平成３０年２月２８日
経　済　産　業　省

IT 製品の調達におけるセキュリティ要件リスト

- 対象となる製品分野

対象製品分野	製品分野定義
デジタル複合機（MFP）	プリント機能を有し、さらに、スキャン、FAX、コピー機能のうちいずれか２つ以上の機能を装備している製品
ファイアウォール	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
不正侵入検知/防止システム（IDS/IPS）	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ネットワークへの外部からの侵入を報告、防御する製品
OS（サーバ OS に限る）	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
データベース管理システム（DBMS）	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
スマートカード（IC カード）	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
暗号化 USB メモリ	製品自体に USB コネクタを備えており、フラッシュメモリを内蔵した持ち運び可能な記憶装置に暗号化機能を有する製品
ルータ／レイヤ３スイッチ	OSI 基本参照モデル第 3 層を利用し、情報システム及びネットワークの基盤においてデータを中継する機能を持った通信回線装置
ドライブ全体暗号化システム	ノート PC 等のハードディスクドライブ、半導体ドライブなどのデータストレージ全体を暗号化するシステム
モバイル端末管理システム	スマートフォン、タブレット等のモバイル端末を安全に運用・管理するシステム
仮想プライベートネットワーク（VPN）ゲートウェイ	公共ネットワークを利用した、仮想的なプライベートネットワークシステムにおける終端装置

対象候補	製品分野定義
―	―

● 本リストの目的及び利用方法

「サイバーセキュリティ 2016」(平成 28 年 8 月 31 日サイバーセキュリティ戦略本部決定）において、安全性・信頼性の高い IT 製品等の利用推進及び、政府調達における情報セキュリティの確保が求められている。

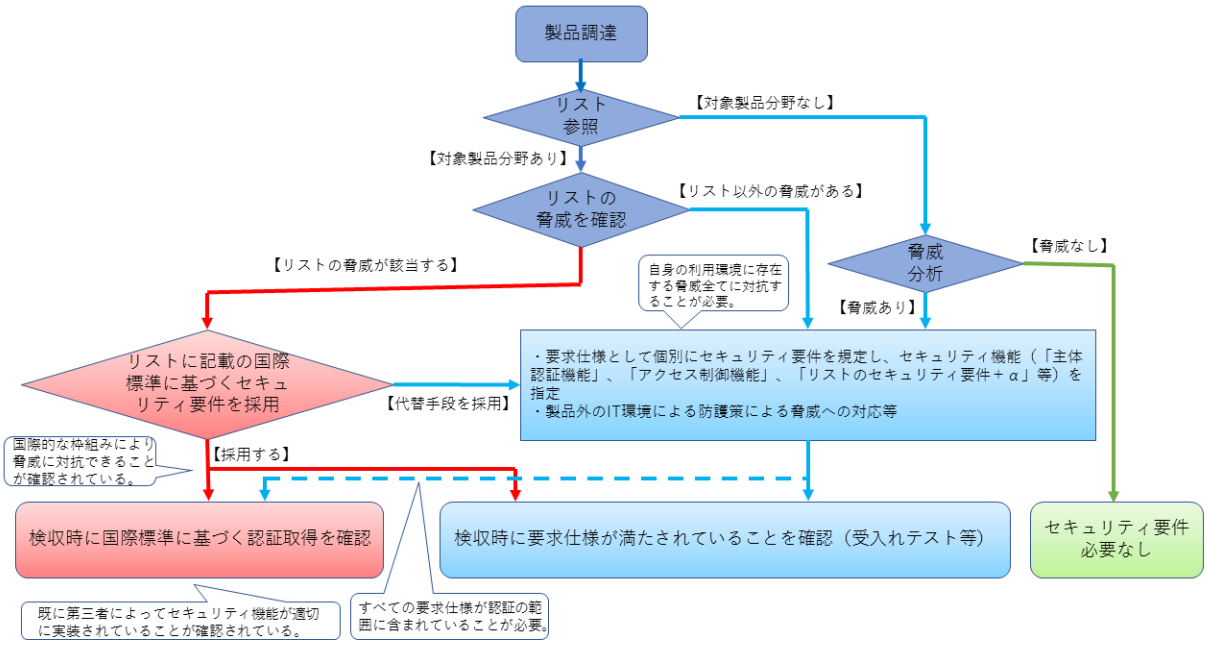
本リストは、上記要請に対応するにあたって、経済産業省が平成 25 年 6 月 27 日に公表した「IT 製品の調達におけるセキュリティ要件リスト」を改定したものである。

本リストでは、次のような観点で、適切な情報セキュリティ対策が必要な製品分野のうち、適切なセキュリティ要件が策定されている製品分野を特定し、セキュリティ上の脅威とそれに対抗する要件を示している。

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

さらに、特定された製品分野のうち、セキュリティ要件を満足する製品が調達可能である等の環境が整った製品分野を本リストに含めている。

本リストを活用した、セキュアな IT 製品を調達するためのフローを以下に示す。



セキュアな IT 製品を調達するための大まかなフロー

【脅威分析と対抗手段策定】

IT 製品を調達する際には、その製品が扱う情報資産に対して、自身の利用環境において脅威が存在するか分析が必要となる。本リストに掲載されている製品分野については、それぞれにどのような「セキュリティ上の脅威」が想定されるかを示しており、調達者は自身の利用環境において当てはまる脅威が存在するかどうかを判断し、脅威が存在する場合には脅威への対抗策を講じる必要がある。

対抗のための手段は調達側に委ねられるが、推奨する「国際標準に基づくセキュリティ要件」と、それらがどの脅威に対抗するかを本リストに併せて示している。

調達者は、この「国際標準に基づくセキュリティ要件」を調達時に活用[1]することで、該当する「セキュリティ上の脅威」に対抗する機能をもつ製品であることを指定することができる。

ただし、当該要件を満たす製品であっても、使用時には利用環境の整備等が必要となる場合があるため、「国際標準に基づくセキュリティ要件」に記載されている「ASSUMPTIONS」、「前提条件」の内容も参照し、想定する利用環境との整合性を確認することが望ましい。

「国際標準に基づくセキュリティ要件」は、調達する製品の機能として脅威への対抗漏れがあることを防ぐために、あくまでベースラインとなる要件を示すものである。利用環境（情報システムの他の構成要素との依存関係）等を背景にして、以下のような状況が認められる場合には、「国際標準に基づくセキュリティ要件」を活用する必要がない、又は個別のセキュリティ要件を策定する必要がある。

① 「セキュリティ上の脅威」への対抗手段を独自に講じることができる

② 「セキュリティ上の脅威」に挙げられていない、固有の脅威が存在する

ただし、「セキュリティ上の脅威」が存在しない利用環境であると判断できる場合においては、セキュリティ要件の考慮や、対抗手段の検討は不要である。

【納品時検査（受け入れテスト等）】

製品調達においては、調達した製品が要求仕様を満たしていることを確認する検査作業が必要になる。調達時に個別にセキュリティ要件を指定した場合には、各組織で定められている確認・検査手続きに従い、受け入れテスト等により要件を満たしていることを確認することが必要となる。

