政府情報システムにおける

セキュリティ・バイ・デザインガイドライン

2022（令和4）年　6月　30日

デジタル庁

〔標準ガイドライン群ＩＤ〕

DS-200

〔キーワード〕

セキュリティ・バイ・デザイン、DevSecOps、システムライフサイクル保護

〔概要〕

情報システムに対して効率的にセキュリティを確保するため、企画から運用まで一貫したセキュリティ対策を実施する「セキュリティ・バイ・デザイン」の必要性が高まっている。本文書ではシステムライフサイクルにおけるセキュリティ対策を俯瞰的に捉えるため、各工程でのセキュリティ・バイ・デザインの実施内容を記載する。

併せてセキュリティ・バイ・デザインの実用性を確保するための関係者の役割を定義する。

改定履歴

改定年月日	改定箇所	改定内容
2022年6月30日	-	初版決定

目次

１ はじめに 2
１．１ 目的とスコープ 2
１．２ 適用対象 2
１．３ 位置づけ 3
１．４ 本書の構成 3
１．５ 用語 3
２ セキュリティ・バイ・デザインの概要 5
２．１ セキュリティ・バイ・デザインの概要 5
２．２ セキュリティ・バイ・デザインの導入メリット 5
２．３ セキュリティ・バイ・デザインの基本方針 7
３ セキュリティ・バイ・デザインのスコープ 9
３．１ セキュリティ・バイ・デザインの構成要素とスコープ 9
４ セキュリティ・バイ・デザインの実施内容 11
４．１ セキュリティ・バイ・デザインの実施工程と概要 11
４．２ セキュリティ・バイ・デザインの実施内容 13
1）セキュリティリスク分析 13
2）セキュリティ要件定義 14
3）セキュア調達 15
4）セキュリティ設計 16
5）セキュリティ実装 18
6）セキュリティテスト 19
7）セキュリティ運用準備 19
8）セキュリティ運用 20
５ セキュリティ・バイ・デザインのリスク管理体制 23
５．１ セキュリティ・バイ・デザインのリスク管理に関わる関係者の役割 23
６ セキュリティ・バイ・デザイン実施における留意事項 26
別紙１ 各工程で参照可能なセキュリティ標準..... 27
別紙２ 各工程のセキュリティチェックリスト..... 31
別紙３ システムにおける一般的なセキュリティ上の問題点..... 36
別紙４ リスクランクに応じたセキュリティリスクアセッサーによる評価例 37
別紙 ５ 政府情報システムにおけるクラウドセキュリティ要件策定、審査手順
..... 38

１　はじめに

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野においてジタル技術の利活用が進んでいる。他方、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。こうした中で、政府情報システムに対しても、今後、サイバー攻撃の脅威は高まっていくことが予想される。

こうした背景から、政府情報システムにおいても、セキュリティ対策を確実かつ効率的に実装するため、システム開発の上流工程からセキュリティ対策を実装する取組として、セキュリティ・バイ・デザインの必要性が高まっている。

１．１目的とスコープ

本書は「デジタル・ガバメント標準推進ガイドライン」のセキュリティ編と位置づけており、政府情報システムの開発や運用業務に従事する関係者に対して、政府機関のシステム開発の各工程で実施すべきセキュリティ・バイ・デザインとしての実施内容、要求事項を示すことを主目的とする。

また、セキュリティ・バイ・デザインにおいてセキュリティ品質を確保するためには、開発業務や運用業務に従事する担当者が各工程でセキュリティ対策を実施するだけでは不十分であり、各工程でのセキュリティ対策の妥当性を客観的に評価し、是正対応までを監督する、セキュリティリスク管理体制の整備も必要になる。よって、本書では、セキュリティリスク評価とリスク管理に関連する関係者の役割もスコープとして記載する。

システム開発、運用の各工程において、本書のセキュリティ・バイ・デザインの方針に従い、標準化されたセキュリティ対策を実施し、組織的で継続的なセキュリティリスク管理を実施することにより、システムごとの独自方針に基づいて実施されていたセキュリティ対策のばらつきや不十分なリスク管理が解消され、政府情報システムにおけるセキュリティレベルの向上が期待される。

なお、本書と合わせて、企画段階から情報セキュリティ対策を考慮し、調達仕様にセキュリティ要件を適切に組み込むことを目的として策定された NISC（内閣サイバーセキュリティセンター）の「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（SBD マニュアル）」を調達段階において参照されたい。

１．２　適用対象

本文書は、政府情報システムを適用対象として想定している。なお、本文書はセキュリティ・バイ・デザインへの理解を深める参考文書であり、適用の遵

守を求めるものではない。

１．３　位置づけ

本文書は、標準ガイドライン群の一つとして位置づけられる。

１．４　本書の構成

第 2 章ではセキュリティ・バイ・デザインの概要や導入メリットを示すとともに、セキュリティ・バイ・デザインの原則となる基本方針について説明する。セキュリティ・バイ・デザインに関する知見がない読者は、本章を理解することで、第 3 章以降の記載内容の理解を深めることができるため、一読することを推奨する。

第 3 章では、第 2 章の基本方針を踏まえて、セキュリティ・バイ・デザインを実現するための構成要素を示すとともに、本書における、政府情報システムに対するセキュリティ・バイ・デザインのスコープについて説明する。

第 4 章では、政府情報システムにおけるセキュリティ・バイ・デザインの実施内容として、システム開発、運用の各工程におけるセキュリティ対策の実施内容とセキュリティ要求事項を記載する。また、セキュリティ専門家の知見や昨今のセキュリティトレンド等を踏まえ、確実に抑えるべき、各工程において重要となるセキュリティ対策について、具体的な考え方を示す。本章の記載内容を俯瞰的に理解し、実践することは、システムライフサイクル全体を通してセキュリティ強化を実現することの一助となる。

第 5 章では、セキュリティ・バイ・デザイン実施の品質確保に必須となるセキュリティリスク評価と継続的なリスク管理を実現するための関係者の役割について記載する。各府省あるいは政府機関は本章の記載内容に従い、関係者の任命と当該関係者を含めたセキュリティ・バイ・デザインの運用設計、リスク管理方法を検討し、実践することで、実行的で効果的なセキュリティ・バイ・デザインの実施に努めることが求められる。

第 6 章では、前章までの内容を踏まえて、セキュリティ・バイ・デザイン実施時の留意点を記載する。セキュリティ・バイ・デザインを運用する際は、本章の内容に留意して実施する必要がある。

１．５　用語

本文書において使用する用語は、表１-1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。その他専門的な用語につ

いては、民間の用語定義を参照すること。

表 1-1 用語の定義

用語	意味
サイバーレジリエンス（サイバーレジリエント）	サイバーセキュリティ攻撃の影響を最小限に留めつつ、迅速に元の状態に回復、復元すること
DevSecOps	開発と運用がシームレスに連携する DevOps にセキュリティを組み込むことで、セキュリティを確保しつつ、開発スピードを損なわない開発手法のこと
アタックサーフェス（攻撃対象領域）	システムにおいて、サイバー攻撃を受ける可能性のあるすべての攻撃点、経路のこと

２セキュリティ・バイ・デザインの概要

２．１　セキュリティ・バイ・デザインの概要

サイバー攻撃の大規模化/高度化に伴い、情報システムに対して確実にかつ効率的にセキュリティを確保するため、システム開発の企画工程からセキュリティを実装する「セキュリティ・バイ・デザイン」の必要性が高まっている。

また近年の情報システムは、絶え間なく、多種多様なセキュリティ脅威にさらされるため、システムの開発工程だけでなく、システムの運用工程のセキュリティ確保も同様に重要となり、開発工程と運用工程の双方において、シームレスで一貫性のあるセキュリティ対策が求められる。

一般的に、開発から運用まで含めたシステムライフサイクル全体でセキュリティ確保する方策を（とりわけソフトウェア開発においては）DevSecOps と呼ぶが、本書では政府情報システムの企画工程から設計工程、開発工程、運用工程まで含めた全てのシステムライフサイクルにおいて、一貫したセキュリティを確保する方策のことを「セキュリティ・バイ・デザイン」と定義する。

２．２　セキュリティ・バイ・デザインの導入メリット

セキュリティ・バイ・デザインとして、組織にとって適切な実施プロセス、リスク評価、リスク管理体制を導入することで、企画工程からセキュリティリスクへの対応方針を定め、システム運用に至るまで一貫したセキュリティ対策の実装が可能となるため、致命的なセキュリティ対策の漏れ等による上流工程への手戻りを防止でき、納期確保やセキュリティコスト低減が可能となる。

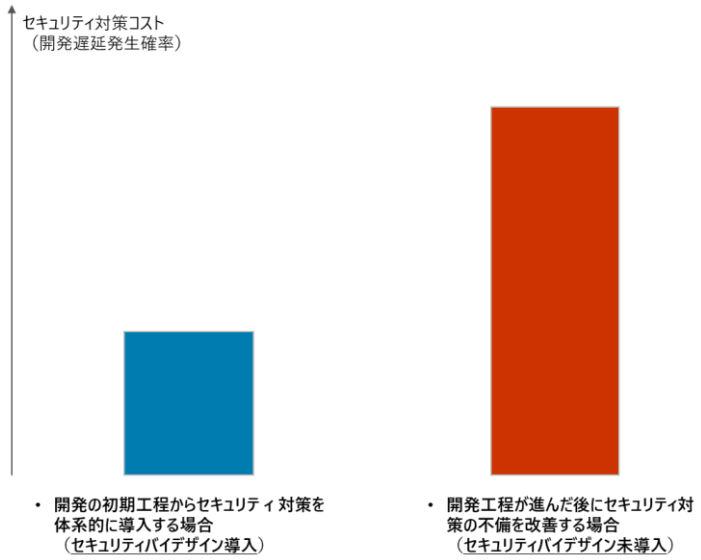


図　2-1 セキュリティ・バイ・デザイン導入時のセキュリティ対策コストイメージ

組織全体の視点でみると、管理対象の全ての政府情報システムを対象に、システム開発から運用まで標準化されたセキュリティ対策を実施し、対策の妥当性を検証する仕組みを導入することで、システムごとのセキュリティ品質のばらつき解消や、組織全体におけるシステムセキュリティ品質の底上げが可能となる。

