



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

2000年5月

平成14年4月翻訳第1.0版
情報処理振興事業協会
セキュリティセンター

IPA まえがき

本書の目的

本書は、CC Project のホームページ(<http://www.commoncriteria.org/registry/ccra-final.html>)に掲載されている、“Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 2000”を情報処理振興事業協会(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理解の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、CC Project のホームページ(<http://www.commoncriteria.org/registry/ccra-final.html>)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。

参加機関

Defence Signals Directorate and Government Communication Security Bureau
from Australia and New Zealand

and

Communications Security Establishment
from Canada

and

Ministry of Finance
from Finland

and

Service Central de la Sécurité des Systèmes d'Information
from France

and

Bundesamt für Sicherheit in der Informationstechnik
from Germany

and

Ministry of Interior
from Greece

and

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
CESIS III Reparto - UCSi
from Italy

and

Ministry of the Interior and Kingdom Relations
from the Netherland

and

HQ Defence Command Norway/Security Division
from Norway

and

Ministerio de Administraciones Públicas
from Spain

and

Communications-Electronics Security Group
Department of Trade and Industry
from the United Kingdom

and

National Institute of Standards and Technology
National Security Agency
from the United States of America

以上の参加機関は、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参加機関は、以下のような目標を共有する。

- a) 情報技術 (IT) 製品およ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、これらの製品およ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 製品およ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 製品およ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 製品およびプロテクションプロファイルに関する、評価・¹認証 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、コモンクライテリアによる認証を取得した IT 製品およ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による認証を発行する認証機関に、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、その認証の基礎となる判断の信頼性を、確信するための根拠が提供されることを追求している。

二者間または多者間の個別契約に基づいて、政府の秘密を扱うシステムが、調達、認証およ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 条に記載される適用除外は、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。

政府および民間によるいずれの認証機関も、信頼できる認証を実施する能力を潜在的に有していること、ならびにいずれの機関についても、それぞれ規定が設けられるべきであることが了解されている。しかしながら、他国において発行された認証を承認することは、その政府特有の決定および約束事項が関与してくる。従って、本アレンジメントにおいては、認証の発行機能と承認機能が区別されている。

¹ ある制度では認証の代わりに確認という用語の使用が選択されることがある。この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、全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。このような判断の行使において、参加機関はそれぞれの基準として、評価中の IT 製品に関する保証レベルを使用することに努める。したがって、本アレンジメントの参加機関は、それぞれの技術的な判断と能力に関して相互の理解と信頼を醸成および維持し、公開された議論を通じて全体的に一貫性を維持することとなっている。

参加機関は、評価基準と評価方法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保証パッケージを作成および確立したり、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、参加機関は、例えば評価の申請者に対して、関心を持つものに評価で得られた情報を提供するよう奨励して、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

参加機関

本アレンジメントの参加機関は、自国または複数国を代表する政府組織または政府省庁である。参加機関は評価認証書の発行機関、評価認証書の利用機関、または両方である。認証書を利用する参加機関は、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。認証書を認可する参加機関は、自国または複数国で運営されている（第 5 条で説明する）準拠認証機関のスポンサであり、それぞれの認証書を認可する。認証書を認可する参加機関であって、準拠認証機関の資源と専門技術を自由に利用できる組織は、有資格参加機関として定義される。

第 2 条

範囲

参加機関は、IT 製品とプロテクションプロファイルに関して、他の認証書認可参加機関が本アレンジメントの条件と、各参加機関に適用される法律および規則に従って認可したコモンクライテリア認証書を承認することを相互に了解する。本アレンジメントは、評価保証レベル 1 から 4 で要求されるコモンクライテリア保証コンポーネントのいずれかに対する準拠要求について扱う。他の保証レベルまたはコンポーネントを追加することによる範囲の拡大は本アレンジメントの参加機関の合意により、いつでも可能である。

第 3 条

例外

コモンクライテリア認証書の承認によって、参加機関が適用される国家、国際、または欧州共同体の法律または規制に違反することになる場合は、その参加機関はかかる認証書の承認を断ることができる。特に、国家の法律、法令、行政規則、または公職規定の下で要求または認可されたセキュリティ分類または同等の保護マーキング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、参加機関はその適用のみについて認証書の承認を断ることができる。

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、各参加機関は、認証書認可参加機関が認可した、適切なコモunkライテリア認証書を承認するべきである。かかる認可によって、評価・認証手続き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. 受け入れられた IT セキュリティ評価基準に基づく
- b. 受け入れられた IT セキュリティ評価方法を使用
- c. 認可参加機関の国で、*準拠認証機関*が管理する評価・認証制度で実施
- d. 認可されたコモunk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

