平成２３年４月２１日
経　済　産　業　省

IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト

１．はじめに

昨今、情報通信技術（IT）が社会の重要な基盤となるに伴って、個人情報や知的財産といった情報資産の価値が高まっており、その滅失・漏えい等による影響は飛躍的に増大している。また、情報セキュリティ上のリスクが多様化・高度化・複雑化してきており、情報資産を保有する情報システムのセキュリティをこれまで以上に確保することが求められている。

このような状況下で、政府機関における情報システムのセキュリティ対策については、「政府機関の情報セキュリティ対策のための統一基準」（現行は第 4 版（平成 21 年度修正）：平成 22 年 5 月 11 日情報セキュリティ政策会議決定）（以下、「政府機関統一基準」という。）を始めとする一連の施策により、斉一的な向上が図られているところである。一方で、各府省庁においてその利用目的や利用環境に対応した適切な情報セキュリティを確保していくことが重要な課題となっており、今後、自発的・能動的な情報セキュリティ対策を実施するとともに、国民に対して政府機関における IT 関連製品及びシステムのセキュリティ対策について明確な説明責任を果たすことが求められる。

２．ISO/IEC15408 に基づくコモンクライテリアについて

こうした IT 関連製品及びシステムのセキュリティ対策については、第三者による評価・認証を行う制度として、ISO/IEC15408 に基づくコモンクライテリア（以下、「CC」という。）制度が我が国を含む主要各国において整備されている。

CC 制度とは、ISO/IEC15408 として国際標準化された評価基準に基づき、情報技術に関連した製品やシステムが適切に設計され、その設計が正しく実装されているかどうかを第三者が評価及び認証する制度である。当該制度により、評価・認証された製品については、各国の認証機関により公表され、その評価認証の結果を関係国間で相互認証することとなっている。我が国において CC 制度は、「IT セキュリティ評価及び認証制度」として、独立行政法人情報処理推進機構（以下、「IPA」という。）において、運営されているところである。

CC 認証（CC 制度による認証）の取得のためには、評価・認証対象となる製品のセキュリティ機能の範囲をあらかじめ定め、評価保証レベル（EAL）によって当該セキュリティ機能の評価方法のレベルを設定し、評価を受けることになる。ここで、評価・認証対象となる製品のセキュリティ機能については、製品ごとに PP（プロテクションプロファイル）[1]という形で、海外を含む政府機関や業界団体等において定型的に取りまとめられている場合もある。

[1] PP(Protection Profile)：特定の分野の製品について必要とされる典型的なセキュリティ要件、環境などを記述した要求仕様書。

３．海外の主要国政府における CC 認証の活用状況

上記 CC 認証については、IT 関連製品の政府調達基準としての利用も想定されている。具体的に、CC 制度による認証取得製品の導入は、米国、ドイツ、フランス等の主要国政府において進んでおり、これにより、当該製品により構成される情報システムの技術的安全性の説明責任を担保している。

４．目的

海外の主要国政府において、国民への説明責任を果たす観点からも CC 認証の活用がなされる一方で、我が国政府機関における CC 制度の活用については、現行の政府機関統一基準において明記されているものの、強化遵守事項であり、各府省庁での必須として実施すべき対策事項である基本遵守事項とはなっていない。しかしながら、我が国の政府機関の情報システムにおいては、個人情報や経済活動に影響する機微な情報など多様な情報資産を有するものが数多く存在するものと考えられることから、当該システムに応じた適切な情報セキュリティ対策を実施し、その対策の有効性を国民に説明できるようにするため、構成要素である製品に対する CC 制度の活用を促進する必要がある。

こうした背景から、「情報セキュリティ２０１０」（平成 22 年 7 月 22 日情報セキュリティ政策会議決定）において、「情報セキュリティに配慮したシステム選定・調達の支援」として、**「諸外国における状況も勘案しつつ、政府機関統一基準に定められている政府情報システム等の調達時における『IT セキュリティ評価及び認証制度』、『暗号モジュール試験及び認証制度』の認証取得の要否に関する要件の一つである『重要なセキュリティ要件』がある場合等について、その明確化を行い、上記統一基準の反映に資する」**（内閣官房及び経済産業省）ことが求められている。

他方、上記要請に対応するにあたっては、製品分野やその利用環境を踏まえ必要なセキュリティ要件について、具体的な考え方及び指針を示す必要がある。そこで、**CC 認証を取得するべきセキュリティ機能及び評価保証レベル（EAL）を製品分野ごとに明確化し、「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」（以下、「製品分野リスト」という。）としてとりまとめる**ことにする。各府省庁においては、調達時に当該製品分野リストを活用することにより、政府機関の情報システムの構成要素における適切な情報セキュリティ対策の確保と当該情報セキュリティ対策の説明責任を果たすことができるものと考える。