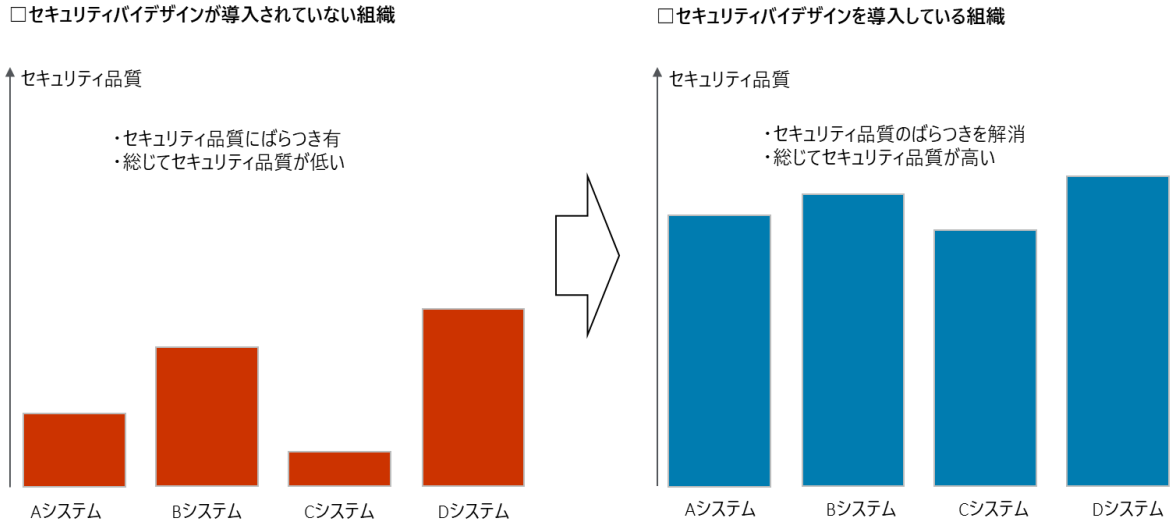


図　2-2　セキュリティ・バイ・デザイン導入組織のセキュリティ品質メリット

２.３　セキュリティ・バイ・デザインの基本方針

セキュリティ・バイ・デザイン実施にあたっては、表層的で効果の薄いセキュリティ対策の実施に終始することを避けるため、セキュリティ・バイ・デザインの根底にある考え方（原則）を理解することが肝要となる。

本項では政府情報システムにおけるセキュリティ・バイ・デザインの原則となる基本方針を示す。政府情報システムにおけるセキュリティ・バイ・デザインは、下記基本方針に則ってシステムの開発工程、運用工程におけるセキュリティ対策を実施することが求められる。

1. 事後的ではなく、予防的にセキュリティ対策を組み込むこと
   - セキュリティ・バイ・デザインは、インシデント等の発生を契機に取組むのではなく、予防的にセキュリティ・バイ・デザインを実施することが求められる。

2. 全てのシステムライフサイクルを保護すること
   - セキュリティ・バイ・デザインは特定工程においてのみ実施するのではなく、全てのシステムライフサイクルを通して、一貫したセキュリティ対策を実施することが求められる。
   - 委託先等の関係者間でセキュリティ対策の責任範囲を明確にし、抜け漏れなくセキュリティ対策を実施することが求められる。

3. 初期設定値においてセキュリティが担保された状態を実現すること
   - システムの初期設定値としてセキュリティが担保された状態を実現し、システム運用者や利用者による設定ミスを極力少なくすることが求められる。

4. システム特性に応じて過不足ないセキュリティ対策を実施すること
   - 全てのシステムに画一的なセキュリティ対策を講じるのではなく、システム特性や重要度等に応じて過不足なくセキュリティ対策を実施することが求められる。

5. セキュリティリスクの評価、管理を実施すること
   - セキュリティ対策を実施するだけでなく、セキュリティ対策の充足性や残存リスクの評価が求められる。また、セキュリティリスクを適切に管理するための体制やリスク管理プロセスの導入が求められる。

6. 利便性を損なわないように、セキュリティを確保すること
   - システムにおける利便性確保とセキュリティ強化を同時に実現し、双方に利益があるポジティブサムを目指すことが求められる。

3　セキュリティ・バイ・デザインのスコープ

3.1　セキュリティ・バイ・デザインの構成要素とスコープ

政府情報システムに関するセキュリティ・バイ・デザインの基本方針に基づき、実行的で効果的なセキュリティ・バイ・デザインを実現にあたっては、表 3-1 で記載される構成要素を準備、検討することが必要になる。

本文書ではセキュリティ・バイ・デザインの主要な構成要素となる、各工程での実施内容（項番 1）及び、セキュリティリスク管理のための関係者の役割定義（項番 2 の一部）をスコープの構成要素として記載する。

その他の構成要素（セキュリティリスク管理プロセス、参照すべきセキュリティ標準、関連ツール等）については、各政府機関の管理体制や IT 環境、セキュリティポリシー等によって最適化される要素であるため、本書でのスコープには含めない。

表 3-1　セキュリティ・バイ・デザインの構成要素と本書のスコープ

項番	構成要素	スコープ	本書で記載方針
1	システム開発・運用の各工程におけるセキュリティ・バイ・デザインの実施内容	○	システムライフサイクル全体を対象に工程ごとに、セキュリティ・バイ・デザインの実施内容を要求事項と合わせて記載する。 開発手法としてウォータフォール型を選択した場合に合わせて記載している。アジャイル型を選択した場合は、同じ作業が繰り返し発生することを考慮して読み替えるものとする。 本書の位置づけをふまえ、デジタル・ガバメント推進標準ガイドラインのシステム開発工程定義と整合して記載する。

項番	構成要素	スコープ	本書で記載方針
2	セキュリティ・バイ・デザインにおけるセキュリティリスク管理体制/プロセス	△ （関係者の役割、責任のみ）	セキュリティリスク評価とリスク管理に必要となる関係者の役割を定義する。 リスク管理の運用フロー等具体的な実現プロセスは、各政府機関の管理体制やセキュリティポリシー等によって最適化される要素であるためスコープには含めない。
3	セキュリティ・バイ・デザインとして参照すべきセキュリティ標準（セキュリティベースライン）、関連ツール	×	セキュリティ・バイ・デザインを導入にあたり参照すべきセキュリティ標準やフレームワーク、関連ツールは、各政府機関の IT 環境やセキュリティポリシー等に依存するためスコープには含めない。

4　セキュリティ・バイ・デザインの実施内容

本章では、読者が担当システムのライフサイクル全体で実施すべきセキュリティ対策を俯瞰的に検討するために必要となる、セキュリティ・バイ・デザインにおける各工程で満たすべき要求事項、実施内容を定義する。

加えて、各工程でのセキュリティ品質の維持に不可欠となる実務上陥りやすい留意点や昨今のセキュリティの傾向の変化等をふまえ、確実に抑えるべき、重要なセキュリティ対策の考え方ついても記載する。

4．1セキュリティ・バイ・デザインの実施工程と概要

本項でセキュリティ・バイ・デザインの実施工程と概要を表 4-1 に示す。本書は「デジタル・ガバメント推進標準ガイドライン」のセキュリティ編と位置付けているため、両ガイドラインの関係が理解できるよう、セキュリティ・バイ・デザインの工程と「デジタル・ガバメント推進標準ガイドライン」の工程を併記する。

表 4-1 セキュリティ・バイ・デザインの実施工程と概要

項番	デジタル・ガバメント推進標準ガイドラインおける工程名	セキュリティ・バイ・デザインの工程名	概要
1	サービス・業務企画	セキュリティリスク分析	•想定脅威にかかるセキュリティリスク分析の実施 •セキュリティ対応方針の決定
2	要件定義	セキュリティ要件定義	•システムにおける機能面、非機能面でのセキュリティ要件の定義
3	調達	セキュア調達	•セキュリティ調達仕様の策定、責任範囲の明確化 •安全な委託先、安全なプロダクトの選定
4	設計・開発	セキュリティ設計	•機能面と非機能面でのセキュリティ設計
5		セキュリティ実装	•セキュリティ機能の実装 •アプリケーションのセキュアコーディング •プラットフォームのセキュリティ設定の実施(堅牢化)
6		セキュリティテスト	•セキュリティ機能のテスト •脆弱性診断
7	サービス・業務の運営と改善	セキュリティ運用準備	•セキュリティ運用体制の確立 •セキュリティ運用手順の整備
8	運用及び保守	セキュリティ運用	•平時のセキュリティ運用 •有事のセキュリティ運用

４．２セキュリティ・バイ・デザインの実施内容

本項では、セキュリティ・バイ・デザインの工程ごとに、実現すべき状態を要求事項として記載し、それらを実現するためのタスクを実施内容として記載する。

加えて、各工程でのセキュリティ品質の維持に不可欠となる実務上陥りやすい留意点や昨今のセキュリティ対応の傾向の変化等をふまえ、確実に抑えるべき、重要なセキュリティ対策の考え方ついても記載する。

1)セキュリティリスク分析

ア 要求事項

- システムにおけるセキュリティ脅威が特定されていること
- 当該脅威にかかる発生可能性、システムへの影響度を踏まえて、リスク分析が実施されていること
- リスク分析結果に基づき、セキュリティ対応方針を検討し、リスク対応優先度や遵守すべきセキュリティ標準（セキュリティベースライン)、対応リソース等を決定していること

イ 実施内容

- システムで取扱う重要情報、アクター、実施業務、他システムとの連携方法等、システムで取扱う重要情報のフローやライフサイクルが分かる内容を記載したシステムプロファイルの作成
- システムプロファイルに基づくセキュリティ脅威の特定
- セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施
- リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソース等)

ウ 重要なセキュリティ対策の考え方

- システム特性や重要度に適したセキュリティ対応方針の決定
  - システム開発においては、システムの特性や重要度に応じた適切なセキュリティ対応方針が示されず、システムに対するセキュリティ対策が不十分、または、過剰なセキュリティ対策が実施されることがある。
  - 適切なレベルのセキュリティ対策を実施するため、システムにて想定される脅威にかかる発生可能性、システムへの影響度を踏まえて、リスク分析を実施する。

- リスク分析結果から、システム特性や重要度に見合った適切なセキュリティ対応方針を検討し、主要なセキュリティ脅威に伴うリスクシナリオへの対策や遵守すべきセキュリティ標準（ベースライン）を決定する。また、開発工程や運用工程で実施する第三者チェック（脆弱性診断やセキュリティレビュー）の方針、必要なリソース等を決定する。

2)セキュリティ要件定義

ア 要求事項

- セキュリティリスク分析結果、セキュリティ対応方針に従い、システムで満たすべきセキュリティの状態が、機能面、非機能面ともに定義されていること

イ 実施内容

- 遵守すべきセキュリティ標準（セキュリティベースライン）や、詳細リスク分析結果等に基づいた、システムとして満たすべきセキュリティ要件の定義（機能、機能面）

ウ 重要なセキュリティ対策の考え方

- 多層防御の実施
  - サイバー攻撃は成功する（発生する）前提で、多層のセキュリティ対策を実施し、一つのセキュリティ対策が破られたとしても、別のセキュリティ対策により被害を極小化することを目的とした考え方に基づいて、セキュリティ要件を定義することが重要である。
  - OS やミドルウェア、ネットワーク、アプリケーションの各コンポーネント等において、多層のセキュリティ対策を実施することで、攻撃者にとって攻撃コストの高いシステムを実現する。
  - 攻撃や事故の発生自体を防止する防御に類するセキュリティ対策に偏らず、速やかなインシデント（兆候）の検知、インシデント対応、サービス復旧のための対策も含め、多層的にセキュリティ対策を実装することが求められる。

