デジタル社会推進実践ガイドブック　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

～　ベースラインと事業被害の組み合わせアプローチ　～

2023（令和 5）年 3 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〕
リスク、リスク分析、ベースライン、セキュリティ・バイ・デザイン

〔概要〕
情報システムのセキュリティを確保するためには、リスクを認識して確実に管理することが不可欠である。セキュリティリスク分析には、さまざまな手法があるが、本文書では、ベースラインと事業被害を組み合わせたリスク分析の手順を紹介し、作業効率と分析精度とをバランスをとって向上させることを目的としている。
本文書は、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」のセキュリティリスク分析の手順の事例として具体的に示したものである。

改定履歴

改定年月日	改定箇所	改定内容
2023年3月31日	-	・初版決定

目次

1. はじめに

政府情報システムにおいて、セキュリティ対策を確実かつ効率的に実装するためにはシステム開発の上流工程から取り組むことが重要であることを、「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(2022 年 6 月デジタル庁発行)」で説明を行った。この中でセキュリティ対策の最初のプロセスとしてセキュリティリスク分析を行うことが示されている。

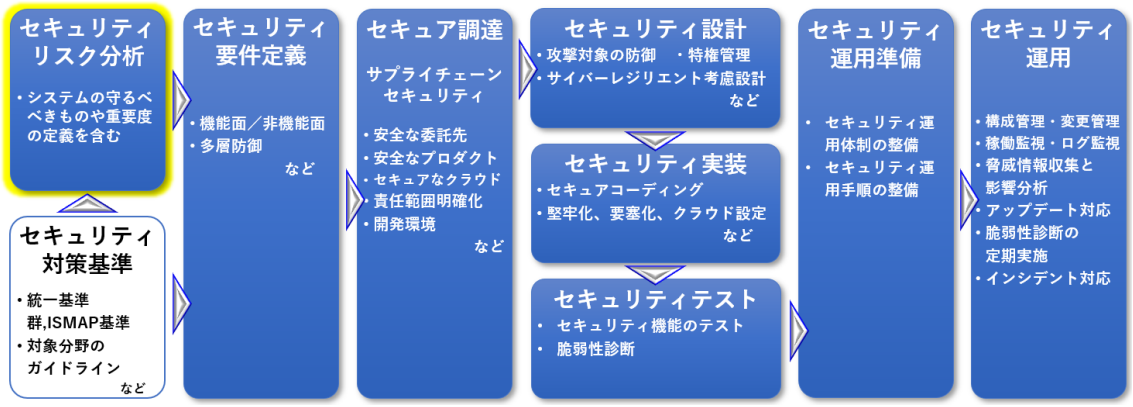


図１－１　セキュリティ・バイ・デザインのプロセス

セキュリティリスク分析には様々な方法がある、多くのガイドラインでは、脅威事象の発生レベル、脆弱性の対策レベル、事業への影響の組み合わせでセキュリティリスクを分析する方法が紹介されている。この方法では、脅威の洗い出しや各レベルを決めてマトリックス表を作るための作業が必要であり、脅威事象を網羅させることやレベルの決め方などに苦労することがある。

本文書では、分析の前に対象システムの特性をプロファイルとして定義することで分析の根拠を固め、ベースラインのアプローチと事業被害のアプローチを組み合わせてリスク分析をする手順を提案している。この方法は、作業効率と分析精度のバランスがよく、リスク分析の結果をセキュリティ・バイ・デザインのプロセスに反映しやすい方法と考えている。

1.1. 目的とスコープ

本文書は、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、セキュリティ・バイ・デザインの中のセキュリティリスク分析の手順を示すこ

とを主な目的としている。また、リスク分析の結果をセキュリティ要件として開発委託先へ提示する方法や、実装後にどのように確認するかについてもスコープとしている。

本文書の利用は、リスク分析の必要性を理解しているシステム管理者が、ベースラインと事業被害の組み合わせアプローチの手順を参考に、セキュリティ・バイ・デザインのためのリスク分析を効果的に実施することを想定している。リスク分析の考え方や手法を詳しく知りたい場合は、参考にしたガイドラインや提供情報を参考資料 A に示しているので、参照いただきたい。

1.2. 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。

1.3. 本書の構成

本文書は、セキュリティ・バイ・デザインでのリスク分析の手順を本文に記載する。リスク分析は手法や手順だけでは理解が進まないこともあるため、記載サンプルと様式を参考資料に掲載する。

第 2 章では、セキュリティリスク分析における一般的な考え方とそれぞれの手法の長所・短所を比較し、本文書で採用するリスク分析の方法とその選択理由について説明する。

第 3 章では、第 2 章で選択したリスク分析のプロセスに沿って、分析対象のシステムにおける事業視点のインパクトの基準とプロファイルの項目、組み合わせ方式のリスク分析の実施手順について説明する。手順を示すことに重点を置き、分析における背景やその理由など説明は避け、プロセス毎の実施事項と記載事項、考え方とに整理して示している。

第 4 章では、第 3 章でのリスク分析の結果を、セキュリティ・バイ・デザインのインプットとしてどのように確実に対策につなげるか、実装の結果が漏れなく対策できているかをどのようにトレースするかについて説明している。

1.4. 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
セキュリティ	本ガイドラインでは、サイバーセキュリティ基本法第二条で定義された「サイバーセキュリティ」を「セキュリティ」と表現する。
リスク	「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。 （引用元：政府機関等の対策基準策定のためのガイドライン　令和３年度版）
リスク分析	リスク分析の意義は、必要に応じてリスクのレベルを含め、リスクの性質及び特徴を理解することである。リスク分析には、不確かさ、リスク源、結果、起こりやすさ、事象、シナリオ、管理策及び管理策の有効性の詳細な検討が含まれる。 （引用元：JIS Q 31000:2019）
システム・プロファイル	本ガイドラインでは、リスク分析対象のシステムの事業への影響度、利用形態や特性・特質を分析・整理したものをシステム・プロファイルと表現する。これから開発するシステムでは、完成時を想定したプロファイルとする。 本文中では、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)の「業務要件の検討」を参考に本ガイドライン向けに再定義している。

2．セキュリティリスク分析の概要

2.1.　セキュリティリスク分析の必要性

事業における情報セキュリティを確保するためには、対象システムが担う業務や取り扱う情報、そして情報システムの特性に応じてリスクが異なるため、リスク分析が必要となる。リスク分析の結果は、リスクへの対処法や、講ずべき対策の程度を決定するための根拠として使用する。

実際にリスク分析を行って正しい結果を得るためには、リスク分析手法の習得や実務経験が必要となる。もし、分析手法の理解や実務経験が十分な要員が不在の場合にリスク分析を省略することや、簡易的に済ませてしまうことはせず、セキュリティ専門家（セキュリティリスクアセッサー）の支援を受けて必ずリスク分析を実施する。

2.2.　セキュリティリスク分析の考え方

リスク評価手法については、対象組織の情報セキュリティに係るマネジメント能力の成熟度や対象組織の置かれた環境に応じたふさわしい手法を選ぶとされている。リスク評価に係る規格には、「ISO31000:2018, Risk management－Guidelines[1]」等がある。

（1）セキュリティリスク分析の種類[2]

リスク分析の例として、以下に４種類の手法を示す。

① ベースラインアプローチ

既存の標準や基準をもとに、想定する典型的なシステムに対して、予め一定の確保すべきセキュリティレベルを設定し、それを達成するためのセキュリティ対策要件を定め、分析対象となるシステムの対策の適合性等をチェックする。

② 非形式的アプローチ

組織や担当者の経験や判断によってリスク分析を実施する。

③ 詳細リスク分析

[1] ISO31000:2018, Risk management－Guidelines（国内標準としては、JIS Q 31000:2019 リスクマネジメント－指針）

[2] セキュリティリスク分析の種類は、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（令和３年）の2.1.3項　2.1.3 情報セキュリティ関係規程の整備　より引用している。

分析対象のシステム自体に対して、そのシステムもしくはそれにより実現されている事業を、「重要度」（あるいは損なわれた場合の被害レベル）「脅威」「脆弱性」の評価指標の下で、リスク分析を実施する。