これら全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（コモunkライテリア）であって、管理委員会が承認する版に規定する。評価方法は Common Methodology for Information Technology Security Evaluation（共通評価方法）であって、管理委員会承認する版に規定する。認証報告書の最小限の要件は、本アレンジメントの付属書 I に規定する。評価・認証制度の最小限の要件は、本アレンジメントの付属書 B に規定する。評価・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
 - EN 45001 または ISO Guide 25 に従って、または全ての参加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 に従って許諾または承認されていること
 - その国で有効な法律、法律文書、またはその他の公式の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

および

- b) *認証機関*の*準拠性*が承認され、次のいずれかの条件を満たすこと
 - EN 45011 または ISO Guide 65 に従って、または最小限でも本アレンジメントの付属書 C に規定する要件を満たす EN 45011 または ISO Guide 65 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、規則、またはその他の公式の行政手続きに基づいて設立され、EN 45011 もしくは ISO Guide 65 の条件、または本アレンジメントの付属書 C に規定されている要件を満たしていること

評価・認証制度間でコモンクライテリアと共通評価方法を一貫性をもって適用するために、参加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話し合いを行うこととなっている。この目標に向けて、参加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情報の定期的な交換を行うこととなっている。コモンクライテリアと共通評価方法の一貫した、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、認証機関は制度内で進行中の全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；

- a) 評価を公平に行う
- b) コモンクライテリアと共通評価方法を正確かつ一貫性をもって適用する
- c) 保護情報の秘密性を適切に保護する

第 6 条

任意の定期的な査定

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 準拠認証機関 の査定を行う。かかる査定の形式については、本アレンジメントの付属書 D に規定する。

第 7 条

公開

認証書認可参加機関によって認可されたコモンクライテリア認証書は、参加機関または評価・認証制度固有のロゴまたは識別記号に加えて、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する。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。

それぞれの認証書認可参加機関は、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、別の認証書認可参加機関によって認可された認証書を有する全ての 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るべきである。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

情報の開示が参加機関の国の法律または規則に違反しない限り、各参加機関は本アレンジメントの適用に関する全ての情報と文書を他の参加機関に提供することに努める。

この義務の履行に関して、評価機関、認証機関、または参加機関は、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、第三者の営業上の秘密情報または保護情報を開示することができる。

特に、各参加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ること。

参加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

新しい参加機関

参加機関

既存の参加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支持を意図している国の代表者は、本アレンジメントの参加機関となることができる。

認証機関

既存の参加機関全員が同意すれば、ある認証機関は本アレンジメントの第 5 条の目的に準拠しているとみなされる。ただし、既存の参加機関が、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規定する承認条件を満たし、シャドー認証を含む本アレンジメントの付属書 G に規定する手続きに従った準拠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

管理委員会が本アレンジメントを管理する。管理委員会は本アレンジメントの状態、条件、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。全ての参加機関は管理委員会に出席すべきである。管理委員会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

参加機関間の意見の不一致は、話し合いによって解決すべきである。参加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管理委員会に委ねられる。管理委員会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、個々の参加機関は、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管理委員会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

参加機関が本アレンジメント、特にその付属書 D、付属書 G.3 または G.4、付属書 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、他の参加機関に通知するべきである。保護情報は、付属書 F.4 の規定に従って、情報発生元の合意があった場合にのみ、請負業者に渡すことができる。

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、各参加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全てを負担する。

第 14 条

修正

本アレンジメントの条件の修正には、参加機関全員の合意が必要である。採択された変更は文書に記録し、全ての参加機関が署名する。

第 15 条

期間

参加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

自発的な参加の取り止め

参加機関は書面で他の参加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、代表している認証機関の準拠資格を取り消すことができる。

第 17 条

開始

本アレンジメントに基づく活動は 2000 年 5 月 23 日に開始する。

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者で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、各参加機関は認識し、受け入れる。また、各参加機関は、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全てに関して拘束力を持たず、参加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。認証機関によって発行された報告書または参加機関によって認可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参加機関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認可されたコモンクライテリア認証書の承認は、別の認証機関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、別の参加機関によって認可された認証書を、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コモンクライテリアまたは共通評価方法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。かかる定義はコモンクライテリアおよび共通評価方法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、定義文の中でイタリック体で示す。

認定：

公平性と、一般的な技術、方法、手続き上の能力に関して、決められた標準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：

承認された標準に照らして他の組織の業務実施能力を評価し、それらの組織が標準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。

承認：

*許諾*を参照。

承認方針：

*許諾方針*を参照。

準拠認証機関の査定：

特定の*準拠認証機関*によって実施される*評価・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。

認可：

参加機関が、*準拠認証機関*による*コモンクライテリア認証書*の発行と*コモンクライテリア認証マーク*の使用を許可すること。

CB :

認証機関。

委託認証機関 :

有資格参加機関から委託される準拠認証機関。

準拠認証機関 :

付属書 K に準拠認証機関としてリストされている認証機関。

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 (2.01 版は ISO-IEC-15408 と同じである)。

