IT 製品の調達における
セキュリティ要件リスト
活用ガイドブック

第 2.0 版

2018 年 2 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. はじめに

(1) 対象読者

本ガイドブックは「IT 製品の調達におけるセキュリティ要件リスト」（以下、「要件リスト」という）を活用して、安全な IT 製品を調達したい方を対象とし、特に以下のような立場の方向けの内容となっている。

① 政府機関において、IT システムや IT 製品の調達を担当しており、内閣官房情報セキュリティセンターが策定した「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」（以下、「政府統一基準」という）を参照して、調達要件を定めることを求められている方。
② 民間の企業・組織や地方公共団体に所属し、IT システムや IT 製品を調達する担当の方で、「要件リスト」を活用して、セキュアな IT 製品を調達したい方。

(2) 情報システムのライフサイクルにおける「要件リスト」の位置づけ

「政府統一基準」は、情報セキュリティに関する政府機関全体の統一的な枠組みを構築し、各府省庁の対策の斉一的な引き上げを図ることを目的としたものである。

「政府統一基準」には、情報システムのライフサイクルの各段階における対策として、企画・要件定義、調達・構築、運用・保守、更改・廃棄の各段階における対策が遵守事項として記されている。

「要件リスト」は、情報システムの構成要素となる IT 製品を調達する時に活用することとなる。

「要件リスト」は、「政府統一基準」の中で、機器等の調達にあたって参照することが遵守事項として規定されている。

第 5 部　情報システムのライフサイクル
5.2　　情報システムのライフサイクルの各段階における対策
5.2.1 情報システムの企画・要件定義
…
遵守事項
(2) 情報システムのセキュリティ要件の策定
…

(d)情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

※「政府機関の情報セキュリティ対策のための統一基準[1]」から引用

また、「政府統一基準」に準拠して府省庁対策基準を策定する際に参照するものとして「府省庁対策基準策定のためのガイドライン」が併せて内閣官房情報セキュリティセンターから公開されている。

「府省庁対策基準策定のためのガイドライン」は、各府省庁が情報セキュリティ対策基準を策定する際の手順や、統一基準の遵守事項を満たすために採られるべき基本的な対策事項の例示、考え方等を解説することを目的としたものであり、「要件リスト」に関しては以下のように記されている。

【 基本対策事項 】
＜5.2.1(2)(d)関連＞
5.2.1(2)-6
構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。

a) 「IT 製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「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を調達時のセキュリティ要件とすること。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

[1] 内閣官房情報セキュリティセンターの Web サイトからダウンロード可能
http://www.nisc.go.jp/active/general/index.html

2018/02/01 リンク先の有効性確認

※「府省庁対策基準策定のためのガイドライン[2]」から引用

民間の企業・組織や地方公共団体に所属する IT システムや IT 製品の調達担当者は、「要件リスト」及び本書を活用してセキュアな IT 製品を調達することが可能であるが、さらに「政府統一基準」及び「府省庁対策基準策定のためのガイドライン」を参照することで、情報システム全体のライフサイクルの各段階で「要件リスト」を活用する場面がより明確になるとともに、他に必要となる対策を確認することもできる。

[2] 内閣官房情報セキュリティセンターの Web サイトからダウンロード可能
http://www.nisc.go.jp/active/general/index.html

2018/02/01 リンク先の有効性確認

2. 「要件リスト」の基本的な活用方法

(1) セキュアな IT 製品を調達するためのフローについて

「要件リスト」では、IT 製品のセキュリティ要件を定めるために有用な情報が提供されている。利用者は、一般的な用途においては「要件リスト」の「国際標準に基づくセキュリティ要件」を指定することで、必要とされるセキュリティ要件を仕様に含めることができる。

「要件リスト」には、以下の図 1 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」が記載されている。

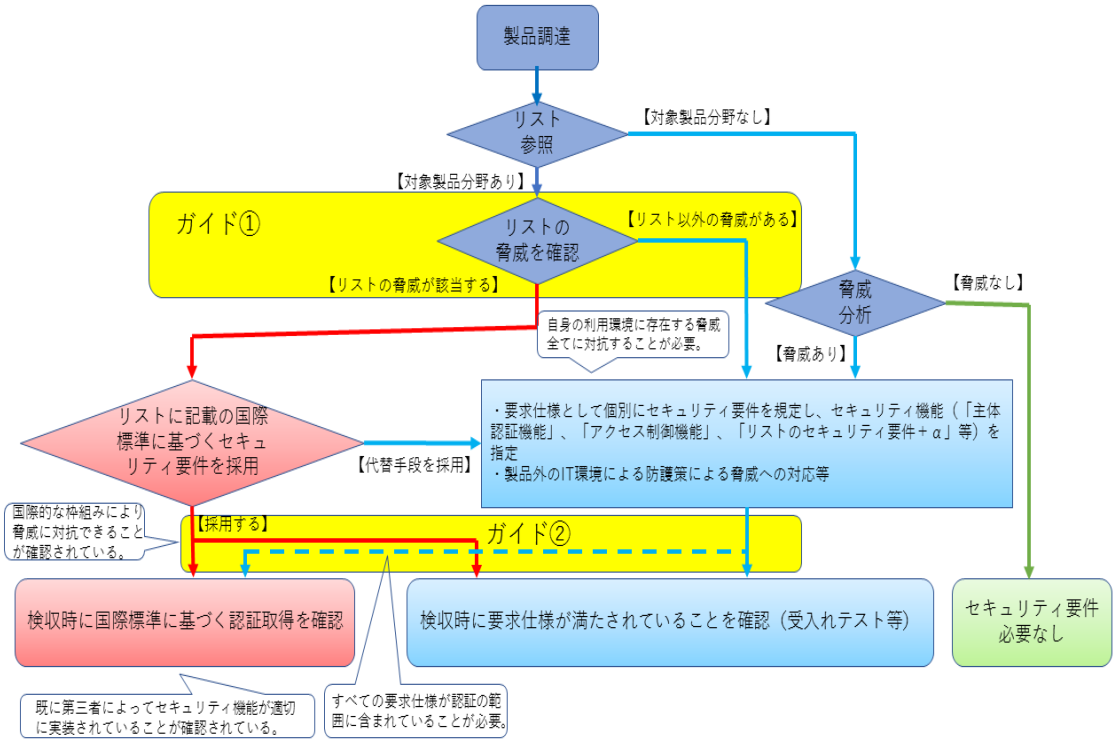

図 1　セキュアな IT 製品を調達するための大まかなフロー

フローの分岐における判断ポイントについて、図 1 のガイド①、ガイド②について具体例を用いて解説する。

(a) 「ガイド①」における判断ポイント

「ガイド①」については、従来からの IT 製品の調達におけるセキュリティ要件の策定時の脅威分析のプロセスである。

「要件リスト」に示されている「セキュリティ上の脅威」を参考にすることで、最低限考慮すべきセキュリティ対策を理解した上で、セキュリティ要件を適切に策定することができる。

- 【リストの脅威が該当する】の場合

  「要件リスト」に示されている「セキュリティ上の脅威」が該当する場合には、当該脅威に対して対抗することが必要となる。

  ただし、「セキュリティ上の脅威」に示されている脅威の内、1 部の脅威のみが該当する場合もあり得る。

  例えば、「要件リスト」の製品分野：OS（サーバ OS に限る）において、以下の表 1 に示すよう 5 つの脅威を記載している。

表 1　要件リストに記載している OS（サーバ OS に限る）のセキュリティ上の脅威

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）通りに各種操作（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。

OS を搭載しているサーバ装置が、不正な通信が発生することがない信頼できるネットワークのみに接続される場合には、上記の脅威の内③は該当しないと考えられる。

しかし、そのような場合においても①、②、④、⑤の脅威が該当するものとして残っている場合には、「国際標準に基づくセキュリティ要件」を活用することは有用となる。もちろん、「国際標準に基づくセキュリティ要件」をベースに③の脅威がない場合の要件を独自に策定しても良いが、相応の技術的な理解が必要である。

一方、上記に示した 5 つの脅威の内、1 つだけに対抗すれば良い場合などでは、「国際標準に基づくセキュリティ要件」をそのまま用いるのでは過剰な要件となることが考えられるため、実際の運用を想定した上で、調達側で過不足の無いセキュリティ要件を独自に策定することも選択肢の 1 つとなり得る。

- 【リスト以外の脅威がある】の場合

  「要件リスト」に示されている「セキュリティ上の脅威」は、当該製品分野において最低限考慮すべき脅威のベースラインであるが、IT 製品の利用・運用環境等を背景に、「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場合には、当該脅威に対抗する必要がある。

  この場合は、「国際標準に基づくセキュリティ要件」では対抗することが出来ない脅威であるため、システムや利用・運用環境によってその脅威を無効化するか、調達側で独自にセキュリティ要件を策定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」として示しているプロテクションプロファイル等では、製品を利用するにあたっての前提条件（利用環境、人的管理状況等）が示されているので、特に機密性が高い情報を扱うシステム等に用いる製品については、この前提条件を分析、確認することが望ましい。

（4 章 「(1)製品利用における前提条件（設置環境、利用形態、人員教育等）の確認」を参照。）

(b) 「ガイド②」における判断ポイント

「ガイド②」における判断ポイントは、採用した調達要件に対して、どうやってその要件を満たしていることを確認するかという点にある。

「ガイド②」の箇所においては、以下の 4 つのケースが考えられる。

① 「リストに記載の国際標準に基づくセキュリティ要件を採用」
⇒「検収時に国際標準に基づく認証取得を確認」

② 「リストに記載の国際標準に基づくセキュリティ要件を採用」
⇒「検収時に要求仕様が満たされていることを確認（受け入れテスト等）」

③ 「要求仕様として個別にセキュリティ機能を指定」
⇒「検収時に国際標準に基づく認証取得を確認」

④ 「要求仕様として個別にセキュリティ機能を指定」
⇒「検収時に要求仕様が満たされていることを確認（受け入れテスト等）」

以下に 4 つのケース毎の具体例を以下に示すので、実際の調達時にどのケースを選択するかの判断材料とされたい。

① 「要件リスト」の【「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】の①に該当する。
調達時に第三者認証の取得を求め、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）をベンダ等に提出してもらい、その妥当性を確認することや、調達者自身で当該製品が第三者認証を取得していることを Web ページ[3]等で確認することにより調達のフローが完結するため、要件策定及び納品検査において、調達側の負荷が低く抑えられた上で、セキュアな IT 製品を調達することが可能となる。