3) セキュア調達

ア 要求事項

- セキュリティ要件に基づいて、システム調達におけるセキュリティ仕様が策定され、委託先との責任範囲が明確になっていること
- システムのセキュリティ仕様を実装できる能力を有し、セキュリティ管理基準を満たす安全な委託先が選定されていること
- システムで利用する機器、ミドルウェア、ライブラリ等について、不正侵入の経路となるバックドア等が含まれていないことを確認し、サポートを受けられる安全なプロダクトを選定すること

イ 実施内容

- セキュリティ要件に基づき、調達仕様書のセキュリティ仕様策定
- セキュリティ仕様に関する、委託先との責任範囲の明確化
- 委託先に求めるセキュリティ管理基準の策定
- セキュリティ仕様を満たす能力を有した安全な委託先の選定
- 不正侵入の経路となるバックドア等が含まれていない、サポートを受けられる安全なプロダクトの選定

ウ 重要なセキュリティ対策の考え方

- 委託先との責任範囲の明確化
  - ➢ デジタル革新による委託事業者の多様化に伴い、委託先とのセキュリティ仕様の責任分界の曖昧さに起因するインシデントやセキュリティ運用不備等が多発している。
  - ➢ セキュリティ対策やセキュリティ運用の抜け漏れが発生しないよう、開発業務、運用業務の双方において、委託元と委託先の責任範囲を明確にする。
  - ➢ 特にクラウドサービス事業者を利用する場合は、クラウドサービスの責任共有モデルを理解した上で、クラウドサービスの提供形態（IaaS、PaaS、SaaS）に合わせて委託元、委託先の責任範囲を明確にする。
  - ➢ 当然ながら、委託元のセキュリティ対策の不備について、委託元の管理責任や説明責任が問われることも発生しうることから、責任範囲を明確にした上で、委託元として、委託先のセキュリティ実施状況を管理、監督すること。

- セキュリティ仕様を満たす能力を有した委託先の選定、管理
  - ➢ 委託先の能力不足、管理不足が原因によるセキュリティインシデントが多

発しているため、安全な委託先を選定し、適切な管理を行うことが肝要である。

- システムのセキュリティ要件に基づくセキュリティ仕様を策定した上で、当該仕様を満たす能力を有した委託先を選定する。
- システム基盤にクラウドサービスを使用する場合は、ISMAP の運用フローに従ってクラウドサービスを選定する。
- 委託先のセキュリティ管理の不備によるインシデント等を防止するため、委託先に求めるセキュリティ管理基準を策定し、委託先を管理、監督する。

- バックドア等が含まれていない安全なプロダクトの選定
  - サプライチェーンの多様化、グローバル化に伴い、調達したソフトウェアや機器が原因による、セキュリティインシデントが多発している。
  - システムで利用するサードパーティのライブラリやミドルウェア、機器については、信頼できる事業者が提供する、不正侵入の経路となるバックドア等が含まれていない安全なプロダクトを選定する。
  - システムの稼働期間中、脆弱性が検出された場合にセキュリティパッチ提供等のサポートが受けられる、プロダクトを選定する。

4)セキュリティ設計

ア 要求事項

- セキュリティ要件を満たすように実装方針を具体化し、システムにおける機能面と非機能面でのセキュリティ設計が実施されていること
- 堅牢（攻撃経路が少なく、多層多重で守られている）でサイバーレジリエントな設計が実施されていること

イ 実施内容

- セキュリティ設計の実施
  - アプリケーションセキュリティ
  - OS セキュリティ
  - ミドルウェアセキュリティ
  - ネットワークセキュリティ
  - クラウドセキュリティ
  - 物理セキュリティ
  - セキュリティ運用（平時、有事）

ウ 重要なセキュリティ対策の考え方

- アタックサーフェス（攻撃対象領域）の管理、防御
  - セキュリティ設計においては、攻撃対象となるアタックサーフェス（攻撃対象領域）を極力減らす設計を行い、防御することが重要となる。
  - システムにおけるアタックサーフェス（攻撃対象領域）を把握するため、システムで使用する資材の資産管理を実施し、最新な状態を維持する。
  - システムで使用するハードウェアやソフトウェア等の資産に関して、脆弱性管理可能な仕組みを導入する。
  - 攻撃者による悪用を防止するため、システムにおいて不要な機能やサービスは実装しない。プラットフォームに初期設定でインストールされているような機能、サービスも使用しない。
  - 外部 I/F への入力に関しては、信頼せず、必ず入力値検証を実施する。

- 管理者アカウントの保護
  - 権限管理に起因するインシデント被害を極小化するため、ユーザアカウント、管理者アカウントに対して過剰なアクセス権限は付与しない。
  - とりわけ、管理者アカウントの悪用は被害が大きくなるため、管理者権限の利用者は必要最小限にとどめ、管理者アカウントによるアクセスには多要素認証等を用いて十分に保護する。
  - 管理者アカウントの利用者を特定可能な仕組みを導入し、追跡可能な状態にする。

- サイバーレジリエントな設計の実施
  - サイバー攻撃の大規模化、高度化に伴い、攻撃は成功し、インシデントは発生する前提にたち、防御力だけでなく回復力（サイバーレジリエンス）を高める設計が重要となる。
  - システムアーキテクチャの設計においても、ネットワーク分離やアクセス権の必要最小権限付与、ゼロトラストセキュリティの考えに基づく対策の導入等、インシデント発生時のシステムへの被害を極小化するための設計が求められる。
  - 必要な機器やソフトウェアのログ、セキュリティ製品のアラート等を収集/分析し、インシデント等異常な状態を速やかに検知するため、独立した監視環境を用意することが、セキュリティ運用上重要となる。
  - インシデント検知をした際は、速やかなインシデント対応やサービス復旧を可能とする、運用体制や運用プロセスの整備が求められる。速やかなサービス復旧を行うため、重要データのバックアップやリストア手順を事前

に準備する。

5)セキュリティ実装

ア 要求事項

- 設計に基づいて、セキュリティ機能の実装が完了していること
- セキュリティ設計方針に基づいて、脆弱性を作りこまないよう、アプリケーションのセキュアコーディングが実施されていること
- セキュリティ設計方針に基づいて、システム基盤となるプラットフォームのセキュリティ設定の実施（堅牢化）が完了していること

イ 実施内容

- 設計に基づくシステムにおけるセキュリティ機能の実装
- セキュリティ設計に基づくアプリケーションのセキュアコーディング
- セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施(堅牢化)
  - OS セキュリティ
  - ミドルウェアセキュリティ
  - ネットワークセキュリティ
  - クラウドセキュリティ
  - 物理セキュリティ

ウ 重要なセキュリティ対策の考え方

- セキュリティテンプレート、自動化技術の活用
  - セキュリティ実装においては、担当者によるミスやばらつきの発生を防止することが重要であるため、セキュリティ関連のコーディングや設定は、テンプレートの使用や、自動化機能を用いて対応することが望ましい。
  - アプリケーション開発は、安全で利便性の高い、セキュアコーディングをサポートするような機能を有した開発用ツールやフレームワークを活用することで、人為的なミスを抑え、セキュリティ確保することが有効である。
  - システム基盤のセキュリティに関しては、各種プラットフォーム向けに最適化されたセキュリティベンチマーク（ベストプラクティス）やセキュリティ設定が組み込まれたシステムイメージ、テンプレート等を使用することで、人為的なミスや担当者による品質のばらつきを防止する。また、ベンチマークやテンプレートを用いてセキュリティ設定を可視化し、ベースラインとすることで、セキュリティ監査等の実行容易性も向上する。

6)セキュリティテスト

ア 要求事項

- セキュリティ機能に対する各種テストが実施され、品質が確保されていること
- 脆弱性診断を実施し、システムにおける脆弱性が取り除かれていること

イ 実施内容

- セキュリティ機能テストの実施（単体テスト、結合テスト、システムテスト等）
- 脆弱性診断の実施
  - webアプリケーション脆弱性診断
  - プラットフォーム脆弱性診断
  - スマートフォンアプリケーション診断
  - 高度セキュリティ診断（ペネトレーションテスト、レッドチームテスト等）
- 機能テストで検出されたバグの是正対応
- 脆弱性診断で検出された脆弱性に対する、リスクベースの是正対応

ウ 重要なセキュリティ対策の考え方

- システム特性、システム重要度に応じた適切な脆弱性診断の実施
  - 脆弱性診断の実施に関しては、アタックサーフェス（攻撃対象領域）に対して漏れなく脆弱性診断が実施されるように、システム特性に応じた適切なスコープな脆弱性診断を実施する。
  - また、重要度の高いシステムにおいては、脆弱性診断ツールのみを実行する表層的な脆弱性診断では不十分であるため、専門家による高度な診断を追加で実施する等、リスクレベルに応じた適切な品質の脆弱性診断を実施することが重要となる。

7)セキュリティ運用準備

ア 要求事項

- セキュリティ運用（平時、有事）を実施するのに十分な運用体制が確立されていること。
- セキュリティ手順が策定され、運用の実行性が確保されていること

イ 実施内容

- セキュリティ運用体制の確立
- 下記項目に対応したセキュリティ運用手順の整備

  □平時の運用
  - 構成管理、変更管理
  - セキュリティ製品のアラート、システムログ等を活用したセキュリティ監視、検知
  - 脅威情報収集、自システムへの影響分析
  - CVSS 等に基づく、リスクに応じた脆弱性対応
  - 定期的な脆弱性診断の実施

  □有事の運用
  - インシデント対応
- 有事を想定したセキュリティ運用訓練の実施

ウ 重要なセキュリティ対策の考え方

- インシデント発生を想定した運用訓練の実施
  - セキュリティ運用手順等を整備しても、実際にインシデントが発生すると、手順どおりに対応が進まず、対応に時間を要して被害が拡大するケースが多々ある。
  - 主要な想定脅威（リスクシナリオ）については、関係者を含めて、インシデント発生を想定した訓練を実施し、実運用上の課題を特定し、体制や手順の見直しを行うことで、インシデント対応の実行性を担保する。
  - 運用訓練実施後に関係者にフィードバックを行うことで、セキュリティ意識の向上やインシデント対応手順の理解の定着をはかる。

8)セキュリティ運用

ア 要求事項

- システムに影響する脅威情報、脆弱性情報が定常的に収集、分析されていること
- 速やかなインシデント（予兆）の検知、インシデント発生時の対応、システム復旧を実施すること

イ 実施内容

- セキュリティ運用の実施（下記）

□平時の運用

- 構成管理、変更管理
- セキュリティ製品のアラート、システムログ等を活用したセキュリティ監視、検知
- 脅威情報収集、自システムへの影響分析
- CVSS 等に基づく、リスクに応じた脆弱性対応
- 定期的な脆弱性診断の実施