５．製品分野リスト作成方針

CC 認証を取得するべき製品分野リストの作成に当たっては、保護すべき重要度の高い情報を扱う情報システムか否かを判断し、その上で、当該システムに対する情報漏えい、改ざん、なりすまし等の脅威への適切な情報セキュリティ対策が求められる具体的な製品分野を特定していく必要がある。そのため、高い機密性、完全性、可用性が求められる「保護すべき重要度の高い情報」の該当範囲を提示するとともに、当該情報を扱う情報システムの構成要素である製品分野を特定する上での考え方を以下に示す。

１）保護すべき重要度の高い情報の該当範囲

政府機関における保護すべき重要度の高い情報としては、一般的に、国民の生命・健康・財産に係る情報をはじめとする個人情報、我が国の経済・企業活動に多大な影響を与えうる情報、政策意思決定に関する機微な情報などが考えられる。

保護すべき重要度の高い情報の例としては、政府統一基準にあるとおり、「秘密文書等の取扱いについて」（昭和４０年４月１５日付け事務次官等会議申合せ）に基づく文書管理規程上の秘密文書に相当する機密性を要する情報、秘密文書には相当しないが、「行政機関の保有する情報の公開に関する法律」（平成１１年５月１４日法律第４２号）に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報が挙げられる。そのような情報については、意図しない公開すなわち漏えい等があってはならない機密性の高い情報であるといえる。

（参考）「行政機関の保有する情報の公開に関する法律」に基づく処分に係る審査基準で不開示情報に該当すると考えられる情報の例

① 個人に関する情報（第５条第１号）
② 法人等に関する情報（第５条第２号）
③ 国の安全等に関する情報（第５条第３号）
④ 公共の安全等に関する情報（第５条第４号）
⑤ 審議、検討等に関する情報（第５条第５号）
⑥ 事務又は事業に関する情報（第５条第６号）

２）上記情報を扱う情報システムの構成要素である製品分野の特定

上記の保護すべき重要度の高い情報を扱う政府機関の情報システムにおいて、当該情報の処理、保管等に関わり、かつ攻撃等により当該保護情報の漏えいや改ざんの被害を生じうる恐れのあることが技術的・経験的に判明している製品分野に対しては、適切な情報セキュリティ対策が必要な製品として、CC 認証を取得するべきと考えられる。

具体的には、

① 情報システムの構成上、攻撃の脅威に曝されやすい製品分野
② 情報システムの基盤となる製品分野
③ 情報システムの中で保護すべき重要度の高い情報を保管しているため攻撃事例の報告が多い製品分野

といった考え方をもとに、CC 認証を取得するべき製品分野を特定する。

上記方針１）、２）により特定した分野製品について、認証を取得する際に考慮するべき、利用用途・利用条件、一般的に評価されるべきセキュリティ機能及び評価保証レベル（EAL）等についても製品分野リストに明記する。

ただし、当該製品分野において、最新の脅威に対応している認証取得済みの製品の数が十分に調達可能なほど流通していない場合については、現時点での製品分野リストへの掲載を見合わせることとする。

６．対象とする製品分野

上記５．の条件を満たす製品分野を、本リストの対象として以下に示す。その上で、保護すべき重要度の高い情報を扱う政府機関の情報システムにおいて当該製品分野が利用されている場合には、適切な情報セキュリティ対策の実施のため、CC 認証取得製品を調達することとする。

①スマートカード（IC カード）

広く国民の身分証明書等に利用される IC 旅券、住民基本台帳カード、運転免許証（IC チップが入ったもの）や、入退室管理などに利用されている公務員カードなどのスマートカードは、万一、なりすまし、改ざん、偽造等があった場合に国民への影響が甚大である。一方、利用者が持ち歩いて利用するという性質上、常時施錠されたキャビネット等に保管するなど統一的に厳重に管理することが難しい。そのため、紛失や盗難などにより、カード自体が攻撃者に渡り、直接多様かつ高度な攻撃（回路の書き換えなどの物理的攻撃を含む）を受ける恐れがあるため、耐タンパ性[2]を持つなどの厳重な情報セキュリティ対策を講じる必要がある。こうした適切な情報セキュリティ対策を講じているか第三者の評価・認証を受ける必要がある。