② 「要件リスト」の【「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】の②に該当する。
上記の①と異なり、第三者による評価・認証を求めていないため、調達者による納品検査作業が必要となる。実際に調達者が実施する場合には、「国際標準に基づくセキュリティ要件」の内容を調達側で理

[3] CCRA ポータルサイト　認証製品リスト
https://www.commoncriteriaportal.org/products/
IT セキュリティ評価及び認証制度　認証製品リスト
https://www.ipa.go.jp/security/jisec/certified_products/cert_list.html

解した上、受け入れテストにより要求仕様を満たしていることを確認するか、ベンダ等が実施したテスト／評価／同等性説明に関する資料の提出を要求し、その検査内容の確認等でセキュリティ機能要件が満たされていることを確認する必要がある。

しかし、調達側における技術的スキルや工数などの事情により、調達者が実施できない場合には、外部委託等を行うこと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認可された IT セキュリティ評価及び認証制度における評価機関[4]等を活用することが考えられる。

③ 「要件リスト」の「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を採用するが、第三者による評価・認証された製品を調達するケースである。

「要件リスト」で示されている「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 IT 製品も多数市場に流通している。

そのような認証取得製品も、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が、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確認することが必要となる。

必要なセキュリティ要件を含まずに認証されている場合には、不足のセキュリティ要件を調達仕様書等で別途示した上で、システム設計段階、または納品前までに当該要件に対する検査作業が必要となる。

④ 調達者が独自にセキュリティ要件を策定し、その要件が満たされていることを調達者が納品検査するケースであり、「要件リスト」を活用しない通常の調達フローとなる。

[4] IT セキュリティ評価及び認証制度　評価機関リスト
https://www.ipa.go.jp/security/jisec/eval-list.html

2018/02/01 リンク先の有効性確認

(2)「国際標準に基づくセキュリティ要件」と同等であることの確認

「要件リスト」では、「国際標準に基づくセキュリティ要件」を活用する場合において、以下のような調達仕様書への記載例と検査方法を例示している（デジタル複合機（MFP）の場合）。

【「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。[1]

・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）

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。

IT 製品によっては、「要件リスト」の「国際標準に基づくセキュリティ要件」ではなく、同等若しくはよりセキュリティ水準の高いセキュリティ要件を独自に策定し、第三者認証を取得している場合がある。

そのような製品においても、セキュアな IT 製品として調達対象に含めることは有用であり、第三者認証を取得しているため調達者の納品検査作業の負荷軽減にもつながる。

ただし、当該製品が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について認証されていることが前提であり、必要と考えるセキュリティ要件の一部を含まずに認証されている場合には、その不足しているセキュ

リティ要件について、提案、納品、検査のいずれかの時点で確認が必要となる。

ベンダ独自に策定したセキュリティ要件が「国際標準に基づくセキュリティ要件」と同等以上であることの確認は調達者に求められる。

提案時等に、ベンダに対して同等性に関する説明資料（例えば、以下の表 2 に示すような「国際標準に基づくセキュリティ要件」とベンダ独自のセキュリティ要件の比較表等）の提出を求め、その妥当性を確認する。

表 2　デジタル複合機（MFP）における同等性に関する説明資料例
（「国際標準に基づくセキュリティ要件」とベンダ独自のセキュリティ要件の比較表）

「要件リスト」に記載されているセキュリティ上の脅威	国際標準に基づくセキュリティ要件	対応する製品のセキュリティ機能（例）
①他の利用者による不正な操作	・利用者の識別認証機能 （ログイン機能等） ・利用者データ保護機能 （アクセス制御機能等）	・ユーザ認証機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）
②通信データの盗聴、改ざん	・通信データ暗号化機能 （各種暗号通信プロトコル） ・外部インタフェース制御機能 （FAX から内部ネットワーク間の不正データ転送禁止等）	・ネットワークデータ保護機能 ・ファックスフローセキュリティ機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）
③管理機能への不正なアクセス	・セキュリティ管理機能	・管理者セキュリティ管理機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）
④複合機のソフトウェアの改ざん・破損	・自己テスト機能 （完全性検証機能等）	・自己テスト機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）
⑤監査ログの改ざん・不正な削除	・セキュリティ監査機能 （監査データ生成機能、監査ログのレビュー機能・保護機能、タイムスタンプ機能等）	・セキュリティ監査ログ機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）

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、または廃棄処理時）	・残存情報保護機能（HDD/SSD等の残存データを利用不能にする機能等）	・HDD データ上書き消去機能 ・HDD データ暗号化機能 （その他にベンダ独自のセキュリティ機能がある場合もあり得る）

(3) 他のガイドライン等との関係

IT 製品及び IT システムの調達に関しては、様々な組織から各種ガイドライン、マニュアル等が公開されている。

ここでは、以下のガイドライン、マニュアルについて解説する。

- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル[5]

政府調達においては「情報セキュリティを企画・設計段階から確保するための方策（SBD: Security By Design）に係る検討会」において、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（以下、「SBD マニュアル」という）がまとめられ、公開されている。

「SBD マニュアル」は、「情報システムに係る政府調達の基本指針[6]（以下、「調達指針」という）に基づいて情報システムを調達する際に、セキュリティ要件の策定にあたって活用されることが想定されている。

「SBD マニュアル」は、政府機関における情報システムの調達仕様書に記載する「セキュリティ要件」の策定方法を解説することによって、情報システムの企画段階からセキュリティ対策を適切に組み込むことを目的としている。

以下に示す表 3 は「調達指針」において定められている「調達仕様書」に記載する事項であり、「SBD マニュアル」が対象とする記載箇所は、主に「5 信頼性要件」、「6 情報セキュリティ要件」、「8 テスト要件定義」、「10 運用要件定義」及び「11 保守要件定義」となっている。

「要件リスト」ではそのうち、主に「6 情報セキュリティ要件」、「8 テスト要件定義」に関して活用可能であるため、以下に「要件リスト」活用の際の注意点を解説する。

---

[5] 内閣官房情報セキュリティセンターの Web サイトからダウンロード可能
http://www.nisc.go.jp/active/general/sbd_sakutei.html

[6] 総務省の Web サイトからダウンロード可能
http://www.soumu.go.jp/main_content/000070266.pdf

2018/02/01 リンク先の有効性確認

表 3　調達指針が定める調達仕様書に記載する事項

項目		主な記載内容
1	調達件名	情報システムに係る工程名
2	作業の概要	(1) 目的、(2) 用語の定義、(3) 業務の概要、(4) 情報システム化の範囲、(5) 作業内容・納入成果物
3	情報システムの要件	(1) 機能要件、(2) 画面要件、(3) 帳票要件、(4) 情報・データ要件、(5) 外部インタフェース要件
4	規模・性能要件	(1) 規模要件、(2) 性能要件
5	信頼性等要件	(1) 信頼性要件、(2) 拡張性要件、(3) 上位互換性要件、(4) システム中立性要件、(5) 事業継続性要件
6	情報セキュリティ要件	(1) 権限要件、(2) 情報セキュリティ対策
7	情報システム稼働環境	(1) 全体構成、(2) ハードウェア構成、(3) ソフトウェア構成、(4) ネットワーク構成、(5) アクセシビリティ要件
8	テスト要件定義	要求仕様の適合性を検証するためのテストに係る要件
9	移行要件定義	(1) 移行に係る要件、(2) 教育に係る要件
10	運用要件定義	(1) システム操作・監視等要件、(2) データ管理要件、(3) 運用施設・設備要件
11	保守要件定義	(1) ソフトウェア保守要件、(2) ハードウェア保守要件
12	作業の体制及び方法	(1) 作業体制、(2) 開発方法、(3) 導入、(4) 瑕疵担保責任
13	特記事項	その他、特記すべき要件
14	妥当性証明	調達仕様書の妥当性を確認した調達担当課室の長の氏名

(4) 認証取得見込み（セキュリティ評価中）製品を調達する場合の注意点

IT 製品が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、調達時に国際標準に基づく第三者認証の取得を求める場合に、調達対象となる製品が認証取得中（セキュリティ評価中）であることが考えられる。

しかし、必ずしもベンダからの製品提案時に第三者認証が取得されている必要性はなく、例えば納品検査において第三者認証が取得されていることでセキュリティ要件を満たしていることを確認する場合においては、検査時までに第三者認証を取得していればよい。

そのため、調達時の要件として、提案時に第三者認証を取得していなくても、ある期日までに第三者認証を取得していれば良いとする「認証取得見込み」を選択肢に含めることも考えられるが、その場合には、セキュリティ評価の結果、最終的に第三者認証が取得できなかった場合の対処を勘案した上で、いつまでに認証取得していなければならないかを定めた要件とすべきである。

最終的に第三者認証が取得できなかった場合の対処としては、以下のような対策を講じられることが考えられるが、瑕疵担保責任に関する条件は、利用する情報システムの重要度に合わせて調達側で吟味する必要がある。

- 提案時に指定日までに第三者認証が取得できなかった場合の代替案を受注側に提出させ、発注側でその内容を確認する。
  （代替案としては、指定日までに第三者認証が取得できなかった場合には、同等以上の性能を有する他の認証取得製品を納入させることなどが考えられる。）

