デジタル社会推進実践ガイドブック　DS-200

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

2024（令和 6）年 1 月 31 日

デジタル庁

〔ドキュメントの位置付け〕

Informative

参考とするドキュメント

〔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
2024年1月31日		第二版決定、改定内容は下記 • 各工程での実施内容や構成を見直して品質強化、実用的なセキュリティ対策のポイントを拡充し、使いやすさを向上 • リスク管理体制整備の重要性、具体的な体制整備に関連する内容の見直し • システム利用者や開発者/運用者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記 • CISAのセキュア・バイ・デザイン、セキュア・バイ・デフォルト原則の内容を踏まえて更新 • クラウド・バイ・デフォルトを前提としたクラウドベースの記載を拡充 • 文章全体の誤記や不明瞭な表現を修正 • 別紙各種のセキュリティ・バイ・デザイン導入をサポートする補助資料の軽微な修正

目次

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デ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・ガバメント推進標準ガイドライン」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における開発から運用まで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ための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、セキュリティに関するリスク評価とリスク管理における関係者の役割も記載スコープに含める。

システム開発、運用の各工程において、本書記載のセキュリティ・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、組織的かつ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、システムごとに独自方針で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、適用の遵守を強制するものではない。

１．３　位置づけ

本文書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

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、政府情報システムに対するセキュリティ・バイ・デザインの本書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傾向等を踏まえ、確実に抑えるべき、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、実践することで、システム開発ライフサイクル全体を通したセキュリティ強化の実現が可能となる。

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・デザインの運用方法、リスク管理方法を整備し、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、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）	サイバー資源を有するシステムが、困難な状況下、ストレス下、攻撃下にある、もしくは侵害されている状態に陥ったとしても、それを予測し、それに耐えて、そこから回復し、それに適応できる能力
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の体制や手法
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。またサービスそのもの仕様や人的ミスに起因するセキュリティ事故についても大きな社会問題となっていることから、システムセキュリティの確保だけでなく、「サービス」や「人（開発者/運用者、サービス利用者)」も対象とした総合的なセキュリティ対策が求められることも認識する必要がある。

一般的に、開発から運用まで含めたシステム開発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開発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施が可能となるため、致命的なセキュリティ対策の漏れ等による上流工程作業等への手戻りを防止でき、納期の確保やセキュリティコストの低減が可能となる。