□有事の運用

- インシデント対応

ウ 重要なセキュリティ対策の考え方

- ソフトウェアの構成管理
  - アプリケーションで使用するライブラリやミドルウェア等に深刻な脆弱性が発見された場合、自システムで該当のライブラリやミドルウェアが該当のものが含まれるかどうかを迅速に判断できるよう、システムで使用するソフトウェアの開発元、バージョン、ライセンス、依存関係などを容易に参照できるような構成管理を行う（SBOM 等を利用したソフトウェア構成管理を行うことも有用)。

- 定常的な脅威情報の収集、分析、リスクに応じた対応（脆弱性対応含）
  - 日々新たに出現するセキュリティ脅威や脆弱性に対処するため、定常的に脅威情報や脆弱性情報を収集し、自システムへの影響含めてリスク分析を行う。
  - 脆弱性においては CVSS の値に基づき、当該脆弱性によるシステム環境への影響を分析し、甚大な被害の発生が想定される脆弱性に対しては緊急にセキュリティパッチを適用する等、対応方針決定する。
  - 上記の脅威情報や脆弱性への対応方針については、都度個別判断を実施するのではなく、事前に脆弱性対応方針を整理し、それに従った運用を実践することで円滑な対応が可能となる。

- サイバーレジリエントなセキュリティ運用
  - インシデント（その兆候）の早期検知、速やかなインシデント対応やサービス復旧を実践することで、インシデント発生時のシステム被害やサービスへの影響を極小化する。
  - インシデント対応やサービス復旧の実行性を維持するため、定期的にインシデント対応手順やサービス復旧手順の見直しを行い、不具合が特定され

た際は速やかに改善する。また、運用開始後の定期的なインシデント対応訓練の実施は、組織の緊張感を高めるとともに、インシデント対応手順の実行性担保に有効である。

- セキュリティインシデントが発生した際は、根本的な発生源の原因究明を行い、再発防止策を講じる。また、実際のインシデント対応で円滑に進まなかった点について振り返りを行い、改善を繰返すマネジメントサイクルを構築することで、インシデント対応レベルの成熟度向上に努める。

５　セキュリティ・バイ・デザインのリスク管理体制

５．１セキュリティ・バイ・デザインのリスク管理に関わる関係者の役割

セキュリティ・バイ・デザイン実施にあたっては、システムライフサイクル全体を通して俯瞰的にセキュリティを確保できる能力や経験を有した専門家をシステム開発チームに指名することが、人材不足により、困難なケースが多い。仮に開発チームに専門家が指名可能な場合でも、セキュリティ対策の妥当性が検証されずに、後工程に進めてしまうケースも散見される。

よって、セキュリティ品質確保の観点から、政府情報システムにおけるセキュリティ・バイ・デザインにおいては、開発チームが各工程でセキュリティ対策を実施するだけでなく、専門的な知見を有した、評価者による客観的なリスク評価の実施を必要とする。

また、評価者によるリスク評価結果に基づいて確実に是正対応が行われるよう、リスク対応状況を継続して管理するための、リスク管理の仕組み（体制、運用プロセス）を整備することも肝要となる。

したがって、本項では、セキュリティ・バイ・デザインにおけるリスク評価、リスク管理に関わる関係者の役割（呼称）と当該役割に求められる責任を示す。

3 章記載のとおり、本書のスコープをふまえ、リスク評価、リスク管理の具体的な運用プロセスは、各政府機関のセキュリティルールや環境に依存するため規定しない。

表 ５-1　セキュリティ・バイ・デザインに関わる関係者の役割と責任

項番	役割（呼称）	責任
1	システム管理者	•システムライフサイクル全体を通して漏れのないセキュリティ対策が実施できるよう、委託先実施者との責任範囲を明確にし、セキュリティ対策全体を管理する。 •システム開発、運用の各工程において、要求事項を満たすようにセキュリティ対策を実施するとともに、工程間のセキュリティ対策の整合性を担保する。 •セキュリティリスクアセッサーによる、セキュリティ対策に対するリスク評価結果に対して、ビジネス/リスクオーナーの指示に従って、是正対応を行う。 •セキュリティリスクアセッサーによるリスク評価の実施を補助する。

項番	役割（呼称）	責任
2	委託先実施者	•システム管理者からの委託を受け、責任範囲にかかるセキュリティ対策を実施する。 •セキュリティリスクアセッサーによるリスク評価の実施を補助する。
3	ビジネス/リスクオーナー	•セキュリティリスクの管理主体として、ビジネスリスク（機会損失、財務リスク等）を総合的に勘案し、セキュリティリスク対応方針（リスク回避、低減、保有、移転等）を決定するための考え方を整理する。 •上記考え方に基づいて、セキュリティリスク対応方針（リスク回避、低減、保有、移転等）を決定し、システム管理者に対してセキュリティリスクへの是正対応方針を指示する。 •残存リスクを総合的に判断し、サービス運用を認可する。 •システム管理者によるセキュリティリスクへの是正対応状況を管理する。
4	セキュリティリスクアセッサー（評価者）	•セキュリティ・バイ・デザインの任意の工程または全工程において、業務観点及びシステム観点でのセキュリティリスク評価（文書レビュー、脆弱性診断等）を実施する。（具体的にどの工程でセキュリティリスク評価を実施するかは、環境に依存するため、明記しない） •セキュリティリスク評価結果や是正対応の推奨策をシステム管理者に進言する。 •システムのセキュリティリスク対応状況をモニタリングし、セキュリティ上問題がある場合、システム管理者やビジネス/リスクオーナーに対して勧告、提言をおこなう。

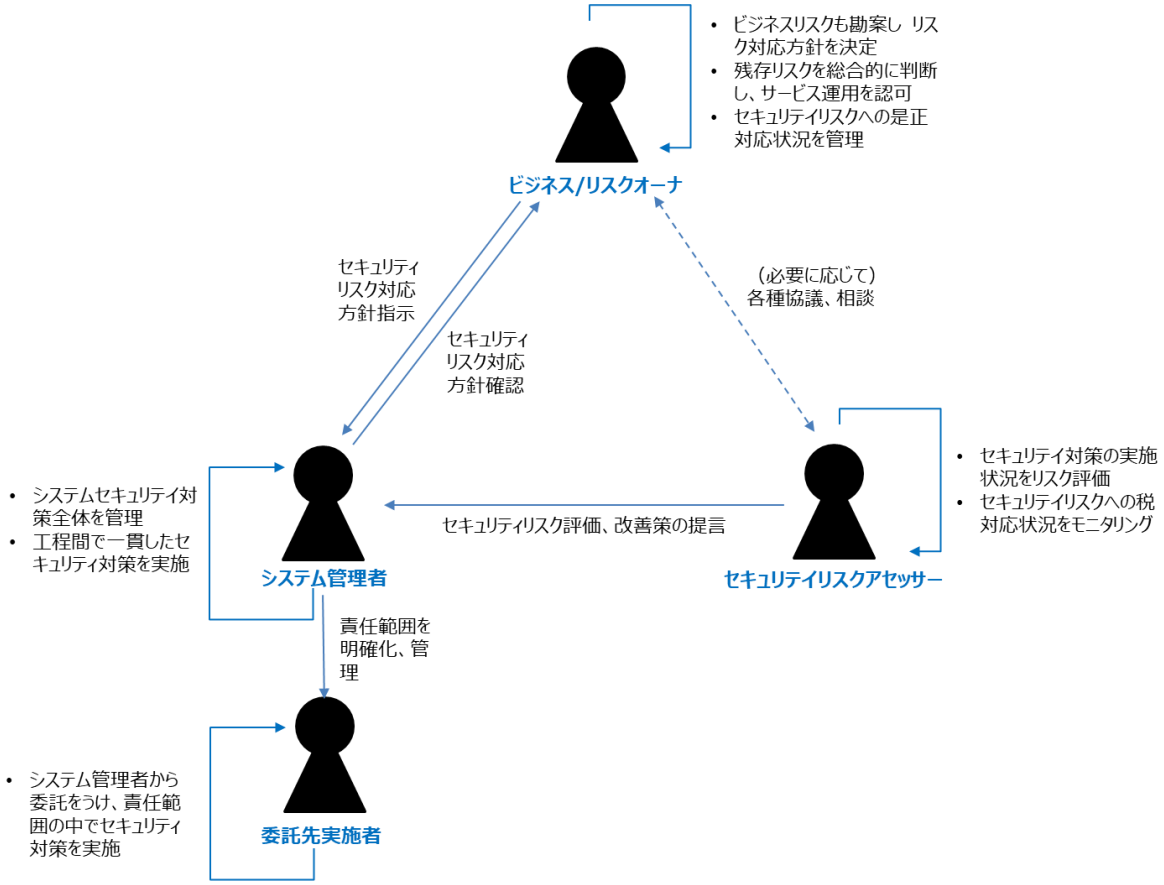


図 5-1 セキュリティ・バイ・デザインに関わる関係者

６　セキュリティ・バイ・デザイン実施における留意事項

本書の最後に、前章までの内容もふまえて、セキュリティ・バイ・デザイン実施にあたっての留意事項について示す。

- セキュリティ・バイ・デザインにおいては、工程間で不整合なセキュリティ対策が実施されることにより、システムのセキュリティ品質を確保することが困難になるため、工程間で一貫した、整合性が確保されたセキュリティ対策を実施する。

- 本紙記載のセキュリティ・バイ・デザインの実施内容の全てを同時期に実現することは困難であることが想定される。自組織の開発プロセスやルール等を考慮し、実施可能な箇所から運用(各工程でのセキュリティ対策の実施、リスク評価)を開始し、課題の改善と内容の拡充をはかりながら、成熟度を向上していくことが求められる。

- セキュリティ・バイ・デザインは一度実施して終了でなく、新たなセキュリティ脅威の出現やシステム変更等の場合においては、セキュリティ・バイ・デザインの再実施要否、(要の場合) 再実施方法を検討し、継続的にセキュリティリスクの軽減をはかることが肝要である。

別紙 1　各工程で参照可能なセキュリティ標準

#	提供元	セキュリティ標準名	対象工程	URL
1	NISC(内閣サイバーセキュリティセンター)	政府機関等のサイバーセキュリティ対策のための統一基準（以下、「統一基準群」という。）	工程全般	https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf
2	NISC(内閣サイバーセキュリティセンター)	政府機関等の対策基準策定のためのガイドライン	工程全般	https://www.nisc.go.jp/pdf/policy/general/guider3.pdf
3	NISC(内閣サイバーセキュリティセンター)	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(SBD マニュアル)	セキュリティ要件定義	https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html
4	NISC(内閣サイバーセキュリティセンター)	インターネットの安心・安全ハンドブック	工程全般	https://security-portal.nisc.go.jp/handbook/index.html
5	デジタル庁	政府情報システムにおける脆弱性診断ガイドライン	セキュリティテスト、セキュリティ運用	https://www.digital.go.jp/resources/standard_guidelines/#ds221
6	デジタル庁	ゼロトラストアーキテクチャ適用方針ガイドライン	セキュリティ要件定義、セキュリティ設計	https://www.digital.go.jp/resources/standard_guidelines/#ds210
7	デジタル庁	CRSA アーキテクチャ技術レポート	セキュリティ要件定義、セキュリティ設計	https://www.digital.go.jp/resources/standard_guidelines/#ds211
8	IPA（情報処理推進機構）	安全な web サイトの作り方	セキュリティ設計	https://www.ipa.go.jp/security/vuln/websecurity.html
9	IPA（情報処理推進機構）	TLS 暗号設定ガイドライン	セキュリティ設計	https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
10	IPA（情報処理推進機構）	組織における内部不正防止ガイドライン	セキュリティ要件定義 セキュリティ	https://www.ipa.go.jp/security/fy24/reports/insider/index.html