なお、認証取得見込み（セキュリティ評価中）製品の調達を検討する際には、以下の表 4 に、現在セキュリティ評価中の製品が掲載されている各国の認証制度における評価中製品リストを参考にされたい。

表 4　各国の認証制度における評価中製品リスト

認証制度を運営している国	評価中製品リスト
日本	https://www.ipa.go.jp/security/jisec/certified_products/in_eval_list.html　（製品分野「ソフトウェア」） https://www.ipa.go.jp/security/jisec/hardware/hw_in_eva_list.html（製品分野「ハードウェア（スマートカード等）」）
カナダ	https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/publication/list/evaluation-product
フランス	https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/les-evaluations/　（フランス語 Web サイト）
ドイツ	https://www.bsi.bund.de/EN/Topics/Certification/incertification.html
イギリス	https://www.ncsc.gov.uk/index/certified-product?f%2525B0%2525255D=field_assurance_statusZAssured&f%5B0%5D=field_assurance_status%3AIn%20Evaluation （「Filter」欄の「Assurance Status」を「In Evaluation」にする。）
アメリカ	https://www.niap-ccevs.org/CCEVS_Products/in_eval.cfm
オーストラリア ニュージランド	http://www.asd.gov.au/infosec/epl/index.php （Web サイト下部の「In Evaluation」に掲載）
ノルウェー	http://sertit.no/productsearch/ （「Text search」欄に検索ワード入力もしくは「Product type」を選択した後に、「Status」欄を「Under evaluation」にし「Search」ボタンを選択））
イタリア	http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione　（イタリア語 Web サイト）
マレーシア	http://www.cybersecurity.my/mycc/mycprC.html
インド	http://www.commoncriteria-india.gov.in/productinevaluation.php
オランダ	http://www.tuv-nederland.nl/nl/38/ongoing_certifications.html
韓国	評価中の製品リストは未公開
スウェーデン	http://fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/In-evaluation-list/

トルコ	評価中の製品リストは未公開

2018/02/01 リンク先の有効性確認

3. IT 製品分野毎の「要件リスト」の活用例・注意点

(1)　情報システム構築時の注意点

「要件リスト」に記載している製品分野では、既に情報システムの構成要素として稼働しているものをリプレースする際に製品単体で調達する場合もある一方、情報システムを新規に構築する際若しくは情報システム全体をリプレースする場合等では、システム全体の仕様をまず検討した中で、応札等で提案として提示する場合、構成要素となる製品を選択することが考えられる。

以下に、システム全体を調達する場合と製品を単体で調達する場合について「要件リスト」の活用の仕方について解説する。

(a) 情報システム全体を調達する場合

情報システムを全体で調達する場合においては、「要件リスト」に記載している「ファイアウォール」、「不正侵入検知/防止システム（IDS/IPS）」、「OS（サーバ OS に限る）」、「データベース管理システム（DBMS）」の製品分野では他の情報システムの構成要素との依存関係等を考慮した上で製品を選択する場合があり得る。

図 2 に情報システムの構成例として、支部/支社から専用線で送られてきたデータを収集して、本庁/本社で統計処理し、Web 上で公開する情報システムを示す。

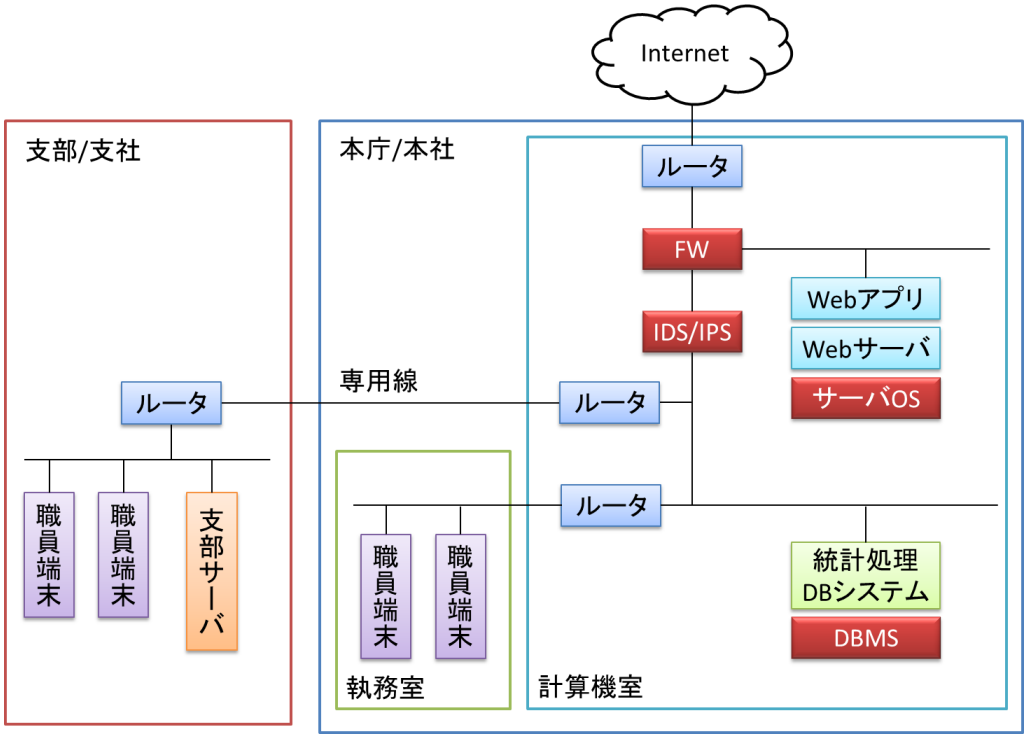

図 2　情報システムの構成例

構成例と示した情報システムの中には、「要件リスト」に記載している製品分野の製品が含まれるので、「要件リスト」の「国際標準に基づくセキュリティ要件」を調達時の要件として活用することができる。

しかし、例えばサーバ OS では Web サーバ、Web アプリとの依存関係より OS の種別が限定される場合や、ファイアウォール、IDS/IPS ではネットワーク構成により、「要件リスト」の「セキュリティ上の脅威」が必ずしも存在しない場合が考えられる。

そのような場合には、情報システム稼働環境、運用要件、拡張性要件、上位互換性要件等を考慮した上でセキュリティ要件を提示する必要がある。

そのような場合において、情報システム全体の調達の中で「要件リスト」を活用したい時の調達仕様書の記載例を以下に示す。

【システム全体として共通的なセキュリティ要件とする場合の記載例】

構築する情報システムの構成要素となる機器及び導入するソフトウェアの内、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている製品分野であり、且つ「IT

製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」が 1 つ以上存在する環境に設置・導入される製品については、それぞれ以下のいずれかの要件を満たすこと。

① 「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「国際標準に基づくセキュリティ要件」に準拠した第三者認証を取得していること

② 「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」の内、システム稼働環境において存在する脅威に対抗するためのセキュリティ機能が実装されていることを受注者が示すこと

ただし、システム稼働環境において「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「セキュリティ上の脅威」以外の対抗すべき脅威が当該製品に存在している場合においては、存在する全ての脅威に対抗できるセキュリティ機能が実装されていることを受注者が示すこと。

なお、情報システムに含まれる IT 製品単位に対する脅威が存在しない場合でも、情報システム全体としては、その脅威が該当する場合が有る。

調達者は IT 製品単体のセキュリティ要件のほか、システム全体での脅威の有無を評価する必要が有る。

(b) 製品を単体で調達する場合

前提として、IT 製品単体を調達する場合においても、既存の情報システムに新たに組み込む場合には、既存の情報システムに対してセキュリティ上の影響を分析した上で調達することが必要となる。

その上で、「要件リスト」に記載の製品分野について以下に注意点を解説する。

(2)　デジタル複合機に関する注意点

(a)「要件リスト」が対象とする製品モデル

「要件リスト」で定義しているデジタル複合機は用途・機能等でモデル分けがされており、市場に流通している製品のモデルとしては、以下の表 5 に示す[A]～[D]のモデルが想定される。

表 5　デジタル複合機のモデルと「要件リスト」活用の可否

モデル		「要件リスト」活用の可否
[A]	印刷等業務向けプロダクションプリンター	×
[B]	オフィス向け大型複合機	○
[C]	小規模オフィス（SOHO）向け小型複合機	△
[D]	家庭向けインクジェット複合機（プリンタ）	×

※　○：「要件リスト」における製品分野「デジタル複合機（MFP）」で想定されるモデル。

△：「要件リスト」を活用することが可能な場合もある。活用には注意が必要。

×：現状では活用できる製品はほとんど存在していないため、そのまま活用するのは困難。

上記の内、[B]のモデルでは、「要件リスト」に記載している国際標準に基づくセキュリティ要件に準拠した認証取得製品が市場に多く流通しているため、「要件リスト」を活用することがセキュアな製品を調達することの近道となる。

一方、[A]、[C]、[D]のモデルは「要件リスト」に記載している国際標準に基づくセキュリティ要件に準拠した認証取得製品はあまり市場に流通していないため、「要件リスト」を活用して調達することは困難となる。

[A]、[C]、[D]のモデルを調達する際の注意点を以下に示すので、調達時に活用されたい。

[A]：印刷等業務向けプロダクションプリンター：

[B]のモデルに比べ、印刷スピードが高速、高精細な印刷が可能であること、図面等 A2 サイズ以上の印刷が可能であること等が特徴であるモデルのため、用途としては[B]とは異なり、組織内のネットワーク上で共有されず、限られた印刷業務専用オペレータのみが利用可能な環境で利用することが考えられる。

[B]のモデルで実装されているセキュリティ機能が、[A]のモデルでは実装されていない場合もあるため、調達仕様書で[B]と同様のセキュリティ要件を示したとしても、調達できる製品が限られるあるいは存在しない場合が考えられる。