認証 :

認証機関によって遂行される手続きでコモンクライテリア認証書の発行を伴う。

認証機関 :

認証の実施と評価・認証制度の日々の運用を監督することに責任を負う組織。

認証報告書 :

評価の結果を要約し、全般的な結果を確認するために認証機関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、およ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。

認証製品リスト :

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。

申請者 :

評価のために評価機関と契約している当事者。

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。

コモンクライテリア認証書：

特定の IT 製品またはプロテクションプロファイルが評価機関の評価に合格したことを確認するために、準拠認証機関によって発行され、参加機関によって認可される公開文書。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：

主張の正当性を判断するために、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評価すること。

評価・認証制度：

高い基準の能力と公平性が維持され、一貫性が実現していることを確認するための、認証機関の権限の下での評価・認証機能の組織的な体制。

評価機関：

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に、通常は商業ベースで評価を実施する組織。

評価方法：

IT セキュリティ評価方法を参照。

評価報告書：

認証報告書の主要な基礎となるものとして、評価機関から認証機関に提出される、評価結果に関する詳細を示す報告書。

解釈：

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：

多様な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：

評価・認証制度を通じて、効果的かつ一貫した標準に従って評価が実施されることを確認するための基礎として、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：

評価・認証制度を通じて、効果的かつ一貫した標準に従って評価が実施されることを確認するための基礎として、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。

IT セキュリティ評価機関：

特定の IT セキュリティの評価・認証制度に沿って評価を実施することを許諾または承認された、認定された評価機関。

許諾：

IT セキュリティ評価の特定の分野で、技術的な能力を持つことが認証機関により査定され、特定の評価・認証制度に沿って評価を実施することが正式に承認されること。

許諾方針：

全ての評価・認証制度に不可欠な文書の一部。これは申請を許諾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訓練要件とセキュリティ要件を規定する。

管理委員会：

本アレンジメントの規則に従って、本アレンジメントの履行を確保するために、全ての参加機関の代表者が出席する機関。

評価の監督：

評価機関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、認証機関の代表者が進行中の評価を観察し、完了した評価を審査する手続き。

情報発生元：

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、*評価機関*、または*参加機関*。

参加機関：

本アレンジメントの署名機関。

認証書利用参加機関：

*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参加機関。

認証書認可参加機関：

単数または複数の*準拠認証機関*を代表する参加機関。

有資格参加機関：

*準拠認証機関*でもある参加機関（または*シャドー認証*を引き受ける専門技術者を派遣するために、*準拠認証機関*の資源と専門技術を自由に利用できる参加機関）。この認証機関は有資格参加機関の*委託認証機関*である。

保護情報：

本アレンジメントの手続きまたは活動に基づいて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：

*コモンクライテリア*で定義される公式文書で、特定の利用者のニーズを満たす *IT 製品*のカテゴリに対する、実装に依存しないセキュリティ要件のセット。

保護マーキング：

現在、英国で正式に使用されている *セキュリティ分類*の別名。

コモンクライテリア認証書の承認：

準拠認証機関によって実施された評価・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全ての条件を満たしていることを参加機関が認め、その結果発行される全てのコモンクライテリア認証書に同等の価値を与える意図を示すもの。

承認：

コモンクライテリア認証書の承認を参照。

セキュリティ分類；

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キング。

シャドー認証：

少なくとも 1 つの有資格参加機関の代表者が、本アレンジメントに従って IT 製品の評価・認証を監視して認証機関を査定すること。

(認証機関の) スポンサー：

準拠認証機関 (または候補準拠認証機関) の利益を代表し、そのコモンクライテリア認証書を認可する参加機関。

システム：

特定の目的と運用要件を持つ特定の IT 設備。

評価対象：

評価の対象となる IT 製品、並びに関連する管理者 / 利用者ガイダンス文書。

付属書 B

評価・認証制度

B.1 制度の目的と主な特性

評価・認証制度（以下「制度」という）の主な目的は、評価・認証機能の組織的な体制と管理を通じて、高い基準の能力と公平性が維持され、一貫性が実現していることを確認することである。

このため、各制度は評価を受ける製品とプロテクションプロファイルの認証だけでなく、同様に重要である、セクション B.2 にリストされているその他の機能にも責任を負う単一の認証機関によって管理される。

制度の全般的な方針（許諾および承認方針を含む。以下参照）は、認証機関自体または理事会のいずれかによって決定することができる。後者の場合、理事会はその規則と方針に従って、制度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、認証機関は制度を管理し、理事会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、制度の運用において、評価と認証活動に利害関係を有する全ての参加機関の利益を適切に考慮に入れるための機構を確保することが非常に重要である。

かかる制度の存在は、承認のために非常に重要である。これは共通評価基準および評価方法の正しく一貫した適用と共に、全ての IT セキュリティ評価機関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、IT セキュリティ評価機関間で一貫していることについて信頼感を与える唯一の基盤となる。このことは全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 認証機関の役割と主な特性