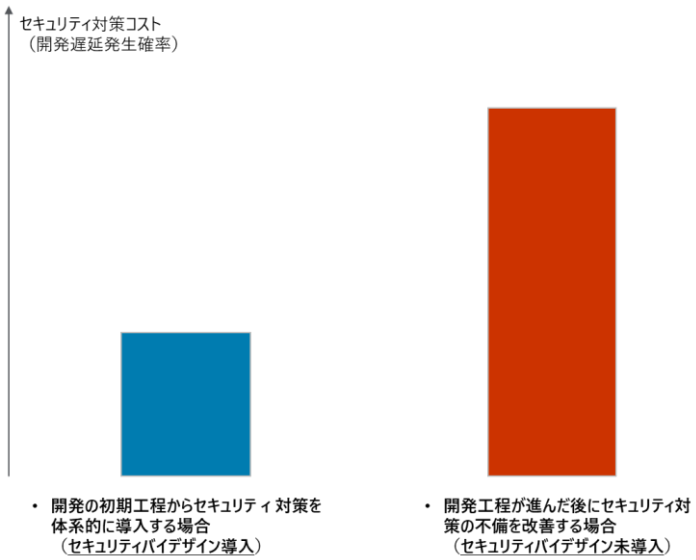


図　2-1 セキュリティ・バイ・デザイン導入時のセキュリティ対策コストイメージ

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。

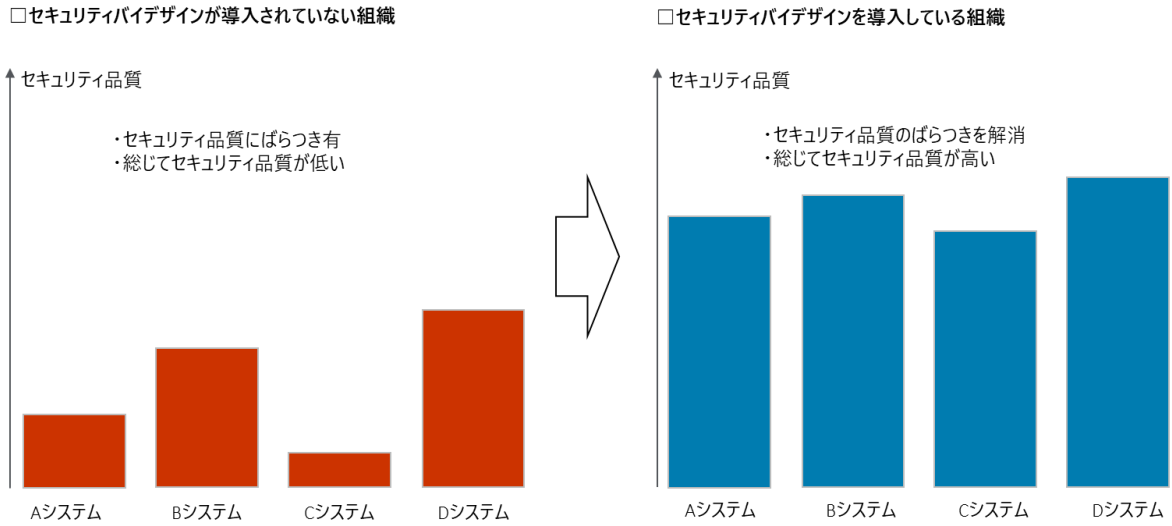


図　2-2　セキュリティ・バイ・デザイン導入組織のセキュリティ品質メリット

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・デザインの実施にあたっては、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（基本方針）を理解することが肝要となる。

政府情報システムにおけるセキュリティ・バイ・デザインでは、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. 全てのシステム開発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、全てのシステム開発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（セキュリティ・バイ・デフォルトの実施)。
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。
   - セキュリティ対策を検討する際は、システム仕様に起因するセキュリティ事故だけでなく、サービス仕様や人的ミスに起因するセキュリティ事故の発生も考慮し、多角的に対策を検討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リスクの継続的な評価が求められる。
   - セキュリティリスクを継続的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、双方にとって利益がある状態（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・デザインの実現にあたっては、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の各工程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具体的なセキュリティ標準（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、読者が各工程で実施すべきセキュリティ対策を俯瞰的に把握するため、各工程でセキュリティ・バイ・デザインにおいて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傾向等をふまえ、セキュリティリスク低減のため、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・デザインの各工程と、紐づく「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	•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 •セキュリティ運用設計
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、要塞化)
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

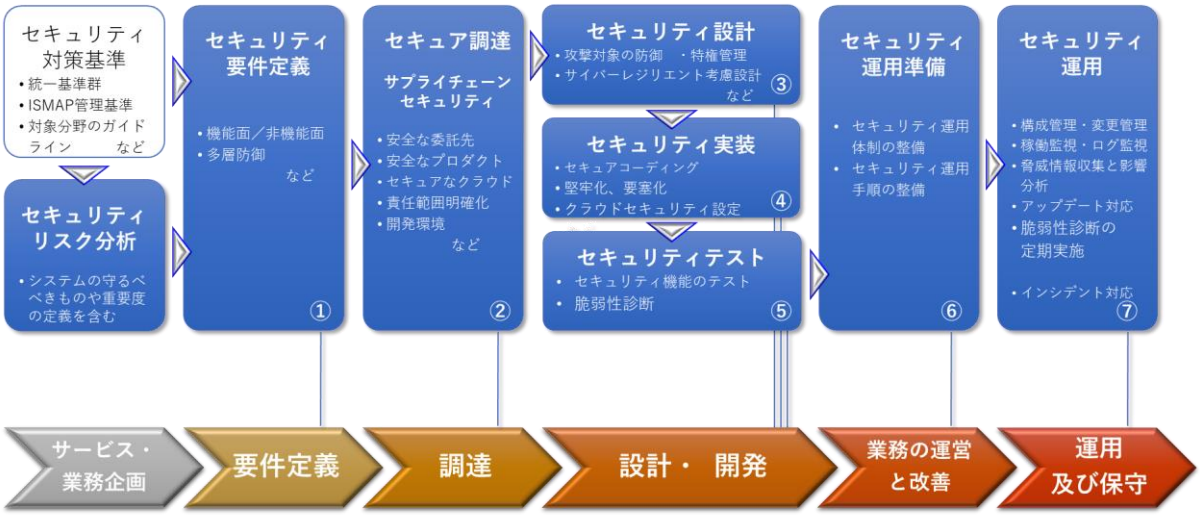


図　3-1 セキュリティ・バイ・デザインの実施プロセス

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（システム面でのセキュリティ脅威だけでなく、サービス仕様上の脅威や利用者や開発/運用担当者等の人的ミスによるセキュリティ脅威も含めて検討すること）
- 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）、対応リソース等が決定していること