[A]のモデルの調達時のセキュリティ要件の策定にあたっては、「要件リスト」に記載されているセキュリティ上の脅威を参考にした上で、物理的な設置環境、論理的なネットワーク環境を適切に構築すること、搭載されているリモート管理機能を業務上使用しないこと、暗証番号などを設定すること等により、業務遂行にあたってセキュリティ上の脅威が発生しない利用環境を構築することが重要となる。

[B]：オフィス向け大型複合機

「要件リスト」に記載している国際標準に基づくセキュリティ要件が活用可能なモデルである。市場には、国際標準に基づくセキュリティ要件に準拠し且つ第三者認証を取得している製品が数多く流通している。

ただし、安全な製品を調達したとしても、ファイアウォールで保護されていない環境に設置されるなど、国際標準に基づくセキュリティ要件の想定外の運用環境で利用された場合にはセキュリティの確保が困難になる。

後述する「(b)オプション機能」や、4章「調達したIT製品の利用・運用時の注意点」の「(1)製品利用における前提条件（設置環境、利用形態、人員教育等）の確認」等を確認した上で、認証取得時の前提条件保たれるように運用環境を適切に整備することが重要となる。

[C]：小規模オフィス（SOHO）向け小型複合機

一般的に、プリンタ、スキャン、FAX、コピー機能を有している製品が多いが、[B]のモデルに比べ、内蔵ストレージ（HDDやSSD）が搭載されていない製品が多く流通している。

そのため、[B]のモデルで想定される脅威（「要件リスト」のセキュリティ上の脅威④、⑥等）が、[C]のモデルでは想定されない製品も多くなる。

（ただし、内蔵ストレージ（HDDやSSD）が搭載されている製品では、当然「要件リスト」のセキュリティ上の脅威④、⑥等は想定される。）

一方、ネットワークへの接続環境によっては、「要件リスト」のセキュリティ上の脅威②、複数の利用者が使用できる環境に設置される場合には「要件リスト」のセキュリティ上の脅威①、③、④等が脅威として想定される。

[C]のモデルを調達するにあたっては、[B]と同等の機能を備えている場合には、「要件リスト」に記載している国際標準に基づくセキュリティ要件が活用できるが、それ以外の製品については、自身の利用環境に応じて以下のセキュリティ機能等を要件とすることを検討すべきである。

- 溜置き印刷（セキュアプリント）機能
- 通信データの暗号化機能
- 管理者・利用者の識別認証機能
- 監査ログの保護機能

なお、製品の特性上、無線 LAN 環境での利用が想定されるが、その場合には、適切なセキュリティ設定を行うことが必要となる。

[D]：家庭向けインクジェット複合機（プリンタ）

製品の構造としては[C]のモデルに近く内蔵ストレージ（HDD や SSD）が搭載されていない製品が多く流通しており、その場合には[C]のモデルと同様に、要件リスト」のセキュリティ上の脅威④、⑥等は想定されない。

さらに、個人利用を想定している製品の特性上、複数の利用者が存在するオフィス環境で必要となるセキュリティ機能が実装されていない製品が多い。

そのため、[D]のモデルでは「要件リスト」に記載されているセキュリティ上の脅威を参考にした上で、脅威が存在しない利用環境で使用することが重要となる（例えば、管理者・利用者のデスクサイドで利用する等）。

オフィス環境で複数の利用者が共用で利用する場合には、[B]のモデルなどの調達を検討すべきである。

なお、製品の特性上、無線 LAN 環境での利用が想定されるが、その場合には、適切なセキュリティ設定を行うことが必要となる。

(b) オプション機能について

デジタル複合機では、FAX やスキャン機能がオプション機能として扱われている場合があり、FAX やスキャンのオプション機能が含まれた状態で、ISO/IEC 15408（Common Criteria）認証を取得している製品もある。

調達側の機能要件として特に FAX 等のオプション機能を求めていない場合において、ISO/IEC 15408（Common Criteria）認証取得を求める場合の判断基準として「要件リスト」には以下の内容を記載しているので参考にされたい。

【「要件リスト」P8　脚注 6 の内容】
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。

(c)「要件リスト」に掲載している国際標準に基づくセキュリティ要件について

「要件リスト」には、デジタル複合機（MFP）の国際標準に基づくセキュリティ要件として、[1]、[2]、[3]の 3 種類の国際標準に基づくセキュリティ要件を記載している。

以下の表 6 にそれぞれの概要を記す。

表 6　デジタル複合機（MFP）の国際標準に基づくセキュリティ要件とその概要

国際標準に基づくセキュリティ要件	概要
[1]：IEEE Std 2600.1™-2009,Protection Profile for Hardcopy Devices,Operational Environment A Version 1.0[7]	IEEE Std 2600.1™-2009 は、高度な文書セキュリティ、運用上の説明責任、情報保証が要求され、企業秘密等を取り扱う基幹業務等で運用される、デジタル複合機の要求仕様に係る標準規格。
[2]：U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0（IEEE Std. 2600.2™-2009)[8]	IEEE Std 2600.2™-2009 は、一般的な文書セキュリティ、ネットワークセキュリティ、セキュリティ保証が要求され、日常的な文書等を取り

[7] CCRA ポータルサイト経由で IEEE 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 の Web 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
[8] CCRA ポータルサイト経由で IEEE 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

2018/02/01 リンク先の有効性確認

	扱う環境で運用される、デジタル複合機の要求仕様に係る標準規格。 尚、左記は NIAP CCEVS Policy #20[9] により IEEE Std 2600.2™ -2009 を拡張し、IEEE Std 2600.1™ -2009 と同等のセキュリティ機能要件となるよう拡張されている。
[3]：Protection Profile for Hardcopy Devices （Version 1.0[10]以上）	日本、米国政府においてデジタル複合機の政府調達のためのセキュリティ要件として使用することを目的に作成された国際標準。日米認証機関主導のもと、デジタル複合機ベンダ、評価機関により構成される MFP TC（Multifunction Printers Technical Community）によって策定された。

[1][2]はともに IEEE から発行され、[1]は機微な情報を扱う高度なセキュリティ環境での使用を想定し、[2]はより一般的なデータの扱いを想定したセキュリティレベルを要求している。扱うデータの種類や運用環境によって調達者は[1]か[2]を選択するが、多くの調達では[2]で十分とみなされている。
[3]は[1][2]での実績を踏まえて、より実効的でかつ効率的な評価項目に焦点を当てており、ベンダ及び調達者にとって最低限のセキュリティ要件を満たした認証製品のタイムリーな供給と調達が可能となることから、今後の調達の主流となることが期待されている。

[9] NIAP の Web サイトからダウンロード可能
https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/archived/policy-ltr-20.pdf
[10] 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

2018/02/01 リンク先の有効性確認

(3)　サーバ OS の調達

情報システムの他の構成要素との依存関係から、調達対象となる製品が限定されることが考えられる。例えば、サーバ OS では、情報システムの特性により OS の種別が限定されることが考えられるが、「要件リスト」では OS の種別を選択できるように、表 7 に示すように、複数の「国際標準に基づくセキュリティ要件」を提示している。

表 7　OS（サーバ OS に限る）の国際標準に基づくセキュリティ要件と当該要件に準拠した認証取得製品

国際標準に基づくセキュリティ要件	市場に流通している第三者認証取得製品の例
[1]：Operating System Protection Profile BSI-CC-PP-0067 Version 2.0[11]	SUSE Linux、Red Hat、IBM AIX 等の Linux、Unix 系の製品等において複数の認証取得製品が存在している。
[2]：US GOVERNMENT PROTECTION PROFILE FOR GENERAL-PURPOSE OPERATING SYSTEMS IN A NETWORKED ENVIRONMENT Version 1.0[12]	Windows 7、Windows Server 2008、Linux 系の製品等で認証取得済み。
[3]：General-Purpose Operating System Protection Profile Version: 3.9[13]	Windows 8, Windows RT, Windows Server 2012 等で認証取得。
[4]：Protection Profile for General Purpose Operating Systems （Version 4.1, PP-OS-v4.1 以上）	Windows 10, Windows Server 2012 R2 等の認証取得製品が存在している。

サーバ OS に関して「要件リスト」の国際標準に基づくセキュリティ要件に準拠した第三者認証を取得している製品を調達したい場合には、表 7 及び「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リスト」（OS（サーバ OS に限る））[14]を参照し、適切なセキュリティ要件を選択されたい。

---

[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 の Web サイトからダウンロード可能
https://www.niap-ccevs.org/pp/pp_gpos_v3.9.pdf
[14] IPA の Web サイトからダウンロード可能
https://www.ipa.go.jp/security/it-product/os

2018/02/01 リンク先の有効性確認

(4)　ファイアウォール、IDS/IPS の調達

ファイアウォール及び IDS/IPS を単体で調達する場合に注意すべき点として、近年では、複数のセキュリティ機能を統合的に管理する UTM（Unified Threat Management, 統合脅威管理）が広く流通している。

UTM では、ファイアウォールや IDS/IPS の他にも VPN、アンチウイルス、Web フィルタリングなどの機能が 1 台の機器に実装されているため、従来の単機能のファイアウォールや IDS/IPS を利用するのに比べ、購入コストや管理コストを抑えられるメリットから、利用される場面も多い。

しかし、多機能であるが故に、悪意のある第三者に乗っ取られた場合などは、被害範囲も広範囲に及ぶため、従来以上に UTM 自身に対するセキュリティ対策が必要となってくる。

「要件リスト」には、ファイアウォール及び IDS/IPS に関する「セキュリティ上」の脅威を示しているが、ファイアウォール機能、IDS/IPS 機能を実装する UTM においても当然あてはまる脅威となるため、調達時に活用することが可能である。

ただし、活用可能であるのは、あくまでファイアウォール及び IDS/IPS に関するセキュリティ要件であり、その他の VPN、アンチウイルス、Web フィルタリング等に関するセキュリティ要件は必要に応じて調達者が独自にセキュリティ要件を追加する必要がある。