認証機関は評価機関から独立しており、適切な資格を持つ人員を有する。

認証機関は、その国の有効な法律、法令、またはその他の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 EN 45011 もしくは ISO Guide 65 の要件、または本アレンジメントの付属書 C に規定する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) 評価機関の制度への参加を認可する（以下を参照）。
- b) 参加評価機関の業務実施能力、特に承認された評価基準と評価方法への準拠、適用、および解釈を監督する。

- c) 評価を受ける製品およびプロテクションプロファイルと、評価自体の手続きに係る重要な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認するために、制度内に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、評価機関に追加のガイダンスを発行する。
- e) 適切なレベルで、制度内で進行中の全ての評価を監督する。
- 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認するために、全ての評価に関する報告書（特に評価報告書を含む）を審査する。
- g) 制度の元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制度内で評価された全ての製品と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／確認製品リスト）。
- j) 制度の組織、方針、規則、およ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) 制度の規則が遵守されていることを確認する。
- l) 制度の規則と方針を決定し、必要に応じて修正する。
- m) 制度の活動に利害関係を有する全ての参加機関の利益が制度の運用において適切に考慮に入れられていることを確認する。

本アレンジメントへの参加の一環として、有資格参加機関の委託認証機関は、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 評価期間の認定と許諾

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、制度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
- b) 制度の管理に責任を負う認証機関によって許諾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、および手続き上の能力を示し、特に IT セキュリティの領域の特性と一貫している限り、EN 45001 または ISO Guide 25 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能力を有し、関係する制度の全ての規則に従うことができる立場にあることを認証機関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手続きに関する秘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れなければならない。

特定の制度内で評価を実施することを許諾または承認された評価機関は、IT セキュリティ評価機関と呼ばれている。

各制度の許諾方針または承認方針には、秘密保護と訓練要件の詳細と、許諾または承認のための申請手続きの詳細、並びに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

認証機関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。認証機関を運営する手続きは公平な方法で管理する。

C.2 管理構成

認証機関は公平でなければならない。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、認証機関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

認証機関は次のものを所有し、要求されたときに提供する。

- 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・認証制度について記述した文書
- d) 法的状態を明確に示した文書

C.4 認証要員

認証機関の要員は引き受ける機能に関する能力を有していなければならない。各スタッフの資格、訓練、および経験に関する情報は認証機関によって最新の状態に維持される。

要員にはそれぞれの義務と責任に関する明確で最新の指示文書を与える。

外部機関に作業を請け負わせる場合は、認証機関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しなければならない。

C.5 文書と変更管理

認証機関は、その評価・認証制度に関する全ての文書の管理のためにシステムを維持し、次のことを確保する。

- a) 適切な文書の最新版が、全ての関係する場所で入手可能であること。

- b) 適切な許可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り、迅速で効果的な措置をとる立場にある者に、変更についてただちに通知すること
- d) 無効になった文書は組織と関連機関全体で使用を止めること
- e) 制度に直接の利害関係を有する者に変更について通知すること

C.6 記録

認証機関は、その固有な状況に適応させ、参加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。全ての記録は最低 5 年間、安全で参照可能な場所に保存する。

C.7 認証手続き

認証機関は、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および方法に従って実施されるように、必要な設備と手続き文書を用意する。

C.8 IT セキュリティ評価機関の要件

認証機関は、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。

認証機関は、各 IT セキュリティ評価機関に対して、全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。これには、保護情報と評価・認証手続きの秘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

認証機関は、本付屬書の要件に準拠するための手続きを規定した品質マニュアルと文書を用意する。これ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の表明
- b) 認証機関の法的状態に關する簡潔な説明
- c) 上級管理者およびその他の認証要員の氏名、資格、および義務
- d) 認証要員の訓練計画の詳細
- e) 上級管理者から生じる権限、責任およ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ショ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乱用を防止する手続きの詳細
- h) 請負業者の名称と、能力を評価し、監督する手続き文書の詳細
- i) 訴訟または和解の手続きの詳細

C.10 秘密保持

参加機関の国の法律、制定法、行政命令、または規則によって許可されている範囲で、認証機関はその組織の全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秘密性を確保するために十分な手はずを整えなければならず、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 公開

認証機関は認証製品リストを作成し、必要に応じて更新する。リストに示す各 IT 製品とプロテクションプロファイルは明確に識別する。このリストは一般に公開する。

評価・認証制度の説明は、公開された形式で提供する。

C.12 上訴または和解

認証機関は、認証機関自体、関連する評価機関、およびそれぞれの申請者間の意見の不一致を処理するための手続きを設定する。

C.13 定期的な審査

認証機関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認するために、制度の運営について定期的な見直しを引き受ける。