②ファイアウォール

ファイアウォールは、外部からの不正アクセス等の攻撃を遮断し、内部のシステムや重要な情報を保護する役割がある。特に、政府機関の内部システムとインターネットの境界に設置されているファイアウォールは、外部からの攻撃に最も曝されるため、その機能を適切に果たす製品であるかについて、第三者の評価・認証を受ける必要がある。

③OS（サーバ OS に限る）

保護すべき重要度の高い情報を取り扱う情報システム、IT 製品の基盤として稼働する OS については、情報の漏えい、改ざん、外部からの不正アクセス等への対策を講ずることが重要であり、適切な情報セキュリティ対策を講じているか第三者の評価・認証を受ける必要がある。

④デジタル複合機（MFP）

政府機関で利用されるデジタル複合機では、国民の個人情報等の保護すべき重要度の高い

[2] 耐タンパ性：内部の情報に対する不正な読み出し、改ざんなどの攻撃が困難であることを示す度合いのこと。一般に、「耐タンパ性を備えている」「耐タンパ性がある」と表現する場合、そのような攻撃が極めて困難であることを意味することが多い。

情報について、複写やデジタルデータ化、送信等に利用されるが、これらの情報が、内部のハードディスクなどの記憶媒体に保存されるため、ネットワークを介した外部からの攻撃や職員の操作ミス等により、保存されている保護すべき重要度の高い情報が漏えいする恐れがある。そのため、個人情報などの保護すべき重要度の高い情報を取り扱うデジタル複合機や、外部からの訪問者が利用可能なデジタル複合機などについては、アクセス制御機能や情報の自動消去機能など、適切な情報セキュリティ対策を講じているか第三者の評価・認証を受ける必要がある。

⑤不正侵入検知システム/不正侵入防止システム（IDS/IPS）

保護すべき重要度の高い情報を保管するコンピュータへの不正アクセスが成功した場合の影響は甚大であり、その侵入検知・防御を実施する製品は適切な情報セキュリティ対策を講じているか第三者の評価・認証を受ける必要がある。

⑥データベース管理システム（DBMS）

個人情報や経済・企業活動等に関する機微な情報を取り扱うデータベース管理システムについては、機密情報の漏えいや改ざんなどが生じると、当該システム自身や関連する制度、政府機関に対する国民の信頼を失墜するため、適切な情報セキュリティ対策を講じているか第三者の評価・認証を受ける必要がある。

７．製品分野リスト

製品分野名	**スマートカード**（IC カード）	**ファイアウォール**	**OS（サーバ OS に限る）**
製品分野定義	プラスチック製カード等に IC チップを埋め込み、情報を記録できるようにした製品	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
利用用途	住民基本台帳カードや IC 旅券等、広く国民に配布され身分確認に利用される。または国民の情報アクセスの認証のために利用される	不正アクセスから保護すべき重要度の高い情報を扱う情報システムを保護する	保護すべき重要度の高い情報を扱う情報システムの基盤として稼動する OS
準拠すべき規格・制度	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)
一般的に必要となるセキュリティ機能	セキュリティ監査、送受信の否認不可、暗号化サポート機能、アクセス制御、データ認証、送出データ保護、情報フロー制御、入力データ保護、内部転送データ保護、残存情報保護、ロールバック、蓄積データ完全性、転送データ機密性、転送データ完全性、識別・認証、セキュリティ管理、プライバシー保護、セキュリティ機能保護、資源利用管理、TOE アクセス制御、高信頼パス/チャネルの各セキュリティ機能について、調達者のニーズに応じて選択。個別製品ごとにどのセキュリティ機能が認証されているかについては、IPA ポータルサイトを参照。		
参照 PP[3]	IC 旅券：旅券冊子用 IC のためのプロテクションプロファイル (http://www.ipa.go.jp/security/jisec/certified_pps/c0247/c0247_it9276.html)	U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments (http://www.commoncriteriaportal.org/files/ppfiles/pp_fw_tf_br_v1.1.pdf)	Controlled Access Protection Profile (http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/protection-profiles/capp.pdf)
標準 EAL	EAL4+以上	EAL4 以上	EAL3 以上