(5)　ドライブ全体暗号化システムの調達

「ドライブ全体暗号化システム」の実現形態としては、ハードウェアと、ソフトウェアの 2 種類に大別できる。ハードウェアによる暗号化には、HDD や SSD などのドライブ単体で実現しているもの、RAID 装置、SAN、NAS などの複数のドライブで実現しているもの、あるいは、サーバに装着する HBA カードなどで実現するものなどが考えられる。

一方、ソフトウェアによる暗号化には、OS レベル又はプリブート実行環境を使ったものなどがある。

次の表は、「国際標準に基づくセキュリティ要件」と同等のセキュリティ要件に適合しているとして、当面認められるレベルにある製品の例を示したものである。

表 8

ドライブ全体暗号化システムの実現形態		市場に流通している 第三者認証取得製品の例[15]
ハードウェア	ドライブレベルでの実現形態	Toshiba MQ01ABU050, MQ01ABU032, MQ01ABU025
ソフトウェア		Bitlocker ドライブ暗号化を有効化した Microsoft Windows 10, Microsoft Windows Server 16 が稼働している環境。 Check Point Full Disk Encryption が稼働している環境。

この表では、ハードウェアによる暗号化に関して、複数のドライブで実現している製品分類に対する共通的なセキュリティ要件は現在整理されていないため、ドライブ単体で実現しているものの例を記載している。

[15] 当面、対象としている FIPS 140-2 に適合し、かつ市場に流通している製品の例を記載している。

(6)　IC カードのセキュリティ要件の策定

IC カードは、施設への入退出、個人の証明書、交通・金融等の様々な用途で用いられるが、用途毎に保護すべき資産が異なるため、想定される脅威や対策は異なる。

IC カードに求められるセキュリティ要件は、利用される情報システム、保護すべき資産、想定される脅威等を十分検討した上でそれぞれ独自に策定することが必要となる場合が多い。

（セキュリティ機能が不十分であることは当然問題となるが、不必要（過剰）なセキュリティ機能は不要なコストを計上することに繋がりかねない。）

ここでは、IC カードにセキュリティ要件を求める場合においての注意点を解説する。

IC カードは製品の構成上、IC チップに求められるセキュリティ要件と IC カード（IC チップにアプリケーション・ソフトウェアを搭載し、カード形状としたもの）に求められるセキュリティ要件が異なる。

そのため、IC カードの調達者は搭載する IC チップを考慮した上で、IC カードのセキュリティ要件を策定することが必要となる。具体的な内容の検討にあたって、ISO/IEC15408 に基づく第三者認証を前提として IC カードのセキュリティ要件を策定しようとする場合には、以下の認証機関[16]もしくは、IT セキュリティ評価及び認証制度（JISEC）における評価機関（ハードウェア）[17]に問い合わせることで相談することが可能である。

IC カードのセキュリティ要件に関連する状況について補足すると、IC カードに対するセキュリティ要件を定めた現在のプロテクションプロファイルの多くが、評価保証レベル(EAL:Evaluation Assurance Level)4 以上を標準的に要求している。

一方で、現在の CCRA の相互承認の枠組みでは、本ガイドブックの 5.(3)で言及する cPP によらない場合、相互承認範囲は EAL2 までとされている。これは、言い換えると、海外の認証スキームで仮に EAL4 以上で評価認証された IC カードであっても、日本として見た場合には EAL2 という扱いになる。

---

[16] IT セキュリティ評価及び認証制度　ハードウェア（スマートカード等）評価・認証
https://www.ipa.go.jp/security/jisec/hardware/index.html　（ページ下部に問い合わせ先を掲載）

[17] IT セキュリティ評価及び認証制度　評価機関リスト（ハードウェア）
https://www.ipa.go.jp/security/jisec/hardware/hw_ef_list.html

2018/02/01 リンク先の有効性確認

ICカードに対する調達の条件として、EAL4以上のセキュリティ要件を設けようとする場合に、調達側は、予めこの制約条件についても承知しておくべきである。

加えて、ICカードのセキュリティ要件を一旦策定した後、次に挙げるような様々な要因から、そのセキュリティ要件を見直さなければならない状況が発生することが想定される。

- 機能の追加/変更/削除
- 新しい攻撃又は当初想定しなかった脆弱性への対処
- 暗号の危殆化
- 運用の変更

そのような場合には、速やかに認証機関に相談すべきである。調達者は、認証機関と相談し、セキュリティ要件を適宜見直すことによって、説明責任を継続的に果たしていくことが重要である。

(7)　暗号化 USB メモリの調達

USB メモリはその携帯性から、様々な利用環境で用いられるため、利用環境毎に想定される脅威は異なる。

USB メモリを管理している組織の外部に持ち出すことが可能な環境（第三者が容易にアクセスできる環境）と、人的・組織的に厳重に管理され、アクセス制限がかけられた環境では想定される脅威が異なるため、それぞれの脅威毎にセキュリティ要件を検討する必要がある。

また、USB メモリに関するセキュリティ対策としては、USB メモリ自体の暗号化機能等で想定される脅威に対抗する場合もあれば、情報システム側で接続された USB メモリに対して暗号化を実施する機能を実装することや、情報システムに接続できる USB メモリを制限することなど厳格な制御を行うことで想定脅威を減少させる方法等も考えられる。

「要件リスト」は、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暗号化 USB メモリを対象としており、ここでは、その調達に関する注意点、及び「要件リスト」に掲載している国際標準に基づくセキュリティ要件について解説する。

(a) 調達に関する注意点

例えば、PC に接続する外部ストレージに対して、書き込み禁止等のアクセス制御を行う制御ソフトウェアを導入し、USB メモリ経由で外部に情報が持ち出されないようにすることや、USB メモリへのデータ書き込み時に自動的に暗号化を実施することで、暗号化機能を備えていない USB メモリが放置・紛失・盗難等の理由で所有者以外の手に渡った場合においても、情報漏えいが発生しないように情報システム側で対策が講じられている場合もある。このように、情報システム側で書き込みデータの暗号化等が行われる場合においては、USB メモリ自体に暗号化機能を求めることは過剰なセキュリティ要件となることも考えられる。

(b)「要件リスト」に掲載している国際標準に基づくセキュリティ要件について

「要件リスト」では、国際標準に基づくセキュリティ要件として以下の[1]と[2]の 2 つの国際標準に基づくセキュリティ要件を記載している。

各国際標準に基づくセキュリティ要件の概要を以下の表 9 で解説する。

表 9　USB メモリの国際標準に基づくセキュリティ要件の概要

国際標準に基づくセキュリティ要件	概要
[1]：ISO/IEC 19790 （対応する JIS 規格 ： JIS X 19790） [Security Level 2 以上][18]	攻撃者が放置または盗難 USB メモリ（USB フラッシュドライブ）を入手したとして、その中のデータを暗号化し、暗号鍵への物理的・論理的アクセスを保護・制御することができれば、暗号化される前の平文のデータを復元することはできない。 ISO/IEC 19790 では、暗号を実現するための暗号鍵が主たる保護資産であるという考えの下、暗号鍵を物理的・論理的に保護することが求められている。 ISO/IEC 19790 の Security Level 2 以上では、利用者認証にグループ又は個人を識別する認証メカニズムが求められる。 物理的な保護としては、内部構造の解析や内部を流れる信号のプロービングを妨げる、金属または硬いプラスチック製の囲いが求められる。 また、暗号化 USB メモリ（USB フラッシュドライブ）内部に組み込まれるファームウェアを更新できる場合、ファームウェアが悪意のあるファームウェアに書き換えられないように、暗号を用いて真正性が確認できるファームウェアのみを暗号化 USB メモリ（USB フラッシュドライブ）内に展開できる機能が求められる。 ISO/IEC 19790 では、暗号を実現する部分のセキュリティを対象としており、それ以外の、（例えば、悪意のあるソフトウェアがコンピュータに展開させないといった、）暗号化 USB メモリ（USB フラッシュドライブ）が接続されるコンピュータのセキュリティを扱っていない。

[18] 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
http://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
2018/02/01 リンク先の有効性確認

[2]：Protection Profile for USB Flash Drives Version 1.0[19] (ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様)	(1)：組織が2つのデバイス間で情報を転送する、 (2)：単一利用者がデバイスにファイルを保存する、 というUSBメモリ（USBフラッシュドライブ）の2つの使用シナリオが想定されている。 攻撃者が放置または盗難USBメモリ（USBフラッシュドライブ）を入手し、機密データを抽出する、またはホスト環境に侵入するために使用できる悪意のあるシステムファイルをデバイスに配置しようとする主な脅威を取り扱っている。 対象となるのは、USBメモリ（USBフラッシュドライブ）及びその上のデータにアクセスし管理するために使用される関連ソフトウェアである。
[3]：Protection Profile for USB Storage Media Versio4 1.4 (BSI-PP-0025-2006) (ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様)	攻撃者が放置または盗難USBメモリ（USBフラッシュドライブ）を入手し、機密データを抽出するという、主な脅威を取り扱っている。その他には、電源断などでデータが暗号化されないままになるといった脅威も取り扱っている。
[4]：CSEC Protection Profile Encrypted Storage Device (Version 2.1 (FMV-PP-ESD) (ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様)	[1]とほぼ同等の内容を取り扱っている。

[19] NIAPのWeb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のWebサイトから翻訳版をダウンロード可能
https://www.ipa.go.jp/files/000015355.pdf

2018/02/01 リンク先の有効性確認

4. 調達した IT 製品の利用・運用時の注意点

(1) 製品利用における前提条件（設置環境、利用形態、人員教育等）の確認

IT 製品の利用においては、製品利用における前提条件（設置環境、利用形態、人員教育等）を考慮することが重要になる。

例えば、悪意ある第三者が物理的にアクセスできる環境に設置された場合、管理者が付与された特権を悪用し不正な設定を行った場合、管理者及び利用者に利用手続きに関する教育を行わなかった場合等では、セキュリティ上の脅威は増大する。