C.14 コモンクライテリア認証書の誤使用

認証機関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。

認証機関は認証書の誤使用を防止し、対抗するために、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・認証制度に関する誤った、誤解を生じる、または不適切な表明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

認証機関はコモンクライテリア認証書の取り消し手続きを文書化し、認証製品リストの次の版で取り消しについて通知する。

付属書 D

任意の定期的な査定

管理委員会は、準拠認証機関の定期的な査定を実施するために、単数または複数の有資格参加機関（該当認証機関のスポンサを除く）を選出することができる。査定は、スポンサ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。かかる同意は査定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。スポンサは、査定チームの選出に関して懸念がある場合は、管理委員会に説明する必要がある。査定は以下の説明に従って、また管理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。このガイダンスは、査定が確実に統一基準に従って実施され、予測される資源を確保する必要があるからである。

査定を実施する参加機関は、資格を有し管理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査定チームを指名することができる。参加機関は、自らの費用で追加の専門家を指名することができる。委託認証機関に対して主要査定チームを提供する費用は、執行小委員会によって合意された公平な方法で有資格参加機関間で分担する。査定を受ける認証機関が委託認証機関でない場合は、その認証機関が査定から生じる主要査定チームの全ての費用（交通費、宿泊費、その他生活に要する費用、および給与を含む²）を負担する。

定期的な査定を受ける認証機関は、1 ヶ月以内にその時点で適用される完全な制度文書を提出する。専門家はその文書を検討し、その認証機関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、検討の結果を管理委員会に報告する。

シャドー認証は、直接に関係する参加機関の合意に従って、共通基準評価保証レベル 3 または 4 で適切な IT 製品に関して実施し、関係参加機関間で秘密保持契約を締結する。

専門家は、定期的な査定を受ける認証機関が、評価・認証プロセスの全ての点において一貫して活動していることを確認する。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。査定を受ける認証機関は、専門家の参加が円滑に実施されるよう努める。

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秘密性を確保するために、手続きの適用状態についても調査する。

評価・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。

- a) セキュリティターゲット
- b) 評価報告書

² 査定を実施する有資格参加機関が、国の法律または規則によって、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。

- c) 認証機関によって作成される文書に関する書面のコメント
- d) 認証報告書

その他の評価に関する報告書は、管理委員会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。

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。評価報告書は、必要がある場合にのみ翻訳する。査定に同意した参加機関は、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。

専門家は管理委員会に査定結果を報告し、査定結果に関する勧告を行う。管理委員会はシャドー認証報告書を審査する。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管理委員会が確認したら、査定を受けている認証機関にその結果を引き渡す。査定を受けている認証機関は、遅くとも6ヶ月以内に査定結果に指摘された問題点を修正したことを示さなければならない。

付属書 E

認証およびサービスマーク

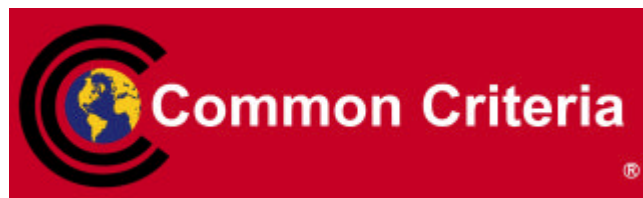
本アレンジメントの条件に基づいて発行されるすべてのコモンクライテリア認証書には、次に示すマークを表示する。



このマークは、本アレンジメントの参加機関によってコモンクライテリア認証書が承認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件に従って発行されたことを示す参加機関の表明である。

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、および販売に関してこのマークを使用することができる。本アレンジメントの参加機関は、その参加機関の商品またはサービスをプロモートするためにマークを使用してはならない。

本承認アレンジメントのサービスマークを次に示す。



このサービスマークは、本アレンジメントに従って、参加機関（または準拠認証機関）によって実施されるサービスを識別、広告、およびマーケティングするために使用することができる。

本アレンジメントへの参加を止めた参加機関は、それ以降このサービスマークを使用してはならない。

付属書 F

参加機関に提供する情報

F.1 制度文書

各準拠認証機関は、担当する評価・認証制度の次の側面に関する文書のコピーを参加機関に提供する。

- 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・認証に関する国の規則と規制
- b) 制度の組織構成
- c) 認証機関の品質マニュアル
- d) 認定または許諾 / 承認方針
- e) 制度に関連する IT セキュリティ評価機関の名称および住所と、それぞれの状態（例えば、政府か民間か）
- f) EN 45001 または ISO guide 25 の国による解釈（該当する場合）

上記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全ての参加機関に提供する。

F.2 コモンクライテリア認証書および認証報告書

各参加機関は、認可したコモンクライテリア認証書、認証報告書、および認証製品リストのコピーを他の参加機関に提供する。準拠認証機関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、かかる認証機関はただちに参加機関に通知する。

