制度における

追補情報

JISEC では、主に政府調達における安全な IT 製品の供給に資することを目的とし、国際的なセキュリティ評価基準である CC に基づく IT 製品評価を行っています。本制度を運営するに当たり CC では規定されていない運営側の判断を本制度の追補情報として記載しています。

認証申請にあたっては、必ず当該追補情報をご確認ください。申請以降、関係者は当該追補情報をご理解していることを前提とさせていただきますので、内容について不明な点がありましたら申請前に JISEC にお問い合わせ願います。

IPA 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　2014 年 5 月 23 日発行

◆認証制度(JISEC)における暗号の取扱い

CC では、暗号の使用方法や鍵管理の適切性、実装における脆弱性について評価を実施しますが、ハッシュ関数を含む暗号の特定と暗号アルゴリズムの数学的特性の評定は制度の範疇とされています。

JISEC における暗号の特定は、PP 等において政府調達要件で指定する暗号アルゴリズムを基本とします。

また、総務省及び経済産業省によって定められた「電子政府における調達のために参照すべき暗号リスト（CRYPTREC 暗号リスト）」のうち、「電子政府推奨暗号リスト」に掲げられているものは、制度として受け入れます。

上記以外の暗号アルゴリズムを用いる場合（つまり政府調達要件ではなく独自に要件を想定した ST を作成し、かつ電子政府推奨暗号リスト以外の暗号を用いる場合）、申請者は想定する調達者[1]とあらかじめ用いる暗号について合意を取り付けておくとともに、安全性について客観的な証拠資料を評価機関に提出し、要件に対する適切性を評価してください。

特に脅威への対抗として独自暗号の機能要件を用いる場合、一般的に暗号の安全性に関する客観的な評価には専門的な技法が必要であり、また実績をともなうことも要求されます。申請者はあらかじめこの分野における十分な専門性がある評価機関を選択し指定する必要があります。

制度は、このような電子政府推奨暗号リスト以外の暗号の安全性についての検証については関与しませんが、ST で当該暗号を要件とする調達者が明確となっていないものは制度として受け入れません。

[1] 認証申請書（様式 1）の「認証取得の目的」に書かれた機関等

◆組織のセキュリティ方針(OSP)

PP において OSP が規定されることがあります。OSP は TOE の利用者環境において課せられるセキュリティ上の規則、手続きまたはガイドラインであり、一般的にはその TOE 分野に係る法的な規制や政府機関のセキュリティ方針、さらには調達部門の独自のセキュリティ方針に基づきます。

PP 作成（あるいは開発者による独自 ST 作成）において OSP を要件として指定する場合、根拠となる規制や方針の充分な背景を考慮した書き方をしてください。たとえば、「通信路は暗号化されなければならない」という要件を OSP として指定しているが、実は「電子政府推奨暗号リスト」を用いることが暗黙の方針としてあり、また同組織の別のセキュリティ方針として暗号使用時の鍵長やその他が規定されていた場合、OSP の情報だけではその根拠となる規則や手続きを満たすことはできません。

評価では、OSP ステートメントが TOE の利用者環境に課せられる方針を反映し作成されたかを決定します。そのため、申請者が独自に ST において OSP を設定する場合にも、想定する調達者[2]の TOE の利用環境に課せられる具体的なセキュリティ上の規則、手続きまたはガイドラインを特定する必要があります。

OSP の根拠となる具体的なセキュリティ上の規則、手続きまたはガイドラインが特定できない場合、OSP としては不適切です。そのような内容は、ST で脅威として述べられることになるでしょう。根拠となるべき規則や手続き、また脅威も存在しないような内容を安易に OSP として記載してはなりません。

[2] 認証申請書（様式 1）の「認証取得の目的」に書かれた機関等

◆評価証拠資料の準備

当該評価の申請に責任を負う申請者（TOE 開発者自身あるいはそのスポンサー）は、評価保証の範囲に応じて評価に必要となる技術的証拠資料（設計書や使用した開発・テストツールなど）や保証手続き（入退出管理ログや開発環境の視察受け入れ等）の提供義務を負います。評価の対象の開発において開発者が行わなければならない事項については「開発者のアクションエレメント」として、また開発者が準備・提示すべき資料については「内容・提示エレメント」として CC Part3[3]に記載されています。

申請者は、評価に先立ち PP で要求されている評価保証範囲に必要な対応を認識し準備をする必要があります。事前に申請者が、対応が必要な事項の検討を認識せずに開発を完了させ、あるいは証拠資料を準備せずに評価を開始した結果、評価スケジュールの遅延を発生させ、場合によっては評価継続が不可能となるリスクと責任を申請者が負うことになります。