イ 実施内容

- システムで取扱う重要情報、ステークホルダー、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（セキュリティベースライン）を決定する。
  - セキュリティ対応方針の中では、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）の方針を決め、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）やリスク分析

結果等に基づく、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前提にたち、特定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多層防御の考え方に基づいて、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、アプリケーション等の各コンポーネントにおいて、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。
  - サイバー攻撃や事故の発生自体の防止を目的とする対策（防止策）に偏らず、速やかなインシデント（兆候）の検知、有事のインシデント対応、サービス復旧のための対策をバランスよく、多層的に実装することが求められる。

3)セキュア調達

ア 要求事項

- 委託先とのセキュリティ対応の責任範囲を明確にした上で、必要なシステムにおけるセキュリティ要件やサプライチェーンリスク対策を含めた網羅的なセキュリティ仕様を策定していること
- クラウドサービスを利用する際はサービス形態（SaaS、IaaS、PaaS 等）を踏まえて責任範囲を特定し、責任共有モデルに基づく義務を果たす能力と内部統制について透明性の高いサービスを選定すること
- システムのセキュリティ仕様を実装できる能力を有し、求めるセキュリティ管理基準を満たし、セキュリティリテラシーおよび意識が高い、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は、それら自身がセキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を取り入れており、不正侵入の経路となるバックドア等が含まれていない、サービス提供期間中継続的なサポートを受けられる安全なものを選定すること

イ 実施内容

- セキュリティ要件に基づいて、調達仕様における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、継続的な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

- 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、継続的に社内全体でセキュリティ意識向上施策を講じ、セキュリティに関する高いリテラシーを有する委託先を選定し、適切な管理を行う。
  - 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、当該仕様を実装可能な、十分な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、各政府機関等における ISMAP 制度の利用の考え方を踏まえ、統一基準群の遵守事項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等の不備によるインシデント等を防止するため、委託先に求める具体的な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、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を製品開発に取り入れている事業者から提供されており、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の提供や緩和策の提示のサポートが受けられる、プロダクトを選定する。
  - サービス運用中のプロダクトのセキュリティ確保については、利用者側に管理責任があるため、構成管理、脆弱性管理、ライフサイクル管理等を適切に実施する。

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
- 堅牢化（攻撃対象領域が少なく、多層多重で守られている）されていること
- サイバーレジリエントな設計が実施されていること
- サービスデザインの観点から、システムの利用者や運用者等による人的ミスを引き起こす可能性が十分に低減された仕様になっていること

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リソースの資産管理を徹底し、最新な状態を維持するとともに脆弱性を管理可能な仕組みを導入する。
  - 攻撃者による脆弱性や設定ミスの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使用しない。また、ソフトウェアやミドルウェアに設定されている初期設定値をそのまま使用しない。
  - 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、管理者アカウントでの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や高度化に伴い、攻撃は成功してインシデントは発生する前提に立ち、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の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。
  - インシデントを検知した際は、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。また、速やかなサービス復旧を行うため、重要データやシステムのバックアップを行い、リストア手順を事前に準備する。

- 人的ミスへの対応策の検討
  - サービス利用者やシステム管理者、運用者等による人的ミスにつながる可能性のあるシステム仕様については、デザイン（UI、UX）の改善することで事故発生防止につとめる。
  - システム仕様の改善に加えて、ワークフロー（ダブルチェックや承認フローを設定等）や作業者のリテラシーを高めるための取組みとして必要な教育コンテンツを事前に提供する等の対策を講じることで、人的ミスの発生可能性をできるだけ低減する。
  - 人的セキュリティの対応については、システム開発部門や運用部門だけでなく、システム利用者となる国民や自治体等多くのステークホルダを事前に巻きこみ、過去のインシデント事例等に基づいて事故発生防止に向けた建設的な議論やサンプル等を用いた検証を重ね、システム仕様や業務の改

善をはかることが重要となる。

- また人的ミスによる事故は必ず発生するという前提の下、発生状況の定期的な確認、事故発生時に速やかに上層部まで報告される体制や事故発生時の被害を極小化する対応手順を事前に整備する。

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、要塞化）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、要塞化)
  - 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セキュリティ設定は、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、人的なミスの発生をおさえ、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、IaCテンプレート等を使用することで、人的なミスや担当者依存の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ベースラインを定義することで、セキュリティ監査の実行容易性も向上する。

- 他方、システムイメージや IaC テンプレートに脆弱性やセキュリティ設定の不備がある場合、複数のリソースに広範囲に悪影響が及ぶことが懸念されるため、有識者や外部サービス等による事前の検証を必ず実施すること。