④ 組み合わせアプローチ

複数のアプローチを併用し、作業の効率化、異なった評価視点の活用によって、分析精度の向上と、作業工数増大の回避を図る。

以下に、それぞれのセキュリティリスク分析手法の長所と短所の比較を記載する。

表２－１ セキュリティリスク分析手法の比較

リスク分析手法	長所	短所
ベースライン アプローチ	・決められた対策要件をチェックすることにより、作業の工数は大きくない。 ・既存の基準をもとにしているので、あるレベルの評価の目安としては利用できる。	・対策基準に対する適合レベルのチェックであり、自分のシステムの状況に沿ったリスク分析にはなっていない。 ・事業被害を起こさない裏づけには間接的にしかならない。 ・未実施の対策群があった場合、自分のシステムに沿った選択基準が得られない。
非形式的 アプローチ	・経験値を活用するので、属人的ではあるが工数は小さい。	・リスク分析にはなっていない。 ・起こりうる脅威、あるいは新たな脅威に対しての対応が困難である。 ・属人的であり、継続的なセキュリティレベルの向上は困難である。
詳細リスク分析	・自分のシステム自体に対する、正確なリスク分析が可能である。 ・一度実施すると、それをベースに継続的なセキュリティレベルの向上が可能となる。	・システムの規模や手法によっては、かなりの工数がかかることがある。 ・リスク分析の結果の評価に技量を要する。また、技量を持つ評価者のアサインが難し

リスク分析手法	長所	短所
	・セキュリティ投資の優先順位等、組織として戦略的に検討していくことができる。	い。※
組み合わせアプローチ	・上記、各手法の長所の取り込みの可能性である。 ・上記、各手法の短所の改善の可能性がある。	・どう組み合わせるのか、それぞれのシステムや事業者によって異なってくるが、その指針は示されていない。

（出典）ＩＰＡ「制御システムのセキュリティリスク分析ガイド　第２版」より作成

※下線の箇所は、出典に対して本ガイドラインとして追記した箇所

（２）詳細リスク分析について[3]

リスク分析の中でも、詳細リスク分析は、以下の点で、最も実態の把握と対策を検討するのに適している。

- 分析対象の実態に沿った評価を行うことで、分析対象のリスクを明確化できる。
- 対策の優先順位の客観的な決定と、リスク低減に最も効果的な選定が可能である。（組織内における対策の優先順位の共通の理解と認識を有することができる。）
- 一度確立しておくと、それをベースに、システムの拡張や新たな脅威の出現等にも継続的に見直しや更新をしていくことが可能である。

詳細リスク分析には、いくつかのアプローチがある。

- 資産ベース

  保護すべきシステムを構成する各資産（サーバ、端末、通信機器等）に対して、その重要度（価値）、想定される脅威、脆弱性の３つを評価指標として、リスク分析を実施する。

  この場合のリスク値としては、想定される「脅威の受容の可能性とそれにより損なわれる資産価値」の相乗値を算出することになる。リスク値が高い脅威に対しては、その受容性を低減する対策の強化を検討することになる。

- 事業被害ベース（シナリオベース）

  保護すべきシステムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被

[3] 詳細リスク分析の説明は、ＩＰＡ「制御システムのセキュリティリスク分析ガイド　第２版」2.1（３）項　詳細リスク分析の概要と長短解説から引用している。

害を起こしうる攻撃シナリオによる脅威、攻撃シナリオに対する脆弱性（攻撃シナリオの受容可能性）の３つを評価指標として、リスク分析を実施する。この場合のリスク値としては、攻撃シナリオの「成功可能性と発生する被害のレベル」の相乗値を算定することになる。リスク値が高い攻撃シナリオに対しては、その成功可能性を低減する対策の強化を検討することになる。

2.3. 本ガイドラインで採用するセキュリティリスク分析

前項で各リスク分析手法の長所・短所の比較をしたが、セキュリティ・バイ・デザインで採用するリスク分析として重要視する要件を以下に挙げる。

① 対策の網羅的な把握
保護すべき事業（行政サービス）に対して、想定される脅威とその対策を一通り把握して評価できること。
② レビューによる品質確認
システムを知るシステム管理者、事業影響を知るビジネスオーナ、分析手法を知るセキュリティリスクアセッサーがリスク分析の結果を相互確認できること。
③ リスク分析のリソース
人員や予算は限られており、現実的な工数でリスク分析の達成が可能であること。

この①を満たすものとして、シナリオベースのリスク分析があるが、このシナリオベースのリスク分析を全て詳細に実施するとなると、システムによっては膨大な工数となり、③の要件が満たせないことが想定される。また、非形式的アプローチや複雑・大規模な詳細リスク分析などリスク分析者の力量に依存するアプローチでは、②のリスク分析の結果が確認できない可能性がでてくる。

これらのリスク分析での要件を満たすために、本ガイドラインでは、リスク分析にはベースラインと事業被害ベースの組み合わせアプローチを採用する。既存の基準をもとに一定レベルの評価が可能かつ作業の工数が大きくないベースラインアプローチを軸として、ベースラインの短所である事業被害が測れない点を事業被害ベースのリスク分析でカバーする。事業被害ベースでは、攻撃の起点と被害の起点のすべての攻撃ツリー洗い出すことはせず、最も大きな事

業被害（トップリスク）を回避できるか否かを評価することにフォーカスさせることで工数の爆発的な増大を回避する。

なお、今回採用したリスク分析のアプローチは多くのシステムをカバーするが万能ではない。高度標的型攻撃の対象となりうるシステムや国民の資産を預かるようなきわめて影響度が大きいシステム、新しい技術基盤を採用したシステムでは十分ではない。そのようなシステムに対して、リスク分析の手法はそのシステムのインパクトや特性に見合ったものを検討いただきたい。

2.4. リスク分析のプロセス

リスク分析のプロセスは、「ISO31000:2018, Risk management－Guidelines」のプロセスを参考に、本ガイドラインで採用する組み合わせアプローチのプロセスを以下のように定義する。

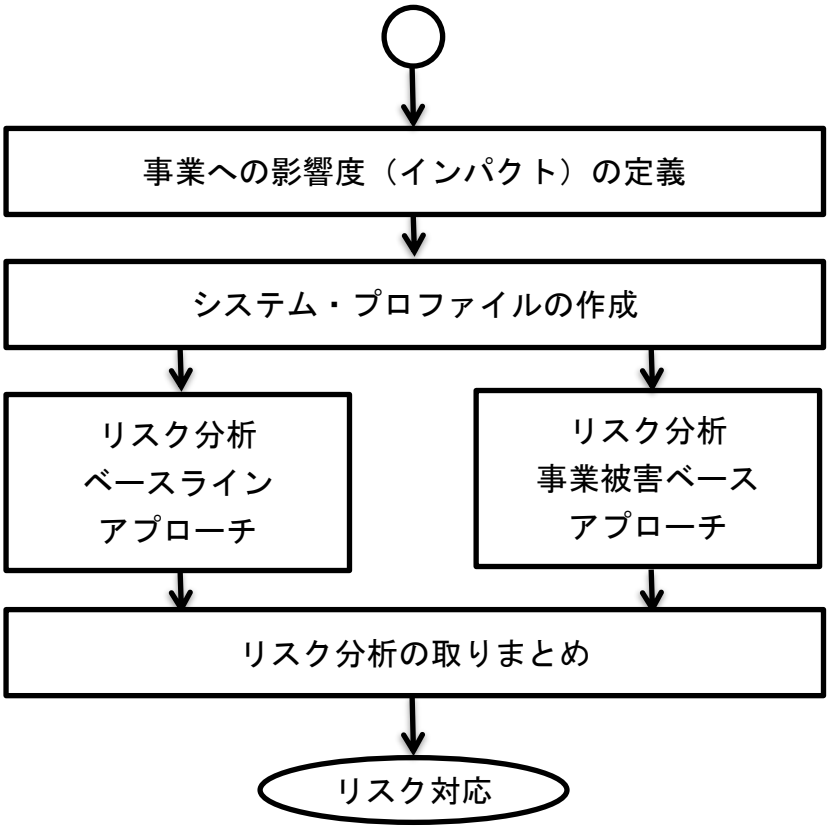


図２－１　本ガイドラインのリスク分析のプロセス

表２－２ リスク分析のプロセスの実施事項

プロセス	実施事項
事業への影響度（インパクト）の定義	事業の影響度を定義し、それぞれのリスク分析で共通した基準とする。
システム・プロファイルの作成	システムの利用形態や特性・特質を分析しプロファイルを作成する。作成したプロファイルはそれぞれのリスク分析で使用する。
リスクアセスメント	リスク特定、リスク分析及びリスク評価のプロセス全体。
ベースラインアプローチ	対象システムにあったセキュリティ管理策をチェックすることにより、確保すべきセキュリティレベルを達成するためのセキュリティ対策要件を分析する。
事業被害ベースアプローチ	事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被害を起こしうる攻撃シナリオによりリスク分析を実施する。
リスク分析の取りまとめ	２つのリスク分析の結果から、設定したセキュリティレベルを達成するセキュリティ対策を取りまとめる。

