



情報技術セキュリティ
の分野における
コモンクライテリア認証書の承認
に関する
アレンジメント

2014年7月2日

平成26年9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

IPA まえがき

本書の目的

本書は、CCRA*のホームページ(<http://www.commoncriteriaportal.org/>)に掲載されている、“Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, July 2, 2014”を独立行政法人情報処理推進機構 (IPA)が日本語訳したものである。本書は、「情報技術セキュリティ評価の国際的な承認アレンジメント」を理解するための補助資料として作成されたものであり、正式な文書ではない。

使用上の注意

本書は、用語及び体裁の統一、記述内容などに不備がある可能性がある。疑問点については、CCRA のホームページ(<http://www.commoncriteriaportal.org/>)に掲載されている原文で確認して頂きたい。本書は、参照利用されることのみを目的として公開される。本書の改編、及び他への転載は禁止する。

* CCRA: Common Criteria Recognition Arrangement
(CC に基づいて評価及び認証した IT 製品を相互に承認する国際的なアレンジメント)

加盟機関

Defence Signals Directorate
from Australia

and

Secure Information Technology Center – Austria (A-SIT)
from Austria

and

Communications Security Establishment
from Canada

and

National Security Authority
from Czech Republic

and

Centre For Cyber Security
from Denmark

and

Finnish Communications Regulatory Authority
from Finland

and

Agence Nationale de la Sécurité des Systèmes d'Information
from France

and

Bundesamt für Sicherheit in der Informationstechnik
from Germany

and

National INFOSEC Authority (National Intelligence Service)
from Greece

and

Ministry of National Development
from Hungary

and

**Government of India, Ministry of Communications and
Information Technology, and Department of Electronics and
Information Technology**

from India

and

The Standards Institution of Israel

from Israel

and

**Istituto Superiore delle Comunicazioni e delle Tecnologie
dell'Informazione**

from Italy

and

**Ministry of Economy, Trade and Industry, and
Information-technology Promotion Agency**

from Japan

and

CyberSecurity Malaysia

from Malaysia

and

Ministry of the Interior and Kingdom Relations

from The Netherlands

and

Government Communication Security Bureau

from New Zealand

and

Norwegian National Security Authority

from Norway

and

Ministry of Defence

from Pakistan

and

**National Intelligence Service and
National Security Research Institute**
from Republic of Korea

and

Infocomm Development Authority of Singapore
from Singapore

and

**Ministerio de Hacienda y Administraciones Públicas and
Centro Criptológico Nacional**
from Spain

and

Swedish Defence Materiel Administration (FMV)
from Sweden

and

Turkish Standards Institution
from Turkey

and

CESG
from the United Kingdom

and

National Security Agency
from the United States of America

以上の加盟機関は、次のように協力することを計画している：

前文

アレンジメントの目的

本アレンジメントの加盟機関は、以下のような目標を共有する：

- a) 情報技術 (IT) 製品及びプロテクションプロファイルの評価が、高度で一貫した基準で実施され、これらの製品及びプロファイルのセキュリティに対する信頼性に、大きく貢献することを保証すること；
- b) 評価が実施されセキュリティが強化された IT 製品及びプロテクションプロファイルの入手可能性を向上させること；
- c) IT 製品及びプロテクションプロファイルの評価を繰り返す労力を省くこと；
- d) IT 製品及びプロテクションプロファイルに関する評価及び認証¹ プロセスの効率ならびに費用対効果を継続的に向上させること。

本アレンジメントの目的は、CC 規格の要件通りに、コモンクライテリア認証書を取得した IT 製品及びプロテクションプロファイルを、再度評価することなく、調達または使用できる状況を作り出すことによって、これらの目標を推進することにある。これは、コモンクライテリア認証書を発行する認証機関 (CB) に、高度で一貫した基準を満たすことを要求することにより、元の認証書に関する判断の信頼性を確信するための根拠が提供されることを求めている。

特定の利用者の戦略的なニーズのための要件、あるいは、二者間または多者間の個別契約に基づいて、政府の機密を扱う IT システムが調達され、認証及び承認される場合もありうる。本アレンジメントは、このような契約に制約を加えるものではない。特に、第 3 条に記載される例外は、このような個別交渉による契約には適用されないものである。

1 つの加盟機関による複数の認証機関 (CB) の運営または純粋に商業的な CB の運営は、特定の基準の順守に加えて、政府機関間の相互の理解と信頼を必要とする本アレンジメントの意図に適合しない。したがって、本アレンジメントの運営は、複数の CB または純粋に商業的な CB を受け入れることはできない。

さらに、他国において発行された認証書を承認することは、その政府特有の決定及び約束事項が関与してくるため、本アレンジメントにおいては、認証書の発行と承認の機能が区別されている。

¹ あるスキームでは Certification の代わりに Validation という用語の使用が選択されることがある。本承認アレンジメントでは、これらの用語は、付属書 A の用語集に示すように、意味と目的に関して同等であると見なされる。

本アレンジメントの精神

情報システムの複雑さのために、非常に慎重に記述されたセキュリティの評価基準と評価方法をもってしても、すべての事態に対処できないことがある。多くの場合、基準を適用するためには、専門家の判断と、その適用の監督が必要になる。したがって、本アレンジメントの加盟機関は、それぞれの技術的な判断と力量に関して相互の理解と信頼を築くとともに維持し、公開された議論や討論を通じて全体的に一貫性を維持することを計画している。

本アレンジメントの加盟機関は、評価基準、評価方法、及びその適用を改善するために積極的に活動することに努める。例えば、より費用対効果の高い、一貫性のある、再現可能な保証パッケージを作成及び確立したり、保証のためにあまり役に立たない要件を特定し破棄することなどである。また、加盟機関は、例えば評価のスポンサーが評価で得られた情報に関心のある者へ提供しよう奨励して、かかる情報の経済的な再利用を推進することとしている。

第 1 条

参加資格

本アレンジメントの加盟機関は、自国または複数の国を代表する政府組織または政府省庁である。加盟機関は評価認証書の発行機関、評価認証書の受入機関、または両方である。認証書受入国は、IT セキュリティの評価能力を有しないことがあるが、それでも認証済みの IT 製品とプロテクションプロファイルの使用に関心を表明している。認証書生成国は、自国で運営している適合認証機関 (CB) (第 5 条で説明する) のスポンサーであり、自国の認証書を発効する。認証書生成国であって、適合 CB としての資源と専門知識を兼ね備えた組織が、承認された加盟機関として定義される。

第 2 条

適用範囲

IT 製品及びプロテクションプロファイルに関して、加盟機関は、他の認証書生成国が本アレンジメントの条項と各加盟機関に適用される法律及び法令に従って発効したコモンクライテリア認証書を承認することが相互に了解されている。本アレンジメントは、以下のいずれかのコモンクライテリア保証コンポーネントに対する適合を主張する認証書について取り扱う：

- 1) 付属書 K に従って開発及び維持された コラボラティブプロテクションプロファイル (cPP) で、マネジメントコミティが承認した国際的なテクニカルコミュニティを通じて開発された、評価保証レベル 4 まで及び ALC_FLR を含むものより選択された保証アクティビティを持つもの；または
- 2) 評価保証レベル 1 から 2 及び ALC_FLR²

適用範囲については、第 14 条の規定に基づき、保証レベルまたはコンポーネントを追加または削除することによって、本アレンジメントの加盟機関の合意による修正がいつでも可能である。

第 3 条

例外事項

コモンクライテリア認証書の承認によって、加盟機関が適用される国の法律、国際法、または欧州共同体の法律または法令に違反することになる場合は、その加盟機関はかかる認証書の承認を断ることができる。特に、国の法律、法令、行政規則、または公職規定の下で要求または承認されたセキュリティ機密区分または保護マークの対象となる情報の保護に関して、IT 製品またはプロテクションプロファイルの適用が検討されている場合、加盟機関はその適用のみについて認

² ITセキュリティ評価のコモンクライテリアのパート 3 に詳述してある通り。

証書の承認を断ることができる。本アレンジメントの付属書 F.3 及び G.2 は、本条項に従って、例外を求める加盟機関によって適用されるべきである。

第 4 条

定義

本アレンジメントの意味に関して重要な用語または本アレンジメントに独特の意味で使用される用語は、本アレンジメントの付属書 A の用語集で定義する。かかる用語は本アレンジメントの本文に初めて現れたときに、イタリック体で示す。

第 5 条

承認の条件

本アレンジメントに別段の規定がない限り、各加盟機関は、認証書生成国が発効した、適切なコモンクライテリア認証書を承認すべきである。かかる認証書の発効によって、評価及び認証プロセスが正当かつ専門的な方法で実施されたことが確認される。

- a) 認められた IT セキュリティ評価基準に基づくこと；
- b) 認められた IT セキュリティ評価方法及びサポート文書を使用すること；
- c) 認証書生成国において、適合 CB が運営する評価及び認証スキームで実施すること；及び
- d) 発効されたコモンクライテリア認証書と、発行された認証報告書が本アレンジメントの目標を満たしていること。

これらすべての条件を満たす認証書は、本アレンジメントの目的に照らして等価であると見なされる。

IT セキュリティ評価基準は、Common Criteria for Information Technology Security Evaluation (CC) の、マネジメントコミティが承認したバージョンにおいて制定する。評価方法は Common Methodology for Information Technology Security Evaluation (CEM) 及び CC サポート文書の、マネジメントコミティが承認したバージョンにおいて制定する。認証報告書のミニマム要件は、本アレンジメントの付属書 I において制定する。評価及び認証スキームのミニマム要件は、本アレンジメントの付属書 B において制定する。評価及び認証は、最小限、次の条件を満たす場合に、正当かつ専門的な方法で実施されたものと見なされる：

- a) 評価機関が次のいずれかの条件を満たすこと
 - ISO/IEC 17025 とその後継規格に従って、またはすべての加盟機関が承認したその解釈に従って、承認された認定機関によりそれぞれの国で認定されており、かつ付属書 B.3 に従ってライセンス付与または承認されていること

- その国で有効な法律、法定文書、またはその他の公的な行政手続きに基づいて設立され、本アレンジメントの付属書 B.3 に規定されている要件を満たしていること；

及び

b) CB の適合性が承認され、次のいずれかの条件を満たすこと

- ISO/IEC 17065 とその後継規格に従って、または最小限、本アレンジメントの付属書 C に規定する要件を満たす、それらのそれぞれの国の解釈に従って、承認された認定機関によりそれぞれの国で認定されていること
- その国で有効な法律、法定文書、またはその他の公的な行政手続きに基づいて設立され、本アレンジメントの付属書 C に規定されている要件、または ISO/IEC 17065 またはその後継規格を満たしていること