過去、PP を参照せず申請者みずから ST を作成し評価保証範囲を宣言しているにも関わらず、十分な証拠資料を提供できなかったケースもあります。

たとえば、評価対象の一部が申請部門と関わりのある関連会社が開発しており、申請部門と同レベルの開発手法を用いておらず必要なレベルの資料が提供できないことが後に判明したり、開発の一部を完全に外部に委託しており、委託先と開発者の契約に評価に関する事項を含めておらず評価者や認証者がサイトへの立ち入りを一部許可されなかったなどの問題が実際に発生しています。

申請者がみずからの責任で対応できない、つまり証拠資料を提供できない範囲を含め評価保証範囲として宣言することは、結果として関係者に無駄な費用や時間を発生させることに十分留意をしてください。

[3] 情報技術セキュリティ評価のためのコモンクライテリア　パート 3:セキュリティ保証コンポーネント

◆同一書類での認証申請について

原則、ひとつの TOE についてひとつの認証申請をお願いします。ひとつの TOE とは、調達の際の識別が一意となること、評価構成や評価保証レベルが固定されていることを示します。これは、複数の構成や異なる課題定義をひとつの評価で行うことにより、ST や認証報告書が煩雑となり調達者が調達において誤解を生むことを避けるためです。また、CC 評価は多岐にわたるため、評価報告書に複数の製品の細かい差分が記載されることは、認証作業のミスを誘発しやすいこと、認証費用の適正な負担という観点からも本制度で規定するものです。

ただし、上記の観点から TOE としては同一であるが、販売の都合により製品型番を分けている場合などについては、同一申請書類での申請を可能とします。たとえば、同一の TOE であるが、販売上の便宜から使用ライセンス数やサポートプラットフォームを区別するために製品型番を分けることがあります。このような場合、いずれの製品型番に対応する TOE の評価結果についても、調達者にとって差異がないものであるならば、その TOE の認証申請は同一の書類として受け付けるものとします。

ただし、調達者が認証対象を誤解する危険があるため、基本的には TOE 識別としての TOE 名称及びバージョンはすべて同一の場合に限ります。

また認証書は一申請に対し一通であり、申請記載のすべての TOE が評価の対象となります。よって、申請された一部のライセンスやプラットフォーム型番の評価結果や認証維持の条件は同一申請時のすべての TOE に影響します。一部の TOE で認証が取消しされた場合でも、認証書に記載されたすべての TOE が認証取消しの対象となりますので、複数の TOE を一申請で申請する場合には留意願います。

なお、ここでは認証の申請形式についてのみ言及しています。複数類似 TOE の評価における費用・工数等の取り扱いについては各評価機関の判断となりますので、事前に評価機関にご相談ください

◆認証製品の信頼維持義務

当該評価の申請に責任を負う申請者は、認証取得後に TOE の評価の信頼性及び脆弱性に係る事象が明らかになった場合、それらを報告または是正する義務を有します。

認証製品の評価結果に疑義が発生した場合、申請者は制度の指示に基づき評価結果への疑義に対する調査及び報告、是正を行わなければなりません。この間、認証製品としての販売はできません。また申請者は、調達者に対して問題の概要と影響、是正のための手順等を記載したウェブページを公開しなければなりません。具体的な手順は JISEC の規程のサーベイランスの項を参照ください。

評価結果への疑義は、第三者や制度関係者からの指摘、あるいは申請者自らの届け出によることがあります。これらの疑義は、評価の過程における証拠資料の充分性や評価判断の妥当性などが要因となりますが、制度としてその切り分けは行いません。申請者は、評価結果に対する疑義が生じた場合に、どのような対応をするか等の SLA について評価機関と事前に協議しておくことをお勧めします。

また、認証取得後に技術的な状況の変化や新たな攻撃手法の開発により、脆弱性が顕在化することがあります。申請者は、調達者に注意喚起を行うために、脆弱性の概要と影響、その対策方法について制度に通知する義務があります。
この脆弱性関連情報は、制度が公開する認証製品リストに掲載されます。これにより調達者が重大な脆弱性が悪用されるリスクを知らないまま認証製品を運用または調達することを避けることができます。

また、この脆弱性が評価の妥当性に起因するものであると判明した場合、制度はその認証製品をサーベイランスの対象とすることがあります。

認証製品が、政府調達等で用いられている状況において脆弱性によるインシデントが発生した場合、信頼の回復は困難となります。制度は、そのような状況を回避するために脆弱性に係る情報等を調達者に開示しますので、サーベイランスへの協力と脆弱性情報の提供については積極的にお願いいたします。