リスク分析のプロセスでは、セキュリティ・バイ・デザインでの対策へ効率的につなげるために、以下の点を考慮する。

・リスク分析のプロセスは、セキュリティ要件をシステム開発（調達）前に決定するためにシステムの企画フェーズ（要件定義フェーズ）で実施する。
・リスク分析の精度及びレビューの精度を上げるために、事業への影響度（インパクト）の定義とシステムのプロファイルをアセスメントの前に作成する。
・リスク分析のプロセス毎にレビューを実施し、リスク分析の妥当性を評価する。

3. リスク分析の実施

リスク分析の実施において、関係者の役割や事業への影響度の基準、システム・プロファイルの正確さは分析結果に影響するため重要となる。

本章では、リスク分析の基準と手順を説明する。

3.1. リスク管理に関わる関係者の役割

リスク分析では、開発チームがリスク分析や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って分析内容の妥当性を検証し進める必要がある。事業への影響度については、システム開発の都合でなく、行政サービスに責任をもつビジネス／リスクオーナーが事業視点で評価する必要がある。

以下に、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を示す。

表 3-1 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	•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。 •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。
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。
3	ビジネス/リスクオーナー	•事業被害の設定し、セキュリティ対策によるリスク軽減の有効性、残存リスクが許容できるかを判断する。 •システム対策と事業リスクのトレードオフの関係を判断する。 •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）	•業務観点及びシステム観点でのセキュリティリスク分析及び対策の妥当性を評価する。 •適合するセキュリティ・ベースラインやセキュリティ管理策をシステム管理者へ進言する。 •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、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。

【参照】デジタル庁「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」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

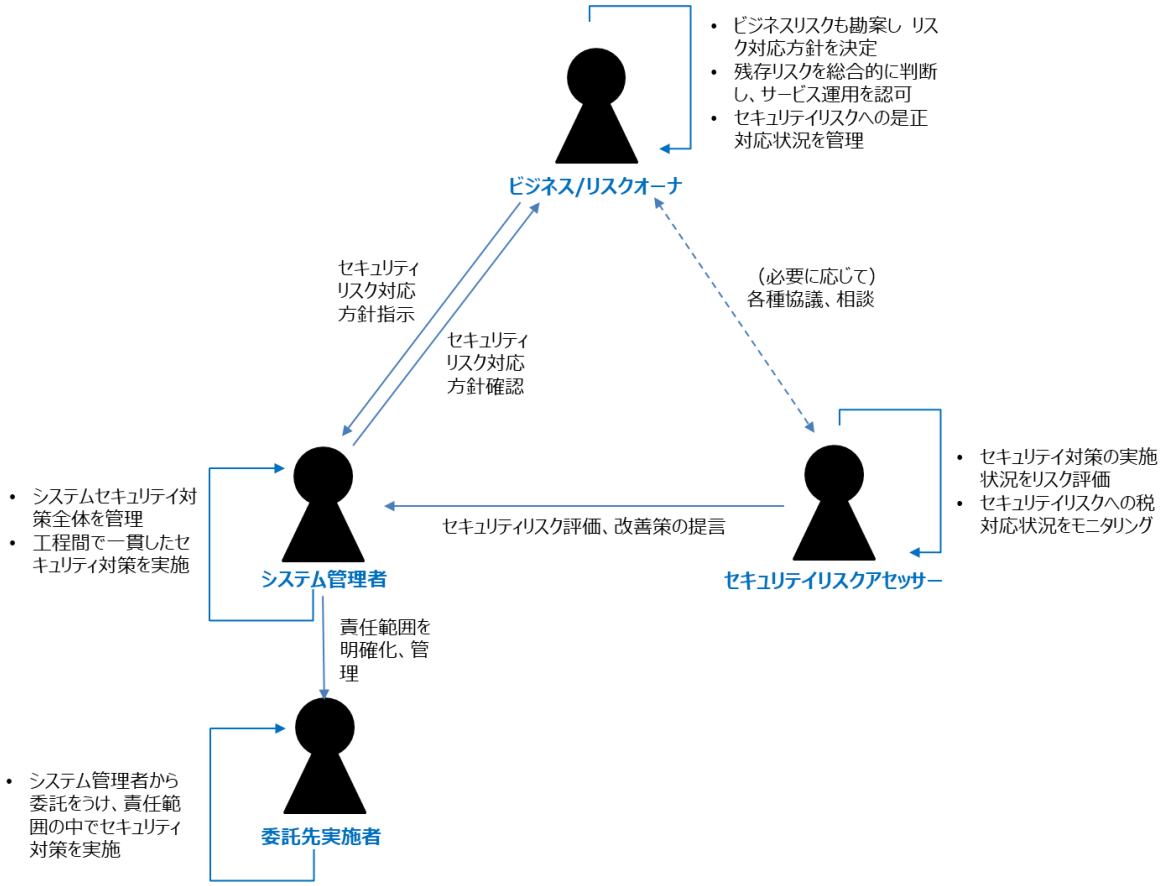


図 3-1 セキュリティ・バイ・デザインに関わる関係者

3.2. 事業への影響度（インパクト）の定義

政府情報システムが提供する国民や事業者向けの行政サービスや、行政機関の業務において生じる負の影響を、事業リスクとして以下のように定義する。この定義は、リスク分析を実施する際の共通の基準として用いられ、事業に責任をもつビジネス／リスクオーナーが影響度と最も大きな事業被害（最悪シナリオ）を評価する際に使用する。

（1）事業リスクの種類

事業リスクの種類を、NIST SP 800-63-3「Digital Identity Guidelines（電

子的認証に関するガイドライン)」を引用して以下のとおり定義する。

表３－２　事業リスクの種類

#	事業リスクの種類 Impacts per Category
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う Potential impact of inconvenience, distress, or damage to standing or reputation:
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を与える Potential impact of financial loss:
③	機関等の活動計画や公共の利益に対して影響を与える Potential impact of harm to agency programs or public interests:
④	利用者の個人情報などの機微な情報が漏洩する Potential impact of unauthorized release of sensitive information:
⑤	利用者の身の安全に影響を与える Potential impact to personal safety:
⑥	法律に違反する The potential impact of civil or criminal violations is:

（出典）NIST SP 800-63-3「Digital Identity Guidelines（電子的認証に関するガイドライン)」より作成

事業への影響度を評価する場合、情報セキュリティの 3 要素である機密性・完全性・可用性が失われた場合に関係する事業にどの程度の影響があるかによって評価する方法が一般的である。しかしながら、この 3 要素が失われた状況をリスクと認識して事業の影響まで評価しないミスを犯すことがある。本文書では、ビジネスオーナが影響度を認識しやすい NIST SP 800-63-3 の Impacts per Category を事業リスクの定義として採用することでミスを回避することを意図している。

（２）　事業への影響度の定義

事業への影響度を、「連邦政府の情報および情報システムに対するセキュリティ分類規格（連邦情報処理規格 FIPS 199)」を引用して以下の通り定義する。

表３－３.事業への影響度の定義

影響度	内容
高位 (High)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に致命的又は壊滅的な悪影響を及ぼすと予想される

中位 (Moderate)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に重大な悪影響を及ぼすと予想される
低位 (Low)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に限定的な悪影響を及ぼすと予想される
非該当 (NA)	該当しない　または　当該リスクによる影響がないと予想される