「国際標準に基づくセキュリティ要件」に関連した国際標準に基づく第三者認証を取得している場合には、国際標準に基づく認証プロセスに従って第三者によってセキュリティ要件が満たされていることが確認されているため、調達者は調達した製品が国際標準に基づく第三者認証を取得済みであることの確認をもって受け入れテスト等

[1] 本リストでは、【各製品分野の補足事項】の頁において、調達仕様書の記載例として、『「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件』という表現を用いている。これは、「国際標準に基づくセキュリティ要件」で想定されている脅威（もしくはそれ以上の脅威）に対して、「国際標準に基づくセキュリティ要件」で求められている対抗手段であるセキュリティ要件とは異なるセキュリティ要件を、製品ベンダが独自に考案している場合等があり得るためであり、その旨について調達者（発注者）が確証を得られる場合には、要件を満たしていると判断して差し支えない。

に替えることができる。

例えば、ISO/IEC15408 に基づく認証取得製品は、情報セキュリティの専門家が国際標準化されたセキュリティ評価手法（ISO/IEC 18045）に従った検査を実施し、セキュリティ要件が満たされていることが確認されている。

そのため、第三者認証の活用は IT 製品の調達において有用であるが、以下の点について注意されたい。

① 本リストで示す「国際標準に基づくセキュリティ要件」以外のセキュリティ要件ついて

現在、本リストで推奨している「国際標準に基づくセキュリティ要件」以外の「国際標準に基づくセキュリティ要件」や「製品ベンダが独自に策定したセキュリティ要件」での第三者認証を取得している製品が流通している。

そのような認証取得製品も、調達側で想定される脅威に対抗するためのセキュリティ要件が全て含まれて認証されていることをベンダが証明し、調達者がその妥当性を確認できる場合には、国際標準に基づく第三者認証を取得済みであることの確認をもって受け入れテスト等に替えることができる。

② パッチの適用等に伴うバージョンアップについて

IT 製品ではベンダがセキュリティパッチを提供することで継続的なセキュリティ強化・修正が行われていることが多いが、国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、セキュリティパッチ等の適用によりバージョンアップした後の製品は認証の対象外となる。

そのため、バージョンが変更された製品に対しても当初の認証を維持する保証継続という仕組みがあり、調達者は、認証取得製品がバージョンアップ等で変更がなされた場合でも、その変更が評価され認証されたセキュリティ事項に影響を及ぼさないことが確認できる。（保証継続では、ベンダがバージョンアップ等による変更がセキュリティに影響を及ぼさないことを分析した影響分析報告書の妥当性を認証機関が確認する。）

検査にあたって、調達者は、調達対象の製品がバージョンアップし認証取得製品とバージョンが異なる場合には、保証継続されている製品であるかの確認を行うことが必要となる。保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを証明する資料を求め、その妥当性を調達者自身が確認することが必要となる。

また、認証取得は調達時に有用な事項であり、製品の運用中においては、必要に応じてセキュリティパッチを適用することが重要となる。

③ 調達時に認証取得が完了していない製品（セキュリティ評価中の製品）について

国際標準に基づく第三者認証を取得するためには時間を要するため、調達対象となる製品が認証取得中（セキュリティ評価中）であるため、調達時の要件として「認

証取得見込みの製品」を含める場合も考えられる。

そのような場合には、納品又は稼働開始までに認証取得が間に合わない、あるいは、最終的に認証が取得できない場合もあり得ることを想定する必要があり、「認証取得見込みの製品」を要件に含める場合には、これらのリスク回避のため、瑕疵担保責任を求める内容等を含んだ仕様とするべきである。

④　その他

一方、調達側が必要と考えるセキュリティ要件の一部が評価範囲に含まれていない認証取得製品や、本リストに記載していない製品分野等の国際標準に基づく第三者認証が活用できない（認証取得製品が市場に流通していない）製品においては、納品物がセキュリティ要件を満たしていることを調達者自身で確認することが必要となる。

しかし、セキュリティ要件のレベル、検査担当者のスキルや検査に掛かる工数等の事情により、納品時検査（受け入れテスト等）を調達側で実施することが困難な場合には、外部委託も選択肢として考えられる。外部委託先としては、セキュリティ診断等を業務として行っている組織や ISO/IEC 17025 の要求事項に基づいて承認された IT セキュリティ評価及び認証制度における評価機関[2]等を活用することが考えられる。

【製品分野の拡大等に関する本リストの見直し】

本リストには、将来対象製品分野となる予定の「対象候補」を併記している。「対象候補」には、「国際標準に基づくセキュリティ要件」が策定直後又は策定過程であり、直ちに国際標準に基づく認証取得製品を入手することが困難である製品分野を挙げている。これらについては、適切なセキュリティ対策を実施する必要がある製品であることを認識し、「セキュリティ上の脅威」について分析、対策することが望まれる。今後の見直しにおいて、同分野の認証取得状況に応じて「対象製品分野」に移行させるものとしている。

国際的に IT 製品ベンダや評価機関、認証機関、政府機関の有識者が様々な技術分野において、最先端の技術を基に政府調達のための「国際標準に基づくセキュリティ要件」（cPP: collaborative Protection Profile）の策定を継続的に進めている。それらの策定状況に合わせて、本リストの複数の「対象製品分野」、「対象候補」及び本リストで推奨する「国際標準に基づくセキュリティ要件」を更新していくことで、「国際標準に基づくセキュリティ要件」及びそれに基づく認証取得製品についても調達に幅広く活用されるよう、本リストは、定期的又は必要に応じて見直しを行う。

[2] IPA サイト https://www.ipa.go.jp/security/jisec/eval-list.html

製品分野名	デジタル複合機（MFP）

セキュリティ上の脅威	① **他の利用者による不正な操作** 各利用者が複合機を操作するにあたり、取り扱う文書データに適切な保護（データアクセス権、各種操作の制御等）を行うことができなければ、蓄積される文書及び文書関連データの漏えい、情報の改ざん等が発生する。
	② **通信データの盗聴、改ざん** 複合機を利用（プリント、スキャン等）するために使用する PC やファイルサーバと複合機の間でやりとりされるネットワーク上の通信データが盗聴、改ざんされる可能性がある。
	③ **管理機能への不正なアクセス** 取り扱う文書データに対する設定された規則（セキュリティポリシー）や複合機の利用者情報を管理する機能等に対して、操作できる者を適切に識別認証できない場合には、不正に操作される可能性がある。
	④ **複合機のソフトウェアの改ざん・破損** 複合機のソフトウェアが改ざん・破損された場合、設定されたセキュリティポリシーが適切に実施されない可能性がある。
	⑤ **監査ログの改ざん・不正な削除** 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。
	⑥ **複合機内に保存された文書データの漏えい（リース終了返却、又は廃棄処理時）** プリントやコピー、FAX 機能で扱われる文書データは、複合機の HDD/SSD 等の記憶媒体に一時的又は継続的に保存される場合があり、リース終了返却、又は廃棄処理となった複合機から、それらの文書データが漏えいする可能性がある。これらの文書データは、暗号化されていない、又は物理的に消去されていない場合、表面的にはアクセスできないようになっていても復元される可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：IEEE Std 2600.1™ -2009,Protection Profile for Hardcopy Devices, Operational Environment A Version 1.0 [3] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥
[2]：U.S. Government Approved Protection Profile－U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™ -2009) [4] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥

[3] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp_hcd_br_v1.0.pdf
IPA サイトから翻訳版をダウンロード可能
https://www.ipa.go.jp/security/publications/ieee/documents/2600.1/index.html
[4] CCRA ポータルサイトからダウンロード可能
https://www.commoncriteriaportal.org/files/ppfiles/pp_hcd_eal2_v1.0-add1.pdf

[3]：Protection Profile for Hardcopy Devices （Version 1.0[5]以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①，②，③ ④，⑤，⑥

（備考）［３］のセキュリティ要件は、ソフトウェアの更新を安全に行う機能も要求している。

【デジタル複合機（MFP）に関する補足事項】

この製品分野においては、プリント機能を有し、さらにスキャン、FAX 又はコピー機能のうちいずれか２つ以上の機能を有しており、かつネットワーク通信、管理機能を有する、いわゆるオフィス用大型複合機を対象としている。

デジタル複合機は、様々な機能が実装されるが、製品によっては、例えば FAX が実装されていない製品も存在し得るため、製品種別毎に必要となるセキュリティ要件が異なる場合がある。

また、複合機内に保存された文書データの漏えいに対抗する手段として、記憶領域の完全消去機能により対抗している製品もあれば、暗号化機能により対抗している場合もある。

上記のようなデジタル複合機の特性上、製品が備えている機能に応じて想定される脅威へ対抗するため、「国際標準に基づくセキュリティ要件」で求められる機能要件とは異なる要件をベンダ独自に策定し脅威に対抗している場合もある。そのような場合には、製品提供側がどのような脅威を想定した上でセキュリティ要件を定義しているのかを、調達側が確認することが重要となる。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（デジタル複合機（MFP））を参照し、 「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/mfp

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。[6] ・ IEEE Std 2600.1 ™ -2009,Protection Profile for Hardcopy

[5] IPA サイトからダウンロード可能 https://www.ipa.go.jp/security/publications/pp-jp/hcd.html

[6] デジタル複合機の分野において該当することが多い注意点として、ISO/IEC 15408（Common Criteria）認証では、既に認証を取得している機器において、構成要素（例えば FAX オプションの有無等）が異なると、認証取得製品とみなせない場合があり得る。ただし、既に認証を取得している機器の構成要素でもってのみ構成されている場合、当該認証を取得している機器と同等のセキュリティレベルを実現しているとみなし、その旨について調達者（発注者）が確証を得られる場合、要件を満たしていると判断して差し支えない。

Devices,Operational Environment A Version 1.0 ・U.S. Government Approved Protection Profile－U.S. Government Protection Profile for Hardcopy Devices Version 1.0（IEEE Std. 2600.2™-2009） ・Protection Profile for Hardcopy Devices Version 1.0以上）

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合でも、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合）：

（記載例）

以下のいずれかと同等以上のセキュリティ機能要件を満たしていること。 ・ IEEE Std 2600.1™-2009,Protection Profile for Hardcopy Devices,Operational Environment A Version 1.0 ・U.S. Government Approved Protection Profile－U.S. Government Protection Profile for Hardcopy Devices （Version 1.0（IEEE Std. 2600.2™-2009） ・Protection Profile for Hardcopy Devices （Version 1.0以上）

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。なお、これらの「国際標準に基づくセキュリティ要件」は、それぞれ和訳版をIPAが公開している。

https://www.ipa.go.jp/security/publications/pp-jp/index.html

製品分野名	ファイアウォール

セキュリティ上の脅威	① **管理機能等への不正アクセスによる不正な通信の発生** 不正な通信を制御するための規則（セキュリティポリシー）等を管理する機能等に対してアクセス権限のない者が、正当な利用者になりすますことができれば、不正に操作される可能性がある。不正操作により、本来実施されるべき情報フロー制御が実施されず、組織内外からの不正な通信を排除できず、セキュリティ侵害に繋がる可能性がある。例えば、インターネット等のオープンな環境からの通信が、管理されるべき内部のネットワークへとアクセスされ、内部のネットワークに接続されるサーバ等が何らかの被害を受ける可能性がある。またインターネット等のオープンな環境に存在し、利用が禁止されているサービスに対して、内部のネットワークから通信し、秘匿されるべき情報が流失する等の可能性がある。
	② **ネットワーク処理の残存情報からの情報漏えい** 送信したネットワークパケットが使用しているバッファ又はメモリエリアに、パケットに含まれるデータが残存している場合、別のパケットがそのバッファを再利用することで、送信済みのデータが別のパケットに含まれ、機密情報（に関連したデータ）が漏えいする可能性がある。
	③ **リモートで管理する場合の通信データの盗聴、改ざん** 管理権限のある者が遠隔地からリモートで管理する際に、製品との間で通信されるセキュリティ関連情報を含むデータが盗聴、改ざんされる可能性がある。管理者パスワード等が盗聴により不正に取得された場合には、ファイアウォールの設定が不正に変更される可能性がある。
	④ **監査ログの改ざん・不正な削除** 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：Protection Profile for Traffic Filter Firewall In Basic Robustness Environments Version 1.1 [7] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）（1年後に削除）	①, ②, ③, ④
[2]：Protection Profile for Network Devices Version 1.1 [8] 及び Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall（Version 1.0 [9]以上）	①, ②, ③, ④

[7] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp_fw_tf_br_v1.1.pdf
[8] NIAP（米国国家情報保証パートナーシップ）サイトからダウンロード可能 https://www.niap-ccevs.org/pp/pp_nd_v1.1.pdf
IPA サイト（翻訳版をダウンロード可能） https://www.ipa.go.jp/files/000015354.pdf
[9] NIAP サイトからダウンロード可能 https://www.niap-ccevs.org/pp/pp_nd_tffw_ep_v1.0.pdf
IPA サイト（翻訳版をダウンロード可能） https://www.ipa.go.jp/files/000015352.pdf

（ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	
[3]： collaborative Protection Profile for Stateful Traffic Filter Firewalls（v1.0（CPP_FW v1.0)以上）（ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①，②，③，④

（備考）［３］のセキュリティ要件は、ソフトウェアの更新を安全に行う機能も要求している。

【ファイアウォールに関する補足事項】

この製品分野においては、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、トラフィックフィルタ型（パケットフィルタ型）ファイアウォール製品を対象としている。

ファイアウォールに関しては、「国際標準に基づくセキュリティ要件」として、3 つの要件を掲載しているが、[1]は、すでに廃止されており、2012 年に 3 製品が認証された後、新たな認証製品はないため、2019 年 2 月に本セキュリティ要件を削除する。[2]は、2014 年に 1 製品、2015 年に 7 製品、2016 年に 3 製品が認証されている。[3]は、2015 年に策定されたセキュリティ要件で、国際標準に基づく第三者認証を取得している製品がまだ市場に流通していないため、国際標準に基づく第三者認証を調達時に求める場合には、 [2]と[3]の両方を要件として活用し、いずれかへの適合を要求することが望ましい。(2018 年 2 月現在)

なお、UTM（Unified Threat Management, 統合脅威管理）のように、ファイアウォールを含む複数のセキュリティ機能を統合的に管理する機器についても、本リストに示した脅威分析及びセキュリティ要件の策定が必要となる。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（ファイアウォール）を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/fw