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、レッドチーム演習等）
- 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で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脆弱性診断を実施が重要となる。

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
- システム運用において人的ミスが発生する可能性のある箇所の洗い出し、是正
- 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事前に整備しても、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、多くの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

- システムの構成監理、変更管理が適切に実施されていること
- システムに影響する脅威情報、脆弱性情報が定常的に分析され、脆弱性対応等継続したリスク管理が行われていること
- 速やかなインシデント（予兆）の検知が行えること
- インシデント発生時に速やかな対応、システム復旧が実施できること

イ 実施内容

- セキュリティ運用を行う要員の教育/訓練の実施、重要な情報を取り扱う要員のスクリーニング（要員のスキルや行動特性等を考慮）
- 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、是正対応
  - 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/脆弱性情報の収集、分析、リスクに応じた対応
  - 日々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 等の値に基づき、当該脆弱性によるシステム環境へ

の影響を分析し、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、セキュリティパッチが適用できないケースは暫定対処として仮想パッチを用いる、システムの利用機能を制限する等、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、当該方針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、関係者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確保に有効である。
  - 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発生時において、円滑に進まなかった作業についても振り返りを行い、継続した改善を繰返すことで、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求められるが、実際には人材不足等の理由により困難なケースが多い。仮に開発チームにセキュリティ専門家をアサイン可能な場合でも、セキュリティ対策の妥当性が十分に検証されずに、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、開発チームによる各工程でのセキュリティ対策の実施だけでなく、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求める。

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的に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。

本項では、セキュリティ・バイ・デザインにおけるリスク管理体制としてリスク評価、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。

開発プロジェクトが開始する前に必要なリソースをアサインし、リスク管理体制を整備することが、セキュリティ・バイ・デザインを効果的に実施するための必須条件となる点に留意すること。

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本書では規定しない。

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、セキュリティ対策の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。

項番	役割（呼称）	責任
		•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。
2	委託先実施者	•システム管理者からの委託を受け、責任範囲に関連す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 システムの規模や社会的影響等により、組織の長が担うこともあれば、幹部相当の役職者が担うこともある	•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。 •残存リスクへの対応方針を決定し、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、監督する。
4	セキュリティリスクアセッサー（評価者） 開発者とは役割の異なるセキュリティ専門知識を有した者が相当する	•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。 •セキュリティリスク評価結果や是正対応に関連する推奨策をシステム管理者に提言する。 •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、セキュリティ上の問題がある場合、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。