(出典)「連邦政府の情報および情報システムに対するセキュリティ分類規格(連邦情報処理規格 FIPS 199)」より作成

【補足説明】

致命的または壊滅的な悪影響：

事業が滞り元の状態に戻せない損失が発生した事象

重大な悪影響：

事業が滞り大きな影響はあったが、発生前の状況へ復旧できた事象

限定的な悪影響：

事業への影響は短期間または一部であった事象

NA：影響なし（NOT APPLICABLE）

（3） 事業リスク毎の事業への影響度の導出

上記の事業リスクの種類と事業への影響度を組み合わせて事業リスク毎の事業への影響度を定義する。

表３－４　事業への影響度の定義

#	事業リスク Impacts per Category	影響度	影響度の定義
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う	高位	深刻または重大かつ長期的な不便、苦痛、損害。この影響は、特に深刻な影響や多くの利用者に影響するレベル
		中位	相当かつ短期間ないしは限定的だが長期間の不便、苦痛、損害
		低位	限定的かつ短期間の不便、苦痛、損害
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を	高位	重大または致命的な経済的損失または賠償責任
		中位	相当な経済的損失または賠償責任
		低位	些細でとるに足らない経済的損失または賠償責任

#	事業リスク Impacts per Category	影響度	影響度の定義
	与える		
③	機関等の活動計画や公共の利益に対して影響を与える	高位	組織の運用や資産、公共の利益への致命的な悪影響（長期間の機能停止または深刻な損害）
		中位	組織の運用や資産、公共の利益への相当な悪影響（長期間の機能低下または著しい損害）
		低位	組織の運用や資産、公共の利益への限定的な悪影響（処理効率の低下または軽微な損害）
④	利用者の個人情報などの機微な情報が漏洩する	高位	情報の不当な開示が、組織活動、組織資産、または個人に致命的または壊滅的な悪影響を及ぼすことが予想されうる(FIPS 199)
		中位	情報の不当な開示が、組織活動、組織資産、または個人に重大な悪影響を及ぼすことが予想されうる(FIPS 199)
		低位	情報の不当な開示が、組織活動、組織資産、または個人に限定的な悪影響を及ぼすことが予想されうる(FIPS 199)
⑤	利用者の身の安全に影響を与える	高位	重傷または死亡のリスク
		中位	医療治療を必要とする怪我のリスク
		低位	治療を必要としない軽傷
⑥	法律に違反する	高位	特に重要とされている民事上又は刑事上の違反のリスク
		中位	法執行の対象となる可能性のある民事上又は刑事上の違反のリスク
		低位	法執行の対象とならない性質の民事上又は刑事上の違反のリスク

（出典）NIST SP 800-63-3「Digital Identity Guidelines（電子的認証に関するガイドライン)」より作成

3.3. システム・プロファイルの作成

次に、対象システムの利用形態や特性・特質を分析する。これはリスク分析を正しい情報を根拠に正確に実施することを目的としているが、ビジネス/リスクオーナーやセキュリティリスクアセッサーなどレビュー関係者が分析結果を評価するためにも使用する。実際の記載例を、参考資料Cに掲載する。

（1）事業の概要(Business Scope)

システムの事業（行政サービス）の内容とインパクトを以下の項目に整理する。

表３－５　システム・プロファイル（事業の概要）の記載項目

項目	記載事項
事業目的・ミッション	事業において達成する目的やミッション（達成しようとしている目標）を記載する。図示を交えてもよい。
事業の影響度 システムの保証レベル	3.1項「事業の影響度の定義」を参考に事業の影響度を記載する。 ➢ ６つの事業リスクそれぞれに対して最も大きな事業被害と影響度を記載する。この事業被害は、後の事業被害ベースの分析のインプットにする。 ➢ ６つの事業リスクの影響度から、後述の「システムの保証レベルのデシジョンフロー」に従ってシステムの保証レベルを求める。この保証レベルは、後のベースラインの要否判断をする際に使用する。
情報システム運用継続計画の復旧優先度	「NISC　政府機関等における情報システム運用継続計画ガイドライン(第 3 版)」で定める当該システムをどのくらいの時間で復旧させるかというRTO(目標復旧時間)とどの水準まで復旧させるかという RLO(目標復旧レベル)及び RTO・RLO から定めた復旧優先度を記載する。まだ、復旧優先度が設定されていない場合は、「未設定」と記載する。
統一基準での情報格付区分	システムで取り扱う情報の格付区分を「NISC　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)」の基準により記載する。
その他の格付区分	このほかにシステム格付区分がある場合は記載する。

・システムの保証レベルのデシジョンフロー[4]

[4] 「NIST SP 800-63-3 の保証レベル（AAL：Authentication Assurance Level)」から引用

６つの影響度からシステムの保証レベルを求める。

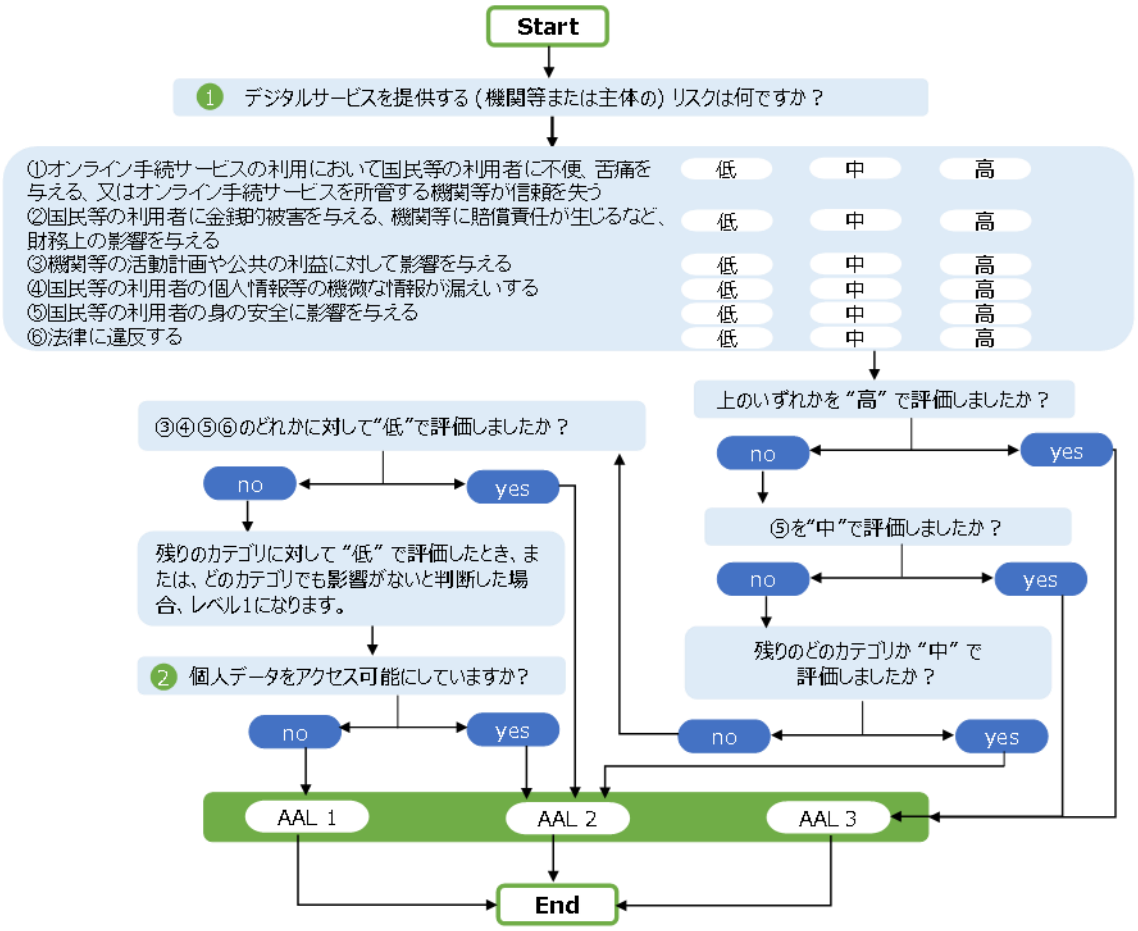


図３－２　システムの保証レベルのデシジョンフロー

※「システムの保障レベルのデシジョンフロー」は、個人情報や手続きを扱う行政サービスを提供するシステムを対象としている。ただし、国民の資産を預かるシステムや人命に関わるシステムでは、非常に高い保証レベルが求められるため、影響度判断に専門家が参加し、決定されることがある。このデシジョンフローは、上記以外のシステムに対して使用する。