#	提供元	セキュリティ標準名	対象工程	URL
			設計	
11	ISMAP 運営委員会	政府情報システムのためのセキュリティ評価制度	セキュリティ選定	https://www.ismap.go.jp/csm
12	METI（経済産業省）	クラウドサービス利用のための 情報セキュリティマネジメントガイドライン	セキュリティ要件定義 セキュリティ設計	https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf
13	各府省情報化統括責任者連絡会	行政手続におけるオンラインによる本人確認の手法に関するガイドライン	セキュリティ要件定義 セキュリティ設計	https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf
14	CRYPTREC	電子政府推奨暗号リスト	セキュリティ実装	https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf
15	IPA（情報処理推進機構）	『高度標的型攻撃』対策に向けたシステム設計ガイド	セキュリティ設計	https://www.ipa.go.jp/security/vuln/newattack.html
16	総務省	サイバー攻撃（標的型攻撃）対策防御モデルの解説	セキュリティ設計	https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html
17	総務省	テレワークセキュリティガイドライン	セキュリティ設計	https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
18	NIST（National Institute of Standards and Technology）	Cybersecurity Framework	工程全般	https://www.ipa.go.jp/files/000071204.pdf https://www.ipa.go.jp/files/000071205.xlsx
19	NIST（National Institute of Standards and Technology）	SP 800-53（組織と情報システムのためのセキュリティおよびプライバシー管理策）	セキュリティ要件定義 セキュリティ設計	https://www.ipa.go.jp/files/000092657.pdf https://www.ipa.go.jp/files/000092658.pdf
20	FedRAMP	FedRAMP(米国政府機関におけるクラウドセキュリティ認証制度)	セキュリティ要件定義 セキュリティ設計	https://www.fedramp.gov/documents-templates/

#	提供元	セキュリティ標準名	対象工程	URL
21	NIST (National Institute of Standards and Technology)	SP 800-190 (アプリケーションコンテナセキュリティガイド)	セキュリティ設計	https://www.ipa.go.jp/files/000085279.pdf
22	NIST (National Institute of Standards and Technology)	SP-800-207 (ゼロトラストアーキテクチャ)	セキュリティ設計	https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html
23	ANSSI (フランス国家情報システムセキュリティ機関)	EBIOS RISK MANAGER	セキュリティリスク分析	https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/
24	NCSC (National Cyber Security Centre)	Secure design principle	セキュリティ設計	https://www.ncsc.gov.uk/collection/cyber-security-design-principles
25	CIS (Center for Internet Security)	CIS controls Version 8	セキュリティ設計	https://www.cisecurity.org/controls/v8/
26	CIS (Center for Internet Security)	CIS Benchmarks	セキュリティ実装	https://www.cisecurity.org/cis-benchmarks/
27	JPCERT/CC	セキュアコーディング (関連資料)	セキュリティ実装	https://www.jpcert.or.jp/securecoding/
28	OWASP	OWASP 10	セキュリティ設計	https://owasp.org/www-project-top-ten/
29	ISO	ISO27017, ISO27018	セキュリティ要件定義 セキュリティ設計	-
30	MVSP (Minimum Viable Secure Product)	Minimum Viable Secure Product Controls	セキュリティ要件定義 セキュリティ設計	https://mvsp.dev/mvsp.en/index.html

#	提供元	セキュリティ標準名	対象工程	URL
31	CSA (Cloud Security Alliance)	クラウドコンピューティングのためのセキュリティガイダンス	セキュリティ要件定義 セキュリティ設計	http://www.cloudsecurityalliance.jp/guidance.html
32	CSA (Cloud Security Alliance)	Cloud Controls Matrix (CCM)	セキュリティ要件定義 セキュリティ設計	https://cloudsecurityalliance.org/research/cloud-controls-matrix/
33	JSSEC	スマートフォン&タブレットの業務利用に関するセキュリティガイドライン	セキュリティ設計	https://www.jssec.org/dl/guidelines_v2.pdf
34	JSSEC	Android アプリのセキュア設計・セキュアコーディングガイド	セキュリティ実装	https://www.jssec.org/report/securecoding.html
35	JPCERT/CC	高度サイバー攻撃への対処におけるログの活用と分析方法	セキュリティ設計 セキュリティ運用準備	https://www.jpcert.or.jp/research/apt-loganalysis.html
36	JPCERT/CC	インシデントハンドリングマニュアル	セキュリティ運用準備 セキュリティ運用	https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf
37	IPA (情報処理推進機構)	共通脆弱性評価システム CVSS v3 概説	セキュリティ設計 セキュリティ運用準備	https://www.ipa.go.jp/security/vuln/CVSSv3.html
38	各府省情報化統括責任者連絡会	標準ガイドライン群	工程全般	https://cio.go.jp/guides
39	IPA (情報処理推進機構)	情報セキュリティ普及啓発資料	工程全般	https://www.ipa.go.jp/security/keihatsu/index.html
40	NISC(IPA)	セキュリティ関連 NIST 文書	工程全般	https://www.ipa.go.jp/security/publications/nist/

#	提供元	セキュリティ標準名	対象工程	URL
41	METI（経済産業省）	サイバーセキュリティ政策	工程全般	https://www.meti.go.jp/policy/netsecurity/index.html
42	総務省	情報管理担当者の情報セキュリティ対策	工程全般	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html

別紙 2　各工程のセキュリティチェックリスト

本紙は、4 章に記載したセキュリティ・バイ・デザインの実施内容に基づいた、各工程で実施すべき項目をチェックリストとして示す。

セキュリティ・バイ・デザインの関係者は、本チェックリストを用いて各工程でのセキュリティ・バイ・デザインの実施状況を把握し、本来実施すべき内容の抜け漏れを防止することが求められる（原則全ての項目を実施することが望ましいが、システム特性等に応じて該当しない項目が生じる場合もあることを考慮する）。

①セキュリティリスク分析/セキュリティ要件定義のチェックリスト

#	確認項目	チェック
1	システムで取扱う重要情報の種類、重要情報のフローやライフサイクルが分かる内容、アクター、実施業務、他システムとの連携方法等を記載したシステムプロファイルを作成している	□
2	一般的な脅威分析モデルなどを用いて、対象システムにて発生が想定されるセキュリティ脅威を特定している	□
3	セキュリティ脅威に対するリスク分析を実施し、セキュリティ対応方針を決定している（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソース等）	□
4	セキュリティ対応方針に従って、システムで満たすべきセキュリティの状態を機能面、非機能面ともに要件として定義している	□
5	サイバー攻撃は成功する前提で、多層でセキュリティ対策を実施することで被害を極小化する考え方に基づいて、セキュリティ要件を定義している	□

②セキュア調達のチェックリスト

#	確認項目	チェック

1	セキュリティ要件に基づき、調達におけるセキュリティ仕様（外部委託業務）を策定している	□
2	システムのセキュリティ対策、セキュリティ運用に抜け漏れが発生しないよう、自組織と委託先のセキュリティ対策に関する責任範囲を明確化している	□
3	セキュリティ仕様を実装できる能力を有し、セキュリティ管理基準を満たす安全な委託先を選定している	□
4	システムで利用する機器、ミドルウェア、ライブラリについて、不正侵入の経路となるバックドア等が含まれておらず、サポートを受けられる安全なプロダクトを選定している	□

③セキュリティ設計のチェックリスト

#	確認項目	チェック
1	セキュリティ設計の取りこぼしや属人化を避けるため、セキュリティベースラインやセキュリティフレームワークを導入して、セキュリティ設計を検証または実施している	□
2	外部からのアタックサーフェスを必要最小限に抑えるため、システムの操作に必要な外部インターフェースのみを公開する仕様としている	□
3	不要な機能、サービス、データはシステムから取り除いている	□
4	全ての外部入力は信頼せず、検証した上で、システムに被害が発生しないよう、安全に変換処理している	□
5	特定のセキュリティ対策が無効化された場合でも、システムに被害が発生しないように、多層/多重でのセキュリティ対策を実施している	□
6	アプリケーションセキュリティ、ネットワークセキュリティ、プラットフォームセキュリティ（OS、ミドルウェア）の全構成要素において、もれなくセキュリティ対策を実施している	□
7	セキュリティ対策方針として、セキュリティインシデントの発生防止は困難という前提で、防御力だけでなく、回復力（サイバーレジリエンス）を高める設計を実施している	□
8	システム分離（ネットワーク分離）、アカウントへの必要最低限のアクセス権付与等、インシデント発生時の被害拡大を防止するための対策を実施している	□
9	セキュリティ運用設計として、想定脅威の検知に必要なログやセキュリティアラートを定義し、収集/一元管理する設計を実施して	□

#	確認項目	チェック
	いる	
10	セキュリティ運用設計として、ログやセキュリティアラートを定期的に分析し、異常な状態を速やかに検知するための仕組みを検討している	□
11	セキュリティ運用設計として、インシデント発生時に速やかにインシデント対応、システム復旧を可能とするための体制や手順を策定している	□
12	運用フェーズで発生する脆弱性に対する対応基準、対応方針を策定している	□

④セキュリティ実装のチェックリスト

#	確認項目	チェック
1	アプリケーションセキュリティに関して、セキュリティ設計に基づき、コーディング規約を遵守してセキュアコーディングを実施している	□
2	セキュアコーディングをサポートする機能を有した開発用フレームワークやツール等を活用することで、脆弱性を作りこまないようにセキュアコーディングを実施している	□
3	アプリケーションセキュリティに関して、信頼できる安全なライブラリやミドルウェアを利用している。	□
4	プラットフォームセキュリティに関して、セキュリティ設計に基づいてセキュリティ設定（堅牢化）を実施している（クラウド含む OS、ミドルウェア、ネットワーク等）	□
5	プラットフォームセキュリティに関して、セキュリティ設定（堅牢化）の属人性を排除するため、セキュリティテンプレートやセキュリティ設定が組み込まれたシステムイメージを利用している	□