評価及び認証スキーム間でコモンクライテリアと共通評価方法の一貫性をもった適用を支援するために、加盟機関は現在適用されているコモンクライテリアと共通評価方法の解釈の統一に向けて、サポート文書の開発及び統一された適用を通じて話し合いを行うことを計画している。また、この目標に向けて、加盟機関は解釈の相違を解決するために必要な解釈と議論に関する定期的な情報交換を行うことを計画している。コモンクライテリア、共通評価方法、及びサポート文書の一貫した、信頼性の高い、要求にかなう適用という目標をさらに推進するために、CB はスキーム内で進行中のすべての評価を適切なレベルで監督する責任を負い、また傘下の IT セキュリティ評価機関が以下に示す事項を実施することを保証するためのその他の手続きの遂行に責任を負うべきである：

- a) 評価を公平に行う；
- b) コモンクライテリア、共通評価方法、及び CCRA サポート文書群による方法を正確かつ一貫性をもって適用する；
- c) 保護情報の機密性を適切に保護する

第 6 条

定期審査

本アレンジメントの目標を共有し、本アレンジメントの目標の達成のために努力していることを確認するために、5 年以内の間隔で適合 CB の審査を行うべきである。かかる審査の方法については、本アレンジメントの付属書 D に制定する。

第7条

公表及びサービス、認証マークの使用

認証書生成国によって発効されたコモンクライテリア認証書は、加盟機関または評価及び認証スキーム固有のロゴまたは識別するための意匠に加えて、承認アレンジメントのマークと標準形式の記述内容を明確に表示しなければならない。マークと記述内容の形式は、本アレンジメントの付属書 E と付属書 J に規定する。

それぞれの認証書生成国は、その認証製品リストの一部として、またはその他の方法で、別の認証書生成国によって発効された認証書を有するすべての IT 製品とプロテクションプロファイルの簡潔な特徴を公開すべきである。ただし、本アレンジメントの第3条に規定する理由など、本アレンジメントに基づいて公開すべきでない理由がある場合はこの限りではない。

第8条

情報の共有

情報の開示が加盟機関の国の法律または法令に違反しない限り、各加盟機関は本アレンジメントの適用に関するすべての情報と文書を他の加盟機関に提供することに努めるべきである。

この義務の履行に関して、IT セキュリティ評価機関 (ITSEF)、CB、または加盟機関は、当事者から事前に書面による合意を得ている場合にのみ、第三者の営業上の機密情報または保護情報を開示することができる。

特に、各加盟機関は自らの承認条件を満たす能力に影響を与えうる、または本アレンジメントの運用または意図をその他の方法で妨げうる変更の見込みに関してはただちに情報を提供すべきである。

加盟機関が共有すべき情報と文書の性質と範囲については、本アレンジメントの付属書 F でさらに詳細に説明する。

第9条

新しい加盟機関

加盟機関

既存の加盟機関全員の同意を条件として、本アレンジメントの原則の順守を意図する国の代表者は、本アレンジメントの加盟機関となることができる。

認証機関

既存の加盟機関全員が同意すれば、ある CB は本アレンジメントの第 5 条の目的に適合しているとみなされる。ただし、既存の加盟機関が、その認証機関が本アレンジメントの第 5 条と第 5 条に引用されている付属書に制定する承認条件を満たし、シャドー審査を含む本アレンジメントの付属書 G に制定する手続きに従った適合条件を満たしていると確信する場合に限られる。

第 10 条

本アレンジメントの管理

マネジメントコミティが本アレンジメントを管理するべきである。マネジメントコミティは本アレンジメントの状態、条項、または適用に関する事項を検討するために、必要に応じて会合を開くべきである。すべての加盟機関はマネジメントコミティに出席する。マネジメントコミティの手続きと主な責任については、本アレンジメントの付属書 H に規定する。

第 11 条

意見の不一致

加盟機関間の意見の不一致は、話し合いによって解決するべきである。加盟機関は交渉によって相互間の不一致を解決するために最善を尽くすべきである。話し合いまたは交渉によって解決しない場合は、その不一致は最初にマネジメントコミティに委ねられる。マネジメントコミティは不一致に関する調査結果を文書化する。不一致を話し合いまたは交渉によって解決できない場合は、個々の加盟機関は、関係するコモンクライテリア認証書を承認せずに、かかる不承認についてマネジメントコミティに通知する方法を選ぶことができる。

第 12 条

請負業者の使用

加盟機関が本アレンジメント、特にその付属書 D、G3、G4、または H に規定する手続きの実施と運用に関して、請負業者の使用を企てる場合は、その請負業者が適切な専門技術を持つことを確認して、他の加盟機関に通知するべきである。保護情報は、付属書 F.4 に制定される通り、情報発生元の合意があった場合にのみ、請負業者に渡されるべきである。

第 13 条

本アレンジメントの費用

本アレンジメントに別段の規定がある場合を除き、各加盟機関は本アレンジメントへの参加によって生じる自らの費用のすべてを負担する。

第 14 条

修正

本アレンジメントの条項の修正には、加盟機関全員一致の同意が必要である。採択された変更は文書に記録し、すべての加盟機関が署名すべきである。

第 15 条

期間

加盟機関が本アレンジメントの終了を全員の同意によって決定しない限り、本アレンジメントに基づく協力は継続される。

第 16 条

参加の取り止め

加盟機関は書面で他の加盟機関に通知することによって、本アレンジメントへの参加を取り止めたり、代表している CB の適合資格を取り消すことができる。

第 17 条

施行

本アレンジメントまたは後続の修正は、すべての加盟機関によって署名された日付より施行すること。

継続に関しては、マネジメントコミティによる別段の承認がない限り、すべてのメンバー（認証機関）の適合状況は、本アレンジメントの前バージョンの下で、最後の定期審査／シャドー審査の日付から 5 年間有効である。

本アレンジメントの前バージョンの下で、認証書生成国への昇格に関する申請を行ったが、シャドー審査がまだ完了していない認証書受入国は、本アレンジメントの前バージョンの条件の下で、シャドー審査を完了することを選択してもよい。

さらに、すべての加盟機関は以下のことに合意する：

- a) 本アレンジメントの前バージョンに適合する、その下で発行された認証書を承認すること；
- b) 本アレンジメントの合意前に本アレンジメントの前バージョンに従って、認証プロセスを受け入れられた製品の認証書を承認すること；及び

- c) 本アレンジメントがすべての加盟機関によって署名された日付から 36 ヶ月間、本アレンジメントの前バージョンに従って発行された再認証と認証維持の追加情報を承認すること。その後、すべての加盟機関は、第 2 条に従って発行された認証の承認を制限しなければならない。

第 18 条

本アレンジメントの効果

本アレンジメントは、本アレンジメントの署名機関に属さない者には実質上または手続き上の権利、責任、または義務を生成しないことを、各加盟機関は認識し、受け入れる。また、各加盟機関は、本アレンジメントが国家、国際、または欧州共同体の法律のいずれかまたはすべてに関して拘束力を持たず、加盟機関は国内の裁判所または国際裁判所で本アレンジメントを強制しようとしなかったことを認識し、受け入れる。CB によって発行された報告書または加盟機関によって発効されたコモンクライテリア認証書は、IT 製品またはプロテクションプロファイルの認証機関または加盟機関それぞれによる承認または保証を示すものではない。また、認証活動の結果として発効されたコモンクライテリア認証書の承認は、別の CB によって発行された認証報告書、またはその結果作成され、別の加盟機関によって発効された認証書を、いかなる意味でも承認または保証するものではない。

付属書 A

用語集

この用語集では、本アレンジメントで独特な意味で使用される、または本アレンジメントの解釈のために重要な意味を持つ、本アレンジメントの本文または付属書の特定の用語を定義する。また、この用語集には、この付属書で使用されるその他の用語の定義も含まれている。この付属書の定義が CC または CEM での同じ用語の定義と異なる場合は、この付属書の定義を使用して本アレンジメントが意図する意味とする。かかる定義は CC 及び CEM での定義と広義では一致するものであり、一般的に有効性を失わない。この相違は、本アレンジメントの特定の文脈において、意味をより明確にするために生じる。用語集の別の場所で定義されている用語は、定義文の中にイタリック体で示す。

認定 (Accredited) :

公平性と、一般的な技術、方法、手続き上の力量に関して、あらかじめ定められた規格を満たしていることが、*認定機関*によって公式に確認されること。

認定機関 (Accreditation Body) :

承認された規格に照らして他の組織の業務実施能力を審査し、それらの組織が規格を満たしている状態を正式に確認することに責任を負う独立組織。

達成可能なセキュリティ保証の共通レベル (Achievable Common Level of Security Assurance) :

適切な、比較可能な、再現可能な、費用対効果の高い結果をもたらす *コラボラティブプロテクションプロファイル* で定義されているセキュリティ保証要件。すべての承認された *加盟機関* の *CB* が *コラボラティブプロテクションプロファイル* 及び関係する *サポート文書* に対する *評価* を認証する素質があると承認されている。スキームは、自分達のビジネスニーズに基づいて、*cPP* を使用することができる。

承認 (Approved) :

ライセンス付与 を参照。

承認/ライセンス付与の方針 (Approval/Licensing Policy) :

すべての *評価* 及び *認証* スキームに不可欠な文書の一部。これは申請を *ライセンス付与* または *承認* する手続き、かかる申請を処理する手続き、承認を受けるために申請者が満たさなければならない教育・訓練要件とセキュリティ要件を規定する。

適合 CB の審査 (Assessment of Compliant CBs) :

特定の適合 CB によって実施される評価及び認証が、本アレンジメントの規定に従っていることを確認する手続き。

認証書発効 (Authorisation) :

加盟機関が、適合 CB によるコモンクライテリア認証書の発行と CC 認証マークの使用を是認すること。

CC :

コモンクライテリア。Common Criteria for Information Technology Security Evaluation。IT セキュリティ評価基準の特定のセットについて記述している文書の表題。

CEM :

共通評価方法。Common Methodology for Information Technology Security Evaluation。IT セキュリティ評価方法の特定のセットについて記述している技術文書の表題。