（２）システムの意図する使用（Intended Use）

対象のシステムを、誰が、どこで、どのようなアクセス方法で利用するかを整理する。意図する使用方法を整理することで、何が不正なアクセスであるかを明らかにする。

表３－６　システム・プロファイル（システムの意図する使用）の記載項目

項目	記載事項
システムの概要・機能	システムの概要や機能を記載する。リスク分析に必要とする情報を含むこと。図示を交えてもよい。
意図する使用者 想定する利用者数	システムが意図している使用者と想定人数を列挙する。システム管理者や運用担当も含む。許可されない利用者（unauthorized user）を明確にする目的もある。
意図する使用環境、アクセス方法	システムが意図している使用環境・アクセス方法を列挙する。不正アクセス（unauthorized access）を明確にする目的もある。
ネットワークの構成と設定条件	システムを機能させるためのネットワーク構成を図示する。イメージや概念でなくセキュリティ確保のための機器やアクセス経路は明示する。保守や監視のアクセスも含む。記載粒度は、リスク分析が可能なレベルでよい。ポリシーやアクセス制御があれば併記する。

（3）システムの特質(Characteristics related to security)

情報資産とデータフローからシステムの特質を明らかにする。

表３－７　システム・プロファイル（システムの特質）の記載項目

項目	記載事項
情報資産（保護されるべき情報とプロセス)	情報資産を列挙する。また、可用性の対象とするサービスも列挙する。機微な情報については情報の件数も併記する。
システムの機能と権限、認証方法	システムの機能と機能を使用する権限（ロール)、使用者の認証方法を記載する。機能には管理者機能を含む。記載粒度は、リスク分析で確認するパターンが判別できるレベルでよい。
システムのアーキテクチャモデル	システムを構成するアーキテクチャに関連するパーツ（サーバの役割やモジュールの階層構造、I/Fやプロトコルなど）を図示または列挙する。
システムの相互運用性（システム連携)	他システムとのデータ連係やAPI、共通使用する基盤を記載する。インターフェース仕様や依存関係

項目	記載事項
	があれば併記する。
使用シナリオ またはデータフロー	脅威を洗い出す場合に重要になるが、システムの企画段階で網羅的に作成するのは負担が大きいため、今回は必須とはしない。最も大きな事業被害（トップリスク）が想定されるシナリオだけでもよい。

（4）システム・プロファイル作成での注意事項

リスク分析が不十分な理由の一つに、システムの現状把握や分析が不正確のまま実施されていることがあげられる。本ガイドラインでは、リスク分析の精度を確保するために、プロファイルを丁寧に作成することを推奨する。

- 分析の粒度は、セキュリティのリスク分析の根拠とできるレベルでよい。ビジネス/リスクオーナー、セキュリティリスクアセッサーがレビューにあたって必要とするレベルを想定する。また、足りないとわかってから追記しても問題ない。

- システム・プロファイルは、資料作成が目的ではなくリスク分析の根拠を明らかにするために作成するものなので、開発ドキュメントがある場合は引用しても問題はなく、プロファイル作成にかかる負担を軽減するように工夫する。

- リスク分析の時点で決まっていない仕様は、仕様が決まる際に再度リスク分析を行う。特にアジャイルアプローチでセキュリティの実装方式を決めるケースでは、セキュリティ要件を取りこぼさないようバックログとして管理し、あとからトレースできるようにする。

3.4. リスク分析（ベースラインアプローチ）

リスク分析のベースラインアプローチは、「NIST SP800-37 Rev2　情報システムおよび組織のためのリスクマネジメントフレームワーク[5]」を参考に作成した手順を示す。

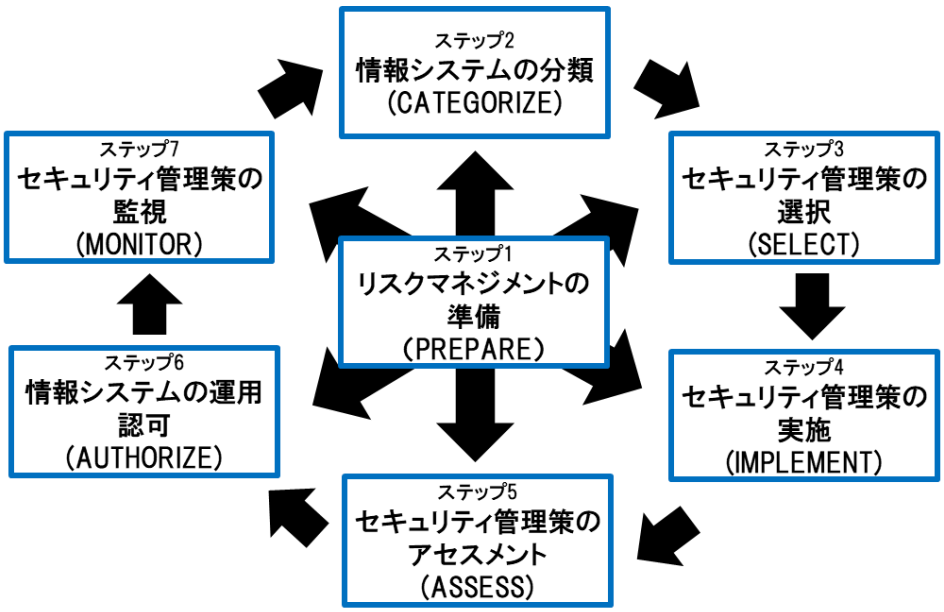


図３－２　リスクマネジメントフレームワーク（SP800-37 Rev2）

このフレームワークのステップ１からステップ３がベースラインアプローチのプロセスに対応する。ステップ４以降は、リスク分析の後のセキュリティ・バイ・デザインのプロセスになるが、分析結果が確実に対策されるようにこれらの手順もあわせて示す。記載例を参考資料Ｃ及び参考資料Ｄに掲載するので合わせて参考にしていただきたい。

【ステップ１】リスクマネジメントの準備（PREPARE）

対象システムの事業目的を明らかにし、そのシステムのプロファイルを作成し、システムの範囲及びリスクアセスメントで必要となる情報を明確にする。

[5] NIST SP800-37 Rev2　情報システムおよび組織のためのリスクマネジメントフレームワーク　ーセキュリティとプライバシーのためのシステムライフサイクルアプローチ「Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy 」

・実施事項
- リスク分析を担当するステークホルダ[6]（システム管理者、ビジネス/リスクオーナー、セキュリティリスクアセッサー）を特定する。
- システムがサポートする事業（行政サービス）の目的とミッション（達成しようとしている目標）及び事業の影響度を定義する。
- システムの使われ方を分析する。
- システムの特性を分析する。

・記載事項

システム・プロファイルを作成する。
- セキュリティリスク分析の担当者
- プロファイル（事業の概要）の記載項目（表３－５の項目）
- プロファイル（システムの意図する使用）の記載項目（表３－６の項目）
- プロファイル（システムの特質）の記載項目（表３－７の項目）

・考え方

NIST SP800-37 では、主に資産管理、ビジネス環境、リスクアセスメント、ガバナンスなどを分析することとされているが、本ガイドラインでは、３章で定義したシステム・プロファイルを作成することでリスクマネジメントの準備とする。

【ステップ 2】情報システムの分類（CATEGORIZE）

対象となる事業の影響度から、当該システムに求められるセキュリティ保証レベルを決定する。

・実施事項
- 事業の影響度（システムの保証レベル）を設定する。
- 事業の影響度の結果をレビューし決定する。

・記載事項
- 事業の影響度（システムの保証レベル）（表３－５の項目）

[6] リスク分析を担当するステークホルダの説明は「4.1.リスク管理に関わる関係者の役割」を参照

・考え方
事業の影響度は、３章で定義した事業の影響度を使用することで情報システムの分類とする。この分類は【ステップ 3】でのセキュリティ管理策の調整で使用する。情報システムの分類は、ビジネス/リスクオーナーが参加しレビューを実施して決定する。

