される。

54 アプリケーションA及びCj（j ∈ [1,m]）は、プラットフォーム認証後にロードされるアプリケーションに対応するが、アプリケーション評価時には既知である。これらのアプリケーションは、発行後（事例3）または発行前（事例1または2）のアプリケーションに対応する。

55 アプリケーションAは、プラットフォーム評価でアプリケーションによって対象とされるアプリケーションである。ここでは、この評価は、以下に関連して、コンポジションプロセス[Compo]に従って行われる。

- セキュリティ機能を提供するアプリケーション用の通常のセキュリティアプリケーション開発ガイダンス
- 隔離特性を維持するためにアプリケーションに課せられる制約を記述するガイド[ISO_VERIF]

- 及び場合により、アプリケーションローディング保護ガイダンス[ORG_LOAD]または[TECH_LOAD]。

56 したがって、ここでは、TOEは「プラットフォームP上のアプリケーションA」である。もちろん、その他の特定のCCアクティビティは、ITSEFによって実行される必要がある。本章では、オープンな隔離プラットフォーム評価によって課せられる要件だけに焦点を当てる。

3.1 評価

3.1.1 プラットフォーム認証書からの目的

57 標準的な評価プロセスでは、すべての既知のアプリケーションを考慮する必要がある。アプリケーションAiは、プラットフォーム評価ですでに考慮されており、プラットフォーム認証報告書で識別される（2.2を参照）。したがって、P認証報告書で得られるAでは、すべての新しい既知のアプリケーションCjは、2.1.1.2に定義されている規則に従って識別される必要がある。

58 OE1及びOE2が実現される方法を明確化するために、セキュリティターゲットは、アプリケーションの開発、検証、及び配付において示されるアクター、ならびにその役割を詳述しなければならない。 セキュリティターゲットは、この詳細なライフサイクルに関する評価範囲も記述すべきである。

59 ITSEFは、すべてのアプリケーションが要件OE1とOE2を遵守すること、及びすべてのアプリケーションAiとCjがアプリケーションAによるセキュリティ機能互換性の制約を満たすことをチェックする必要がある（3.1.2章を参照）。

60 アプリケーションCjでは、要件OE1とOE2の遵守は、プラットフォームガイダンス（段落2.1.4を参照）を参照して、プラットフォーム評価時の既知のアプリケーションAiの場合と同じ規則（段落2.1.5を参照）に従って評価されなければならない。

61 対象となるアプリケーションAでは、2つの要件OE1とOE2はコンポジションアクティビティ（[Compo]の保証要件ADV_COMPを参照）中に実現されなければならず、Cjアプリケーションに関する2.1.4で定義されるプラットフォームガイダンスを参照して、2.1.5で定義されている規則に従う場合がある。

62 Bk（k ∈ [1,m]）のような未知のアプリケーションのローディングは、製品がもはや、P上のAに関するオープンな隔離プラットフォーム認証書で述べられている製品のアーキテクチャに完全に適合していないことを示している。評価結果は、プラットフォームにロードされている他のすべてのアプリケーションがプラットフォーム認証の制約を遵守しない場合だけに有効である。関連付けられている認証書のセキュリティ制約を遵守する製品アーキテクチャは、認証済みと見なすことができる。これは、これらのアプリケーションの展開を担当するアクターが提供するOE1及びOE2の検証の保証に依存する、またはスキーマに依存するリスクマネージャ次第である。この最後の場合、スポンサーは今後、3.3章に述べられている保守を要求する。

3.1.2 アプリケーションセキュリティ機能の互換性

63 対象となるAアプリケーションでは、アプリケーションAのガイドAGD_OPEで明示的に記述されている、いくつかの特定のセキュリティ制約（例えば、電子パスポートアプリ

ケーションは、ユーザの識別情報の送信を承認なしで許可するアプリケーションと共存できない）の共存アプリケーションによる遵守を要求する場合がある。

64 *前提条件：発行前でロードされたアプリケーション（アプリケーションAi（$i \in [1,n]$））の主要機能は、プラットフォーム評価に関連するETR及びETR-COMPに記述されなければならない。*