認証 (Certification/Validation) :

コモンクライテリア認証書の発行の前に CB によって遂行されるプロセス。

認証機関 (CB) (Certification Body) :

認証の実施と評価及び認証スキームの日々の運用を監督することに責任を負う組織。

委託 CB (Associated CB) :

承認された加盟機関から委託される適合 CB。

適合 CB (Compliant CB) :

付属書 L に適合する認証機関としてリストアップされている CB。

認証報告書 (Certification/Validation Report) :

評価の結果を要約し、全般的な結果を確認するために CB によって発行される公開文書。すなわち、評価が正しく実施され、評価基準、評価方法、及びその他の手続きが正しく適用され、評価報告書の結論が提示された証拠と矛盾していないことを確認するための公開文書。

認証製品リスト (Certified/Validated Product List) :

本アレンジメントに従って、現在有効なコモンクライテリア認証書の簡潔な特徴を示す公開文書。

クライアント (Client) :

評価のために ITSEF と契約している当事者。

コモンクライテリア認証書 (Common Criteria Certificate) :

特定の IT 製品またはプロテクションプロファイルが ITSEF の評価に合格したことを確認するために、適合 CB によって発行され、加盟機関によって発効される公開文書。コモンクライテリア認証書は、常に認証報告書と関連付けられる。

評価 (Evaluation) :

主張の正当性を決定するために、共通評価方法を使用し、コモンクライテリアに照らして IT 製品またはプロテクションプロファイルを審査すること。

評価及び認証スキーム (Evaluation and Certification/Validation Scheme) :

力量と公平性が高い基準で維持され、一貫性が達成されていることを確認するための、CB の権限の下での評価及び認証機能の組織的な体制。

評価機関 (Evaluation Facility) :

評価を受ける IT 製品またはプロテクションプロファイルの開発者とは独立して、通常は商業ベースで評価を実施する組織。

評価方法 (Evaluation Methods) :

IT セキュリティ評価方法を参照。

評価報告書 (Evaluation Technical Report) :

認証報告書の主要な基礎となるものとして、評価機関から CB に提出される、評価の所見に関する詳細を示す報告書。

国際的なテクニカルコミュニティ (iTC) (International Technical Community) :

加盟機関、認証機関、ITSEF、開発者及び利用者を含めた専門技術者のグループで、以下を満たすこと :

- a) 公平な競争を促進する方法で活動すること ;
- b) cPP を定義するために特定の技術分野において活動すること ;
- c) マネジメントコミティによって、この目的のために承認されること ; 及び
- d) CCRA 承認プロセスの対象となるサポート文書を通じて cPP にとって必要となる CC 及び CEM 適用の解釈を確立すること。

解釈 (Interpretation) :

評価基準または評価方法の技術的な側面の意味または適用方法に関して、要求された場合に示される専門家の技術的判断。

IT 製品 (IT Product) :

多様な IT システム内で使用し、または組み込むために設計された機能を提供する IT ソフトウェア及び/またはハードウェアのパッケージ。

IT セキュリティ評価基準 (IT Security Evaluation Criteria) :

評価及び認証スキームを通じて、効果的かつ一貫した規格に従って評価が実施されると確信する根拠を提供するために、提示すべき情報と、とるべきアクションをまとめたもの。

IT セキュリティ評価方法 (IT Security Evaluation Methods) :

評価及び認証スキームを通じて、効果的かつ一貫した規格に従って評価が実施されると確信する根拠を提供するために、IT セキュリティ評価基準の適用について評価機関が使用するべき方法をまとめたもの。

ITSEF :

IT セキュリティ評価機関。特定の IT セキュリティの評価及び認証スキームに沿って評価を実施するためのライセンス付与または承認を受け、認定された評価機関。

IT システム (IT System) :

特定の目的と運用要件を持つ特定の IT 設備。

ライセンス付与 (Licensed) :

IT セキュリティ評価の特定の分野で、技術的な力量を持つことが CB により審査され、特定の評価及び認証スキームに沿って評価を実施することが正式に承認されること。

マネジメント委員会 (MC) (Management Committee) :

本アレンジメントの規則に従って、本アレンジメントの運用を確実にするために、すべての加盟機関の代表者が出席する組織。

(評価の) モニタリング (Monitoring (of Evaluations)) :

ITSEF が適切かつ専門的な方法で職務を遂行していることを確認するために、CB の代表者が進行中の評価を観察し、完了した評価をレビューする手続き。

情報発生元 (Originator) :

情報の発生源。例えば、IT セキュリティの評価または認証に関連する保護情報を作成した IT 製品またはプロテクションプロファイルの開発者、ITSEF、または加盟機関。

加盟機関 (Participant) :

本アレンジメントの署名機関。

認証書受入国 (Certificate Consuming Participant) :

コモンクライテリア認証書の承認に国家的な関心を有する加盟機関。

認証書生成国 (Certificate Authorising Participant) :

単数または複数の適合 CB を代表する加盟機関。

承認された加盟機関 (Qualified Participant) :

適合 CB でもある加盟機関 (またはシャドー審査を受ける専門技術者を提供し、適合 CB の資源と専門技術を自由に行使できる加盟機関)。この CB は承認された加盟機関の委託 CB である。

保護情報 (Protective Information) :

本アレンジメントのプロセスまたは活動の下で収集または取得された情報で、その無許可の開示によって次のいずれかの事態を生じると合理的に予想される情報。(i) 競争上、商業的または私的な利益を害する。(ii) 個人のプライバシーを明確に、正当な理由なく侵害する。(iii) 国家安全保障を害する。(iv) その他の方法で国家の法律、法令、行政規則、または公職規定によって保護されている利益を害する。

プロテクションプロファイル (Protection Profile) :

CC で定義される公式文書で、特定の消費者のニーズを満たす IT 製品のカテゴリについて、実装に依存しないセキュリティ要件のセット。

コラボラティブプロテクションプロファイル (cPP) (Collaborative Protection Profile) :

マネジメントコミティが承認した国際的なテクニカルコミュニティによって共同で開発されたプロテクションプロファイル。cPP 及び関係するサポート文書は、共通のセキュリティ機能要件及び達成可能なセキュリティ保証の共通レベルのミニマムセットを定義する。それは、認証された製品が達成可能なセキュリティ保証の共通レベルを達成することを確実にするために、脆弱性分析要件に対処する。

保護マーク (Protective Marking) :

機密性の高い重要な情報、及び／または機密情報を表すマーク。

RA in Confidence :

CCRA 内のみで使用される、潜在的な機密性の高いデータを持つ文書を区別するために使用される保護マーク。使用手続きは、MC 手続き内に明示的に定義される。

承認 (Recognise) :

コモンクライテリア認証書の承認を参照。

コモンクライテリア認証書の承認 (Recognition of Common Criteria Certificates) :

適合 CB によって実施された評価及び認証手続きが、正当かつ専門的な方法で実施され、本アレンジメントのすべての条件を満たしていることを加盟機関が認め、その結果発行されるすべての CC 認証書に同等の価値を与える意図を示すもの。

セキュリティ機密区分 (Security Classification) :

国家の利益に適用する必要がある保護の最低基準を示すために保護情報に適用するマーク。

セキュリティターゲット (ST) (Security Target) :

識別された特定の評価対象に関して必要とされるセキュリティの実装についての文書。

シャドー審査 (Shadow Certification/Validation) :

少なくとも 1 つの承認された加盟機関の代表者が、本アレンジメントに従って IT 製品の評価及び認証をモニターして CB を審査すること。

(CB の) スポンサー (Sponsor (of a CB)) :

適合 CB (または適合 CB 候補) の利益を代表し、そのコモンクライテリア認証書を発効する加盟機関。

サポート文書 (Supporting Document) :

特定の技術分野または技術ドメインにおける IT セキュリティ評価のためのコモンクライテリアまたは共通評価方法の使い方を定める文書。このような文書は、必須文書またはガイダンス文書であると共に、一般的に CC 及び/または CEM の解釈を必要に応じて定めるものである。

評価対象 (TOE) (Target of Evaluation) :

評価の対象となる IT 製品、及び関連する管理者/利用者ガイダンス文書。

付属書 B

評価及び認証スキーム

B.1 スキームの目的と主な特性

評価及び認証スキーム（以下「スキーム」という）の主な目的は、評価及び認証機能の組織的な体制と管理を通じて、高い基準の力量と公平性が維持され、一貫性が達成されていることを確実にすることである。

このため、各スキームは単一の認証機関によって管理され、評価された製品及びプロテクションプロファイルの認証だけでなく、セクション B.2 にリストアップされている、同様に重要な、その他の機能にも責任を負う。

スキームの全般的な方針（ライセンス付与または承認の方針を含む。以下参照）は、認証機関自体またはマネジメントボードのいずれかによって決定することができる。後者の場合、マネジメントボードはその規則と方針に従って、スキームの運用に最終的な責任を負い、適切な場合には、これらの規則と方針の解釈または修正にも責任を負う。他方で、認証機関はスキームを管理し、マネジメントボードの方針ガイダンスに従って規則と方針を適用する。いずれの場合にも、スキームの運用において、評価と認証活動に利害関係を有するすべての関係当事者の利益を適切に考慮に入れることを確実にするための仕組みを整えることが非常に重要である。

かかるスキームの存在は、承認のために非常に重要である。というのは、これは共通評価基準及び評価方法の正しく一貫した適用と共に、すべての ITSEF が同一の高い標準に従って運営されており、その結果が正確で、ITSEF 間で一貫していることを確信する唯一の根拠を提供するからである。そのような確信は、すべての承認アレンジメントに必要な信頼を確立するために不可欠である。

B.2 CB の役割と主な特性

特定のスキームにて評価を実施するためのライセンス付与または承認を得た評価機関は、IT セキュリティ評価機関と呼ばれている。CB は ITSEF から独立しており、適切な資格を有する要員を配置している。

CB は、その国の有効な法律、法定文書、またはその他の公的な行政手続きの条項に基づいて設立されることもできるし、適切な認定機関によって認定を受けることもできる。いずれの場合にも、本アレンジメントの付属書 C に規定する要件、または、ISO/IEC 17065 またはその後継規格の要件のいずれかを満たさなければならない。