F.3 本アレンジメントの条件に影響を与える一般情報

各参加機関は、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に影響を与える国の法律、法令、行政規則、およ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。

各参加機関は、本アレンジメントの条件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管理委員会にただちに通知する。

- a) 国の法律、行政規則、または公職規定

b) 評価・認証制度の運用または手続き

F.4 秘密保持に関する規則

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参加機関、参加機関の関係当事者、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う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。

文書は紙（ハードコピー）または電子形式のいずれかである。

保護情報を含む文書は、特別なマーキング「RA in Confidence」によって識別する。情報発生元がこの特別なマーキングを付加する。

各参加機関は従うべき保護規則を施行し、その規則を適用するシステムを確立することに努める。

F.4.1 保護情報の作成と管理

保護情報を含むすべての文書には、発行者の名称と発行日を簡潔かつ明確に示す。また、一意な識別子（例えば 1 つずつ増加するシリアル番号）も付さなければならない。その文書を修正する場合は、少なくともバージョン番号と発行日に関して、その識別子も修正する。

文書は、その文書に指定されている期間、または指定がない場合は、情報発生元がその保護文書の保護を要求しなくなるまで継続的に保護される。

F.4.2 保護情報の取り扱い手続き

保護情報のマーキング

保護情報を含むハードコピーの文書には、各ページに「RA in Confidence」という言葉と一意の識別子を表示する。保護期間は最初のページに示すことができる。

保護情報を含むコンピュータ用のリムーバブル磁気メディアには、最低限「RA in Confidence」という言葉と一意の識別子を示したラベルを付ける。磁気メディアを参加機関から別の参加機関に輸送する場合には、常に磁気メディアにその内容の一覧を示す用紙を添付する。

保管および保護情報を保護するための規則

保管および保護規則は、保護情報を含む文書に適用される。これには草稿版も含まれる。

保護情報をコンピュータで処理または保存する場合は、適切に保護しなければならない。保護情報を保存するリムーバブル磁気メディアは、同じ情報を含む文書の場合と同様に保護する。

保護情報の郵送

保護情報を含む文書を郵送する場合は、2重の封筒に入れる。外側の封筒には RA 通信の連絡担当者として宛先参加機関が指名した人物の住所を記し、内側の封筒には保護情報を入れて、受取人の名前と共に「RA in Confidence」という言葉を記す。

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。

保護情報のコピー

受取人は、運用上の根拠に基づいて明らかに正当化される場合にのみ保護情報をコピーすることができる。

リムーバブル磁気メディアと保護情報の廃棄

必要がなくなった場合は、保護情報を含むリムーバブル磁気メディアは安全な方法で廃棄し、この処置を適切な記録文書に記録する。

廃棄の前に保護情報は磁気メディアから完全に消去する。

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、参加機関が受け取った保護情報の参照は、その参加機関によって直接に雇用されているスタッフ、またはその参加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。

F.4.3 追加の保護レベル

場合によっては、情報がより高いレベルの保護を要求することがある。これはケースバイケースで決定する。

付属書 G

新しい準拠認証機関

G.1 公式の要求

本アレンジメントの下で準拠認証機関の資格を得ることを希望し、第 5 条と第 5 条に引用されている付属書に規定する条件を満たしていると考えられる場合は、認証機関はその国の参加機関を通じて申請書を提出する（認証機関と参加機関が同一組織の場合もあることに注意すること）。参加機関が申請を支持する場合は、認証機関のスポンサになり、その申請を管理委員会に提出する。提出された申請は、申請者が本アレンジメントに規定する条件を満たすことができることを示す、スポンサ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準拠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表明を加える。

- 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査定チーム（次の G.3 を参照）の全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、申請者がスポンサの委託認証機関となることを申請しない場合に限り、主要査定チームの給与コストも含まれる³）。
- b) 以下に示す文書を提出する。
- c) 単数または複数の参加機関の代表者によるシャドー認証のために、申請者の管理の下で評価・認証を受ける適切な製品を提出する。

G.2 提出する文書

準拠手続き中に取得された全ての文書と情報は、付属書 F.4 に従って取り扱う。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。

- a) 申請者の評価・認証制度の範囲、組織、および運用に関する全ての詳細。これには次のものが含まれる。
 - 認証機関の名称、住所、主な連絡先
 - 認証機関品質マニュアル

³ 査定を実施する有資格参加機関が、国家の法律または規則によって、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。

- 認証機関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制度の全般的な管理を監督するシステム
 - 認証の手続き
 - 制度に参加している IT セキュリティ評価機関の名前および住所と、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許諾 / 承認方針
 - 営業秘密およびその他の秘密情報を保護するために制度内で適用される規則
 - IT セキュリティ評価機関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。
 - 正確かつ一貫して、相互に合意した IT 基準および方法を適用する。
 - 関係する秘密情報の秘密性を保護する。
- b) 制度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および認証報告書
- d) 評価・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全ての国の法律、法令、行政規則、および公職規定の効力に関する説明
- 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 製品およ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の説明