【ステップ 3】セキュリティ管理策の選択（SELECT）

対象システムの現状調査に基づき、ベースラインとなるセキュリティ管理策を選択し、必要な場合はその内容を調整し、文書化する。

・実施事項
- 対象システムの特性にあったセキュリティ管理策を選択する。
- セキュリティ管理策の個々の項目について、要否を調整（テーラリング）する。
- セキュリティ管理策の選択と個々の項目の要否をレビューし決定する。

・記載事項
セキュリティ管理策に対応するベースラインの表を作成する。
ベースラインの表に以下の列を追加して記載する。
- セキュリティ管理策の個々の項目の要否判定
- 判定の理由
- 不要としたために発生するリスク
- 採用した場合の実装検証のタイミング

・考え方
行政サービスでは政府系システムのセキュリティ管理策から、システム構成からクラウドや Web などシステムの特性にあったセキュリティ管理策を選択する。システムの特性をカバーするために複数の管理策を採用してもよい。セキュリティ管理策の選択の判断ができないときはセキュリティリスクアセッサーへ支援を求める。参考資料 B に管理策の候補を示す。
システムの保証レベルやシステム特性にあわせて管理策の適用要否や適用レベルを調整する。セキュリティ管理策セキュリティ管理策の選択と調整の結果はビジネス/リスクオーナーとセキュリティリスクアセッサーへレビューをして妥当であることを確認する。

以上がベースラインアプローチのプロセスとなる。

次に、リスク分析をした後のプロセスを説明する。

【ステップ 4】セキュリティ管理策の実装（IMPLEMENT）

対象システムのセキュリティ管理策を実装する。また、セキュリティ管理策の実装方法を文書化する。

・実施事項
- 選択したセキュリティ管理策をセキュリティ要件として文書化する。
- セキュリティ・バイ・デザインのプロセスで実装する。

・記載事項
- セキュリティ要件
  - 調達仕様書に添付する要件仕様書
    （ステップ３で作成したベースラインの表から要求事項を抽出して作成する。）

・考え方

セキュリティ要求を開発者（委託先）へ示すとき、クライテリアと検証タイミングを合わせて提示することが望ましい。実装方式の決定によってセキュリティ要件が変わった際は、ベースラインの該当項目を満たしているか再度確認する。

【ステップ 5】セキュリティ管理策のアセスメント（ASSESS）

セキュリティ管理策が、正しく実装され、意図したとおりに機能し、セキュリティの要件を満たしているか有効性をアセスメントする。

・実施事項
- セキュリティ管理策が実装されているかを確認する。
- セキュリティ管理策の実装が意図した通りに機能し要件を満たしているか有効性をアセスメントする。

・記載事項

ベースラインの表に以下の列を追加して記載する。
- 管理策の実施の有無
- 実施エビデンスの文書名

・考え方
個々のセキュリティ管理策の要求事項が漏れなく正しく実装されていることを確認する。実装の確認は、受入時に行ってもよいし、委託先が実施したエビデンスを確認することで実施してもよい。セキュリティ管理策に紐付けて確認したエビデンスを記載することでトレーサビリティを確保する。

【ステップ 6】情報システムの運用認可（AUTHORIZE）

システムの運用または共通運用でのセキュリティ管理策について、運用認可責任者の許可をえる。

・実施事項
- セキュリティ管理策で運用対策とした項目について、運用認可責任者より認可を受けていることを確認する。

・記載事項
ベースラインの表に以下の列を追加して記載する。
- 運用対策の認可の有無
- 運用エビデンスの文書名

・考え方
運用体制によって確認先や確認方法が異なるため有効な方法をとること。運用を担当しない開発担当への確認では十分ではない。また、稼動後に運用整備することは原則認められない。やむを得ない理由がある場合は、例外事項として運用整備までの間のリスクと期限を合わせてビジネス/リスクオーナーからの承認をえる。

【ステップ 7】セキュリティ管理策の監視（MONITOR）

セキュリティ管理策の有効性を継続的にアセスメントし、必要な場合は適切に対応する。監視活動を報告し継続的な認可を受ける。また、必要に応じてシステムの廃棄戦略を策定し実施する。

3.5.　リスク分析（事業被害ベースアプローチ）

事業被害ベースのリスク分析は、回避したい事業被害を明確化し、事業被害を引き起こすと想定される攻撃について、事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析手法である。

本ガイドラインでは、分析のフレームワークとして

・IPA「制御システムのセキュリティリスク分析ガイド　第２版」

・ANSSI「EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)」

を参考に、最も大きな事業被害（トップリスク）を洗い出すことより、ベースラインのセキュリティ対応策でカバーができているか確認することに主眼を置いた手順を示している。この手順にあわせた事業被害ベースのリスク分析シートを参考資料 E　に掲載する。

【ステップ１】事業被害の洗い出し

システム・プロファイル（事業の概要）の６つの事業リスクでの最も大きな事業被害（トップリスク）を洗い出す。

・実施事項

- 事業に直接影響を及ぼす被害を洗い出し、各事業被害について現実化した場合の事業への影響の大きさを評価する。

・記載事項

- システム・プロファイル（事業の概要）「表３－５」で作成済み。

・考え方

システム・プロファイルを利用して、事業被害を洗い出す。洗い出しの対象は最も影響度（インパクト）が大きいものとするが、大きなリスクが複数想定できる場合は複数を対象としてよい。この後の分析が正しく実施できるように適切な表現で記載することに留意する。

【ステップ２】脅威の特定

事業被害を引き起こす攻撃シナリオを検討する。

・実施事項

- それぞれのケースで事業被害を引き起こす脅威を想定し攻撃シナリオを作

成する。
　脅威としては一般的な攻撃手法（不正アクセス・なりすまし、脆弱性の悪用、マルウェア、サービス拒否、盗聴、フィッシング、ソーシャル攻撃、物理攻撃など）を想定する。

・記載事項
- システム・プロファイル（事業の概要）「表３－５」から事業影響度の分類①～⑥の最も大きな事業被害を、「事業被害ベースのリスク分析シート」へ転記する。

・考え方
ここでは、専門的な攻撃手法や実施可能性を深掘りせず可能性を列挙すればよい。過去の類似システムのインシデントを参考にしてもよい。明らかに脅威となり得ない場合や事業被害につながらない場合は脅威としなくてもよい。

【ステップ３】攻撃シナリオの分析
攻撃シナリオを実現する攻撃ツリーを構成する。

・実施事項
- 攻撃のシナリオを必要に応じてサブ攻撃シナリオに分類する。攻撃シナリオを実現する攻撃ツリーは、事業被害を最終的に引き起こす最終的な攻撃まで漏れなく記載する。

・記載事項
- 事業被害ベースのリスク分析シートへ攻撃シナリオを記載する。
  攻撃ツリーのステップを分析シートに階層的に記載する。

・考え方
攻撃シナリオの記載では、攻撃者や攻撃の入り口や機器、攻撃内容をできるだけ具体的に記載する。文章に曖昧さがあると分析が不正確になるため注意する。

【ステップ４】リスク値の算定

事業リスクに加え、脅威レベルと脆弱性レベルを評価しリスク値を算定する。

・実施事項

- 攻撃ツリーを構成する一連の攻撃ステップにおける攻撃の難易度から脅威レベルを評価する。
- 攻撃ツリーを構成する一連の攻撃ステップについて、すでに対策済みであるなど脆弱性レベルを評価する。
- 攻撃ツリーを構成する一連の攻撃ステップについて、システム・プロファイルから事業被害レベルを転記する。
- 脅威レベル、脆弱性レベル、事業被害レベルから、参考資料Ｅ「事業被害ベースアプローチでのリスク算定基準」を参考にリスク値を算定する。