次に、認証機関が遂行する主な機能を示す：

- a) 評価機関のスキームへの参加を是認する（以下を参照）；
- b) 参加 ITSEF の業務実施能力、特に承認された評価基準と評価方法への適合、適用、及び解釈をモニターする；
- c) 評価を受ける製品及びプロテクションプロファイルと、評価自体の手続きに関する機密情報が適切に扱われ、必要な秘密保護手段がとられ、かかる手続きが日常的に遵守されていることを確実にするために、スキーム内で手続きが確立されていることを確認する；
- d) 必要に応じて、ITSEF に追加のガイダンスを発行する；
- e) 適切なレベルで、スキーム内で進行中のすべての評価をモニターする；
- f) 結論が提出された証拠と一貫しており、認められた評価基準と評価方法が正しく適用されていることを確実にするために、すべての評価に関する報告書（特に評価報告書を含む）をレビューする；
- g) スキームの下で完了した各評価に関する認証報告書を作成する；
- h) コモンクライテリア認証書及び関連する認証報告書を公開する；
- i) 現在有効なコモンクライテリア認証書を有するスキーム内で評価されたすべての製品及びプロテクションプロファイルについて、簡潔な特徴を示した文書を定期的に公開する（認証製品リスト）；
- j) スキームの組織、方針、規則、及び手続きを文書化し、その文書を公開し、最新の状態に保つ；
- k) スキームの規則が遵守されていることを確実にする；
- l) スキームの規則と方針を確立し、必要に応じて修正する；
- m) スキームの活動に利害関係を有するすべての関係当事者の利益がスキームの運用において適切に考慮に入れられていることを確実にする。

本アレンジメントへの参加の一環として、承認された加盟機関に関する認証機関は、本アレンジメントの規定に従って、本アレンジメントに関連する活動の技術サポートの提供にも責任を負う。

B.3 評価機関の認定とライセンス付与

評価機関が法律または法定文書に基づいて設立されていない限り、スキームに参加するには次の2つの条件を満たす必要がある：

- a) その国で正式に承認されている認定機関の認定を受けること；及び
- b) スキームの管理に責任を負う CB によってライセンス付与またはその他の方法で承認されること

認定では、評価機関はその公平性、一般的な技術、方法、及び手続き上の力量を示し、特に IT セキュリティの領域の特性と一貫している限り、ISO/IEC 17025 またはその後継規格の要件を満たしていることを示さなければならない。

また、評価機関は、IT セキュリティ評価の特定の分野に技術的な力量を有し、関係するスキームのすべての規則に従うことができる立場にあることを CB が納得するように示さなければならない。例えば、適用される評価基準と評価方法を正しくかつ一貫して適用する能力があり、評価中の IT 製品またはプロテクションプロファイルと評価自体のプロセスに関する機密情報または保護情報の保護に必要な厳格なセキュリティ要件を満たしていることを示さなければならない。

各スキームのライセンス付与の方針または承認の方針には、セキュリティと教育・訓練要件の詳細と、ライセンス付与または承認のための申請手続きの詳細、及びかかる申請を処理する手続きの詳細が含まれる。

付属書 C

認証機関の要件

C.1 一般的要件

CB のサービスは過度の財務条件またはその他の条件なしに利用することができること。CB を運営する手続きは公平な方法で管理すること。

C.2 管理構成

CB は公平であること。特に、認証に商業上または財務上の利害関係を有する者によって、不当な影響または統制を受けずに、日々の運営を遂行できるように、CB には上級管理者に責任を負う常任スタッフが必要である。

C.3 組織構成

CB は次のものを所有し、要求されたときに提供できること：

- a) 組織の責任と報告経路を明確に示した図；
- b) 組織が財務支援を得るための手段の説明；
- c) 評価及び認証スキームについて記述した文書；及び
- d) 法的状態を明確に示した文書

C.4 認証要員

CB の要員は担当する職務に関する力量を有していること。各スタッフの資格、教育・訓練、及び経験に関する情報は、CB によって最新の状態に維持されること。

要員は、それぞれの義務と責任に関する、明確で最新の文書化された指示が与えられていること。

外部機関に作業を請け負わせる場合は、CB は請負作業を実施する要員が、本付属書の該当する要件を満たしていることを確認すること。

C.5 文書と変更管理

CB は、その評価及び認証スキームに関連するすべての文書の管理のためのシステムを維持し、次のことを確保すること：

- a) 適切な文書の最新版が、すべての関係する場所で入手可能であること；

- b) 適切な権限なしに文書が修正されたり、無効にされないこと；
- c) 変更について知る必要がある者が、直ちに通知を受け、迅速で効果的な措置をとることができるように、変更が交付されること；
- d) 旧版として無効になった文書は、組織及び関連する機関すべてにおいて使用を止めること；及び
- e) スキームに直接の利害関係を有する者に対して変更を通知すること

C.6 記録

CB は、その固有な状況に適応させ、加盟機関に關係する管轄で適用される關係規則に従うために、記録システムを維持すること。このシステムには、各認証に關連して作成されたすべての記録とその他の書類を含む。これは各認証の過程を追跡できるように十分に完全なものにする。すべての記録は最低 5 年間、安全で参照可能な場所に保存すること。

C.7 認証手続き

CB は、IT 製品またはプロテクションプロファイルの認証が、適用される IT セキュリティ評価基準及び方法（すなわち、CEM、CC サポート文書）に従って正確に実施されるように、必要な設備と手続き文書を保持すること。

C.8 IT セキュリティ評価機関の要件

CB は、IT セキュリティ評価機関が本アレンジメントに規定する要件に従っていることを確認すること。

CB は、各 IT セキュリティ評価機関に対して、すべての關係する手続きに關する、適切な合意文書を作成すること。これには、保護情報と評価及び認証手続きの機密性を確保するための取り決めが含まれる。

C.9 品質マニュアル

CB は、本付属書の要件に適合するための手続きを規定した品質マニュアル等の文書を保持すること。これらには少なくとも次の項目を含む：

- a) 品質の維持に關する方針ステートメント；
- b) CB の法的状態に關する簡潔な説明文書；
- c) 上級管理者及びその他の認証要員の氏名、資格、及び順守義務；
- d) 認証要員の教育・訓練計画の詳細；

- e) 上級管理者から生じる権限、責任及び機能の割り振りをラインとして示す組織図；
- f) IT 製品またはプロテクトンプロファイルの評価を監督する手続きの詳細；
- g) コモンクライテリア認証書の不正使用を防止する手続きの詳細；
- h) 外部委託要員の身分、及びその力量を評価しモニターするための手続き文書の詳細；及び
- i) 異議申立てまたは調停の手続きの詳細

C.10 秘密保持

加盟機関の国の法律、制定法、行政命令、または法令によって許可されている範囲で、CB はその組織のすべてのレベルにおいて行われた認証活動の過程で取得した情報の機密性を確保するために十分な手はずを整えるべきであり、また本アレンジメントに基づく認証活動の過程で取得した保護情報を許可なく開示してはならない。

C.11 公表

CB は認証製品リストを作成し、必要に応じて更新すること。リストに示す各 IT 製品とプロテクトンプロファイルは明確に識別すること。このリストは一般に公表すること。

評価及び認証スキームの概要は、公開された形式で提供すること。

C.12 異議申立てまたは調停

CB は、CB 自体、関連する ITSEF、及びそのクライアントの間での意見の相違について対処するための手続きを保持すること。

C.13 マネジメントレビュー

CB は本アレンジメントの目標を共有し続けていることを確実にするために、スキームの運営についてマネジメントレビューを実施すること。

C.14 コモンクライテリア認証書の誤使用

CB はコモンクライテリア認証書の使用に対して適切な統制を実施すること。

CB は認証書の誤使用を防止し、対処するために、適切な行政手続きまたは法的な措置をとり、認証書または評価及び認証スキームに関する誤った、誤解を生じる、または不適切なステートメントを修正する義務を負う。

C.15 コモンクライテリア認証書の取り消し

CB はコモンクライテリア認証書の取り消しに関する文書化した手続きを保持し、認証製品リストの次の版で取り消しについて通知すること。

付属書 D

定期審査

マネジメント委員会は、適合 CB の定期審査を実施するために、2 つ以上の承認された加盟機関（該当 CB のスポンサーを除く）を選出することができる。審査は、スポンサーの書面による同意または要請がない限り行うことはできない。かかる同意は審査の実施前または実施中に取り消したり、撤回することができる。スポンサーは、審査チームの選出に関して CB が懸念を抱く場合は、マネジメント委員会に説明する必要がある。審査は以下の説明に従って、またマネジメント委員会によって発行されるガイダンスに従って実施するべきである。このガイダンスは、審査が統一基準に従って実施され、予測される資源に関わるということを確認にする。

審査を実施する加盟機関は、マネジメント委員会に受け入れられる 2 人の専門家から構成される主要審査チームを指名することができる。加盟機関は、自らの費用で追加の専門家を提供することができる。委託 CB に対して主要審査チームを提供する費用は、エグゼクティブサブ委員会によって合意された公平な方法で承認された加盟機関間で分担する。審査を受ける CB が委託 CB でない場合は、その CB が審査から生じる主要審査チームのすべての費用（交通費、宿泊費、その他生活に要する費用、及び給与を含む³）を負担する。

定期審査を受ける CB は、1 ヶ月以内にその時点で適用される完全なスキームに関する文書を提出するべきである。専門家はその文書をレビューし、その CB が本アレンジメントの目標を引き続き共有していることを確認し、所見をマネジメント委員会に報告する。

定期審査は、直接関係する加盟機関の決定に従って、本アレンジメントの範囲内の少なくとも 2 つの IT 製品に関して実施されるべきである。秘密保持契約が締結されるべきであり、または、関係する加盟機関の間で、他の適切な情報共有メカニズムが確立されるべきである。

専門家は、定期審査を受ける CB が、評価及び認証プロセスのすべての点において一貫して活動していることを確認するべきである。専門家は、この責任を果たすにあたって、認証プロセスの一部に参加を希望することができる。審査を受ける CB は、専門家の参加が円滑に実施されるよう努めるべきである。

また、専門家は本アレンジメント、特に本アレンジメントの付属書 B と付属書 C に規定する保護情報の機密性を確認するために、手続きの適用状況についても調査すること。