[3] 参照 PP とは、当該製品分野において、必要と考えられるセキュリティ機能を明確化するために参照するもの。

製品分野名	**デジタル複合機（MFP）**	**不正侵入検知/防止システム（IDS/IPS）**	**データベース管理システム（DBMS）**
製品分野定義	プリンタ機能を標準で有しスキャナ、FAX、コピーのいずれか２つ以上の機能を標準で装備している製品	ネットワークやシステムの稼動状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品
利用用途	保護すべき重要度の高い情報の複写やデジタルデータ化、送信等に利用される	ネットワーク上の通信を監視するなどにより、インターネットからの不正アクセスを検知し防止する	国民の個人情報等保護すべき重要度の高い情報をデータベースとして保管するために利用される（サーバ OS 環境下で稼働するものに限る）
準拠すべき規格・制度	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)	ISO/IEC15408 (Common Criteria)
一般的に必要となるセキュリティ機能	セキュリティ監査、送受信の否認不可、暗号化サポート機能、アクセス制御、データ認証、送出データ保護、情報フロー制御、入力データ保護、内部転送データ保護、残存情報保護、ロールバック、蓄積データ完全性、転送データ機密性、転送データ完全性、識別・認証、セキュリティ管理、プライバシー保護、セキュリティ機能保護、資源利用管理、TOE アクセス制御、高信頼パス/チャネルの各セキュリティ機能について、調達者のニーズに応じて選択。個別製品ごとにどのセキュリティ機能が認証されているかについては、IPA ポータルサイトを参照。		
参照 PP	2600.X, Protection Profile for Hardcopy Devices Controlled Access Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp_hcd_br_v1.0.pdf)	U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments (http://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf)	U.S.Government PP for Database Management Systems (http://www.commoncriteriaportal.org/files/ppfiles/PP_DBMS-BR_V1.1-PP.pdf)
標準 EAL	EAL3 以上	EAL3 以上	EAL2 以上

参考として、CC 認証を受けている最新の個別製品のリストについては、IPA のポータルサイト(http://www.ipa.go.jp/security/jisec/certified_products/cert_list.html)に掲載されている。

なお、上記サイトでは CC 認証取得製品において該当するセキュリティ機能の概要を示している。しかしながら、セキュリティ機能の詳細な範囲等は各認証取得製品にて異なることがあることから、詳細については上記サイトを直接参照して確認することが必要である。

また、我が国以外の国際承認アレンジメント（CCRA）参加国における ISO/IEC15408 に基づく認証取得製品がある場合には、当該製品を活用することも可能である。

同様に、特定の製品分野において、個別の製品に一連のバージョンの製品のうち、過去に認証取得製品が存在するが最新のバージョンで CC 認証が取得されていない製品について、以下の方法により、実質的に CC 認証取得製品とセキュリティ機能上同等であると確認されている場合は、採用対象とすることも可能とする。

１）過去の認証取得製品の後継製品について、CCRA 参加国の認証機関において保証継続の認証を受けている製品[4]

２）過去の認証取得製品の後継製品について、メンテナンス型バージョンアップが行われたことを IPA において確認済みの製品[5]

８．製品分野リスト活用における適用除外

各府省庁は、原則として、情報システムを構成する機器の調達時に上記リストを活用することが必要であるが、下記適用除外の例のように、CC 制度を利用する以外の手段で適切な情報セキュリティの確保及び国民への説明責任を果たすことが可能であると判断する場合は、この限りではない。

適用除外の例：

当該情報システムを構成する機器が、外部ネットワークから物理的に遮断されている、あるいは、CC 認証を取得しているファイアウォールに保護されているなどで外部からの不正アクセスから保護されている、かつ当該機器が入退室可能な人員が厳格に制限された管理区域に設置されているなど、当該機器自体のセキュリティ機能以外の手段で不正アクセスや攻撃から保護されている場合。

９．製品分野リストの見直し

本製品分野リストは、IT 製品分野ごとの CC 取得製品件数の増加及び製品の普及、セキュリティ上の障害発生状況等を踏まえるとともに、暗号モジュール試験及び認証制度（JCMVP）など CC 制度以外の第三者認証制度の活用も視野に入れ、定期的又は必要に応じて見直しを行う。

以上

---

[4] CC 制度の認証取得済み製品に対し、バージョンアップなどで変更がなされた場合でも、その変更内容が認証取得済み製品で評価・認証されたセキュリティ事項に影響を及ぼさないことを CCRA 参加国の認証機関が確認した場合、認証機関から変更された製品に対しても認証書を発行する仕組み。
保証継続認証取得製品は、CCRA ポータルサイト（http://www.commoncriteriaportal.org/products/）に含まれている。

[5] 「メンテナンス型のバージョンアップ」とは、セキュリティホールの強化やバグ修正等、そのソフトウェアの本来機能を補修するバージョンアップをいう。CC 制度の認証済み製品に対し、メンテナンス型のバージョンアップを行った製品については、実質的に ISO/IEC15408 認証製品とセキュリティ機能上同様の状況にあると見なせる。
具体的な製品リスト（http://www.ipa.go.jp/security/tax/H21/index.html#slist）