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。 ・Protection Profile for Network Devices Version 1.1 及び Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter

Firewall （Version 1.0 以上）
・ collaborative Protection Profile for Stateful Traffic Filter Firewalls （v1.0（CPP_FW_v1.0)以上）

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合）：

（記載例）

以下のいずれかと同等以上のセキュリティ機能要件を満たしていること。
・Protection Profile for Network Devices Version 1.1 及び Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall （Version 1.0 以上）
・ collaborative Protection Profile for Stateful Traffic Filter Firewalls （v1.0（CPP_FW_v1.0)以上）」

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	不正侵入検知/防止システム（IDS/IPS）

セキュリティ上の脅威	① **監視すべき攻撃** Web アプリケーション等の公開サービスへの攻撃、過度なアクセスによる DoS 攻撃等の脅威が存在するシステムや、脆弱性が公開された場合に早期に対応する必要があるシステムに対しては、これらを関連する情報の分析・検知・警告する機能が必要となる。そのような機能がない場合、攻撃の痕跡を見落とすことにより、適切な対処ができない可能性がある。その結果、脅威が存在するシステムが何らかの被害を受ける可能性がある。
	② **防御すべき攻撃** 攻撃の監視に加えて、状況に応じてそのまま攻撃を防御、又は軽減するための措置を自動的に講じる必要がある。そのような機能がない場合、攻撃が成功してしまうことにより、管理対象のシステムが何らかの被害を受ける可能性がある。
	③ **管理機能等への不正アクセスによるセキュリティ機能の侵害** 不正な通信を制御するための規則（セキュリティポリシー）等を管理する機能等に対してアクセス権限のない者が、正当な利用者になりすますことができれば、不正に操作される可能性がある。 結果、公開サービスへの攻撃、過度なアクセスによる DoS 攻撃等に関連する情報の分析・検知・警告する機能が動作しなくなったり、状況に応じてそのまま攻撃を防御、又は軽減するための措置を自動的に講じることができなくなったりする。
	④ **不正・異常検出したデータの破壊、改ざん、開示** 製品が不正な侵入や、異常な動作を検出した際に生成されるデータが保護されていない場合には、不正に破壊、改ざん、開示される可能性がある。 結果、公開サービスへの攻撃、過度なアクセスによる DoS 攻撃等に関連する情報の分析・検知・警告する機能が動作しなくなったり、状況に応じてそのまま攻撃を防御、又は軽減するための措置を自動的に講じることができなくなったりする。
	⑤ **監査ログの改ざん・不正な削除** 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：Protection Profile Intrusion Detection System - System for Basic Robustness Environments, （Version 1.7 [10]以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤
[2]：Extended Package for Intrusion Prevention Systems （Version 2.1 以上）	①, ②, ③

[10] CCRA ポータルサイトからダウンロード可能
https://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf

及び collaborative Protection Profile for Network Devices （v1.0（ND cPP v1.0）以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	④，⑤

（備考）[2] のセキュリティ要件は、ソフトウェアの更新を安全に行う機能も要求している。

【不正侵入検知/防止システム（IDS/IPS）に関する補足事項】

この製品分野は、ネットワークやシステムの稼働状況を監視し、組織内のコンピュータネットワークへの外部からの侵入を報告、防御する不正侵入検知/防止システム（IDS/IPS）製品を対象としている。

現在、市場に流通している国際標準に基づく第三者認証を取得している製品に関しては、[1]「Intrusion Detection System－System for Basic Robustness Environments, Version 1.7」に基づく第三者認証を取得している製品が複数存在しているため、調達時に活用することが可能である。[2]は、2016年1月に策定されたセキュリティ要件で、国際標準に基づく第三者認証を取得している製品がまだ市場に流通していないため、国際標準に基づく第三者認証を調達時に求める場合には、[1]と[2]の両方を要件として活用し、いずれかへの適合を要求することが望ましい。（2018年2月現在）

なお、UTM（Unified Threat Management，統合脅威管理）のように、IDS/IPSを含む複数のセキュリティ機能を統合的に管理する機器についても、本リストに示した脅威分析及びセキュリティ要件の策定が必要となる。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下のIPAの「IT製品の調達におけるセキュリティ要件リスト」適合製品情報（不正侵入検知システム（IDS/IPS））を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/ids

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合したISO/IEC 15408（Common Criteria）認証を取得していること。
- Protection Profile Intrusion Detection System － System for Basic Robustness Environments, （Version 1.7以上）
- Extended Package for Intrusion Prevention Systems （Version 2.1 以上）及びcollaborative Protection Profile for Network Devices （v1.0（ND cPP v1.0）以上）

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合）：

（記載例）

以下のいずれかと同等以上のセキュリティ機能要件を満たしていること。
・Protection Profile Intrusion Detection System - System for Basic Robustness Environments （Version 1.7 以上）
・Extended Package for Intrusion Prevention Systems （Version 2.1 以上）及び collaborative Protection Profile for Network Devices （v1.0 (ND cPP v1.0)以上）

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	OS（サーバ OS に限る）

セキュリティ上の脅威	① <u>正当な利用者へのなりすまし</u> OS にアクセスするユーザやプロセスが正しく識別されない場合、正当な利用者になりすました不正なアクセスが行われる可能性がある。 例えば、本来登録されていない利用者が、OS の正当な利用者になりすましてログインすることにより、OS が管理するリソースへの不正なアクセス（情報漏えい、情報の改ざん等）が発生する。
	② <u>許可されないリソース、機能への不正なアクセス</u> 識別された利用者に割り当てられた権限に従い、OS が管理するリソースへの操作が適切に制御されない場合、本来の権限を越える不正なアクセスが行われる可能性がある。例えば、ファイル、ディレクトリ、サービス等のリソースや機能に対して、予め設定された規則（セキュリティポリシー）どおりに各種操作（読み込み、書き込み、実行等）の許可/拒否が制御されなければ、情報漏えい、情報の改ざん等が発生する。
	③ <u>OS レベルでの通信データの傍受</u> OS と通信を行うリモートの IT システムとの通信が傍受された場合には、通信データの暴露、改ざんが行われる可能性がある。
	④ <u>監査ログの改ざん・不正な削除</u> 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。
	⑤ <u>不正な通信の発生</u> 不正な通信を制御するための規則（セキュリティポリシー）等を設定・管理する機能等が適切に制御されない場合、OS に対して不正な通信が行われ、サーバ内部の情報に不正にアクセスされる可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：Operating System Protection Profile (BSI-CC-PP-0067b) Version 2.0 [11] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤
[2]：PROTECTION PROFILE FOR GENERAL-PURPOSE OPERATING SYSTEMS IN A NETWORKED ENVIRONMENT Version 1.0 [12] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）（1 年後削除）	①, ②, ③, ④
[3]：General-Purpose Operating System Protection Profile Version: 3.9 [13] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤

[11] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf
[12] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp_gpospp_v1.0.pdf
[13] NIAP サイトからダウンロード可能 https://www.niap-ccevs.org/pp/pp_gpos_v3.9.pdf

[4]：Protection Profile for General Purpose Operating Systems （Version 4.1, PP-OS-v4.1 以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①，②，③ ④，⑤