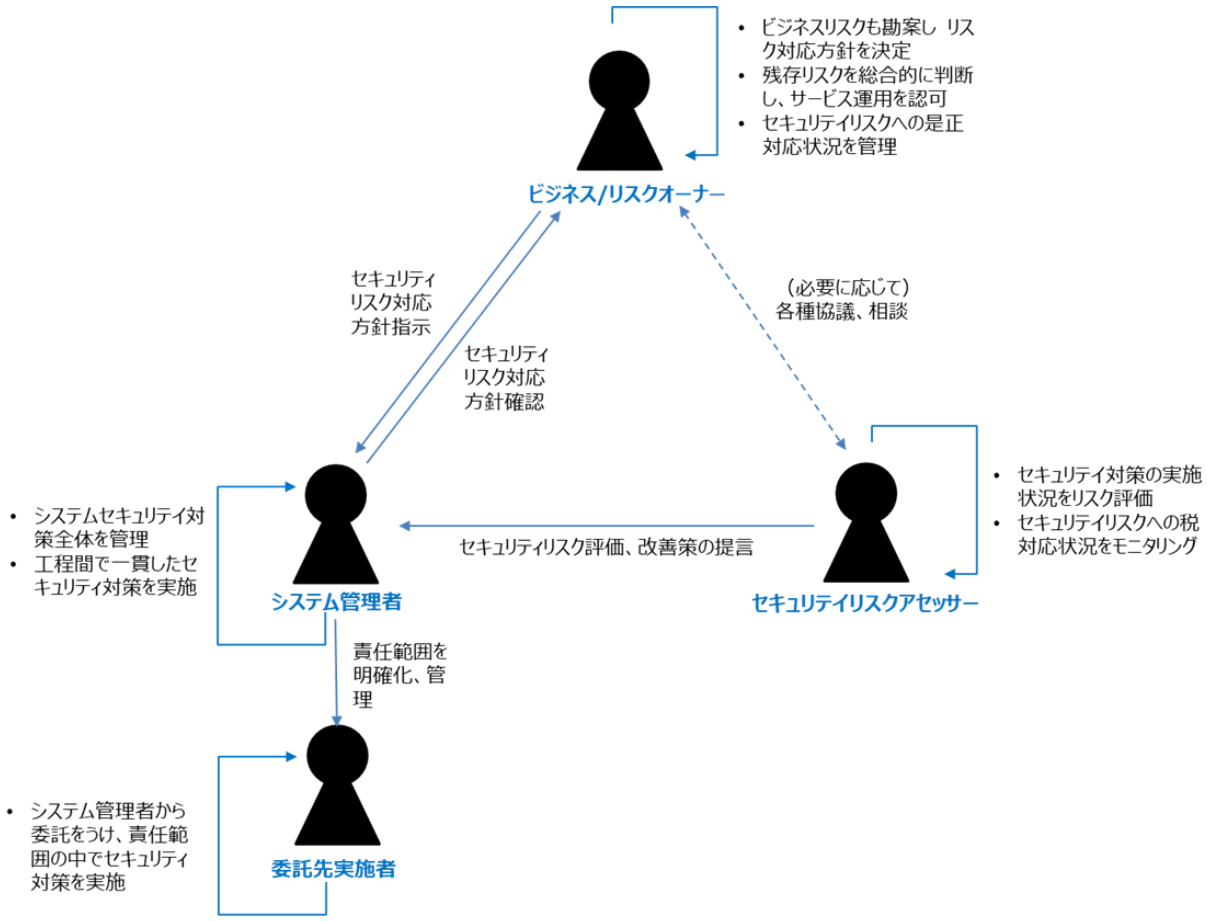


図　5-1 セキュリティ・バイ・デザインに関わる関係者

６　セキュリティ・バイ・デザイン実施における留意事項

本ガイドラインの最後に、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を確保することを念頭に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、組織として考慮すべきリスクや実現可能性を踏まえて実施可能なところから運用を開始し、課題改善と内容拡充をはかりながら、成熟度を向上していくことが現実的である。

- 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更改等の場合において、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対応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群（以下、「統一基準群」という。）	工程全般	https://www.nisc.go.jp/policy/group/general/kijun.html
2	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
3	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
4	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
5	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
6	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
7	IPA（情報処理推進機構）	安全なウェブサイトの作り方	セキュリティ設計	https://www.ipa.go.jp/security/vuln/websecurity.html
8	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
9	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 セキュリティ設計	https://www.ipa.go.jp/security/fy24/reports/insider/index.html
10	ISMAP 運営委員会	ISMAP クラウドサービスリスト	セキュリティ要件定義、	https://www.ismap.go.jp/csm?id=cloud_service_list

#	提供元	セキュリティ標準名	対象工程	URL
		ISMAP-LIU クラウドサービスリスト ISMAP 管理基準	セキュア調達	https://www.ismap.go.jp/csm?id=cloud_service_list_liu https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028
11	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
12	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
13	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
14	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
15	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/main_sosiki/cybersecurity/kokumin/business/business_admin_24.html
16	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/
17	NIST（National Institute of Standards and Technology）	Cybersecurity Framework	工程全般	https://www.ipa.go.jp/files/000071204.pdf
18	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
19	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
20	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
21	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
22	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/
23	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
24	CIS (Center for Internet Security)	CIS controls Version 8	セキュリティ設計	https://www.cisecurity.org/controls/v8/
25	CIS (Center for Internet Security)	CIS Benchmarks	セキュリティ実装	https://www.cisecurity.org/cis-benchmarks/
26	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/
27	OWASP	OWASP 10	セキュリティ設計	https://owasp.org/www-project-top-ten/
28	ISO	ISO27017, ISO27018	セキュリティ要件定義 セキュリティ設計	-
29	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
30	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
31	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/
32	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
33	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
34	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
35	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
36	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
37	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://www.digital.go.jp/resources/standard_guidelines/
38	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
39	IPA（情報処理推進機構）	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
40	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
41	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
42	ENISA	Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity	工程全般（人的ミスのセキュリティ対策関連）	https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

別紙 2　各工程のセキュリティ関連の実施項目

別紙 2 では、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に留意する）。

本チェックリストを用いてセキュリティ・バイ・デザインの実施状況を可視化することで、リスクアセッサー等による検証やセキュリティ監査の効率化や継続的なセキュリティリスク対応の見直しの一助にできるため、積極的に活用すること。

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	【システムプロファイルの作成】 システムで取扱う重要情報の種類、重要情報の処理フローやライフサイクルが分かる内容、ステークホルダー、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	【セキュリティ脅威の特定】 脅威分析モデル（Microsoft STRIDE モデル、MITRE ATT&CK 等）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（システム面でのセキュリティ脅威だけでなく、サービス仕様上の脅威や人的ミスによるセキュ	□