G.3 管理委員会の回答

管理委員会は、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。予備的な回答では、その文書が技術審査とシャドー認証に合格すれば、その申請が受理されることを伝える。

管理委員会が、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、申請者はコモンクライテリア評価保証レベル 3 または 4 を請求する製品を少なくとも 2 つ、シャドー認証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・認証の手配に関する詳細を提供する。管理委員会は候補製品の提示を受理してから 1 ヶ月以内に、シャドー認証のための製品を 1 つ選択し、それを申請者に通知する。

管理委員会はシャドー認証を実施するために、単数または複数の有資格参加機関（スポンサを除く）を選出する。選出された参加機関は、2人の専門家から構成される主要査定チームを指名する。参加機関（スポンサを含む）は、自らの費用で追加の専門家を指名することができる。管理委員会は、専門家の名前と所属組織について申請者に通知する。

G.4 シャドー認証手続き

専門家は、（統一基準に従って査定を実施するために）管理委員会によって発行されるガイダンスに基づき、入手可能な全ての情報を考慮に入れて、どの程度のシャドー評価・認証手続きを実施する必要があるかを決定する。管理委員会のガイダンスは、査定の際に必要な資源を見積もるために申請者の認証機関に提供される。

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・認証手続きの完了から1ヶ月以内に、管理委員会に書面で調査結果を報告し、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。管理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。拒否する場合は、管理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る。承認する場合は、管理委員会は付属書 K を更新することによって、その決定を記録する。

付属書 H

本アレンジメントの管理

H.1 責任と能力

管理委員会は本アレンジメントの状態、条件、および運用に関連する方針のあらゆる事項を扱う。管理委員会は新しい参加機関の承認、新しい認証機関の準拠性、および本アレンジメントの範囲の変更を決定する。

H.2 構成

全ての参加機関は、管理委員会に代表者を出席させる。管理委員会の議長は参加機関の中から管理委員会によって指名され、その任期は 1 年以内とする。各参加機関は順番に議長に任命される。現在の議長は管理委員会に管理上の支援を提供する。

H.3 決定

管理委員会に代表者を出席させる国は、各 1 票の議決権を有する。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規定される場合を除き、決定は単純多数による。

H.4 専門家の招待

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

H.5 専門家の採用

管理委員会は、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

管理委員会は年に 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 執行小委員会

管理委員会は、アレンジメントグループの日々の業務を管理し、管理委員会に技術的な助言と勧告を与えるために執行小委員会を設立する。

執行小委員会は、管理委員会によって決定される員数までの有資格参加機関と追加の任意の参加機関から構成する。

次に、執行小委員会の主な業務を示す。

- a) アレンジメントグループの業務の遂行手続きを作成し、勧告する。
- b) 新しい認証機関の技術的な準拠性を査定する。
- 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) 本アレンジメントの条件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。
- f) 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。
- g) 将来の基準または方法のいずれかに影響を与えうる解釈の背景と、その結果としての決定に関して、履歴データベースを管理する。

付属書 I

認証報告書の内容

I.1 認証報告書とその使用

評価報告書（ETR）は、認証機関のために評価機関によって作成され、認証報告書の主要な基礎としての役割を果たす。評価報告書の目的は、評価実施中に遂行された作業から派生した全ての評決、その根拠、および調査結果を示すことである。これには IT 製品またはプロテクションプロファイルの開発中に発見された誤りと、評価実施中に発見された利用可能な脆弱性が含まれる。評価報告書には、評価結果を正当化するために必要な保護情報が含まれることがある。

認証報告書は、関心を持つものにとって、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利用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、利用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。

I.2 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ものでなければならない。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、利用者、およ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、認定者、管理者）は、おそらく報告書のこのセクションしか読まないため、全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、例えば次のような項目を含むべきである。

- 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、開発者の名前およびバージョン
- b) IT セキュリティ評価機関の名称
- c) 評価の完了日
- d) 次の事項に関する報告結果の簡潔な説明
 - 保証パッケージ
 - 機能
 - 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）」
 - 特別な構成要件
 - 運用環境に関する想定事項

– 否認事項

1.3 識別

評価を受ける IT 製品は、明確に識別しなければならない。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、および周辺機器（テープドライブ、プリンタなど）を識別し、記録する。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。

1.4 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。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 製品が準拠および / または実施する必要がある方針または規則を含む。

1.5 想定事項と範囲の明確化

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。このセクションは、対策のない脅威に関して、評価の範囲を明確に示す手段を提供する。ユーザは 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る。このセクションには、使用、環境上の想定事項、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。