⑤セキュリティテストのチェックリスト

#	確認項目	チェック
1	セキュリティ機能のテストを実施している	□
2	システム特性を考慮して、アタックサーフェス（攻撃対象領域）をカバーするように脆弱性診断を実施している	□
3	システムの重要度等踏まえて、必要な品質レベルの脆弱性診断を実施している（重要度が高いシステムにおいては、脆弱性診断ツールを実行するだけでなく、専門家による高度な診断を実施す	□

#	確認項目	チェック
	る、等）	
4	セキュリティ機能のテスト結果に従って、バグを修正している	□
5	脆弱性診断結果に従って、当該脆弱性によって引き起こされるリスク等を考慮し、脆弱性に対して必要な修正を実施している	□

⑥セキュリティ運用準備のチェックリスト

#	確認項目	チェック
1	セキュリティ運用（平時、有事）を実施するのに十分な運用体制が確立している	□
2	セキュリティ運用の運用手順が整備している	□
3	有事を想定してセキュリティ訓練を実施し、インシデント対応手順の実行性を担保している	□

⑦セキュリティ運用のチェックリスト

#	確認項目	チェック
1	システム構成を管理し、最新化している	□
2	システムで使用するソフトウェアの開発元、バージョン、ライセンス、依存関係などを容易に参照できるような構成管理している	□
3	システム管理者アカウントの適正管理を行っている（古いアカウントが残らないよう、最新化している）	□
4	システムの変更管理に合わせて、セキュリティリスクが増大しないよう、セキュリティ対策を見直している	□
5	システムに影響する脅威情報や脆弱性情報を定常的に収集し、脅威や脆弱性による影響にかんするリスク分析等を実施し、自システムへの対応方針を決定している	□
6	ログやセキュリティアラートを用いた異常な状態の監視等を行い、インシデントやその兆候を早期検知するための仕組みを導入している	□
7	インシデント発生時に速やかに対応するためのインシデント対応体制、インシデント対応手順を整備している	□
8	インシデント発生後、速やかなシステム復旧を実現するため、重要データのバックアップ、システム復旧のリストア手順を整備し	□

#	確認項目	チェック
	ている	
9	インシデント対応プロセスやシステム復旧プロセスは、有効性確保のための定期的に見直し、更新している	□

別紙 3　システムにおける一般的なセキュリティ上の問題点

一般的にシステムにおけるセキュリティ上の問題点の傾向は下記表の通りである。これらのセキュリティ上の問題点を作りこまないよう、留意してシステム開発を進めることが求められる。

	要因	セキュリティ上の問題点
1	認証管理不備	•共用アカウントが使用される際に、利用者特定の仕組みや取扱いに関するルールが整備されていない •推測されやすい脆弱なパスワードが使用されている •認証情報がファイル等に平文で書かれている
2	アクセス制御不備	•必要な強度の認証が行われていない •ネットワーク、システムへのアクセス制限が実施されていない •アクセス権が必要最小限のアクセス権付与が守られておらず、過剰である
3	暗号化不備	•重要情報が流れる各機器間の通信経路で必要な暗号化が実施されていない
4	資産管理、脆弱性管理不備	•利用しているソフトウェアや機器の状態を把握していない（最新状態を維持できていない） •OS やミドルウェア、ファームウェア等の脆弱性対策が適切に実施されていない
5	Web アプリケーションの脆弱性	•SQL インジェクション、クロスサイトスクリプティング等の初歩的な web アプリケーションの脆弱性が存在している •パラメータ改ざんにより、本来アクセス権できないデータを操作できるなどの脆弱性が存在している
6	ログ管理不備	•ログ取得の範囲が目的に応じて定められていない（必要なログが取得されていない） •定期的なログの点検又は分析が実施されていない
7	外部委託の管理不備	• 外部委託に係る契約に、遵守事項で定める委託先の情報セキュリティ対策が含まれていない • 外部委託に係る契約に基づき、委託先における情報セキュリティ対策の履行状況を確認していない

別紙４　リスクランクに応じたセキュリティリスクアセッサーによる評価例

【セキュリティリスクランクに寄与するパラメータ】
■発生可能性
- インターネット公開有無
- 対象利用者（全国民、政府関係者、等）
- 近々のセキュリテイ監査実施状況　等

■影響（の大きさ）
- 予算
- 取扱う機密情報の機微性、量
- 社会的インパクト　等

リスクランクに応じて、各工程でのセキュリテイリスクアセッサーによる評価の内容を決定する
（リスクランクの高いシステムは各工程での検証を手厚く実施する）

優先度	リスクランク	セキュリティ要件定義工程 チェック内容	セキュリティ設計工程 チェック内容	セキュリティテスト工程 チェック内容	リリース判定
S	• 年間予算○○円以上 • セキュリティリスク「高」の場合 （発生可能性、影響を考慮）	• 調達仕様書レビュー • セキュリティ要件レビュー	• セキュリティ設計レビュー(セキュリティ関連の設計全て対象)	• 脆弱性診断（専門Tが全範囲対象に実施） • ペネトレーションテスト	• CISOによる確認 • セキュリティチェックリストリストを用いたプロセスチェック
A	• 年間予算□□以上 • セキュリティリスク「中」の場合 （発生可能性、影響を考慮）	• 調達仕様書レビュー • セキュリティ要件レビュー	• セキュリティ設計レビュー(外部I/Fに関わる部分のみ)	• 脆弱性診断（専門Tが全範囲対象に実施）	• CISOによる確認 • セキュリティチェックリストリストを用いたプロセスチェック
B	• （上記以外）	• セキュリティ要件レビュー	-	• 脆弱性診断（専門Tが一部を対象に実施）	• セキュリティT責任者（CISO代理）による承認

別紙５　政府情報システムにおけるクラウドセキュリティ要件策定、審査手順

1.　本手順の概要

本手順は、クラウドサービス選定にあたり調達仕様書に記載すべきセキュリティ要件の策定および当該要件に基づく事業者からのクラウドサービス提案内容を審査するための手順である。

2.　実施ステップ

本手順における実施ステップは下記の通りである。

ステップ①：クラウドサービスが満たすべき要件を策定
ステップ②：①の要件に基づく事業者からのクラウドサービス提案内容の審査

以降、ステップごとに具体的な実施手順を記載する。

ステップ①：クラウドサービスが満たすべき要件を策定

クラウドサービス選定にあたり調達仕様書に記載すべき要件は、以下の通りに分類される。調達仕様書には下記 a,b および c の要件を記載すること。

a.　統一基準等に基づく委託先に求める要件
b.　ISMAPに関連する要件
c.　個別のセキュリティ要件

以降で各要件の策定方法を記載する。

a.　統一基準等に基づく委託先に求める要件

「政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版 ）（https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf）」「4.1.1 業務委託(2) (b)(c)(d)」に規定されている委託先選定条件の内容を踏まえて、調達仕様書に要件を記載すること。（具体的な委託先選定条件は参考資料「統一基準に規定されている委託先選定条件」を参考にすること）

なお各府省の個別の委託先に求める要件も考慮すること。

b. ISMAPに関連する要件

ISMAP に関連するクラウドサービス事業者およびクラウドサービスが遵守すべき要件は、ISMAP のガバナンス基準、マネジメント基準における全ての基準、管理策基準のうち統制目標及び末尾に B が付された詳細管理策（以下「基本言明要件」という、該当する管理策基準は参考資料「クラウドサービスが遵守すべき ISMAP 管理策基準」を参照）となるため、当該内容を踏まえて調達仕様書に要件を記載すること。

原則、参考資料記載の全ての ISMAP 管理策基準が遵守すべき要件に該当するが、クラウドサービスにおける実施業務や取扱う情報等の特性を踏まえて、適用困難な ISMAP 管理策基準がある場合は、適用除外根拠を合理的に説明することで適用除外が認められる。

c. 個別のセキュリティ要件

上記 a.b の要件に加えて、クラウドサービスを使用する業務の特性や取扱う情報の機微性等を考慮し、リスクに見合ったセキュリティ要件を追加検討すること。

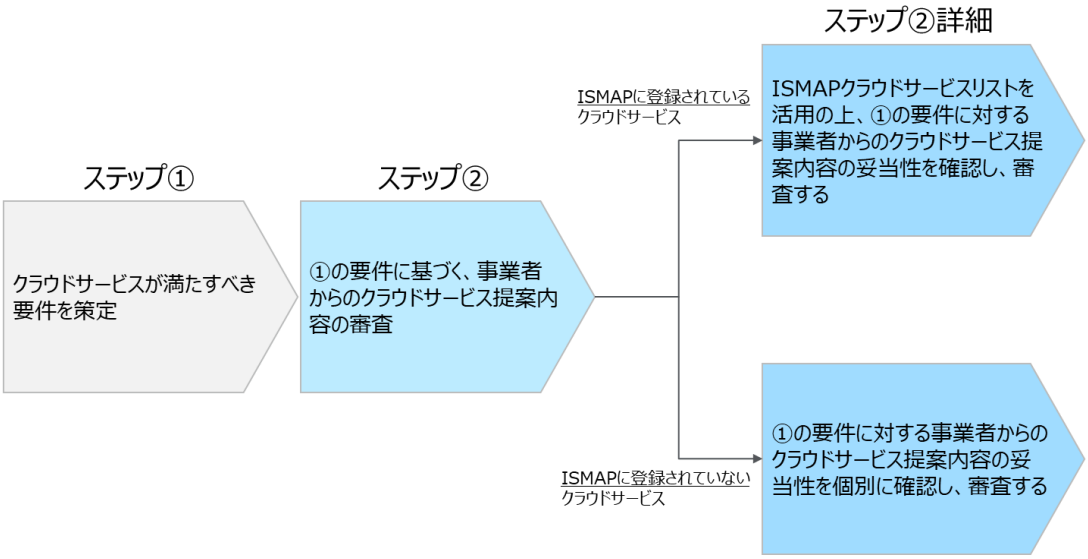
なお、機密性 3 情報をクラウドサービスで取り扱う場合には、ISMAP 管理策基準が想定する情報の格付を踏まえ、ISMAP 管理策基準の末尾に B が付された詳細管理策に加え、B が付されていない詳細管理策を複数要求するなど、必要な管理策をセキュリティ要件として追記する必要がある。

表. 個別のセキュリティ要件

項番	要件分類	セキュリティ要件	補足
例	保存データの暗号アルゴリズム	クラウドサービスで保存するデータの暗号アルゴリズムは、電子政府推奨暗号アルゴリズム（CRYPTREC）を使用可能であること	統一基準群を考慮した個別のセキュリティ要件
1			
2			

ステップ②：①の要件に基づく事業者からのクラウドサービス提案内容の審査

①の要件に基づく事業者からのクラウドサービス提案内容の審査において、下記図の示す通り、ISMAP クラウドサービスリストに登録されているサービスもしくは登録されていないサービスかで審査方法が異なる。