（備考）[4] のセキュリティ要件は、ソフトウェアの更新を安全に行う機能も要求している。

【OS（サーバ OS に限る）に関する補足事項】

この製品分野は、サーバ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（サーバ OS）を対象としている。

OS に関しては、「国際標準に基づくセキュリティ要件」として、4 つの要件を掲載しているが、[2]は、すでにこれに代わるセキュリティ要件として[4]が策定されており、[2]の国際標準に基づく第三者認証を取得している製品が市場に流通していないため、2019 年 2 月に削除する。国際標準に基づく第三者認証を調達時に求める場合には、[1]、[3]及び[4]の要件を併せて活用し、いずれかへの適合を要求することが望ましい。（2018 年 2 月現在）

なお、[1]、[3]、[4]はどれも汎用 OS を対象としたセキュリティ要件であるが、OS の種別（製品ベンダ）毎に、どのセキュリティ要件に基づく第三者認証を取得しているかは様々であるため、セキュリティ以外の要求仕様も考慮した上で、最適なセキュリティ要件を選択することが必要となる。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（OS（サーバ OS に限る））を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/os

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。
・Operating System Protection Profile BSI-CC-PP-0067 （Version 2.0）又は
・General-Purpose Operating System Protection Profile （Version 3.9）
・Protection Profile for General Purpose Operating Systems （Version 4.1, PP-OS-v4.1 以上）

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出

させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合）：

（記載例）

以下のいずれかと同等以上のセキュリティ機能要件を満たしていること。 ・Operating System Protection Profile BSI-CC-PP-0067 (Version 2.0) ・General-Purpose Operating System Protection Profile (Version: 3.9) ・Protection Profile for General Purpose Operating Systems （Version 4.1, PP-OS-v4.1 以上）

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	データベース管理システム（DBMS）

セキュリティ上の脅威	① <u>正当な利用者へのなりすまし</u> データベースにアクセスするユーザやプロセスが正しく識別されない場合、正当な利用者になりすました不正なアクセスが行われる可能性がある。 例えば、本来データベースにアクセスできない利用者が、DBMS に登録された正当な利用者になりすましてアクセスすることにより、DBMS が管理するデータベースへの不正なアクセス（情報漏えい、情報の改ざん等）が発生する。
	② <u>許可されない操作対象、機能への不正なアクセス</u> 識別された利用者に割り当てられた権限に従い、DBMS が管理するリソースへの操作や許可されない機能が適切に制御されない場合、本来の権限を越える不正なアクセスが行われる可能性がある。 例えば、データベース、テーブル、関数等の操作対象、機能に対して、予め設定された規則（セキュリティポリシー）通りに、各種操作（読み込み、追加、更新、削除、実行等）の許可/拒否が制御されなければ、情報漏えい、情報の改ざん等が発生する。
	③ <u>解放した領域からの情報漏えい</u> DBMS がディスク/メモリ上の領域を解放した後に別のユーザやプロセスが解放後の領域に新規にデータベース、テーブルを作成する際、解放前に存在していたデータが適切に消去されていない場合、アクセス権の無いユーザに当該データが読み取られる可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]： PP for Database Management Systems (Version 1.3) [14] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）(1 年後に削除)	①, ②, ③
[2]：Base Protection Profile for Database Management Systems （v2.07 (BSI-CC-PP-0088-2015) 以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③

【データベース管理システム（DBMS）に関する補足事項】

この製品分野は、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データベース管理システム（DBMS）を対象としている。

データベース管理システム（DBMS）に関する「国際標準に基づくセキュリティ要件」については[1]が策定されてから時間が経過しており、新たに[2]が策定されており、

[14] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp_dbms_v1.3.pdf

かつ第三者認証を取得している製品が複数存在しているため、調達時に活用することが可能である。そのため、[1]については、2019 年 2 月に削除する。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】
以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（データベース管理システム（DBMS））を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。
https://www.ipa.go.jp/security/it-product/dbms

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

Base Protection Profile for Database Management Systems （v2.07 (BSI-CC-PP-0088-2015)以上）と同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合）：

（記載例）

Base Protection Profile for Database Management Systems （v2.07 (BSI-CC-PP-0088-2015)以上）と同等以上のセキュリティ機能要件を満たしていること。

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテ

スト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	スマートカード（IC カード）

セキュリティ上の脅威	① **IC チップの偽造** IC チップの複製データを、同様の機能性を持つ別の IC チップに書き込んで IC チップが偽造される可能性がある。
	② **論理的な攻撃による機密情報の漏えい** 機械読取領域に格納されている機密情報（認証データ等）が、非接触インタフェースを用いて不正に読みだされる可能性がある。
	③ **物理的な攻撃による機密情報の漏えい** 物理的な攻撃により IC チップ内に保存されている機密情報（認証データ等）が、不正に読みだされる可能性がある
	④ **認証失敗時の処置** 利用者認証に失敗した際には、認証データを恒常的に無効にする機能がない場合、さまざまな認証データを利用して利用者認証の試行を行うことにより、認証が成功する可能性がある。

国際標準に基づくセキュリティ要件（参考）	対抗できる脅威
[1] 旅券冊子用 IC のためのプロテクションプロファイル- 能動認証対応 -第 1.00 版 [15] （ISO/IEC15408(Common Criteria)に基づいた IC 旅券に対するセキュリティ要求仕様）(1 年後に削除)	①, ②, ③, ④
[2] 旅券冊子用 IC のためのプロテクションプロファイル- SAC 対応（PACE）及び能動認証対応 -第 1.00 版 [16] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③, ④
[3] 旅券冊子用 IC のためのプロテクションプロファイル- SAC 対応（BAC+PACE）及び能動認証対応 -第 1.00 版 [17] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③, ④
[4] 個人番号カードプロテクションプロファイル 第 1.00 版 [18] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③, ④
[5] Security IC Platform Protection Profile Version 1.0, BSI-CC-PP-0035-2007 （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③
[6] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-CC-PP-0084-2014 （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③

【スマートカード（IC カード）に関する補足事項】

[15] IPA サイトからダウンロード可能 https://www.ipa.go.jp/security/jisec/certified_pps/c0247/c0247_pp.pdf

[16] IPA サイトからダウンロード可能 https://www.ipa.go.jp/security/jisec/certified_pps/c0499/c0499_pp.pdf
[17] IPA サイトからダウンロード可能 https://www.ipa.go.jp/security/jisec/certified_pps/c0500/c0500_pp.pdf
[18] IPA サイトからダウンロード可能 https://www.ipa.go.jp/security/jisec/certified_pps/c0431/c0431_pp.pdf

この製品分野は、プラスチック製カードに IC チップを埋め込み、情報を記録できるようにしたスマートカード（IC カード）を対象としている。

スマートカード（IC カード）は用途によって対抗すべき脅威が大きく異なるため、調達するスマートカード（IC カード）の用途毎に調達側で脅威分析し、それに基づいてセキュリティ要件を策定することが必要となる。

このため本リストでは、IC 旅券に対する脅威と、脅威に対抗するためのセキュリティ要件を、「国際標準に基づくセキュリティ要件」の参考として記載している。[1]については、すでに新しいセキュリティ要件として[2]及び[3]が策定されているため、2019 年 2 月に削除する。