評価及び認証の適切な段階で、専門家による調査のために次の文書を提出するべきである：

- a) セキュリティターゲット；

³ 審査を実施する承認された加盟機関が、国の法律または法令によって、かかる支払いを受けることを禁じられている場合は、これが適用されない場合がある。

- b) 評価報告書；
- c) 認証機関によって作成される上記の文書に関する書面のコメント；及び
- d) 認証報告書

その他の評価に関する報告書は、マネジメントコミティが発行するガイダンスに従って、要求があったときに提出するべきである。

上記のすべての文書は、英語または専門家が受け入れるその他の言語で提供するべきである。評価報告書は、必要がある場合にのみ翻訳するべきである。審査に同意した加盟機関は、専門家が受け入れる言語に関して問題がある場合は、その解決策を検討し、実施するべきである。

専門家はマネジメントコミティに所見を報告し、審査に関する勧告を行う。マネジメントコミティは審査チームの報告書をレビューする。その報告書の内容が一貫しており、結論が証拠に基づいていることをマネジメントコミティが確認したら、審査を受けている CB にその結果を引き渡す。審査を受けている CB は、遅くとも 6 ヶ月以内に審査結果に指摘された問題点を修正したことを示すべきである。

付属書 E

認証及びサービスマーク

E.1 コモンクライテリア認証マーク

本アレンジメントの条項に基づいて発行されるすべてのコモンクライテリア認証書には、図 1～図 4 に示すマークを表示すること。



図 1: コモンクライテリア認証マーク

注意：商標™（商標マーク）及び®（登録商標マーク）に関連する 2 つのマークは、マークの状態及びそれに基づく保護のレベルを表す。™はマークの一般的な慣習法に使われうるが、®はマークの所有者のみにしか使われず、国の関係機関への登録を伴い、その地域の商標法の要件に適合するべきである。一般的に、商標マークを意味するマークまたは表示を使用するかどうかの要件や結果は、国別に確認しなければならず、その地域の弁護士と相談することが常に望ましい。

このマークは、本アレンジメントの加盟機関によってコモンクライテリア認証書が発効されていることを証明する。また、これはその認証書が本アレンジメントの条項に従って発行されたことを示す加盟機関のステートメントである。

CB は、認証書の誤使用を防止し、対処するために、適切な行政手続きまたは法的な措置をとり、認証書または評価及び認証スキームに関する誤った、誤解を生じる、または不適切なステートメントを修正する義務を負う。

コモンクライテリア認証書を受け取った後は、ベンダーはその認証書が発行された製品の広告、マーケティング、及び販売に関してこのコモンクライテリア認証マークを使用することができる。認証書生成国は、ベンダーが以下のことを行う必要があることに関して、ITSEF 及びそのクライアントであるベンダーに対して必要な法的措置を取らなければならない：

- a) 正確で可読な形で認証書全体を複製し、証拠書類または販売資料に発行された認証書を使う；

- b) インターネット、パンフレット、または広告やその他の文書のような通信メディアにおいて、その認証状態を照会する際に、本アレンジメント及び加盟機関（または適合 CB）の要件に適合する；
- c) その認証について、誤解を生じるステートメントをしない、または許可しない；
- d) 誤解を生じる方法で、認証文書またはその一部を使用しない、または使用を許可しない；
- e) その認証が取り消された後に、本アレンジメントの加盟機関（または適合 CB）の指示通りに、認証への参照を含むすべての広告の使用を中止する；
- f) 本アレンジメントの加盟機関、またはこの認証書を承認し施行する他の機関が、認証製品を承認し保証するという旨を述べたり示唆したりするように、その製品の認証への参照を認めない；
- g) 認証が、認証範囲外のアクティビティを適用することを示唆しない；及び
- h) 本アレンジメントが評判を落としたり、国民の信用を失ったりするような方法で、その認証を使用しない。

図 1 に示されるコモンクライテリア認証マークは、以下の仕様に従って、複写及び再印刷されなければならない；

- a) 図 2 及び図 3 に示される通りのカラーコーディングで；または
- b) 図 4 及び図 5 に示される通りの白黒で；及び
- c) 均一に拡大または縮小されたサイズで（及びすべての比率を維持する）。

紙上で使用する場合は、エンボス加工またはスタンプで押すこともできる。

ベンダーは、下記の図 2、図 3、図 4 または図 5 に特定された通りの仕様に従わなければならない。

	色	HEX カラーコード
		fa4632 (PMS ウォーメッド*)
		ffffff (白)
		000000 (黒)

図 2: 登録商標マーク付のカラーのコモンクライテリア認証マーク

	色	HEX カラーコード
		fa4632 (PMS ウォームレッド*)
		ffffff (白)
		000000 (黒)

図 3: 登録商標マークなしのカラーのコモンライテリア認証マーク

	色	HEX カラーコード
		5d5d5d
		ffffff (白)
		000000 (黒)

図 4: 登録商標マーク付の白黒のコモンライテリア認証マーク

	色	HEX カラーコード
		5d5d5d
		ffffff (白)
		000000 (黒)

図 5: 登録商標マークなしの白黒のコモンライテリア認証マーク

E.2 承認アレンジメントサービスマーク

図 6 に示した本承認アレンジメントのサービスマークは、本アレンジメントに従って、加盟機関（または適合 CB）によって実施されるサービスを識別、広告、及びマーケティングするために使用すること。



図 6: 承認アレンジメントサービスマーク

注意：商標™（商標マーク）及び®（登録商標マーク）に関連する 2 つのマークは、マークの状態及びそれに基づく保護のレベルを表す。™はマークの一般的な慣習法に使われうるが、®はマークの所有者のみにしか使われず、国の関係機関への登録を伴い、その地域の商標法の要件に適合するべきである。一般的に、商標マークを意味するマークまたは表示を使用するかどうかの要件や結果は、国別に確認しなければならず、その地域の弁護士と相談することが常に望ましい。

本アレンジメントへの参加を止めた加盟機関は、サービスマークの使用、及び、本アレンジメントを参照する認証マークを保有する認証書の配付をただちに止めなければならない。加盟機関は、顧客（カスタマ）にその参加の終了とその結果についての情報を提供しなければならない。

図 6 に示される承認アレンジメントサービスマークは、以下の仕様に従って、複写及び再印刷されなければならない；

- a) 図 7 及び図 8 に示される通りのカラーコーディングで；
- b) 図 9 及び図 10 に示される通りの白黒で；及び
- c) すべての文字が明確に区別できる程度に、均一に拡大または縮小されたサイズで。

紙上で使用する場合は、エンボス加工またはスタンプで押すこともできる。

加盟機関（または適合 CB）は、下記の図 7、図 8、図 9 または図 10 に特定された通りの仕様に従わなければならない。

	色	HEX カラーコード
		fa4632 (PMS ウォームレッド [®])
		000000 (黒)
		ffffff (白)
		f7c621
		212973

図 7: 登録商標マーク付のカラーの承認アレンジメントサービスマーク

	色	HEX カラーコード
		fa4632 (PMS ウォームレッド [®])
		000000 (黒)
		ffffff (白)
		f7c621
		212973

図 8: 登録商標マークなしのカラーの承認アレンジメントサービスマーク

	色	HEX カラーコード
		5d5d5d
		000000 (黒)
		ffffff (白)
		353535
		989898

図 9: 登録商標マーク付の白黒の承認アレンジメントサービスマーク

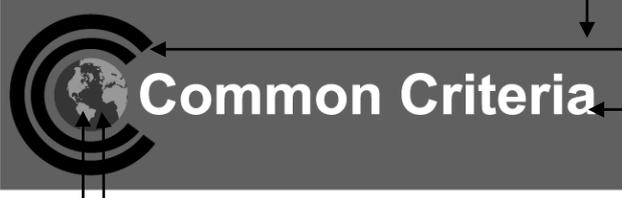
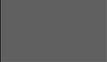
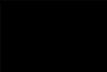
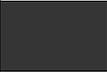
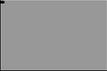
	色	HEX カラーコード
		5d5d5d
		000000 (黒)
		ffffff (白)
		353535
		989898

図 10: 登録商標マークなしの白黒の承認アレンジメントサービスマーク

付属書 F

加盟機関に提供する情報

F.1 スキームに関する文書

各適合 CB は、担当する評価及び認証スキームの次の側面に関する文書のコピーを加盟機関に提供すること：

- a) 相互に合意した IT セキュリティの評価基準と評価方法に対応した評価及び認証に関する国の規則と法令；
- b) スキームの組織構成；
- c) 認証機関の品質マニュアル；
- d) ITSEF の認定またはライセンス付与／承認の方針；
- e) スキームに関連する ITSEF の名称及び住所と、それぞれの状態（例えば、政府か民間か）；及び
- f) 該当する場合、ISO/IEC 17025：試験所及び校正機関の能力に関する一般要求事項（またはその後継規格）の国内規格としての翻訳版

これらの文書に対して変更を加えたり、新しい版を発行するたびに、その修正または新しい版のコピーをただちにすべての加盟機関に利用可能とすること。

F.2 コモンクライテリア認証書及び認証報告書

各加盟機関は、発効したコモンクライテリア認証書、認証報告書、及び認証製品リストのコピーを他の加盟機関に利用可能とすること。適合 CB がその認証製品リストから IT 製品またはプロテクションプロファイルを除外したり、削除するたびに、かかる CB はただちに加盟機関に通知するべきである。

F.3 本アレンジメントの条件に影響を与える一般情報

各加盟機関は、その国において適用され、コモンクライテリア認証書の承認に直接影響を与える国の法律、法令、行政規則、及び公職規定のすべてについて、それらの効力に関する説明書を提供する。

各加盟機関は、本アレンジメントの条項に従って行動する能力に影響を与える次のいずれかに対する変更または変更の予定についてマネジメントコミティにただちに通知するべきである：

- a) 国の法律、行政規則、または公職規定；または
- b) 評価及び認証スキームの運用または手続き

F.4 情報保護の原則

本アレンジメントに基づく一部の手続きは、無許可の開示によって加盟機関、加盟機関の関係当事者、または IT 製品の製造業者などを含む本アレンジメントの関係当事者に実際の損害を与える保護情報の交換を必要とすることがある。この情報を適切に取り扱い、かかる保護を実現するための手続きを定めることが重要である。この目的を達成するために、各加盟機関は、かかる手続きを適用した制度を確立するために努力すること。技術の継続的な進歩が、情報の保存、処理、送信方法に深い影響力を持つことを認識した上で、かかる手続きは、常に最先端の技術に関連し続けるために、定期的なレビュー及び更新を必要とする。その結果、情報保護の全般的な原則はここで述べられているが、一方で、関連する保護手順の具体的な詳細は、マネジメントコミティの標準的な運用手続きで伝達される。