図．クラウドサービス提案内容の審査の全体概要

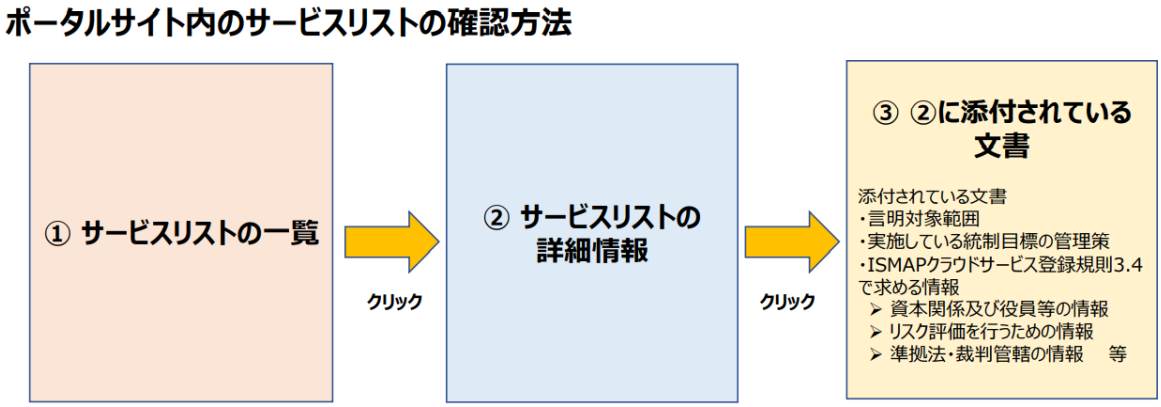
事業者からのクラウドサービス提案内容の具体的な審査方法については、下記表に従って実施すること。

表．クラウドサービスの審査方法

項番	クラウドサービスカテゴリ	クラウドサービス審査方法
1	ISMAP クラウドサービスリストに登録されているクラウドサービスを審査する	ISMAP クラウドサービスリストを活用し(参考資料「ISMAP ポータルサイト内のサービスリストの確認方法」参照)、ステップ①で策定した要件に対する事業者からのクラウドサービス提案内容の妥当性を確認し、審査する。要件の妥当性の確認観点は下記の通りとする。 [確認観点①] ● ISMAPクラウドサービスリストに登録されているクラウドサービスにおいても、対象外としているISMAP管理策基準があるため、対象サービスの「詳細情報の添付文書（統制目標の管理策）」を確認し、①で策定した「b.　ISMAPに関連する要件」に対する事業

		者からのクラウドサービス提案内容の妥当性を確認する。なお、基本言明要件のうち、詳細管理策は「詳細情報の添付文書（統制目標の管理策）」に記載されていないため、詳細について必要な場合はクラウド事業者に対して問合せを行うこと。 [確認観点②] ● ①で策定した「a. 統一基準等に基づく委託先に求める要件」、「c. 個別のセキュリティ要件」に対する事業者からのクラウドサービス提案内容の充足性を確認する。
2	ISMAP クラウドサービスリストに登録されていないクラウドサービスを審査する場合	ステップ①で策定した「a. 統一基準等に基づく委託先に求める要件」、「b. ISMAP に関連する要件」、「c. 個別のセキュリティ要件」に対する事業者からのクラウドサービス提案内容の充足性を確認し、審査する。