また、用途に応じて多数のセキュリティ要件が既に策定されているので、必要に応じて CCRA[19] ポータルサイトを参照し、個別にセキュリティ要件を策定すること。

https://www.commoncriteriaportal.org/pps/

（「ICs, Smart Cards and Smart Card-Related Devices and Systems」タブの「Protection Profile」が用途ごとのセキュリティ要件となる。）

上記ページには、以下の分野についてのセキュリティ要件が掲載されているが、スマートカード（IC カード）に関するセキュリティ要件は、個別の利用環境等を考慮のうえ策定されているため、調達においてそのまま利用することは困難であることが考えられるため、あくまで参考情報とされたい。

- 居住許可系カード [20]
- ヘルスカード [21]
- 金融系カード [22]

また、スマートカード（IC カード）では、カードに搭載される IC チップに対するセキュリティ要件も重要になる。一般には、カードベンダがチップベンダに指定するセキュリティ要件になる場合が多いと想定されるが、スマートカード（IC カード）を調達する者が IC チップに対するセキュリティ要件も指定する場合には、IC チップに関するセキュリティ要件 [23]も参考とすること。

[19] CCRA(Common Criteria Recognition Arrangement)とは、各国の政策実施機関が IT 製品等の安全性を客観的に評価した結果を国際的に相互承認するための枠組。

[20] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp0069b_pdf.pdf

[21] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp0018_v3b_pdf.pdf

[22] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp0038b.pdf

[23] CCRA ポータルサイトからダウンロード可能 https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf
※上記の URL は一例を示しており、他にも CCRA ポータルサイト https://www.commoncriteriaportal.org/pps/ に幾つかのセキュリティ要件が掲載されている。

製品分野名	暗号化 USB メモリ

セキュリティ上の脅威	① **機密情報の漏えい** 暗号鍵・認証データの適切な保護が行われていない場合、暗号鍵・認証データを容易に取得・推測でき、それらの欠陥を悪用されることにより情報漏えいが発生する可能性がある。
	② **暗号鍵・認証データ情報への不正アクセス** USB メモリに格納された悪意あるプログラムが、USB メモリを制御するプログラムの動作を阻害することで、暗号鍵・認証データ情報をアクセスされ、暗号化機能の無効化や暗号鍵・認証データを容易に取得されたりする。
	③ **USB メモリのソフトウェアが不正に書き換えられる** 製品のアップデートプログラムが正当なものであることを検証するしくみがないため、不正なソフトウェアやシステムファイルがアップロードさせられ、暗号化機能の無効化等が引き起こされたり、接続先の PC 等に不正なアプリケーションを導入されたりする。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]ISO/IEC 19790 （対応する JIS 規格 ：JIS X 19790） [Security Level 2 以上][24]	①, ②
[2]Protection Profile for USB Flash Drives （Version 1.0 以上） [25] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③
[3]:Protection Profile for USB Storage Media （Version 1.4 (BSI-PP-0025-2006) 以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③
[4]：CSEC Protection Profile Encrypted Storage Device （Version 2.1 (FMV-PP-ESD)以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③

【暗号化 USB メモリに関する補足事項】

この製品分野は、製品自体に USB コネクタを備えており、フラッシュメモリを内蔵した持ち運び可能な記憶装置（USB メモリ）であって、USB メモリのハードウェアによってフラッシュメモリの内容を自動的に暗号化する製品を対象としている。

暗号化 USB メモリについては、利用・運用形態などから、要求すべき要件が変化する。例えば、USB メモリを接続する情報システム側で接続可能な USB メモリを制限している場合、外部へ持ち出される可能性が一切生じない管理体制で利用する場合、保存するデータに制限をかけている場合等においては、セキュリティ上の脅威の度合いや

[24] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
JISC サイト 「JIS 規格番号から JIS を検索」で「X19790」を入力すると閲覧可能
[25] NIAP サイトからダウンロード可能 https://www.niap-ccevs.org/pp/pp_usb_fd_v1.0.pdf
IPA サイト（翻訳版をダウンロード可能） https://www.ipa.go.jp/files/000015355.pdf

脅威そのものが変化するためである。極端な場合には脅威が想定されない場合もあり得るが、その場合には当該製品分野で求める暗号化機能そのものが不要である。

暗号化USBメモリには､内部に暗号化等を行うモジュールが組み込まれているので、暗号モジュールの情報セキュリティに対する要求事項に関する国際標準であるISO/IEC 19790 に基づいた認証をセキュリティ要件として活用することが可能である。（ISO/IEC 19790 と同等とみなせるFIPS 140-2 のSecurity Level 2 で認証を取得している製品は、既に複数流通している。）

また、ISO/IEC 15408 に基づくセキュリティ要件は、ソフトウェア製品及びハードウェアとソフトウェアを組み合わせた製品を対象として策定されたもので、ISO/IEC 19790 に基づくセキュリティ要件に追加して､ソフトウェア特有の脅威を想定した上で､求められる最低限のセキュリティ要件が規定されている。

このように規格の成り立ちは異なるが、調達対象となる製品の用途に応じて、セキュリティ要件を選択する必要がある。

なお、現在暗号化USBメモリに対するcollaborative Protection Profile が検討されており、近く完成する予定である。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下のIPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（USBメモリ）を参照し､「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/usb

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

電子政府推奨暗号リストに掲載されている暗号アルゴリズムを使用しており､かつ、以下のいずれかの認証を取得していること。

・ISO/IEC 19790（JIS X19790）のSecurity Level 2」の認証又は同等以上とみなせる認証（FIPS 140-2 のSecurity Level 2 の認証等）

・Protection Profile for USB Flash Drives (Version 1.0)と同等以上のセキュリティ要件に適合したISO/IEC 15408（Common Criteria）認証

・「Protection Profile for USB Storage Media （Version 1.4 (BSI-PP-0025-2006)以上)」と同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証

・「CSEC Protection Profile Encrypted Storage Device （Version 2.1 (FMV-PP-ESD)以上)」 と同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合：

（記載例）

電子政府推奨暗号リストに掲載されている暗号アルゴリズムを使用しており、かつ、以下のいずれかを満たすこと。

・「ISO/IEC 19790 （JIS X 19790）の[Security Level 2」又は同等以上とみなせる試験（FIPS 140-2 の Security Level 2 等）に合格していること。

・「Protection Profile for USB Flash Drives Version 1.0」で定義されたセキュリティ機能要件と同等以上の要件を満たしていること。

・「Protection Profile for USB Storage Media （Version 1.4 (BSI-PP-0025-2006) 以上)」で定義されたセキュリティ機能要件と同等以上の要件を満たしていること。

・「CSEC Protection Profile Encrypted Storage Device （Version 2.1 (FMV-PP-ESD)以上)」で定義されたセキュリティ機能要件と同等以上の要件を満たしていること。