そのため、運用時はもちろん製品調達時においても製品利用における前提条件を考慮することが必要となるが、「要件リスト」に示されている「国際標準に基づくセキュリティ要件」では、当該製品において充足すべき前提条件が記載されている。

例えば、デジタル複合機（MFP）の「国際標準に基づくセキュリティ要件」では、以下の表 10 に示す前提条件が記載されている。

表 10　デジタル複合機（MFP）の「国際標準に基づくセキュリティ要件」[1]、[2]及び[3]で定義されている前提条件

①　製品のデータインタフェース及び物理的なコンポーネントへの許可されないアクセスに対する保護のため、制限もしくは監視されている環境に設置する。
②　利用者に、組織のセキュリティ方針と手続きを認識させ、当該方針と手続きに従うよう教育を受けさせる。
③　管理者に、組織のセキュリティ方針と手続きを認識させ、ベンダのガイダンス等に従うよう教育を受けさせ、当該方針と手続きに従って製品を適切に構成・操作できるようにする。
④　管理者は、付与されたアクセス権を悪用しない。

①は製品の設置・利用環境についての前提条件、②は利用者への教育についての前提条件、③、④は及び信頼できる者を管理者とし教育を実施するという、極めて当たり前の条件であるが、これらの前提条件が達成できていない環境においては、製品がセキュリティ要件を満たしていたとしても脅威に対抗できなくなる事態が発生してしまう。

例えば、管理者が自身のアクセス権を悪用し、セキュリティ設定を無効化（通信データ暗号化機能のオフ等）を行った場合には、「要件リスト」のセキュリティ上の脅威に対抗できなくなってしまう。

そのため、「国際標準に基づくセキュリティ要件」により、製品の調達時もしくは運用時に、その製品分野としてどのような前提条件（設置環境、利用形態、人員教育等）が求められているのかを確認することができる。

(2) 認証取得製品とその後のバージョンアップ製品

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。

これは、セキュリティ評価の中では製品の構成管理の適切性の評価として、最終的なソフトウェアのバージョンだけでなく、ソフトウェアを構成するモジュール単位のバージョンまで確認されることや、実際の製品を用いて評価者がテストを実施するため、パッチの適用によりソフトウェアの動作が変化した場合には、パッチ適用前にテストで確認した内容が保証できないためである。

ここでは、セキュリティパッチの適用等により、第三者認証を取得したバージョンとは異なった製品を調達する際の注意点及び調達した製品の運用時におけるセキュリティパッチの適用に関する注意点について解説する。

(a) 保証継続（認証の維持）

上記のような懸念に対処するため ISO/IEC15408（Common Criteria）を利用するための国際的な枠組みである CCRA では、保証継続[20]という仕組みにより、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機能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ことで、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ことが認められている。

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、その変更が認証範囲のセキュリティ機能に影響を及ぼさないことが確認できる。

---

[20] IT セキュリティ評価及び認証制度　保証継続
https://www.ipa.go.jp/security/jisec/assurance_continuity/index.html
2018/02/01 リンク先の有効性確認

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。確認方法としては、保証継続されていることを証明する資料（保証継続報告書等）を提出させることや、調達者自身が Web サイト等で確認する方法などがある。

例えば、日本（IPA）で認証された製品については、IPA の認証製品リスト[21]で確認できる。（各製品の「認証年月日」欄に（保証継続）と記載されている製品が、保証継続が実施されている製品となる。）

また、世界各国の認証制度で第三者認証を取得している製品の保証継続については、CCRA ポータルサイトの認証製品リスト[22]で確認できる。（各製品の欄に「Maintenance Report(s)」とある製品が、保証継続が実施されている製品となる。）

なお、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。

例えば、セキュリティ機能に影響を及ぼさないことが確認できるテスト内容及びテスト結果に関する資料や機能仕様レベルでの変更に関する資料等、調達者自身が確信を持てる資料を要求すべきである。

(b) 運用中のセキュリティパッチの適用

前述のとおり、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が、運用中もそのバージョンを堅持することが必ずしもセキュリティ確保に繋がるわけではない。

通常、ベンダから提供されるセキュリティパッチは、提供中の製品に仕様上の欠陥、実装上のバグ、セキュリティ上の脆弱性等が発見された際に、それに対処するために提供される。

そのような場合に提供されるセキュリティパッチについては、セキュリティ機能に影響を及ぼさないことを確認した上で迅速に適用するか、適用できない場合には別の対処策を講じなければ、セキュリティインシデントの発生や、悪意ある攻撃者に攻撃の機会を与えることになる。

---

[21] IT セキュリティ評価及び認証制度　認証製品リスト
https://www.ipa.go.jp/security/jisec/certified_products/cert_list.html

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

第三者認証の取得の有無は、あくまで調達時の要件・選定条件に活用できる条件であることに注意されたい。

なお、国際標準に基づく第三者認証を取得している製品の中には、製品にセキュリティ上の欠陥が発覚した場合、ベンダの責務として対応を行う仕組みが備わっていることが保証されているものもある（ISO/IEC15408 における「欠陥修正：ALC_FLR」という保証要件に適合している製品）。

ALC_FLR に適合している認証製品であれば、認証取得後に発見された脆弱性問題についての、ベンダの適切な対応が期待できる。

「要件リスト」に記載の「国際標準に基づくセキュリティ要件」の中では、以下の表 11 に示した ALC_FLR 欄が✓となっているものにおいては、ALC_FLR を含んでいるので参考にされたい。

表 11　「国際標準に基づくセキュリティ要件」における ALC_FLR の有無

国際標準に基づくセキュリティ要件		ALC_FLR
デジタル複合機（MFP）	[1]	✓
	[2]	✓
	[3]	
ファイアウォール	[1]	✓
	[2]	
	[3]	
不正侵入検知/防止システム（IDS/IPS）	[1]	✓
	[2]	
OS（サーバ OS に限る）	[1]	✓
	[2]	✓
	[3]	✓
	[4]	
データベース管理システム（DBMS）	[1]	✓
	[2]	✓
スマートカード（IC カード）		
暗号化 USB メモリ	[1]	
	[2]	
ルータ／レイヤ３スイッチ	[1]	
	[1]	

ドライブ全体暗号化システム	[1]	
	[2]	
モバイル端末管理システム		
仮想プライベートネットワーク（VPN）ゲートウェイ	[1]	
	[2]	

5. 「要件リスト」に関する補足説明

(1)「要件リスト」に掲載している国際標準の概要

「要件リスト」では、以下に示す IT セキュリティに関する国際標準を採用している。

- ISO/IEC 15408
- ISO/IEC 19790

ここでは、「要件リスト」で採用している IT セキュリティに関する国際標準の概要を解説する。

(a) ISO/IEC 15408

IT セキュリティの観点から、IT 技術に関連した製品及び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ことを評価するための国際標準規格である。

IT 技術を用いた製品やシステムのセキュリティ機能を対象とし、ソフトウェアだけでなく、ハードウェア、ファームウェア等が評価対象となり得る。

また、製品の形態としては、ファイアウォールのように、直接セキュリティに関係する機能を提供する製品に限らず、OS、DBMS、あるいはグループウェアなど、保護すべき資源を保有する製品はすべて評価対象となり得る。

ISO/IEC 15408 では、セキュリティ機能の技術的な対策や実装、開発におけるプロセスなどを扱い、評価の対象とする。例えば、対抗する脅威に必要な機能が設計書に反映されていること、その機能が設計どおり実装されていること、開発現場や配付過程においてセキュリティが侵害される可能性がないこと、ガイダンス等にセキュリティを保つための必要事項が明確に示されていることなどを評価し、最終的には、それらの証拠や公知の情報から懸念される脆弱性について評定及びテストが実施される。

また、どの深さまで評価するかという保証レベルという概念がある。例えば、機能仕様、インタフェース仕様及び製品ガイダンスのみを入力とした分析より、評価の対象に内部設計資料を加えることでより高い保証が得られることが考えられる。

ISO/IEC 15408 は、評価対象の製品に係る様々な側面を評価するが、製品やシステムを利用する組織における要員のセキュリティ教育やセキュリティ監査の実施といった組織上の運用や管理については、使用上の前提条件として扱われ、評価の対象とはならない。

ISO/IEC 15408 に基づいた評価が、異なる制度や評価機関でなされても、その評価結果が均質である必要がある。そのため、評価に使用される手法

（どのような対象を評価し、どのような判断を要するかなど）を明確にした ISO/IEC 18045（Common Evaluation Methodology ： 共通評価方法）が ISO/IEC 15408 とともに国際標準化されている。

(b) ISO/IEC 19790[23]

暗号アルゴリズムを実装した製品（暗号モジュール）に求められるセキュリティ要件をまとめた国際標準規格。

この規格の適用例としては、暗号化 USB メモリ、ドライブ全体暗号化システム、ネットワーク暗号化装置、暗号鍵管理装置のような製品が挙げられる。

ISO/IEC 19790 では、特に、1）暗号アルゴリズムが正しく実装され、2）それが正しく実行され、3）暗号鍵、パスワードなどの重要情報が適切に保護されていること、の 3 つを主たるセキュリティ上の目標として設定した上で、具体的なセキュリティ確保のための要求事項を述べている。

また、このセキュリティ確保のための要求事項は、暗号モジュールが取り扱うデータの重要度や利用環境の多様性に対応して、4 つのレベルで設定されている。4 つのレベルで、使用可能な暗号技術は同一である。

ISO/IEC 15408 では、セキュリティ上の脅威を想定して、その脅威に対抗することを評価する枠組みをとっている。一方、ISO/IEC 19790 は、暗号鍵の暴露といった、暗号を使う製品に標準的に想定しうる脅威を予め考慮した上で、脅威へ対抗するための要求事項を記述している。

ISO/IEC 19790 で述べられている要求事項が実現されているかどうかを試験するための手順が、ISO/IEC 24759[24]として国際標準化されている。