	リティ脅威も含めて検討している）	
3	【セキュリティリスク分析の実施】 セキュリティ脅威に対するリスク分析を実施し、対象システムにおけるセキュリティ対応方針として 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、対応リソース等を決定している ※リスク分析にあたっては、「DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン」に従った実施を原則とする	□
4	【セキュリティ要件定義】 セキュリティ対応方針（リスク対応優先度、遵守すべきセキュリティ標準等）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	【多層防御の導入】 サイバー攻撃やセキュリティ事故は発生する前提で、多層的なセキュリティ対策を実施して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	【セキュリティ仕様の策定】 調達仕様書やそれに付随する文書の中に、システムに求めるセキュリティ要件に加えて、委託先に求めるセキュリティ（委託先での情報管理等）や機器/ソフトウェア調達時、サービス選定時のセキュリティ要件に関する記載を含めている	□
2	【責任範囲の明確化】 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た上で調達仕様等におけるセキュリティ関連事項を記載している（クラウドサービスにおいては、クラウドサービスの特性（SaaS,IaaS,PaaS）等を踏まえて、責任範囲を明確化している）	□
3	【安全な委託先の選定】 セキュリティ仕様を実装できる能力を十分に有し、セキュリティ管理基準（委託元で提示したもの）を満たすことができる安全な委託先を選定している	□
4	【安全なプロダクトの選定】 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、サービスの提供期間中に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	【セキュリティベースライン、フレームワークの導入】 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フレームワークを参照して、網羅的なセキュリティ設計を実施している 例：CIS control（ver8）をセキュリティベースラインとして用い、具体的な設計（設定）は CIS ベンチマークを用いてシステムにおけるセキュリティ設計を実施している　等	□
2	【アタックサーフェスの最小化】 システムに対するアタックサーフェス（攻撃対象領域）を必要最小限に抑えるため、システムの操作/処理に必要な外部インタ	□

#	確認項目	チェック
	ーフェースや機器のみを公開する仕様としている	
3	【不要な機能、サービス、データの削除】 攻撃への悪用や、被害の拡大を防止するため、システムに不要な機能やサービス、データはシステムから取り除いている	□
4	【外部入力値の検証】 システムに対する外部からの全ての入力は信頼せず、検証した上で、システムに被害が発生しないよう、安全に変換処理等をしている	□
5	【全層におけるセキュリティ対策】 システムの全構成要素（アプリケーション、ネットワーク、プラットフォーム（OS 、ミドルウェア等)）においてセキュリティ対策を実施している	□
6	【インシデント被害拡大防止対策】 システム分離（ネットワーク分離)、管理者アカウントの保護、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	□
7	【セキュリティ監視の準備】 セキュリティ運用設計として、システムで発生が想定される脅威を検知するために必要なログやセキュリティアラートを定義し、収集し、一元的に管理する設計を実施している	□
8	【セキュリティ監視設計】 セキュリティ運用設計として、収集したログやセキュリティアラートを定期的に分析し、システムの異常やその兆候を速やかに検知し、必要な関係者に報告するための仕組み（分析方法、エスカレーションフロー等）を検討している	□
9	【インシデント対応プロセス整備】 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およびシステム復旧を可能とするための体制や対応手順を策定している	□
10	【脆弱性対応方針策定】 システムの運用フェーズで発生するプラットフォームやアプリケーションの脆弱性に対する対応基準、対応方法（セキュリティパッチの適用方法、セキュリティパッチを適用できない場合の代替策等）を策定している	□
11	【人的ミスへの対応策の検討（仕様やサービスデザインでの対	□

#	確認項目	チェック
	応)】 サービス利用者やシステム管理者等の人的ミスの発生可能性のある仕様については、サービスデザイン等を工夫して防止につとめている	
12	【人的ミスへの対応策の検討（その他)】 過去のインシデント事例等も参考に技術的対策、運用的対策、人的対策等を組み合わせて、多角的な視点をもってリスク低減策を実施している	□

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	【セキュアコーディング】 アプリケーションセキュリティに関して、セキュアコーディングを実施するためのコーディング規約を策定している	□
2	【開発用フレームワークやツールの利用】 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（Webアプリケーションであれば、IPA「安全なウェブサイトの作り方（https://www.ipa.go.jp/security/vuln/websecurity.html)」に記載されているような脆弱性への対処が完了している)	□
3	【安全なライブラリ、ミドルウェアの利用】 アプリケーションのセキュリティを確保するため、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	【プラットフォームの堅牢化、要塞化】 プラットフォームのセキュリティに関して、セキュリティ設計に基づき、もれなくセキュリティ設定（堅牢化、要塞化）を実施している（クラウドサービス、OS、ミドルウェア、ネットワーク等)	□
5	【セキュリティテンプレートの利用】 プラットフォームセキュリティに関して、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、IaCテンプレート等を利用し、セキュリティ設定（堅牢化、要塞化）の属人性を排除している	□