1.5.1 使用に関する想定事項

評価作業中に製品のベースラインを示すために、IT 製品の使用に関する想定事項を決定しなければならない。適切なインストールおよび構成、満たされるべき最低ハードウェア要件など、全ての項目について想定する。このセクションには、評価実施中の IT 製品の使用に関するあらゆる想定事項を記述する。

1.5.2 環境に関する想定事項

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想定事項を決定しなければならない。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想定事項を記述する。

1.5.3 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し、説明する。ある顧客が、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事態が生じうる。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全ての脅威をリストすることは实际的でない。

1.6 アーキテクチャに関する情報

このセクションは、Development-High Level Design (ADV_HLD)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。

1.7 ドキュメンテーション

このセクションには、開発者から利用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。全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、少なくともユーザガイド、管理ガイド、およ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。

1.8 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、および結果について概要を示す。

1.9 評価を受ける構成

このセクションでは、評価実施中の 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およ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のセクションに記述する。

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

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全ての参考文献をリストする。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ない。

- a) 基準、方法、制度に関する文書
- b) 技術的な参考文献
- 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、全ての開発者の文書は、適切なリリース日および適切なバージョン番号で一意に識別しなければならない。

付属書 J

コモンクライテリア認証書

以下の情報は、本承認アレンジメントの参加機関のために発行される全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 IT 製品の評価に関するコモンクライテリア認証書

IT 製品の評価の認証に基づいて作成され、参加機関によって承認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。

- a) 製品の製造業者
- b) 製品名
- c) 製品の種類
- d) バージョン番号とリリース番号
- e) 準拠したプロテクションプロファイル（該当する場合）
- f) 評価プラットフォーム（オプション）
- g) IT セキュリティ評価機関の名称（オプション）
- h) 認証機関の名前
- i) 認証報告書の識別子⁴
- j) 発行日
- k) 保証パッケージ⁵

認証書には、次の表明も加える。

この認証書で識別される IT 製品は、Common Criteria for IT Security Evaluation [バージョン番号を挿入] 準拠するために、Common Methodology for IT Security Evaluation [バージョン番号を挿入] を使用して、認定および許諾 / 承認された評価機関、または [参加機関の国名を挿入] 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で評価を受けた。この認証書は、完全な認証報告書と共に、評価を受けた構成に関して、製品の特定のバージョンまたはリリースだけに適用される。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 [参加機関の名前を挿入] による、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い。[参加機関の名前を挿入] または本認証書を承認し、もしくは

⁴ 認証報告書の識別子は、その文書を一意に識別する。これには最低限、認証機関の名称、使用する評価基準、報告書番号、および発行年度を含める。

⁵ 確認済み保証パッケージでは Common Criteria 評価保証レベルパート 3 と Common Criteria 評価保証レベルパート 3 拡張とを区別する。拡張はプラス記号によって指定する（例えば、EAL 3+）。

効力を与えるその他の組織は、明示であれ、黙示であれ、IT 製品に関していかなる保証も行わない。

リストされている情報に加えて、参加機関によって認可された各 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 に示すマークを表示する。

J.2 プロテクションプロファイルの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、参加機関によって認可されたコモンクライテリア認証書には次の情報を記述する。

- a) プロテクションプロファイルの作成者
- b) プロテクションプロファイルの名称 / 識別子
- c) バージョン番号
- d) IT セキュリティ評価機関の名称 (オプション)
- e) 認証機関の名称
- f) 認証報告書番号
- g) 発行日
- h) 保証パッケージ⁶

この認証書には、次の表明も加える。

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] へ準拠するために、Common Methodology for IT Security Evaluation [バージョン番号を挿入] を使用して、認定および許諾 / 承認された評価機関、または [参加機関の国名を挿入] 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、提示された証拠と一致している。この認証書は [参加機関の名前を挿入] による、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プロテクションプロファイルの保証を示すものではない。[参加機関の名前を挿入]、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は、明示であれ、黙示であれ、プロファイルに関していかなる保証も行わない。リストされている情報に加えて、参加機関によって認可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 に示すマークを表示する。

⁶ 確認済み保証パッケージでは Common Criteria 評価保証レベルパート 3 と Common Criteria 評価保証レベルパート 3 拡張とを区別する。

付属書 K

準拠認証機関

Australasian Information Security Evaluation Programme

スポンサ :

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 :

Communications Security Establishment,
カナダ

Schema d'Evaluation et Certification Francais

スポンサ :

Service Central de la Sécurité des Systèmes d'Information,
フランス

Bundesamt für Sicherheit in der Informationstechnik (Zertifizierungsstelle)

スポンサ :

Bundesamt für Sicherheit in der Informationstechnik,
ドイツ

UK IT Security Evaluation and Certification Scheme

スポンサ :

Communications-Electronics Security Group and Department of Trade and Industry,
英国

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme

スポンサ :

National Institute of Standards and Technology, and National Security Agency,
アメリカ合衆国