ISO/IEC 19790 及び/又は ISO/IEC 24759 の内容を日本語で確認したい場合には、国際一致規格である JIS X19790 及び/又は JIS X24759 を参照されたい。

① IT 製品の調達における「暗号モジュール」の考え方

暗号技術は、データの暗号化及び復号、電子署名の生成及び検証、乱数生成等を実現する際に必要な基本的な技術である。暗号技術を用いる際の重要

---

23 ISO/IEC 19790
https://www.iso.org/standard/52906.html

24 ISO/IEC 24750
https://www.iso.org/standard/72515.html

2018/02/01 リンク先の有効性確認

な観点として、電子政府推奨暗号（CRYPTREC 暗号[25]）を正しく実装しているだけでなく、暗号鍵が適切に管理されていることが必要である。

暗号技術が主たる機能である製品は多くない一方で、さまざまな所で暗号技術が使用されて IT 製品に組み込まれており、身近な例では、WEB サーバとの HTTPS 通信、スマートフォンのストレージの暗号化、マイナンバーカードによる電子署名、IC 旅券と旅券検査端末との通信の保護、IP 電話やテレビ会議の通信の保護など枚挙に暇がない。システムやソリューションの中においても、DNS サーバに用いられる DNSSEC、ネットワークの監視・制御するための SNMP v3、シングル・サインオンを実現する要素技術、仮想通貨にも暗号技術が用いられている。

その他、事業継続計画(BCP)を実現するためにバックアップデータを暗号化して遠隔地で保存するようなケースにも用いられる。

このように、IT 製品にはセキュリティ機能を実現するために暗号機能が組み込まれている場合が多く、安全に運用するためには、以下の条件を備えていることを確認する必要がある。

i） 採用している暗号アルゴリズム、あるいは選択できる暗号アルゴリズムが、調達時点で理論的に安全であること。

ii） 上記に加えて、暗号アルゴリズム及びその周辺機能が、着実にかつ脆弱性の無い形で実装されていること。

iii） 安全な設定で運用すること。

iv） 暗号鍵管理を適切に行うこと。

これらが確認できて初めて暗号化等による結果が解読されたり、暗号化等の途中で情報が漏えいしたり、解読のための暗号鍵が盗まれたりといった利用上の脅威を防ぐことができる。

i)の暗号アルゴリズムに関しては、電子政府推奨暗号（CRYPTREC 暗号[26]）リストにより、理論的安全性が確認されたアルゴリズムが示されている。

ii)の暗号アルゴリズムの実装に関しては、実装そのものに脆弱性があったり、暗号鍵の生成や管理に関して脆弱な作りとなっている場合、いくら暗号アルゴリズムとして強固なものであっても、攻撃への耐性が期待されるものとはならない。

---

[25] CRYPTREC 暗号リスト
http://www.cryptrec.go.jp/list/cryptrec-ls-0001-2016.pdf

調達者が、受け入れテストの中で、暗号に関するセキュリティ要件が満たされていることを調達者自身で確認することは極めて難しい。そういった課題を解決するために、暗号アルゴリズムが正確に実装されているかを簡便に確認するための暗号アルゴリズム実装試験ツールや暗号アルゴリズム確認制度[27]が存在しており、それらを利用する、あるいは、そういったツールや制度に基づいて正確に実装されていることが既に確認されている実装[28]を利用するという手段を取るべきと考える。その他、製品レベルでの暗号鍵管理やシステムレベルでの暗号鍵管理など極めて複雑な部分には、専門機関による試験、評価、認証が有効である。

② 「暗号モジュール」という視点からみた、本ガイドブックにおける IT 製品分野

「暗号モジュール」あるいは「暗号機能が主たる機能であるような製品」を調達しようとする例は少ないかもしれない。しかしながら、セキュリティ上の課題を含めた、現実の課題を解決するために暗号機能が少なからず使われている。

例えば、PC 内の重要情報の消去が不適切だと、PC を廃棄又はリース返却することにより情報漏えいするリスクがある。ここで、データ消去ソフトを使って、現在の大容量の HDD のデータ消去にかかる時間は無視できない。SSD の場合は、情報を消去しようとしても本当に消去されたかを利用者が確認できる手段は限られる。

これらを解決する手段として、「ドライブ全体暗号化システム」に代表される HDD や SSD のドライブ全体を暗号化する方法があり、物理的な解析による情報の抜き取りへの対策になるだけでなく、暗号化に使用する暗号鍵を消去する機能によって、ドライブ内の情報を短時間で利用不可能にすることができる。この暗号鍵を消去する方法を選択することは、サーバやデータセンターで用いられる HDD や SSD を考慮した場合には、台数が多い分、効果的である。

このように「ドライブ全体暗号化システム」は、暗号機能が極めて重要な役割を担っている製品である。本ガイドブックでは、「暗号モジュール」と

---

27 JCMVP
https://www.ipa.go.jp/security/jcmvp/index.html

28 暗号アルゴリズム確認登録簿
https://www.ipa.go.jp/security/jcmvp/avallists.html

2018/02/01 リンク先の有効性確認

いう分類の形をとっていないが、IT 製品分野の中には、暗号機能が極めて重要な役割を担っているものが存在することを理解すべきである。

その他、仮想プライベートネットワーク（VPN）も、実現手段としては暗号を用いるものであり、ソフトウェア又はハードウェアといった形態の「暗号モジュール」と見なすことができる。仮想プライベートネットワーク（VPN）の実現方式には、TLS を使用する方式と、IPsec を使用する方式が代表的なものとしてあげられるだろう。ここで、TLS、IPsec それぞれについてのガイドラインが、国内外の諸機関から公開されている。

TLS 設定ガイドライン

IT システムの調達仕様の中には、単純に SSL 又は TLS による暗号化を求めるものもあるかもしれない。しかし、単に SSL 又は TLS の暗号化を可能にするソフトウェア/ハードウェアを調達してデフォルトで使用するだけでは、セキュリティ対策として不十分なケースも存在する。例えば、TLS v1.0 及び v1.1 は、電子政府推奨暗号リストに記載されていない、SHA-1 及び MD5 を使うという課題がある。こういった課題を解決するために、例えば、次のような資料が参考にして、調達及び設定を行うべきである。

- IPA の「SSL/TLS 暗号設定ガイドライン」[29]
- NIST SP 800-52 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations” [30]
- BSI TR-02102-2 “Cryptographic Mechanisms: Recommendations and Key Lengths: Use of Transport Layer Security (TLS)” [31]
- ANSSI “Security Recommendations for TLS”[32]

IPsec 設定ガイドライン

IPsec と一言で言っても現実には多様な実装が存在し、通信したい 2 者間での鍵共有のプロトコルには、IKEv1 と IKEv2 の 2 つが存在する。この内、IKEv1 では、電子政府推奨暗号リストに掲載されていない、SHA-1 又は MD5 が、標準的に選択可能な状態にあるという課題がある。逆に電子政府推奨暗

---

[29] https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

[30] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft.pdf

[31] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7

[32] https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf

2018/02/01 リンク先の有効性確認

号リストに掲載されている、SHA-256、SHA-384、SHA-512 は、実装が必ずサポートしているというものではなく、実装依存である。こういった課題を解決するために、例えば、次のような資料が参考にして、調達及び設定を行うべきである。

- NIST SP 800-57 Part 3 Rev.1 “Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance” [33]
- BSI TR-02102-3 “Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)[34]

③ 「政府機関の情報セキュリティ対策のための統一基準」との関係

「政府機関の情報セキュリティ対策のための統一基準[35]」の中で、暗号化及び/又は電子署名について言及されている個所を次の表 12 に示す。

表 12

政府機関の情報セキュリティ対策のための統一基準の節番号	暗号化又は電子署名への言及
5.2.1 情報システムの企画・要件定義	暗号化、電子署名
6.1.5 暗号化・電子署名	暗号化、電子署名
7.2.2 ウェブ	暗号化
7.2.4 データベース	暗号化、電子署名
7.3.1 通信回線	暗号化
8.1.1 情報システムの利用	暗号化、電子署名

また、「政府機関の情報セキュリティ対策のための統一基準」のガイドラインにあたる「府省庁対策基準策定のためのガイドライン[36]」の基本対策事項として、暗号、電子署名、鍵について言及している個所を次の表 13 に示す。

表 13

[33] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

[34] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-3.pdf?__blob=publicationFile&v=6

[35] http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

[36] http://www.nisc.go.jp/active/general/pdf/guide28.pdf

2018/02/01 リンク先の有効性確認

府省庁対策基準策定のためのガイドライン の該当する節		暗号、電子署名、鍵への言及		
		暗号	電子署名	鍵
3.1.1 情報の取扱い	3.1.1(4)(a)(d)	✓	✓	
	3.1.1(6)(a)	✓		
4.1.4 クラウドサービスの利用	4.1.4(1)(d)	✓		
6.1.1 主体認証機能	6.1.1(1)(b)	✓		
6.1.5 暗号・電子署名	6.1.5(1)(a)	✓	✓	✓
	6.1.5(2)(a)(ア)関連		✓	
7.1.1 端末	7.1.1(1)(b)	✓		
7.2.1 電子メール	7.2.1(1)(b)関連		✓	
7.2.4 データベース	7.2.4(1)(e)	✓		
7.3.1 通信回線	7.3.1(1)(c)関連	✓		
	7.3.1(1)(j)関連	✓		
	7.3.1(4)(a)関連	✓		
	7.3.1(5)(a)関連		✓	
8.1.1 情報システムの利用	8.1.1(1)(a)関連	✓		
	8.1.1(1)(b)関連	✓		
	8.1.1(1)(c)関連	✓		
8.2.1 府省庁支給以外の端末の利用	8.2.1(1)(b)関連	✓		
	8.2.1(1)(d)関連	✓		