・記載事項

- 脅威レベル、脆弱性レベル、事業被害レベルを分析シートへ記載する。
- 算定したリスク値を分析シートへ記載する。

・考え方

ここでのリスク算定は、追加のリスク対策の要否の判断基準となる。

【ステップ５】リスクへの対策

発生可能性を下げる対策を抽出する。

・実施事項

- 攻撃ツリーを構成する一連の攻撃ステップに対して有効なリスク対策の項目を設定する。

・記載事項

- 事業被害ベースのリスク分析シートへ転記する。

・考え方

対策が複数存在してもよい（多層防御）。対策実施がこの段階では決められず設計時に検討する場合は、この後のセキュリティ要件を作成できるよう備考欄へ説明を残す。

3.6. リスク分析結果のとりまとめ

ベースラインアプローチと事業被害ベースアプローチの２つのリスク分析の結果をとりまとめる。

（1）２つのリスク分析のギャップ確認

・実施事項

- 事業被害ベースのリスク分析シートの対策がベースラインの管理策に含まれているかを確認する。このとき、ベースラインの管理策に含まれていても不採用になっていないことを確認する。

・記載事項

- ベースラインの管理策に含まれている場合は、事業被害ベースのリスク分析シートへベースラインの対応策番号を記入する。
- ベースラインの管理策に含まれていない場合は、セキュリティ要件に含むことをできるようにリスク分析シートへ記載する。

・考え方

判断を要する場合は、レビューを開催し判断の根拠を記録に残す。

（2）ベースラインリスク分析の有効性の検証

・実施事項

- 上記の２つのリスク分析のギャップ確認で、事業被害ベースのリスク分析からの対策がベースラインで大きくカバーできなかった場合は、ベースライン管理策の選定の誤りか足りないと判断し、ベースライン管理策の選定を見直しリスク分析を再度実施する。

・記載事項

- 有効／無効の判断をレビューし記録を残す。

・考え方

組み合わせ方式のリスク分析を採用する理由は、リスク分析の欠点であるシステムの特性と合わないものや陳腐化を排除するためである。そのため、ベースラインリスク分析の有効性の検証は確実に実施する。

4. リスク管理プロセス

セキュリティリスク分析は、セキュリティ・バイ・デザインの最初の工程であり、デジタル・ガバメント推進標準ガイドライン[7]におけるサービス・業務企画の工程として実施することを想定している。本ガイドラインは、その手順を示している。リスク分析の結果を対策につなげるためのリスク管理のプロセスは、セキュリティ・バイ・デザインのプロセスに含まれ実施される。

4.1. リスク分析結果の実装への反映

分析されたリスク管理策は、セキュリティ要件として定義され、システム開発のプロセスとして実装され、その結果、リスクが受容可能であることを評価する。この一連のプロセスが、セキュリティ・バイ・デザインのプロセスで実施されるよう以下の点に配慮する。

（1）セキュリティ要件

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。

【参照】デジタル庁「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」4.2.2)項：セキュリティ要件定義

要件は具体的な実装までを指示するものではないが、実装のクライテリア（合否判定基準）があるものは要件の中で示すことが望ましい。

（2）開発委託先の提示

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。

【参照】デジタル庁「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」4.2.3)項：セキュア調達

セキュリティ要件を調達時に示すこと、また実装の検証タイミングと評価者を委託先へ示すことが望ましい。実装の検証は、委託者が受け入れ時に行う方法と、受託者が検証してそのエビデンスを委託者が確認する方法がある。

[7] デジタル・ガバメント推進標準ガイドラインの工程とセキュリティリスク分析を含むセキュリティ・バイ・デザインの工程の対応は、デジタル庁「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」表 4-1 セキュリティ・バイ・デザインの実施工程と概要を参照のこと

（３）リスク対策の実施確認

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。

【参照】デジタル庁「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」4.2.6)項：セキュリティテスト

ここでのセキュリティテストは、セキュリティ要件に対して、実装と検証が実施されているかのホワイトボックス・テストをいう。テストエビデンスにセキュリティ要件の管理番号を記載、または、ベースラインのシートに対策実施のエビデンス番号を記載するなど、トレーサビリティを確保する方法を推奨する。

（４）運用によるリスク対策の確認

セキュリティ管理策で運用対策とした項目について、運用体制が整備され、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。

【参照】デジタル庁「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」4.2.7)項：セキュリティ運用準備

運用によるリスク対策の確認は、開発者でなく運用認可責任者によって認可を受けること。このプロセスはビジネス/リスクオーナーが必ず監督する。

4.2. リスク分析の見直し

リスク分析は、一度実施して終わりでなく、システムのライフサイクルの間、新たなリスクが発生していないかを継続して監視しなければならない。

システムのライフサイクルでのイベントとして

・システムの設計や実装方式の決定
・運用開始後に発見された脆弱性、新しい脅威事象
・使用するプロダクトのサポート終了
・システム改修での機能追加
・システムの使用対象、アクセス環境の変化
・セキュリティ管理策が変化した場合（暗号の危殆化など）

などがある。

これらのイベントが発生した場合は、過去に実施したリスク分析を見直し、分析範囲や管理策に要否に変更がないか判断を行い、必要な場合はリスク分析

の再実施と対策の実装と検証を行う。要否判断をシステム担当者だけで行わず、開発の時と同じくビジネス/リスクオーナーとセキュリティリスクアセッサーが参加し妥当性を確認する。

また、セキュリティ対策の技術や管理策は新たな脅威に対応するよう見直されているため、リスク分析の再実施では、その時点の最新技術や規格（State-of-the-Art）を基準にすることが望ましい。

リスク分析と対策を継続することは、コストが発生するために、再分析は敬遠される傾向にあるが、システムの企画段階から継続実施することを想定しアプローチすることで、効率的な対応が可能となる。本ガイドラインで採用したベースラインと事業被害ベースの組み合わせ方式のリスク分析は、上記イベント時に反復的に実行しやすいものとなっている。

変化するシステムやセキュリティの脅威に対して、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。

4.3. リスク分析ドキュメントの取扱い

リスク分析のドキュメントは、そのシステムの攻撃に有用な情報を含むため、管理対象の文書とする。セキュリティリスクアセッサーはリスク分析のドキュメントを共有する必要があるが、内容の秘匿義務を負い、公開や二次配布などしてはならない。

リスク分析から作成したセキュリティ要件は、他の開発ドキュメントと同じ基準で委託先など開発や検証の関係者へ提示しても問題はない。委託先とは他の開発ドキュメントと同じく契約で決められた守秘義務に則って運用する。

参考資料 A）参照したセキュリティ及びリスク分析のガイドライン

#	発行元	ガイドライン名	URL
1	デジタル庁	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 （令和４年６月 30 日）	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2a169f83/20220630_resources_standard_guidelines_guidelines_01.pdf
2	NISC(内閣サイバーセキュリティセンター)	政府機関等のサイバーセキュリティ対策のための統一基準 （令和３年７月７日）	https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf
3	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 （令和３年７月７日）	https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf
4	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) （2022 年７月 29 日）	https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html
5	ISO/JIS	ISO31000:2018, Risk management－Guidelines JIS Q 31000:2019 リスクマネジメント指針	-
6	IPA（情報処理推進機構）	制御システムのセキュリティリスク分析ガイド第２版 （2020 年 3 月）	https://www.ipa.go.jp/security/guide/vuln/controlsystem-riskanalysis.html
7	IPA（情報処理推進機構）	セキュリティ・バイ・デザイン導入指南書 （2022 年 8月）	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/security-by-design.html
8	NIST（米国国立標準技術研究所）	NIST SP800-63-3 Digital Identity Guidelines (UPDATES AS OF 03-02-2020) デジタル・アイデンティティ・ガイドライン	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
9	NIST（米国国立標準技術研究所）	NIST SP800-37 Rev2 Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy （Dec. 2018) 情報システムおよび組織のためのリスクマネジメントフレームワーク　ーセキュリティとプライバシーのためのシステムライフサイクルアプローチ	https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
10	NIST（米国国立標準技術研究所）	Cybersecurity Framework Version 1.1	https://www.nist.gov/cyberframework/framework-documents
11	NIST（米国国立標準技術研究所）	NIST SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations 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	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
12	NIST（米国国立標準技術研究所）	FIPS PUB 199: Feb 2004 Standards for Security Categorization of Federal Information and Information Systems 連邦情報処理標準（FIPS 199) 連邦政府の情報および情報システムに対するセキュリティ分類規格	https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
13	ANSSI（フランス国家情報システムセキュリティ機関）	EBIOS RISK MANAGER Version 1.0 - November 2019	https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