65 ITSEFは、アプリケーションAによって要求されるセキュリティ制約をアプリケーションCj及びAiの機能が満たすことをチェックする必要がある。

66 機能互換性解析に関して、一部の特定の製品アーキテクチャのみが認証できている場合、ITSEFはその旨を開発者に述べて、それらの製品の各アーキテクチャを提供することを開発者に要求しなければならない。

3.2 認証

67 認定済みのものを持つ、すべての共存するアプリケーション[8] は、オープンな隔離プラットフォームの場合と同様の認証報告書で識別される（2.2を参照）。しかし、認証報告書の「評価構成」の章では、既知のアプリケーションのサブセットで構成される製品も認証されることを明確化する。

3.3 オープンな隔離プラットフォーム上のアプリケーションの保守

68 Bkなどのいくつかの未知のアプリケーションも認定済み製品に含まれることを開発者が要求する場合、これらのアプリケーションに関する認証制限事項が取り上げられなければならない。

69 以下のような場合には、保守報告書が提供されることがある。

- これらのアプリケーションの検証及びローディングが、既知のアプリケーション Ai または Cj と同じ方法で行われることで、OE1 ならびに OE2 の要件に対応する場合。
- ならびに、認証済み A アプリケーションによって要求される機能互換性の制約がない場合。

70 開発者は、インパクト解析を持つそれらの新しいアプリケーションのローディングに関連する証拠を提供する必要がある（アプリケーションAiまたはCjの初期評価プロセス中に提供されたものと同じ種類の証拠）。インパクト解析では、新しいアプリケーションBkの主要機能も記述しなければならない。

71 このローディングが組織的手段に従って行われる場合、認証機関は、サイト訪問報告書がまだ有効である場合だけに保守報告書を発行できる。

[8] 既知のアプリケーション

4 参考文献

[Compo] *Joint Interpretation Library - Composite product evaluation for smart cards and similar devices*, version 1.2, January 2012.

[JCO/2.6] *Java Card System - Open Configuration Protection Profile, version 2.6.* Certified by ANSSI under the reference ANSSI-CC-PP-2010/03.

[JCO/3.0] *Java Card Protection Profile - Open Configuration, version 3.0. Certified* by ANSSI under the reference ANSSI-CC-PP-2010/03-M01.

[USIM] *(U)SIM Java Card Platform Protection Profile – Basic and SCWS Configurations, réf. PU-2009-RT-79, version 2.0.2.* Certified by ANSSI under the references ANSSI-CC-PP-2010/04 (Basic Configuration) and ANSSI-CC-PP-2010/05 (SCWS Configuration).

附属書 A：既存の「オープンプラットフォーム」PP との互換性

72 下表は、PP [JCO/2.6]、[JCO/3.0]または[USIM]に従って実現される評価へのオープンな隔離プラットフォームの認証手法の適用性を識別し、プラットフォームのセキュリティターゲットに含まれなければならない追加用件を定義している。

	[JCO/2.6]	**[JCO/3.0]**	**[USIM] [JCO/2.6]に従う**
O1：アプリケーション間の隔離	*O.FIREWALL*	*O.FIREWALL*	*[JCO/2.6]の O.FIREWALL*
O2：発行後ローディングの保護（真正性及び完全性）	*O.LOAD* ***この対策方針は、検証に関して、ロードされたCAPファイルの完全性及び真正性を保証するように意図されていることも明確化しなければならない***	*O.LOAD*	*[JCO/2.6]の O.LOAD O.APPLI-AUTH*
OE1：プラットフォームの隔離特性に関連する制約に従った、アプリケーションの検証	*OE.VERIFICATION* ***この対策方針は、[ISO_VERIF]ガイドに定義されている検討対象のプラットフォームに関する特定の制約を考慮に入れることまで詳説される必要がある*** *（備考：コンポジション規則によって、この検証が認証済みアプレットに課されるが、非認証アプレットも検証されるべきである）。*	*OE.VERIFICATION*	*[JCO/2.6]の OE.VERIFICATION OE.BASIC-APPS-VALIDATION*
OE2：各アプリケーションの完全性及び真正性の証拠の可用性	***オープンな隔離プラットフォームの認証手法への適合性を評価で主張できるように、対策方針が追加される必要がある。*** *（アプリケーション完全性の検証に関して、O.LOADの適用上の注釈に関連する）*	*OE.CODE-EVIDENCE*	*OE.VERIFICATION -AUTHORITY*