このように、政府機関の情報セキュリティ対策において、暗号の利用を求めるケースは少なくない。調達する IT 製品に対して暗号に係わる機能を求める場合、当該機能実現に必要な暗号モジュールが組み込まれた製品を間接的に調達するとみなして、調達者は当該機能要件に対する性能要件的な位置づけで暗号モジュールが備えるべき要件を提示し、確認する必要が生じる。

ここで関連する「府省庁対策基準策定のためのガイドライン」の「6.1.5 暗号・電子署名」の基本対策事項には、次のように記述している。

【 基本対策事項 】

＜6.1.5(1)(a)関連＞

6.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。

b) 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。

d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

この記述のc)について補足すると、国際標準ISO/IEC 19790に適合していることを、「暗号モジュール試験及び認証制度」に基づく認証を取得することによって確認できる。d)の耐タンパ性についても「暗号モジュール試験及び認証制度」を利用することにより試験することができる。

その他、「政府機関の情報セキュリティ対策のための統一基準」のガイドラインにあたる「府省庁対策基準策定のためのガイドライン」の中に登場する、HSM（ハードウェアセキュリティモジュール、暗号鍵管理装置ともいう）について言及されている。HSMは、暗号技術が主たる機能である製品であって、電子署名を作るための暗号鍵をセキュアに生成する、暗号鍵をセキュアに長期にわたって保管するといった機能を提供する。HSMはISO/IEC 19790又はその国際一致規格JIS X19790に基づく認証を取得することが望ましい製品である。

これに関連して、例えば、HSMを使って運営する認証局のCP/CPS[37]の中には、FIPS 140-1というセキュリティ要件を参照しているものも存在している。米国では、FIPS 140-2に基づく認証製品であっても、認証取得から5年

[37] 認証局（CA）を運用する際の証明書の利用目的を定める証明書ポリシー（CP: Certificate Policy）と、CAの運用方法を定める認証実施規定

を過ぎた製品については、米国連邦政府機関は調達すべきではないとされており、FIPS 140-1 に基づく認証製品は認証取得から 5 年を過ぎていることから、調達すべきではないという扱いになっている。こうした事実を踏まえて、認証局の調達や CP/CPS を見直す場合には、HSM のセキュリティ要件についても ISO/IEC 19790 又はその国際一致規格 JIS X19790 に更新することを検討すべきものと考える。

(2)「セキュリティ上の脅威」と「国際標準に基づくセキュリティ要件」の関係

「国際標準に基づくセキュリティ要件」では、IT セキュリティの専門家等により分析されたベースラインとして想定すべき脅威が定義されている。

ただし、現状の「国際標準に基づくセキュリティ要件」は、それを開発・策定した組織体が様々であるため、開発・策定のプロセスも組織体毎に異なる。

そのため、「国際標準に基づくセキュリティ要件」で定義されている脅威は、技術用語を含んだ表現や漠然としすぎた内容等であるものも存在し、IT セキュリティに関する知識・経験を持たない一般の調達者にとっては理解し難い内容になっている場合がある。

そのため、「要件リスト」では、以下の場合毎に「セキュリティ上の脅威」の記載プロセスを作成し、調達者が対抗すべき脅威を実感できる内容・理解しやすい表現として、「セキュリティ上の脅威」を記載している。

①：「国際標準に基づくセキュリティ要件」に記載されている脅威が調達側にとって理解しやすい内容の場合には、ほぼ同様の内容でリストに記載する

②：「国際標準に基づくセキュリティ要件」に類似の脅威が複数記載されている場合（細かく場合分けされている場合）には、根本的な脅威として 1 つにまとめてリストに記載する

【②のプロセスを用いた例】

IDS/IPS の脅威として以下の 2 つの脅威が定義されている

(1)「権限のないユーザが、セキュリティ･メカニズムをバイパスし、IDS/IPS によって収集・生成されたデータの完全性を損なおうと試みる。」

(2)「権限のないユーザが、セキュリティ･メカニズムをバイパスし、IDS/IPS によって収集・生成されたデータを開示しようと試みる。」

上記(1)、(2)をまとめ、「要件リスト」では、「④ 不正・異常検出したデータの破壊、改ざん、開示」としてリストにまとめて記載している。

③：「国際標準に基づくセキュリティ要件」に記載の脅威が技術用語を含んだ表現や漠然としすぎている内容の場合には、脅威に対抗するために定義されているセキュリティ機能要件等から、想定される脅威を記載する

【③のプロセスを用いた例】

デジタル複合機（MFP）の国際標準に基づくセキュリティ要件では、「利用者文書データが権限のない者に開示されるかもしれない。」 という脅威が定義されており、上記脅威への対抗手段の１つとして「残存情報保護」のセキュリティ機能要件が定義されている。

（「残存情報保護」は、保存データ消去の際に消去前のデータを利用不能にする機能。例えば上書き消去機能等。）

つまり、「残存情報保護」のセキュリティ機能要件が想定している具体的な脅威として、「要件リスト」には「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、または廃棄処理時）」を記載している。

更に、上記のプロセスの他に以下の点を考慮している。

- 「要件リスト」で複数の「国際標準に基づくセキュリティ要件」を記載している製品分野においては、最も新しく開発された「国際標準に基づくセキュリティ要件」をベースにしつつ、全ての「国際標準に基づくセキュリティ要件」に共通している脅威を「要件リスト」の「セキュリティ上の脅威」として記載している。これは、新しい「国際標準に基づくセキュリティ要件」において、第三者認証を取得している製品が少ないため、暫定的に複数の「国際標準に基づくセキュリティ要件」を併記している。

- 「国際標準に基づくセキュリティ要件」で定義されている脅威の中では、セキュリティ機能で対抗できない脅威（例えば、開発者の実装ミスに関する脅威）も記載されているが、「要件リスト」の「セキュリティ上の脅威」には、セキュリティ機能で対抗できる脅威のみを「国際標準に基づくセキュリティ要件」から抽出して記載している。

- 「国際標準に基づくセキュリティ要件」では、実際または仮想上の組織によって、その運用環境において現在及び/または将来に課される（または課されると推定される）セキュリティの規則、手続き、または

ガイドラインとして、「組織のセキュリティ方針」というものが定義されている。「要件リスト」では、定義されている「組織のセキュリティ方針」についても、セキュリティ上の脅威として関係しているものは記載している。

上記の作業を行っているため、「要件リスト」の「セキュリティ上の脅威」と「国際標準に基づくセキュリティ要件」で定義されている脅威は正確に一致するものではない。

調達の際に「国際標準に基づくセキュリティ要件」で定義されている脅威を確認する必要がある場合には、「要件リスト」の脚注にある URL から「国際標準に基づくセキュリティ要件」をダウンロードし確認されたい。

なお、複数の製品分野で現在策定が進んでいる、世界共通の「国際標準に基づくセキュリティ要件」である cPP（collaborative Protection Profile）においては、策定プロセスが統一化されている。
「要件リスト」では cPP を順次採用していくことを検討していくため、ここで示した「セキュリティ上の脅威」の記載プロセスを用いる機会は今後減少していくと考えられる。

(3)「要件リスト」の更新

現在、世界共通の「国際標準に基づくセキュリティ要件」である cPP の策定が複数の製品分野で進んでおり、それらの策定状況に合わせて、「要件リスト」の「対象製品分野」、「対象候補」及び「国際標準に基づくセキュリティ要件」が更新される予定である。

cPP の策定状況については、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である CCRA(Common Criteria Recognition Arrangement)の年 2 回の定期会合の結果等を基に、IPA 内に設立した「IT 製品の調達におけるセキュリティ要件リスト検討委員会」において、「要件リスト」を検討している。

そこでの検討結果を受けて、IPA が「要件リスト」の更新案を作成し、経済産業省への入力とした後、経済産業省から正式に一般の調達者に向けて公開される。

なお、「1 - (2)情報システムのライフサイクルにおける「要件リスト」の位置づけ」で解説したとおり、「政府機関の情報セキュリティ対策のための統一基準」では、IT 製品を調達する時に「要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定することが遵守事項として定められている。

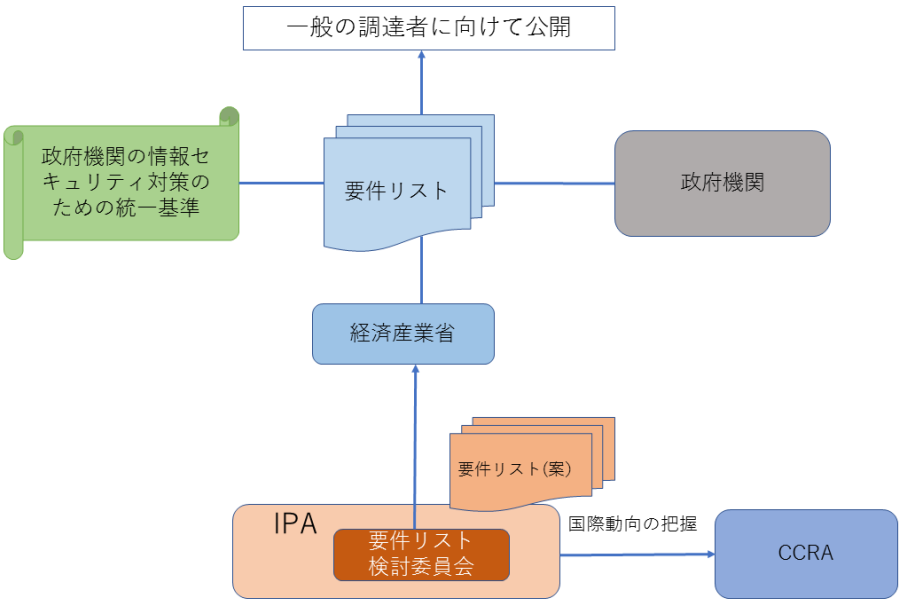

図 3：「IT 製品の調達におけるセキュリティ要件リスト」の検討体制