F.4.1 保護情報の作成と管理

保護情報を含む文書及びメディアは、作成された時からその文書が破棄されるまで、または情報内容を保護する必要がなくなったと判断されるまで、適切に保護され、「*RA in Confidence*」という言葉及び一意の識別情報を付けること。

F.4.2 保護情報の保管と送信

保管中や送信中の文書を保護するために、適切なアクセス制御を整えるべきである。これは、文書のハードコピーの送信に対処するための物理的制御を含むと考えられ、また、可搬メディアを使って文書が共有される場合も関連する。保護情報を電子的に送信する場合は、セキュリティの確保された電子的手段を使用する。

F.4.3 保護情報へのアクセス

情報発生元と別途合意しない限り、また法律によって許可される範囲で、加盟機関が受け取った保護情報の参照は、その加盟機関によって直接に雇用されているスタッフ、またはその加盟機関の組織のトップの裁量により、知る必要がある政府の役人に制限される。保護情報の秘密を保持する義務は、本アレンジメントの終了後も有効である。

付属書 G

新しい適合認証機関

G.1 公式の要求

本アレンジメントの下で適合 CB の資格を得ることを希望し、第 5 条、第 5 条に引用されている付属書、及びマネジメントコミティによって発行された解釈に制定する条件を満たしていると考えられる場合は、CB はその国の加盟機関を通じて申請書を提出すべきである（CB と加盟機関が同一組織の場合もあることに注意すること）。加盟機関が申請を支持する場合は、CB のスポンサーになり、その申請をマネジメントコミティに提出すべきである。提出された申請は、申請者が本アレンジメントに制定する条件を満たすことができることを示す、スポンサーによる正式の保証と見なされるものではない。

申請には、申請者が本アレンジメントに基づいて適合認証機関と見なされることを希望しており、次のことを計画していることを示す書面のステートメントを加えること：

- a) 申請が承認されるかどうかにかかわらず、申請から生じる、または申請の検討と処理から生じる主要審査チーム（次の G.3 を参照）のすべてのコストを負担すること（これには、交通費、宿泊費、その他生活に要する費用が含まれる。また、申請者がスポンサーの委託 CB となることを申請しない場合に限り、主要審査チームの給与コストも含まれる⁴)；
- b) 以下に示す文書を提出すること；及び
- c) シャドー審査のために、申請者の管理の下で評価及び認証を受ける適切な製品を提出すること。

G.2 提出する文書

適合手続き中に取得されたすべての文書と情報は、付属書 F.4 の規定に従って取り扱うこと。これらの秘密保持に関する規則は、秘密保持契約によって補足することができる。

次の文書を提出すること：

- a) 申請者の評価及び認証スキームの範囲、組織、及び運用に関するすべての詳細。これには次のものが含まれる：
 - CB の名称、住所、主な連絡先；

⁴ 審査を実施する承認された加盟機関が、国の法律または法令によって、かかる支払いを受けることを禁じられている場合は、この権利を放棄することができる。

- CB の品質マニュアル；
 - CB の従属機関とその権限の法律上の基礎またはその他の基礎；
 - 方針に関する疑問について決定し、意見の不一致を解決するためのスキームの全般的な管理を監督するシステム；
 - 認証の手続き；
 - スキームに参加している ITSEF の名称及び住所と、それぞれの状態（民間か政府か）；
 - 評価機関を認定するための手続きとライセンス付与／承認の方針；
 - 営業秘密及びその他の機密情報を保護するためにスキーム内で適用される規則；
 - CB が、ITSEF に次のことを行わせるための手続き：
 - 公平に評価を実施する；
 - 正確に IT 基準評価方法（すなわち、CEM、CC サポート文書）を適用する；及び
 - 関係する機密情報の機密性を保護する。
- b) スキームの認証製品リストの最新版；
- c) 申請者の監督の下で発行された 2 つ以上のコモンクライテリア認証書及び認証報告書；
- d) 評価及び認証の実施、またはコモンクライテリア認証書の承認に直接に影響を与える、申請者の国で適用されるすべての国の法律、法令、行政規則、及び公職規定の効力に関する文書；及び
- e) 申請者に対し、またはコモンクライテリア認証書の対象とする IT 製品及びプロテクションプロファイルに対し、本アレンジメントの下で不当な利益を与えるか、またはその他の方法で本アレンジメントの運用または意図を妨げるような、法律、法令、または行政命令によって、申請者が拘束されていないこと、または拘束されようとしていないことを示す文書。

G.3 マネジメントコミティの回答

マネジメントコミティは、申請書を受領後 3 週間以内に申請書を受領したことを確認し、3 ヶ月以内を目標に予備的な回答を示すこと。予備的な回答では、その文書が技術審査とシャドウ審査に合格すれば、その申請が受理されることを伝えるべきである。

マネジメントコミティが、申請者によって提出された情報が十分で、明確化または補足情報の必要がないと認める場合は、申請者はコラボティブプロテクションプロファイル適合評価、または cPP が使用されない場合は少なくとも評価保証レベル 2、及び該当する場合、ALC_FLR を主

張するセキュリティターゲットに対する評価が行われた製品を少なくとも 2 つ、シャドー審査の候補製品として提示することが要求される。

申請者は、各製品の概要とその評価及び認証の手配に関する詳細を提供すべきである。マネジメント委員会は候補製品の提示を受理してから 1 ヶ月以内に、シャドー審査のための製品を 1 つ選択し、それを申請者に通知すること。

マネジメント委員会はシャドー審査を実施するために、2 つ以上の承認された加盟機関（スポンサーを除く）を選出すること。選出された加盟機関は、2 人の専門家から構成される主要審査チームを指名すること。加盟機関（スポンサーを含む）は、自らの費用で追加の専門家を提供することができる。マネジメント委員会は、専門家の名前と所属組織について申請者に通知すること。

G.4 シャドー審査手続き

専門家は、（統一基準に従って審査を実施するために）マネジメント委員会によって発行されるガイダンスに基づき、入手可能なすべての情報を考慮に入れて、どの程度のシャドー評価及び認証手続きを実施する必要があるかを決定する。マネジメント委員会のガイダンスは、審査の際に必要な資源を見積もるために申請者の CB に提供される。

専門家は調査の完了時から 1 ヶ月以内に、また選択された製品の評価及び認証手続きの完了から 1 ヶ月以内に、マネジメント委員会に書面で調査結果を報告する前に、エグゼクティブサブ委員会にレビューのため書面で提出し、申請者の申請を受け入れるべきか、拒否するべきかに関して勧告を行うこと。マネジメント委員会は専門家の報告書を受け取ってから 2 ヶ月以内を目標に、書面で決定内容を申請者に通知すること。拒否する場合は、マネジメント委員会はその決定の理由と、その根拠となる主な証拠の概要を提供すべきである。承認する場合は、マネジメント委員会は付属書 L を更新することによって、その決定を記録すべきである。

付属書 H

本アレンジメントの管理

H.1 責任と力量

マネジメント委員会は本アレンジメントの状態、条項、及び運用に関連する方針のあらゆる事項を扱う。マネジメント委員会は新しい加盟機関の承認、CB の適合性、及び本アレンジメントの範囲の変更を決定する。

H.2 構成

すべての加盟機関は、マネジメント委員会に代表者を出席させること。マネジメント委員会の議長は加盟機関の中からマネジメント委員会によって毎年指名されること。現在の議長はマネジメント委員会に管理上の支援を提供するべきである。

H.3 決定

マネジメント委員会に代表者を出席させる各国は、各 1 票の議決権を有すること。マネジメント委員会は、常に全会一致を達成するために努力するべきであるが、本アレンジメントにおいて、別途全員一致を要求する特別な要件が制定される場合を除き、決定は単純多数によること。

H.4 専門家の招待

マネジメント委員会は特定の問題について助言を受けるために、マネジメント委員会の会議に専門家または技術アドバイザを招くことができる。

H.5 専門家の採用

マネジメント委員会は、必要に応じて支援と助言を提供するために、専門家の特別グループを結成することができる。

H.6 会議の頻度

マネジメント委員会は年に 1 回総会を開き、また適宜、会議を行う。可能な場合は、電子メールによって決定を下す。

H.7 エグゼクティブサブコミティ

マネジメントコミティは、アレンジメントの日々の業務を管理し、マネジメントコミティに助言と勧告を与えるためにエグゼクティブサブコミティを設立するべきである。

すべての加盟機関は、エグゼクティブサブコミティに代表者を出席させることができる。

エグゼクティブサブコミティの主な業務を示す：

- a) アレンジメントの業務の遂行手続きを作成し、勧告する；
- b) CB の技術的な適合性を審査する；
- c) 本アレンジメントの修正を勧告する；
- d) 継続的な監督活動を管理する；
- e) コモンクライテリアのプロモーションを管理する。

H.8 ディベロップメントボード

マネジメントコミティは、本アレンジメントの技術的側面を管理するため、評価基準及び関連する評価方法の開発と維持、及び適切な国際的なテクニカルコミュニティによるコラボラティブプロテクションプロファイルの開発を発展・監視するため、そして、マネジメントコミティに技術的な助言及び提案を提供するために、ディベロップメントボードを設立するべきである。

すべての加盟機関は、ディベロップメントボードに代表者を出席させることができる。

ディベロップメントボードの主な業務を示す：

- a) 本アレンジメントの条項と適用に関する技術的な面における意見の不一致を解決する；
- b) IT セキュリティ評価基準と IT セキュリティ評価方法の開発を管理する；
- c) 将来の基準または方法のいずれかに影響を与える解釈の背景と、その結果としての決定に関して、履歴データベースを維持管理する；
- d) 技術的な一貫性を確実にするために、最新の評価基準、評価方法、CC サポート文書の技術的な承認をする；
- e) 適切なテクニカルコミュニティによるコラボラティブプロテクションプロファイルの効果的な開発を確実にする。

付属書 I

認証報告書の内容

I.1 認証報告書とその使用

認証報告書は、関心を持つ者にとって、IT 製品またはプロテクションプロファイルに関する詳細なセキュリティ情報の情報源となる。その目的は、IT 製品またはプロテクションプロファイルに関する実際的な情報を消費者に提供することである。認証報告書はセキュリティターゲットと同様に、評価を受けた IT 製品を安全に導入するために必要な、消費者向けの情報が含まれるため、保護情報を含む必要はなく、含むべきではない⁵。