参考資料　ISMAP ポータルサイト内のサービスリストの確認方法



ISMAP クラウドサービスリスト（ポータルサイト内）https://www.ismap.go.jp/csm?id=cloud_service_list

図　ISMAP ポータルサイト内のサービスリスト確認方法

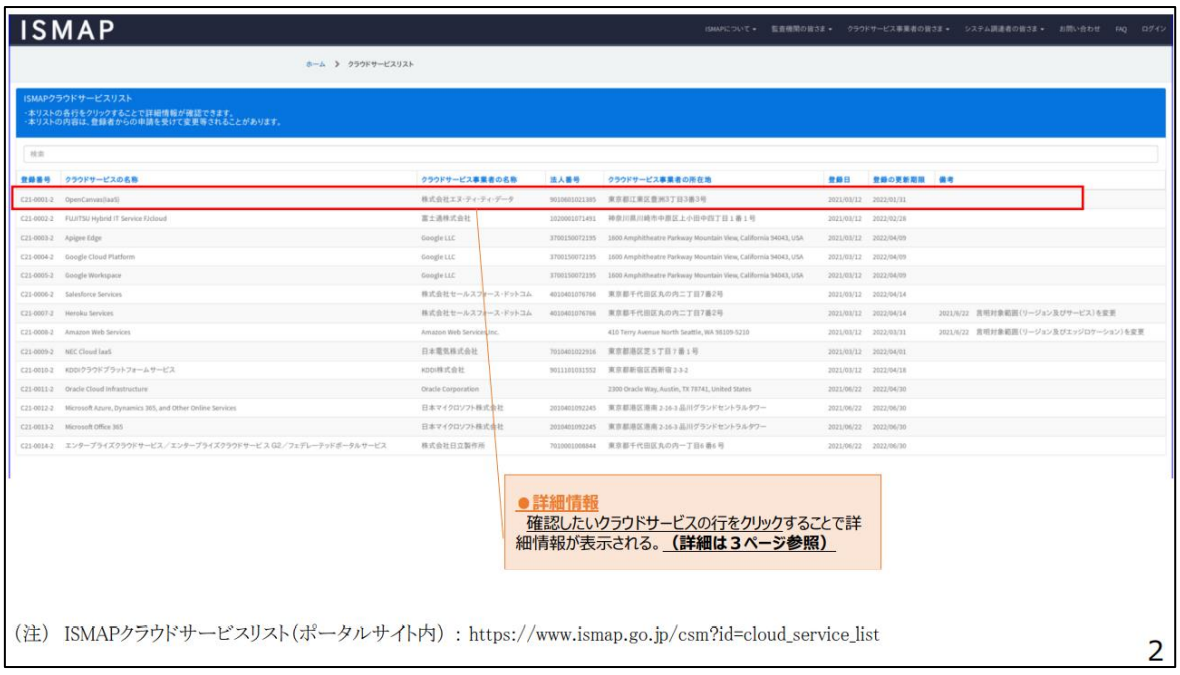


図　サービスリストの一覧について

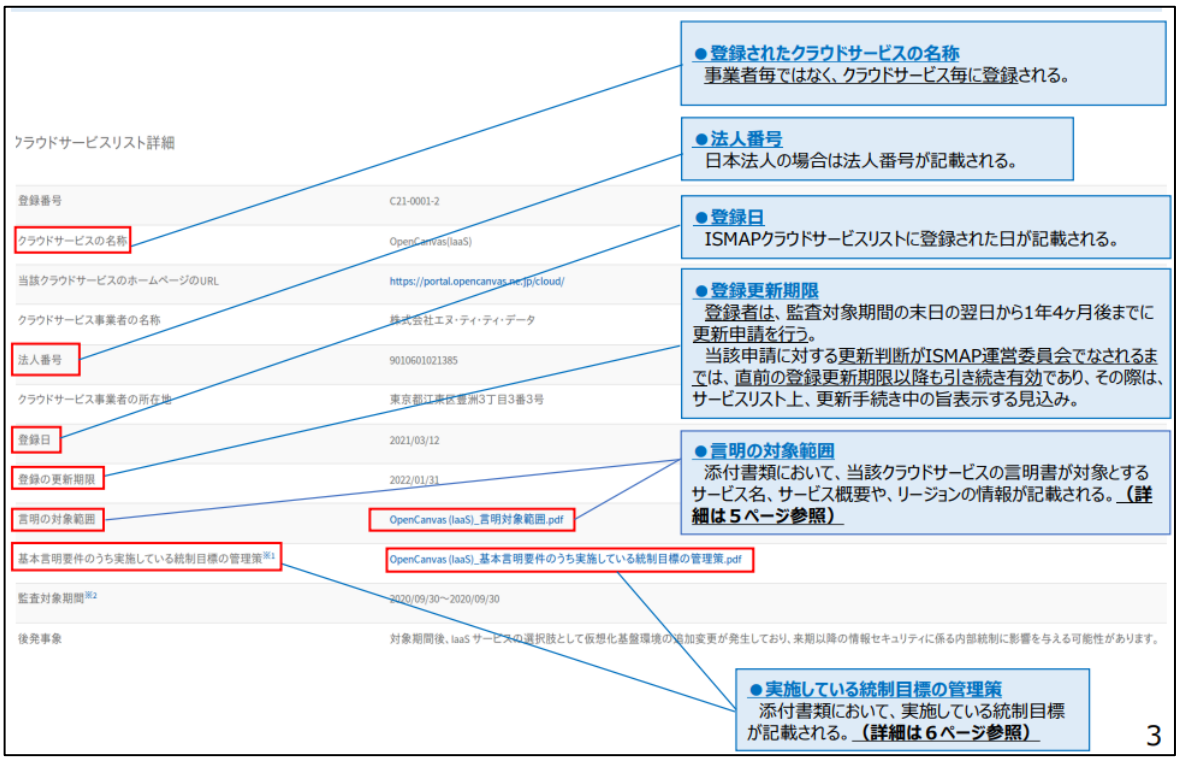


図　サービスリストの詳細情報について（１）

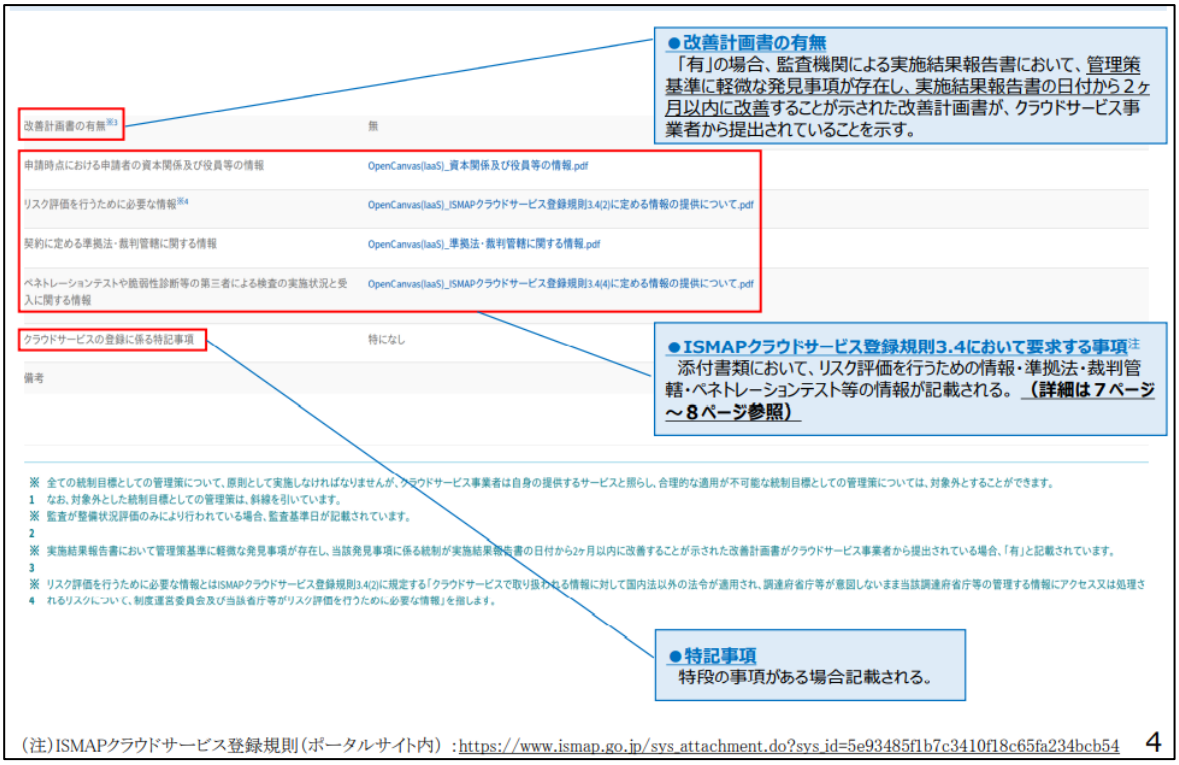


図　サービスリストの詳細情報について（2）

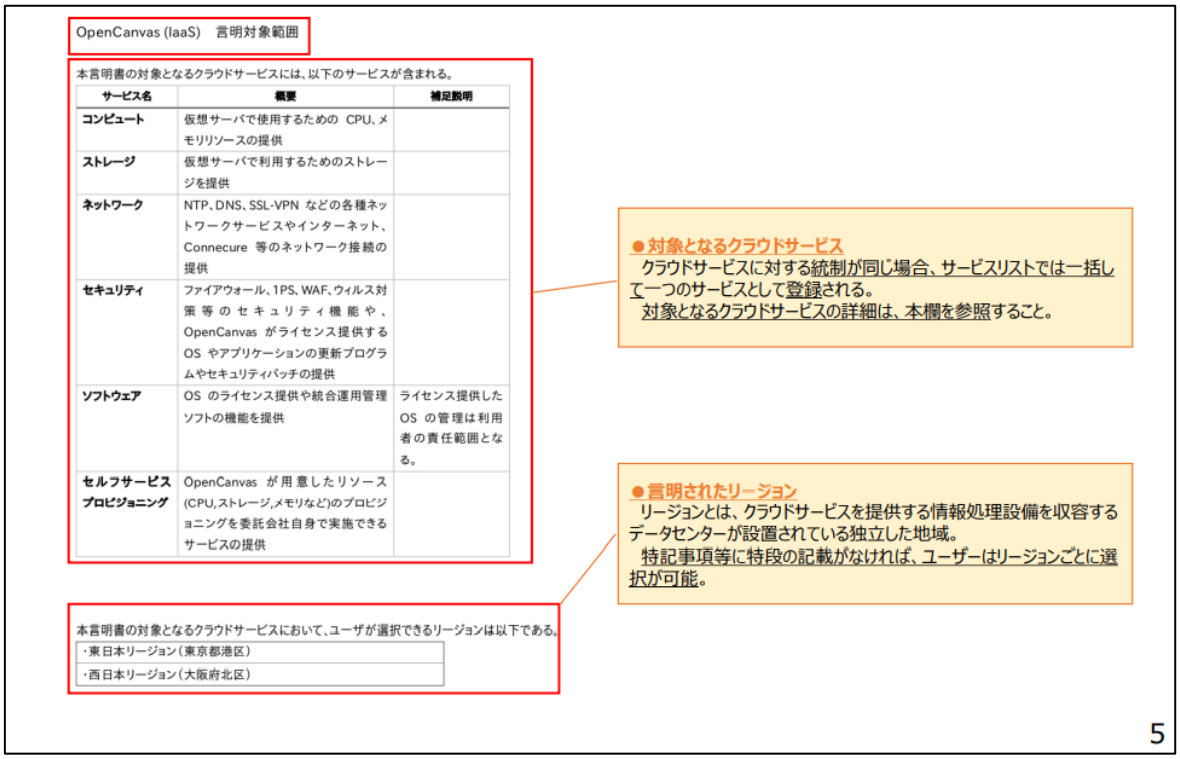


図　詳細情報の添付文書（言明対象範囲）

図　詳細情報の添付文書（統制目標の管理策）

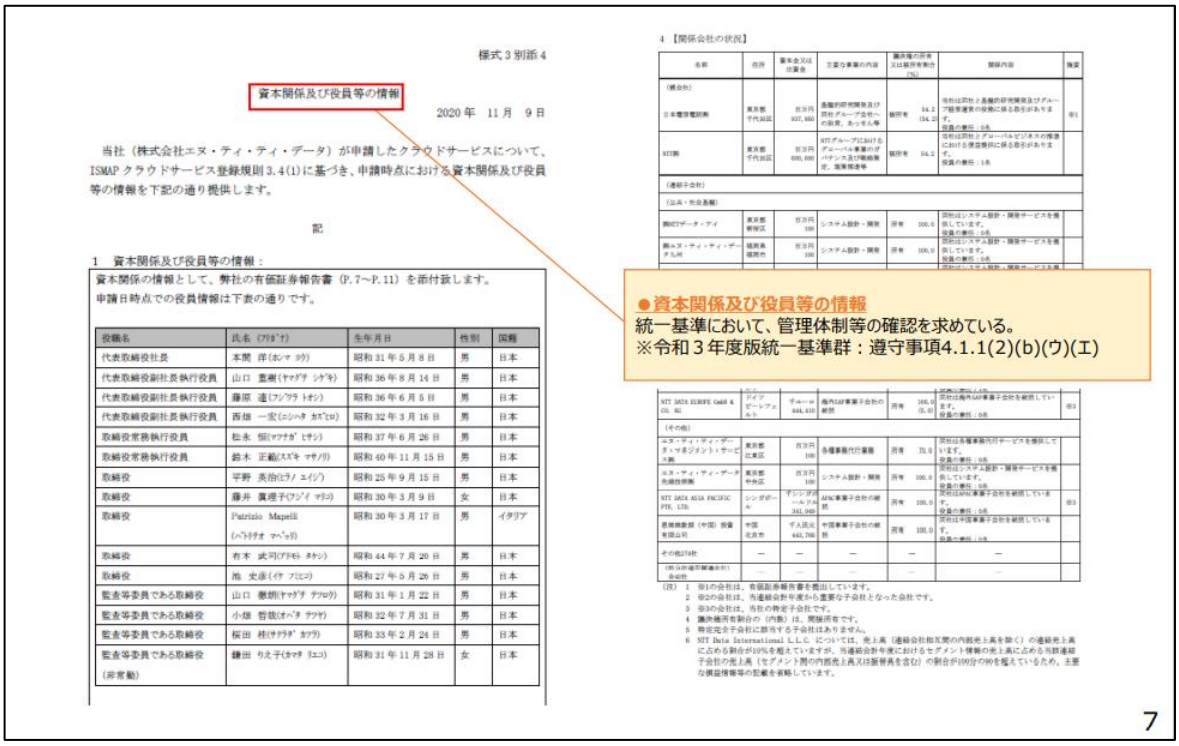


図　詳細情報の添付文書（資本関係および役員等の情報）

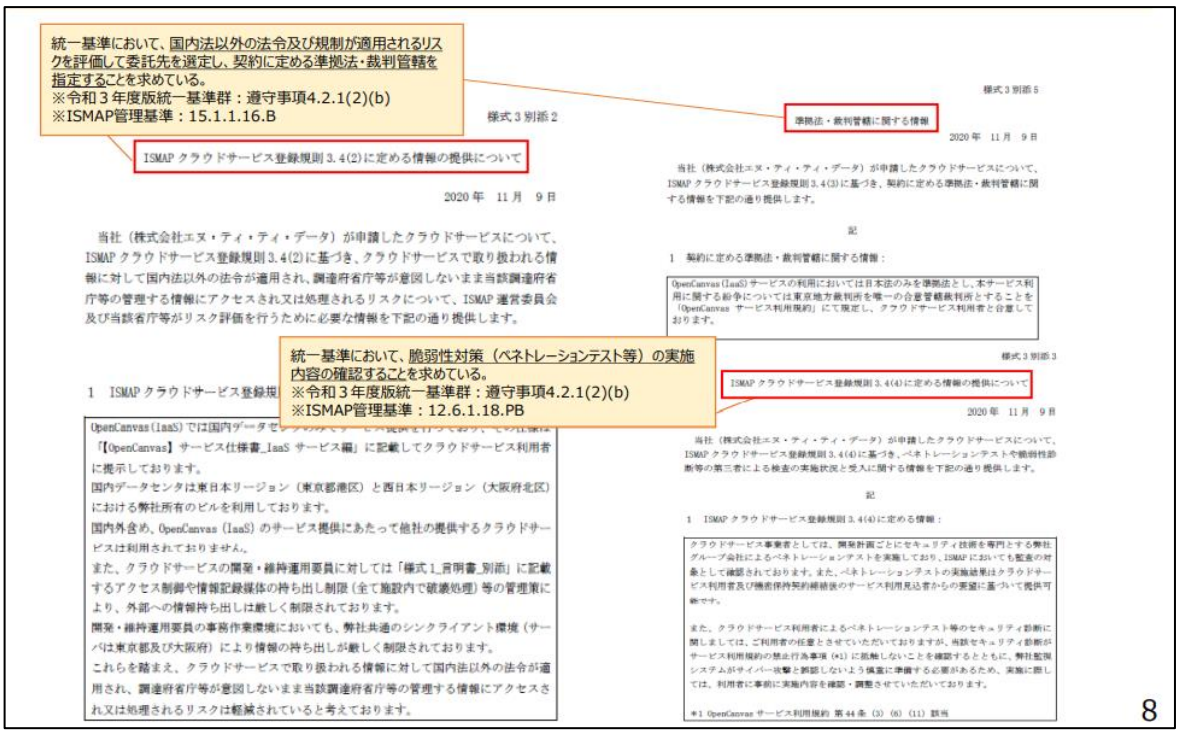


図　詳細情報の添付文書（リスク評価を行うための情報、準拠法・裁判管轄、ペネトレーションテスト等の情報）

参考資料　統一基準に規定されている委託先選定条件

① 以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。

第4部 外部委託
4.1 業務委託
4.1.1 業務委託
(2) 業務委託に係る契約
(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
（ア）委託先に提供する情報の委託先における目的外利用の禁止
（イ）委託先における情報セキュリティ対策の実施内容及び管理体制
（ウ） 委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理　　体制
（エ） 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等)・実績及び国籍に 関する情報提供
（オ）情報セキュリティインシデントへの対処方法
（カ）情報セキュリティ対策その他の契約の履行状況の確認方法
（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

② 委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。
（ア）情報セキュリティ監査の受入れ
（イ）サービスレベルの保証
③ 委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記①、②の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために 必要な情報を機関等に提供し、機関等の承認を受けるよう、仕様内容に含めること。