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	ルータ／レイヤ３スイッチ

セキュリティ上の脅威	① <u>管理機能等への不正アクセスによる不正な通信の発生</u> 不正な通信を制御するための規則（セキュリティポリシー）等を管理する機能等に対してアクセス権限のない者が、正当な利用者になりすますことができれば、不正に操作される可能性がある。不正操作により、本来実施されるべき情報フロー制御が実施されず、組織内外からの不正な通信を排除できず、セキュリティ侵害に繋がる可能性がある。例えば、インターネット等のオープンな環境からの通信が、管理されるべき内部のネットワークへとアクセスされ、内部のネットワークに接続されるサーバ等が何らかの被害を受ける可能性がある。またインターネット等のオープンな環境に存在し、利用が禁止されているサービスに対して、内部のネットワークから通信し、秘匿されるべき情報が流失する等の可能性がある。
	② <u>リモートで管理する場合の通信データの盗聴、改ざん</u> 管理権限のある者が遠隔地からリモートで管理する際に、製品との間で通信されるセキュリティ関連情報を含むデータが盗聴、改ざんされる可能性がある。管理者パスワード等が盗聴により不正に取得された場合には、ファイアウォールの設定が不正に変更される可能性がある。
	③ <u>監査ログの改ざん・不正な削除</u> 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：Protection Profile for Network Devices v1.1 (PP_ND_V1.1) (ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様)	①, ②, ③
[2]：collaborative Protection Profile for Network Devices （v1.0 (CPP_ND_v1.0)以上 ） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③

（備考）[1] 及び[2]のセキュリティ要件は、ソフトウェアの更新を安全に行う機能も要求している。

【ルータ／レイヤ３スイッチに関する補足事項】

この製品分野は、OSI 基本参照モデル第 3 層（ネットワーク層）を利用し、情報システム及びネットワークの基盤においてデータを中継する機能を持った通信回線装置を対象としている。

ネットワーク基盤における重要なコンポーネントとして配置されるルータ／レイヤ３スイッチを含むネットワークデバイスに対する最低限のセキュリティ要件が策定されており、ISO/IEC15408(Common Criteria)に基づく認証を取得している製品がすでに

市場に流通している状況である。
　この他に、利用環境において「セキュリティ上の脅威」が存在する場合には、個別にセキュリティ要件を策定することや、運用面での対策を講じることが必要となる。
　例えば、ルータ／レイヤ３スイッチがファイアウォール機能や不正侵入検知及び防止機能、仮想プライベートネットワーク（VPN）機能を有する場合、本対象製品分野と併せて、追加の機能に対する対象製品分野において示されているセキュリティ上の脅威が想定されることがある。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】
　以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（ルータ／レイヤ３スイッチ　）を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。
　https://www.ipa.go.jp/security/it-product/nd

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】
① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。 ・Protection Profile for Network Devices v1.1（PP_ND_V1.1） ・collaborative Protection Profile for Network Devices　（v1.0（ND cPP v1.0）以上）

（検査方法例）
　提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）
　また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。
（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要

件が満たされていることを確認する場合：

（記載例）

以下のいずれかで定義されたセキュリティ機能要件と同等以上の要件を満たしていること。 ・Protection Profile for Network Devices v1.1 (PP_ND_V1.1) ・collaborative Protection Profile for Network Devices （v1.0 (ND cPP v1.0)以上）

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	ドライブ全体暗号化システム

セキュリティ上の脅威	① **許可されないデータアクセス** 紛失又は盗難にあったPCやタブレット等のドライブを取得した攻撃者は、ドライブ上のデータへのアクセスを試行する可能性がある。
	② **鍵材料の危殆化** 攻撃者は、暗号鍵、鍵生成に必要なパラメタ等の鍵材料を、ドライブ内、運用環境の他の周辺機器を探索して取得するかもしれない。また、攻撃者は、パスワードやPIN等の許可要素を推測し、データ暗号化鍵を取得し、利用者データを暴露する可能性がある。さらに、攻撃者は、鍵空間に対して総当たり攻撃を試行し、鍵及び鍵材料を取得し、利用者データを暴露する可能性がある。
	③ **ファームウェアの不正なアップデート** 攻撃者は、暗号化ドライブのセキュリティ機能を危殆化するようなファームウェアの不正なアップデートを試行する可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1] ISO/IEC 19790 (JIS X 19790) [ハードウェアは、Security Level 2以上、ソフトウェアはSecurity Level 1以上][26]	①, ②
[2]collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition (V1.0以上) 及びcollaborative Protection Profile for Full Drive Encryption - Encryption Engine (V1.0以上) (ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様)	①, ②, ③

【ドライブ全体暗号化システムに関する補足事項】

この製品分野は、ノートPC等のハードディスクドライブ、半導体ドライブなどのデータストレージ全体を暗号化するシステムを対象としている。一般的なITシステム構築における製品調達において、調達者が直接的にこれを調達するという事は少ないと言える。しかし、ノートPCやタブレットなどのハードディスクドライブ（HDD）等に対して暗号化機能を要求する場合に、上記セキュリティ要件の適用を推奨する。

上記セキュリティ要件に対するISO/IEC15408(Common Criteria)に基づく認証を取得している製品は、すでに市場に流通している状況である。

暗号モジュールの情報セキュリティに関する国際標準であるISO/IEC 19790に基づいた認証を活用することも可能である。

このように規格の成り立ちは異なるが、調達対象となる製品の特性に応じて、セキュリティ要件を策定する必要がある。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

[26] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
JISC サイト 「JIS 規格番号から JIS を検索」で「X19790」を入力すると閲覧可能

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（ドライブ全体暗号化技術）を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。（ISO/IEC 19790 と同等とみなして FIPS 140-2 で認証を取得している製品を採用する場合には別途確認する必要がある。）

https://www.ipa.go.jp/security/it-product/fd-enc

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

> 電子政府推奨暗号リストに掲載されている暗号アルゴリズムを使用しており、かつ、以下のいずれかの認証を取得していること。
> ・「ISO/IEC 19790（対応 JIS 規格 ：JIS X 19790）[ハードウェアは、Security Level 2 以上、ソフトウェアは Security Level 1 以上][27]（当面、FIPS-140-2 も対象とする）」の暗号モジュール認証
> ・「collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition （V1.0 以上） 及び collaborative Protection Profile for Full Drive Encryption - Encryption Engine （V1.0 以上）」と同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合：

[27] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
JISC サイト 「JIS 規格番号から JIS を検索」で「X19790」を入力すると閲覧可能

（記載例）

電子政府推奨暗号リストに掲載されている暗号アルゴリズムを使用しており、かつ、以下を満たしていること。 ・「ISO/IEC 19790（対応する JIS 規格 : JIS X 19790）[ハードウェアは、Security Level 2 以上、ソフトウェアは Security Level 1 以上][28]（当面、FIPS-140-2 も対象とする）」の暗号モジュール試験に合格している。 ・「collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition （V1.0 以上） 及び collaborative Protection Profile for Full Drive Encryption - Encryption Engine （V1.0 以上）」で定義されたセキュリティ機能要件と同等以上の要件。

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

[28] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
JISC サイト 「JIS 規格番号から JIS を検索」で「X19790」を入力すると閲覧可能