認証機関は、利用者（リスクオーナー、システムインテグレータ、開発者、最終利用者など）が関連する情報にアクセスできることを確実にしなければならない。この情報のいくつかは他の公開された文書内で提供されることがあり、その場合、認証報告書内に繰り返される必要はないが、明確で正確な参照は提供されなければならない。

国際的なテクニカルコミュニティが、提供されなければならない情報（例えば、cPP またはサポート文書内の情報）を特定した場合、これは、認証報告書内に含有されるか、容易に入手可能であるべきであり、明確に認証報告書に参照されるべきである。

I.2 想定される内容

報告書（直接またはその参照を通じて）は、次の情報を含むことが想定されている。これは、サポート文書が追加の情報を必要とする場合には、拡大される。

I.2.1 概要

概要とは、報告書全体の簡潔な要約である。このセクションに含まれる情報は、評価結果の明確で簡潔な概要を読者に示すべきである。このセクションの読者には、安全な IT システムと IT 製品の開発者、消費者、及び評価者が含まれる。読者は、概要を通じて、その IT 製品またはプロテクションプロファイルについての基礎的な知識と報告結果を得ることができる。一部の読者（例えば、認定機関、経営者）は、おそらく報告書のこのセクションしか読まないため、すべての重要な評価結果をここに記述することが重要である。概要には、少なくとも次の項目を含むべきである：

⁵ 認証報告書の一部または全部が「保護情報」である場合かつ公開されないような製品は、本アレンジメントの対象外とする。

- a) 評価を受ける IT 製品の名称、評価対象に含まれる製品のコンポーネントの一覧、開発者の名前及び製品のバージョン；
- b) IT セキュリティ評価機関の名称；
- c) 認証識別情報⁶；
- d) 評価の完了日；
- e) 有効期限（オプション）；及び
- f) 次の事項に関する報告結果の簡潔な説明：
 - 1) 製品が適合する PP または ST のみの評価における保証パッケージ；
 - 2) 機能；
 - 3) 脅威の概要と評価を受けた IT 製品に関する組織のセキュリティ方針（OSP）；
 - 4) 特別な構成要件；
 - 5) 運用環境に関する前提条件；
 - 6) 免責事項

I.3 識別情報

評価を受ける IT 製品は、明確に識別する必要がある。ソフトウェア、バージョン番号、適用されるソフトウェアパッチ、ハードウェアのバージョン番号、及び周辺機器（テープドライブ、プリンタなど）を識別し、記録しなければならない。上記の項目は、評価を受ける IT 製品を完全に識別するために必要なラベリングと説明情報を提供する。評価を受ける IT 製品を完全に識別しておけば、その IT 製品全体の正確な表現を、使用または将来の評価作業のために再現することができる。

I.4 セキュリティ方針

セキュリティ方針のセクションでは、IT 製品のセキュリティ方針について説明するべきである。セキュリティ方針では、IT 製品をセキュリティサービスの集合として記述する。セキュリティ方針の記述には、評価を受ける IT 製品が適合及び／または実施する必要がある方針または規則を含む。

I.5 前提条件及び範囲の明確化

IT 製品を使用する環境／構成のセキュリティ面は、このセクションに記述するべきである。このセクションは、対策が講じられていない脅威に関して、評価の範囲を明確に示す手段を提供する。利用者は IT 製品の使用に関連するリスクについて、情報に基づいて決定を下すことができ

⁶ 認証識別情報は、認証機関によって定義された認証書の一意な識別情報である（番号とスキーム名略称を含む）。

る。このセクションには、使用、環境上の前提条件、対策が講じられていない脅威に関する評価の範囲の明確化について記述する。

I.5.1 使用に関する前提条件

評価作業中に IT 製品のベースラインを示すために、その製品の使用に関する前提条件を決定する必要がある。適切なインストール及び構成、満たされるべき最低ハードウェア要件など、すべての項目について想定する。このセクションでは、評価中の IT 製品の使用に関するあらゆる前提条件を記述する。

I.5.2 環境に関する前提条件

評価作業中に IT 製品のベースラインを示すために、その製品を使用する環境に関する前提条件を決定する必要がある。このセクションでは、評価中の IT 製品の環境に関するあらゆる前提条件を記述する。

I.5.3 範囲の明確化

このセクションは、評価を受けた製品のセキュリティ機能によって対策が講じられていない IT 製品への脅威をリストアップし、説明する。あるクライアントが、その IT 製品で対策が講じられていると思っていた脅威に対して、実際は対策がなされていないという場合が当てはまる。このような理由のために、対策が講じられていない脅威をリストアップし、明確にするべきである。ただし、個々の製品で対策を講じることができないすべての脅威をリストアップすることは実際的でない。

I.6 アーキテクチャに関する情報

このセクションは、Development-TOE Design (ADV_TDS)という表題のコモンクライテリア保証ファミリに記述される提供物件に基づいて、IT 製品の主要なコンポーネントについて高レベルの説明を提供する。このセクションの目的は、主要なコンポーネントのアーキテクチャに関して独立性の程度を示すことである。

I.7 ドキュメンテーション

このセクションには、開発者から消費者に対して製品と共に提供される IT 製品文書の完全なリストを示す。すべての関係する文書をバージョン番号と共に示すことが重要である。このセクションでは、少なくとも利用者ガイド、管理ガイド、及びインストールガイドについて説明する。管理ガイドとインストールガイドの情報が1つの文書に含まれることがある。

I.8 IT 製品のテスト

このセクションでは、開発者と評価者の両方のテスト作業について説明し、テスト方法、構成、詳細さ、及び結果について概要を示す。

I.9 評価を受ける構成

このセクションでは、評価中の IT 製品の構成について記述する。一般に管理者ガイドまたはインストールガイドは、IT 製品の正確な構成について必要な詳細を示す。IT 製品は使用される環境または組織が実施するセキュリティ方針に従って、さまざまな方法で構成されることがある。

このセクションでは、正確な設定と構成の詳細を示し、各選択肢に対する根拠を示す。運用に関して追加の注記及び観察結果を記述することもできる。このセクションは、評価を受ける製品のインストールに関するベースラインを示すので特に重要である。

I.10 評価の結果

このセクションでは、IT 製品が満たしている保証要件を記述する。これらの要件の詳細、製品が各要件をどの程度満たしているかに関する詳細は、セキュリティターゲットに記述する。

I.11 評価者のコメント／勧告

このセクションは、評価の結果について追加の情報を示すために使用する。評価者のコメント／勧告では、評価中に発見された IT 製品の欠点、または特に有用な機能が指摘されることがある。

I.12 付属書（オプション）

付属書は報告書の読者にとって有用であるが、報告書の所定の表題には論理的に適合しない追加情報の概要を示すために使用する（例えば、セキュリティ方針の完全な記述）。

I.13 セキュリティターゲット

セキュリティターゲットは認証報告書に記述しなければならない。ただし、所有権のある技術情報は削除するか、書き替える必要がある。

I.14 用語集

用語集は、意味が分かりにくい略語または用語を定義して、報告書を読みやすくするために使用する。

I.15 参考文献

参考文献のセクションには、報告書の編集のために参考資料として使用したすべての参考文献をリストアップする。この情報には、例えば次のような項目を含むが、それらのみに限るものではない：

- a) 基準、方法、プログラム／スキームに関する文書；
- b) 技術的な参考文献；及び
- c) 評価作業で使用した開発者の文書

再現可能にするために、すべての開発者の文書は、リリース日及びバージョン番号で一意に識別することが重要である。

付属書 J

コモンクライテリア認証書

以下の情報は、本アレンジメントの加盟機関のために発行されるすべてのコモンクライテリア認証書に記載するためのものである。

J.1 cPP 適合主張する IT 製品評価に関するコモンクライテリア認証書

cPP 適合主張する IT 製品評価の認証の結果、認証書生成加盟機関によって発効されたコモンクライテリア認証書には、次の情報を記載すること：

認証製品の識別情報（認証書上に構造化テキストブロックとして印刷すること）：

- a) 認証識別情報；
- b) 製品の種類；
- c) 製品の名称；
- d) バージョンとリリース番号；
- e) 評価対象の評価プラットフォーム（オプション）；
- f) 製品の製造業者；
- g) 評価スポンサーの名称（オプション）；

認証結果の識別情報（認証書上に構造化テキストブロックとして印刷すること）：

- h) コラボラティブプロテクションプロファイル適合（名称、バージョン及び認証 ID を含む）；

認証書に記載されるその他の項目：

- i) IT セキュリティ評価機関の名称（オプション）；
- j) 認証機関の名称、及び認証書生成加盟機関の名称；
- k) 認証報告書の識別情報⁷；
- l) 発行日；
- m) 有効期限（オプション）；及び
- n) 発行する認証機関の署名；

この認証書には、次のステートメントも加える：

「本認証書に記載された IT 製品は、*Common Criteria for IT Security Evaluation* [バージョン番号を挿入] に適合するために、*Common Methodology for IT Security Evaluation* [バージョン番号を挿入] [該当する場合、「及び認証報告書内にリストアップされた CC サポート文書」を挿入] を使

⁷ 認証報告書の識別情報は、文書を一意に識別するべきである。最低限、認証機関の名称、使用された評価基準、報告書番号、及び発行年を含むべきである。

用して、「[認定及びライセンス付与／承認された評価機関、または[加盟機関の国名を挿入]の法律、法定文書、その他の公的な行政手続きの下で設立された評価機関」を挿入]で評価を受けた。本認証書は、完全な認証報告書と共に、評価された構成に対する製品の特定のバージョン及びリリースのみに適用される。評価は[スキームの公式名を挿入]の規程に従って行われ、評価機関による評価報告書の結論は、提示された証拠と首尾一貫している。本認証書は[認証書生成加盟機関の名称を挿入][及び、(異なる場合) 認証機関の名称]または本認証書を承認し、もしくは効力を与えるその他の組織による IT 製品の保証を示すものではなく、[認証書生成加盟機関の名称を挿入][または、(異なる場合) 認証機関の名称]または本認証書を承認または効力を与えるその他の組織は、明示、黙示を問わず、IT 製品に関するいかなる保証も行わない。」

リストアップされている情報に加えて、加盟機関によって発効された各 IT 製品に関連するコモンクライテリア認証書に、付属書 E に示すコモンクライテリア認証マーク及びスキームのロゴを表示しなければならない。また、承認アレンジメントサービスマークを認証書に印刷することもできる。