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	【セキュリティ関連機能のテスト】 システムで実装しているセキュリティ関連機能（利用者認証機能等）において、十分なテストを実施し、(バグ対応等を実施して）機能の品質を確保している	□
2	【必要な脆弱性診断の実施（アタックサーフェスをカバー)】 システムの特性を考慮して、アタックサーフェス（攻撃対象領域）をもれなくカバーするように脆弱性診断を実施している（Web システムでアプリケーション診断とプラットフォーム診断、スマホアプリを使用する場合はスマホアプリ診断等が対象） ※脆弱性診断にあたっては、「DS-221 政府情報システムにおける脆弱性診断導入ガイドライン」に従った実施を原則とする	□
3	【必要な脆弱性診断の実施（システム重要度に応じた診断品質の確保)】 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る、等） ※脆弱性診断にあたっては、「DS-221 政府情報システムにおける脆弱性診断導入ガイドライン」に従った実施を原則とする	□
4	【一般的なセキュリティ上の問題点への対応】 リリースにあたり、政府情報システムにおいて作りこまれやすい傾向にあるセキュリティ上の問題点（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を参照）について、対応が完了している	□
5	【脆弱性対応】 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やシステムへの影響を考慮し、優先度に応じ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	【セキュリティ運用体制の確立】 セキュリティ運用として平時（通常時のセキュリティ運用)、有	□

#	確認項目	チェック
	事（インシデント発生時の対応）を実施するのに十分な運用体制を確立している （平時（通常時のセキュリティ運用）として求められる実施内容は下記の⑦-1～⑦-6 に該当する項目）	
2	【セキュリティ運用手順の整備】 セキュリティ運用として平時（通常時のセキュリティ運用）、有事（インシデント発生時の対応）を実施するための、具体的な運用手順を整備している （平時（通常時のセキュリティ運用）として求められる実施内容は下記の⑦-1～⑦-6 に該当する項目）	□
3	【インシデント対応訓練の実施】 有事（インシデント発生時の対応）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	【システム構成管理】 通常時のセキュリティ運用として、システム構成を管理し、構成情報を最新化している	□
2	【ソフトウェア構成管理】 通常時のセキュリティ運用として、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	【アカウント管理】 通常時のセキュリティ運用として、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	【変更管理】 通常時のセキュリティ運用として、システムの設定変更に合わせて、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（変更管理を行っている）	□
5	【脆弱性管理】 通常時のセキュリティ運用として、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	□

#	確認項目	チェック
	関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、アラート監視】 通常時のセキュリティ運用として、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	【インシデント対応手順の整備】 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	【復旧手順の準備】 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ている	□
9	【インシデント対応手順等の見直し】 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

一般的な政府情報システムにおけるセキュリティ上の問題点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

8	人的ミス発生の考慮漏れ	• システムを操作する端末が複数人で利用される等、システムのユースケースが網羅的に洗い出されていないことにより、システム仕様や業務運用仕様に不備がある • システムの UI/UX が複雑で、利用者にとって操作困難な仕様となっている • クラウドサービスやノーコードツール、ローコードツール等外部サービスの利用において、利用者による責任範囲の理解不足によって、設定すべきセキュリティ設定がもれている • インシデント報告体制や対応手順等が、人的ミスによるセキュリティ事故の発生が考慮された内容になっていない

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～c の要件を記載すること。

a.　統一基準群等に基づく委託先に求める要件
b.　ISMAP等クラウドサービスリスト登録済みのクラウドサービスに求める要件
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.　統一基準群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群（令和５年度版）（https://www.nisc.go.jp/policy/group/general/kijun.html）」「4.1.1 業務委託(1) (a)(イ)」に規定されている委託先選定基準の内容を踏まえて、調達仕様書に要件を記載すること。（具体的な委託先選定基準は参考資料「統一基準群に規定されている委託先選定基準」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等クラウドサービスリスト登録済みのクラウドサービスに求める要件

ISMAP 等クラウドサービスリストに登録済みのクラウドサービスの管理策の適用状況については、登録サービスごとに異なっている。このため、適用必須と考える管理策については、参考資料「クラウドサービスが遵守すべき ISMAP 管理策基準」及び、ISMAP 管理基準（https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028）第５章管理策基準の内容を踏まえて調達仕様書に要件として記載すること。