製品分野名	モバイル端末管理システム

セキュリティ上の脅威	① **ネットワークの盗聴** 攻撃者は、ネットワーク上の通信を傍受し、アクセスを取得し、データの暴露又は改変を試行する可能性がある。有線だけでなく、無線通信を傍受する可能性がある。
	② **ネットワークからの攻撃** 攻撃者は、無線通信チャネル又はネットワーク基盤上で、モバイル端末と他方の端点との通信を改変し、なりすましをする可能性がある。また、悪意のある管理コマンドを送信することによってモバイル端末の完全性の危殆化を試行する。
	③ **物理的アクセス** モバイル端末の紛失や盗難によって、認証情報を含む利用者データの機密性を危殆化する可能性がある。
	④ **悪意のあるアプリケーション** モバイル端末へロードされるアプリケーションには、悪意のあるコード又は悪用可能なコードが含まれる可能性がある。悪意のあるアプリケーションは、利用者データやシステムソフトウェアへの攻撃を試行し、特権を取得して悪意のあるアクティビティを実行する権利を取得する可能性がある。また、モバイル端末のセンサー（例、GPS、カメラ、マイクロフォン等）を制御し周囲の情報収集活動を行う手段を攻撃者に提供する可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1] Protection Profile for Mobile Device Management （Version 2.0 以上）及び Extended Package for Mobile Device Management Agents （Version 2.0 以上）（ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③, ④

【モバイル端末管理システムに関する補足事項】

この製品分野は、スマートフォンやタブレット等のモバイル端末の運用を管理するためのモバイル端末管理（MDM）サーバと、モバイル端末にアプリケーションとしてインストールされ MDM サーバと連係動作する MDM エージェントの二つの基本的な要素で構成されるモバイル端末管理システムを対象としている。

MDM サーバとして最低限満たすべきセキュリティ要件について定めたものが「Protection Profile for Mobile Device Management」である。また、モバイル端末の管理は、管理サーバと端末エージェントの組み合わせで実現されるため、さらに最低限満たされるべきセキュリティ要件として、「Extended Package for Mobile Device Management Agents」が定められている。

また、「IT 製品の調達におけるセキュリティ要件リスト」に規定されていない IT 製品を含むような場合、その利用環境に応じた脅威に対抗するために必要となるセキュリティ要件を調達側で独自に策定することが重要となる。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（モビリティ）を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/mobility

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

モバイル端末管理システムが、Protection Profile for Mobile Device Management（V2.0 以上）及び Extended Package for Mobile Device Management Agents（V2.0 以上）と同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合：

（記載例）

モバイル端末管理システムが Protection Profile for Mobile Device Management（V2.0 以上）及び Extended Package for Mobile Device Management Agents （V2.0 以上）で定義されたセキュリティ機能要件と同等以上の要件を満たしていること。

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。

製品分野名	仮想プライベートネットワーク（VPN）ゲートウェイ

セキュリティ上の脅威	① **許可されないデータアクセス** 保護されたネットワーク内のサービスに対する中間者攻撃やリプレイ攻撃によって、許可されない外部の攻撃者により不正にアクセスされ、利用者データや設定データの機密性及び完全性が危殆化する可能性がある。
	② **サービスの誤使用** VPN トンネルの設定ミスにより、サービスが適切に動作しない可能性がある。この場合、望ましい通信データの保護が行われず、意図しない弱い暗号化や平文での通信が行われることがある。
	③ **悪意のある更新** 悪用可能な共通攻撃ベクタのほとんどは、良く知られた欠陥を含むソフトウェアの脆弱性に対する攻撃を利用したものである。VPN ソフトウェアに対するタイムリーなパッチの適用を行うことで、脆弱性に対処することができる。 これに対して、攻撃者は、ルートキット、ボット、その他の悪意のあるコードを含んだアップデートのインストールを試行する可能性がある。悪意のあるコードを含むアップデートを IT 製品の管理者がインストールすることにより、セキュリティ機能が危殆化する可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1] Network Device Protection Profile(NDPP) Extended Package VPN Gateway （V1.1 以上）及び Network Device Protection Profile （v1.1 以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③
[2] Extended Package for VPN Gateways （V2.0 以上）及び collaborative Protection Profile for Network Devices （v1.0 以上） （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③

【仮想プライベートネットワーク（VPN）ゲートウェイに関する補足事項】

この製品分野は、仮想プライベートネットワーク(VPN)システムの終端に設置され、VPN 通信を提供するゲートウェイ装置を対象としている。

上記のセキュリティ要件について、ISO/IEC15408(Common Criteria)に基づく認証を取得している製品がすでに市場に流通している。

なお、利用環境において上記以外の「セキュリティ上の脅威」が存在する場合には、個別にセキュリティ要件を策定することや、運用面での対策を講じることが必要となる。例えば、ルータ／レイヤ３スイッチがファイアウォール機能や不正侵入検知及び防止機能、VPN 機能を有する場合、本対象製品と併せて、追加の機能に対する対象製品分野において示しているセキュリティ上の脅威が想定されることがある。

【本リストのセキュリティ要件について第三者認証を取得している製品の確認方法】

以下の IPA の「IT 製品の調達におけるセキュリティ要件リスト」適合製品情報（VPN 技術）を参照し、「国際標準に基づくセキュリティ要件」ごとの認証取得製品として列挙された製品が、当該セキュリティ要件で第三者認証を取得している製品である。

https://www.ipa.go.jp/security/it-product/vpn

【「国際標準に基づくセキュリティ要件」を活用する場合の調達仕様書への記載例と検査方法例】

① 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件とその要件に適合した第三者認証の取得を同時に求める場合：

（記載例）

以下のいずれかと同等以上のセキュリティ要件に適合した ISO/IEC 15408（Common Criteria）認証を取得していること。 ・Network Device Protection Profile(NDPP) Extended Package VPN Gateway（V1.1 以上)及び Network Device Protection Profile （v1.1 以上） ・Extended Package for VPN Gateways （V2.0 以上）及び collaborative Protection Profile for Network Devices （v1.0 以上）

（検査方法例）

提案時又は納入時に認証書（必要に応じて同等性を説明する資料を含む）を提出させ、その妥当性を確認する。国際標準に基づく第三者認証は製品の特定のバージョンに対して付与されるため、バージョンアップ後の製品は認証の対象外となるが、バージョンが変更された製品に対しては「保証継続」という仕組みがあり、保証継続報告書により補完されている場合がある。（Ｐ５②参照）

また、保証継続されていない場合には、ベンダに対しバージョンアップ等による変更がセキュリティ機能に影響を及ぼさないことを保証する資料を求め、その妥当性を調達者自身が確認し、バージョンアップがセキュリティ機能に影響を及ぼさないことを確認できれば、セキュリティ要件を満足していると考えることができる。

（注）IT 製品は、継続的にセキュリティ強化・修正のために、必要に応じて製品のバージョンアップを行うことが重要であり、保証継続にこだわりすぎる必要はない。

② 「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件は求めるが、第三者認証の取得を同時に求めない場合（納品時に調達側でセキュリティ要件が満たされていることを確認する場合：

（記載例）

以下のいずれかで定義されたセキュリティ機能要件と同等以上の要件を満たしていること。 ・Network Device Protection Profile(NDPP) Extended Package VPN Gateway（V1.1）及び Network Device Protection Profile （v1.1 以上） ・Extended Package for VPN Gateways（V2.0 以上)及び collaborative Protection

Profile for Network Devices （v1.0以上）

（検査方法例）

「国際標準に基づくセキュリティ要件」の内容を調達者が理解した上、受け入れテスト等でセキュリティ機能要件が満たされていることの検査を実施する。