J.2 cPP 適合主張しない IT 製品評価に関連するコモンクライテリア認証書

cPP 適合主張しない IT 製品評価の認証の結果、認証書生成国によって発効されたコモンクライテリア認証書には、次の情報を記載すること：

認証製品の識別情報（認証書上に構造化テキストブロックとして印刷すること）：

- a) 認証識別情報；
- b) 製品の種類；
- c) 製品の名称；
- d) バージョンとリリース番号；
- e) 評価対象の評価プラットフォーム（オプション）；
- f) 製品の製造業者；
- g) 評価スポンサーの名称（オプション）；

認証結果の識別情報（認証書上に構造化テキストブロックとして印刷すること）：

- h) （該当する場合）プロテクションプロファイル適合情報（名称、バージョン及び認証 ID を含む）；
- i) 機能要件への適合情報⁸；
- j) 保証パッケージ（オプション）⁹；

⁸ 機能に関する適合性ステートメントは、以下のとおり示すべきである：「PP 適合機能」または「製品独自セキュリティターゲット」、並びに「CC パート 2 適合」または「CC パート 2 拡張」。

⁹ 確認された保証パッケージは、以下のとおり述べるべきである：「CC パート 3 適合」、[保証パッケージの名称（例えば、EAL2）]、及び適用可能な場合「追加の保証要件 [CC パート 3 のコンポーネントの名称]」；または適合するプロテクションプロファイルの保証パッケージを記述すべきである。

認証書に記載されるその他の項目：

- k) ITセキュリティ評価機関の名称（オプション）；
- l) 認証機関の名称、及び認証書生成加盟機関の名称；
- m) 認証報告書の識別情報；
- n) 発行日；
- o) 有効期限（オプション）；及び
- p) 発行する認証機関の署名；

この認証書には、次のステートメントも加える：

「本認証書に記載されたIT製品は、*Common Criteria for IT Security Evaluation* [バージョン番号を挿入] に適合するために、*Common Methodology for IT Security Evaluation* [バージョン番号を挿入] [該当する場合、「及び認証報告書内にリストアップされたCCサポート文書」を挿入] を使用して、[「認定及びライセンス付与／承認された評価機関、または[加盟機関の国名を挿入] の法律、法定文書、その他の公的な行政手続きの下で設立された評価機関」を挿入] で評価を受けた。本認証書は、完全な認証報告書と共に、評価を受けた構成に対する製品の特定のバージョン及びリリースのみに適用される。評価は[スキームの公式名を挿入] の規程に従って行われ、評価機関による評価報告書の結論は、提示された証拠と首尾一貫している。本認証書は[認証書生成加盟機関の名称を挿入] [及び、(異なる場合) 認証機関の名称] または本認証書を承認または効力を与えるその他の組織によるIT製品の保証を示すものではなく、[認証書生成加盟機関の名称を挿入] [または、(異なる場合) 認証機関の名称]、または本認証書を承認または効力を与えるその他の組織は、明示、黙示を問わず、IT製品に関するいかなる保証も行わない。」

リストアップされている情報に加えて、加盟機関によって発効された各IT製品に関連するコモンクライテリア認証書に、付属書Eに示すコモンクライテリア認証マーク及びスキームのロゴを表示しなければならない。確認された保証パッケージが、CCパート3 EAL2を超えるCCパート3のコンポーネント、及び適切であればALC_FLRを含む場合、次の文言をロゴに追加すること：「EAL2までのコンポーネント及びALC_FLRについてのみCCRA承認の対象である」。また、承認アレンジメントサービスマークを認証書に印刷することもできる。

J.3 プロテクションプロファイル評価に関連するコモンクライテリア認証書

プロテクションプロファイルの評価の認証に基づいて作成され、加盟機関によって発効されたコモンクライテリア認証書には次の情報を記載すること：

認証されたプロテクションプロファイルの識別情報（認証書上に構造化テキストブロックとして印刷すること）：

- a) 認証識別情報；
- b) プロテクションプロファイルの名称／識別情報；

- c) プロテクションプロファイルのバージョン番号；
- d) プロテクションプロファイルの開発者；
- e) プロテクションプロファイルのスポンサー（オプション）；
- f) 保証要件への適合関連情報¹⁰；

認証書に記載されるその他の項目：

- g) ITセキュリティ評価機関の名称（オプション）；
- h) 認証機関の名称、及び認証書生成国の名称；
- i) 認証報告書の識別情報；
- j) 発行日；
- k) 有効期限（オプション）；及び
- l) 発行する認証機関の署名；

この認証書には、次のステートメントも加える：

「この認証書で識別されるプロテクションプロファイルは、*Common Criteria for IT Security Evaluation* [バージョン番号を挿入] へ適合するために、*Common Methodology for IT Security Evaluation* [バージョン番号を挿入] [該当する場合、「及び認証報告書内にリストアップされた CC サポート文書」を挿入] を使用して、[「認定及びライセンス付与／承認された評価機関、または [加盟機関の国名を挿入] の法律、法定文書、その他の公的な行政手続きの下で設立された評価機関」を挿入] で評価を受けた。この認証書は、完全な認証報告書と共に、本認証書にリストアップされているプロテクションプロファイルの特定のバージョンだけに適用される。評価は [スキームの公式名を挿入] の規定に従って実施され、評価報告書の評価機関による結論は、提示された証拠と首尾一貫している。この認証書は [認証書生成国の名称を挿入] [及び、(異なる場合) 認証機関の名称] による、または本認証書を承認または効力を与えるその他のいかなる組織による、プロテクションプロファイルの保証を示すものではなく、[認証書生成国の名称を挿入] [または、(異なる場合) 認証機関の名称]、または本認証書を承認または効力を与えるその他のいかなる組織も、明示であれ、黙示であれ、プロテクションプロファイルに関する保証は一切行わないものではない。」

リストアップされている情報に加えて、加盟機関によって発効された各プロテクションプロファイルに関連するコモンクライテリア認証書に、付属書 E に示すコモンクライテリア認証マーク及びスキームのロゴを表示しなければならない。また、承認アレンジメントサービスマークを認証書に印刷することもできる。

¹⁰ 認証製品についての適合主張は、選択された保証コンポーネントをリストアップするか、適用可能な場合は EAL（例えば、EAL2 または EAL2 及び追加の保証要件 [追加されたコンポーネントのリスト]）を記載するか、のいずれかを行わなければならない。

付属書 K

コラボティブプロテクションプロファイル

コラボティブプロテクションプロファイル (cPP) 及び関係するサポート文書は、共通セキュリティ機能要件及び達成可能なセキュリティ保証の共通レベルのミニマムセットを定義する。それは、認証された製品が期待されたセキュリティのレベルを達成することを確実にするために行う脆弱性分析要件を含む。

K.1 cPP の構成

cPP には、国内の適合性評価制度に依存するような要件を含めてはならない。

cPP は、適切な国際標準化団体によって定義された暗号プリミティブ/プロトコルに関する国際規格の例を明示的に特定することができる。cPP は、各国が独自の詳細化を提供できるように、その他の国家承認プリミティブ/プロトコルの使用も許可すべきである。

cPP は、EAL4 以下のアクティビティについて、国際的なテクニカルコミュニティがスキーム間で再現できるという根拠を示すことができる場合を除いて、最高で EAL2 までの保証コンポーネントのみを含むように制限しなければならない。拡張された保証コンポーネントの使用は、その根拠が提供され、CCRA 承認プロセスの対象でない限り、避けるべきである。

K.2 CC 及び CEM

cPP は、相互承認を支持するために、CC 及び CEM の一般的なフレームワークに適合しなければならない。cPP を補足するサポート文書は、必要に応じて、CEM に対する解釈を与えるために作成されることが求められている。cPP 及び/またはサポート文書においてセキュリティニーズを表現できないことを論証する根拠がある場合、CC 及び/または CEM を修正することができ、CCRA 承認プロセスの対象となる。

K.3 相互承認

cPP 適合主張する CCRA 認証書は、かかる cPP と関係するサポート文書に定義された保証要件のみをカバーしなければならない。

cPP 適合主張する CCRA 認証書は、かかる cPP に定義されたセキュリティ機能のみをカバーしなければならない。

付属書 L

適合 CB

Australasian Certification Authority - Australasian Information Security Evaluation Program

スポンサー :

Defence Signals Directorate and Government Communication Security Bureau,
オーストラリアとニュージーランド

Canadian Common Criteria Evaluation and Certification Scheme

スポンサー :

Communications Security Establishment,
カナダ

Schema d'Evaluation et Certification Francais

スポンサー :

Agence nationale de la sécurité des systèmes d'information,
フランス

Bundesamt für Sicherheit in der Informationstechnik (Zertifizierungsstelle)

スポンサー :

Bundesamt für Sicherheit in der Informationstechnik,
ドイツ

Indian Common Criteria Certification Scheme (IC3S)

スポンサー :

Government of India, Ministry of Communications and Information Technology,
Department of Electronics and Information Technology
STQC Directorate,
インド

Organismo di Certificazione della Sicurezza Informatica (OCSI)

スポンサー :

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione,
イタリア

Japan Information Technology Security Evaluation and Certification Scheme

スポンサー :

Ministry of Economy, Trade and Industry, and Information-technology Promotion Agency,
日本

Malaysian Common Criteria Evaluation and Certification Scheme

スポンサー：
CyberSecurity Malaysia,
マレーシア

Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

スポンサー：
Netherlands National Communications Security Agency (NLNCSA) and operated by TÜV Rheinland Nederland B.V.
オランダ

Norwegian Certification Authority for IT Security (SERTIT)

スポンサー：
Norwegian National Security Authority (NSM),
ノルウェー

IT Security Certification Center

スポンサー：
National Intelligence Service and National Security Research Institute,
韓国

Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

スポンサー：
Ministerio de Hacienda y Administraciones Públicas and Centro Criptológico Nacional,
スペイン

Swedish Certification Body for IT-Security

スポンサー：
Swedish Defence Materiel Administration (FMV),
スウェーデン

Turkish Standards Institution Common Criteria Certification Scheme

スポンサー：
Ministry of Science, Industry and Technology,
トルコ

UK IT Security Evaluation and Certification Scheme

スポンサー：

CESG,
英国

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme

スポンサー：
National Security Agency,
アメリカ合衆国