なお、登録サービスごとの管理策の適用状況については、ISMAP クラウドサービスリスト「基本言明要件のうち実施している統制目標の管理策」から確認可能。（具体的な確認手順は参考資料「ISMAP ポータルサイト内のサービスリストについて」を参考にすること）

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。

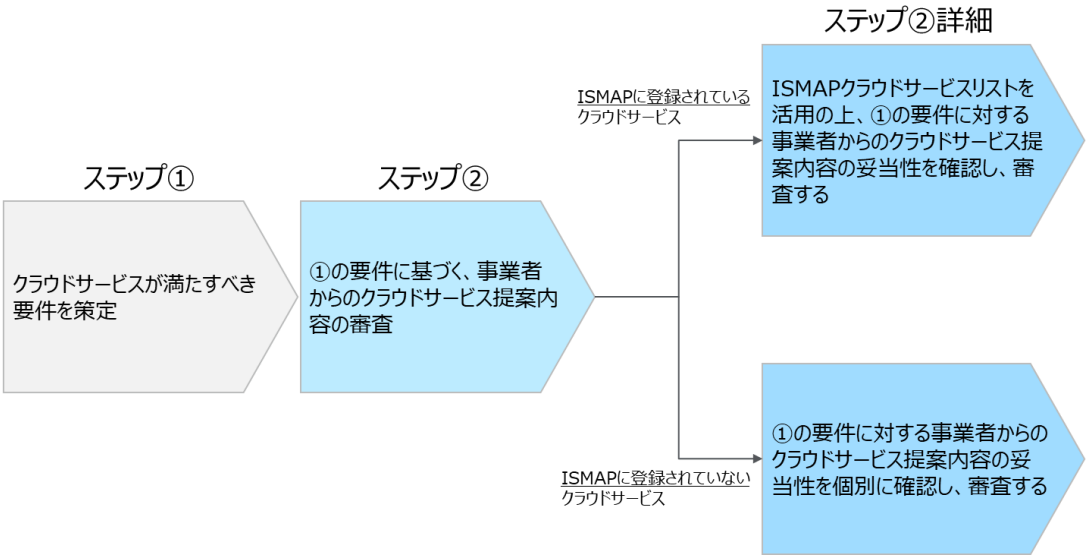
なお、機密性 3 情報をクラウドサービスで取り扱う場合には、ISMAP が前提とする情報の格付（機密性 2 情報）を踏まえて、必要なセキュリティ要件を追記すること。

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 等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 等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 等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について」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等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等クラウドサービスリスト登録済みの

		クラウドサービスに求める要件」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. 統一基準群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 等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. 統一基準群等に基づく委託先に求める要件」、「b. ISMAP 等クラウドサービスリスト登録済みのクラウドサービスに求める要件」、「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について

【参考資料の URL】
ISMAP 等クラウドサービスリストの利用について
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010265

ISMAP ポータルサイト
https://www.ismap.go.jp/

ISMAP クラウドサービスリスト
https://www.ismap.go.jp/csm?id=cloud_service_list

ISMAP-LIU クラウドサービスリスト
https://www.ismap.go.jp/csm?id=cloud_service_list_liu

参考資料　統一基準群に規定されている委託先選定基準

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基準とし、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

遵守事項
(1) 業務委託に係る運用規程の整備
(a) 統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備すること。
(イ) 委託先の選定基準

【 基本対策事項 】
＜4.1.1(2)(a)(イ)関連＞
4.1.1(2)-1 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、以下の内容を全て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、仕様にも含めること。

a) 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
b) 委託先における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制
c) 情報セキュリティインシデントへの対処方法
d) 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
e) 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

4.1.1(2)-2 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、委託する業務において取り扱う情報の格付等を勘案し、以下の内容の全てを必要に応じて仕様に含めること。
a) 監査の受入れ
b) サービス品質の保証

＜4.1.1(2)(a)(ウ)関連＞
4.1.1(2)-4 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、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、基本対策事項4.1.1(2)-1及び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、仕様に含めること。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。

4.1.2 情報システムに関する業務委託

遵守事項
(1) 情報システムに関する業務委託における共通的対策
(a) 情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに機関等の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。

【 基本対策事項 】
＜4.1.2(1)(a)関連＞
4.1.2(1)-1 情報システムセキュリティ責任者は、以下の内容を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託の委託先の選定条件に加え、仕様にも含めること。

a） 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、情報システムに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
b） 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（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報提供