#	発行元	ガイドライン名	URL
14	OWASP	Software Assurance Maturity Model (Version 2.0.3 (2022))	https://owasp.org/www-project-samm/

参考資料 B）セキュリティ管理策のベースライン

ベースラインアプローチのリスク分析でのセキュリティ管理策の候補を示す。ここで示すもの以外のセキュリティ管理策を採用してもよい。なお、セキュリティ管理策の採用ではリスク分析時点で最新のバージョンであることを確認すること。

◆政府系システムのセキュリティ管理策

・NISC　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）

・NISC　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）

・NIST SP800-53 rev5 ： Security and Privacy Controls for Federal Information Systems and Organizations

・CIS Controls V8　（https://www.cisecurity.org/controls/v8）

◆クラウド系のセキュリティ管理策

・ISMAP　政府情報システムのためのセキュリティ評価制度　管理策基準

・CLOUD CONTROLS MATRIX VERSION 4.0
（https://cloudsecurityalliance.org/research/cloud-controls-matrix/）

・CIS　Benchmarks　（https://www.cisecurity.org/cis-benchmarks/）

◆アプリケーション・プロダクト

・OWASP　Application Security Verification Standard　Ver4.03　or　Ver5
（https://owasp.org/www-project-application-security-verification-standard/）

・CIS Benchmarks　（https://www.cisecurity.org/cis-benchmarks/）

・ENISA Good practices for Security of Internet of Things.
（https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1）

◆特定分野

・ISO/IEC　27002:2022（情報セキュリティ管理策）

・総務省　IoT セキュリティガイドライン Ver1.0

・総務省、厚生労働省、経済産業省　民間　PHR　事業者による健診等情報の取扱いに関する基本的指針　チェックシート
（https://www.meti.go.jp/policy/mono_info_service/healthcare/phr.html）

・厚生労働省　医療情報システムの安全管理に関するガイドライン　第 5.2 版
（https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html）

参考資料 C）システム・プロファイルの記載例

以下にシステム・プロファイルの記載例を示す。
記載項目は、本ガイドラインの項目を基本とするが、記載様式は自由に定めてもよい。開発ドキュメントなど他ドキュメントを引用・転用してもよい。

※本記載例は、例示を目的に作成したものであって、実際の業務や組織、システムと異なる。

――― システム・プロファイル ―――

◆セキュリティリスク分析の担当者

システム管理者：	デジタル庁〇〇G△△T	□□、□□、□□
ビジネス/リスクオーナー：	デジタル庁〇〇G△△T	□□
セキュリティリスクアセッサー：	デジタル庁〇〇G△△T	□□、□□

◆システム・プロファイル（事業の概要）

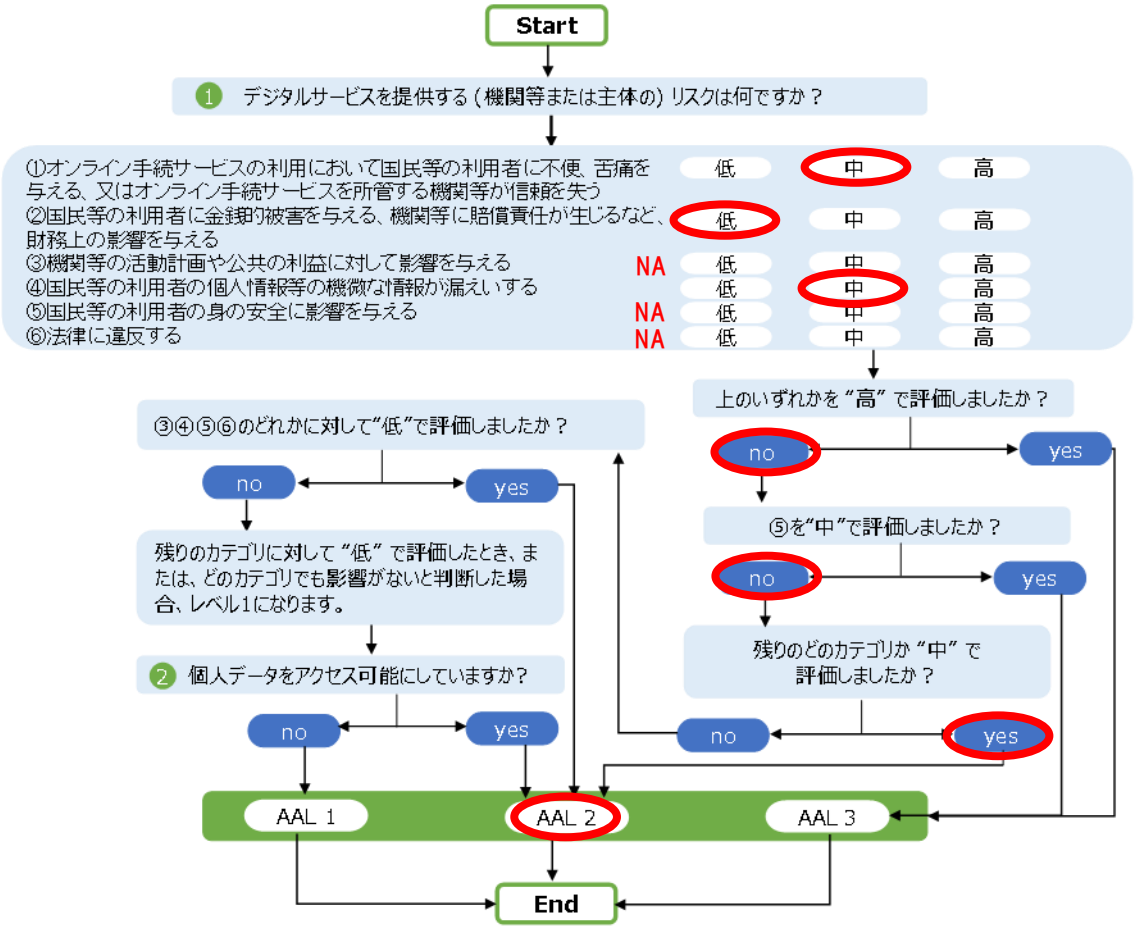
項目	説明・内容
事業目的・ミッション	デジタル庁及び政府各省が管理運営するシステムの全体像把握に必要な情報を収集・蓄積して、デジタル庁としての意思決定・組織運営に活用するため、ダッシュボードを用いてわかりやすく可視化する。
事業の影響度 システムの保証レベル	ＡＡＬ２（中程度） ・リスクの種類別の影響度は下記別表に記載 ・保証レベルは、システムの保証レベルのデシジョンフローから導出
情報システム運用継続計画の復旧優先度	ＲＴＯ(目標復旧時間)：1 週間から 2 週間以内に復旧が必要な情報システム ＲＬＯ(目標復旧レベル)：特になし 復旧優先度：Ｄ
統一基準での情報格付区分	機密性３情報：なし 機密性２情報：あり　（システム構成等非公開情報を含む） 完全性２情報：なし　（オリジナルデータから復元可能） 可用性２情報：なし　（停止しても代替方法あり）
その他の格付区分	特になし

◆リスクの種類別の影響度

#	事業リスク Impacts per Category	最も大きな事業被害	影響度
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う	サイバー攻撃によってシステムが停止し、利用できなくなる。 サイバーインシデントの被害が公になり、デジタル庁の信頼低下を招く。	中位
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を与える	サイバー攻撃によって、システムのデータやプログラムが改ざんされてしまい、復旧のための工数（費用）が発生する。	低位
③	機関等の活動計画や公共の利益に対して影響を与える	影響なし（効率は悪化するが、このシステムだけに異存はしていないので実害はない）	NA
④	利用者の個人情報などの機微な情報が漏洩する	システムの構成情報が漏洩し、セキュリティ攻撃に悪用される	中位
⑤	利用者の身の安全に影響を与える	影響なし	NA
⑥	法律に違反する	影響なし	NA

◆システムの保証レベルの導出

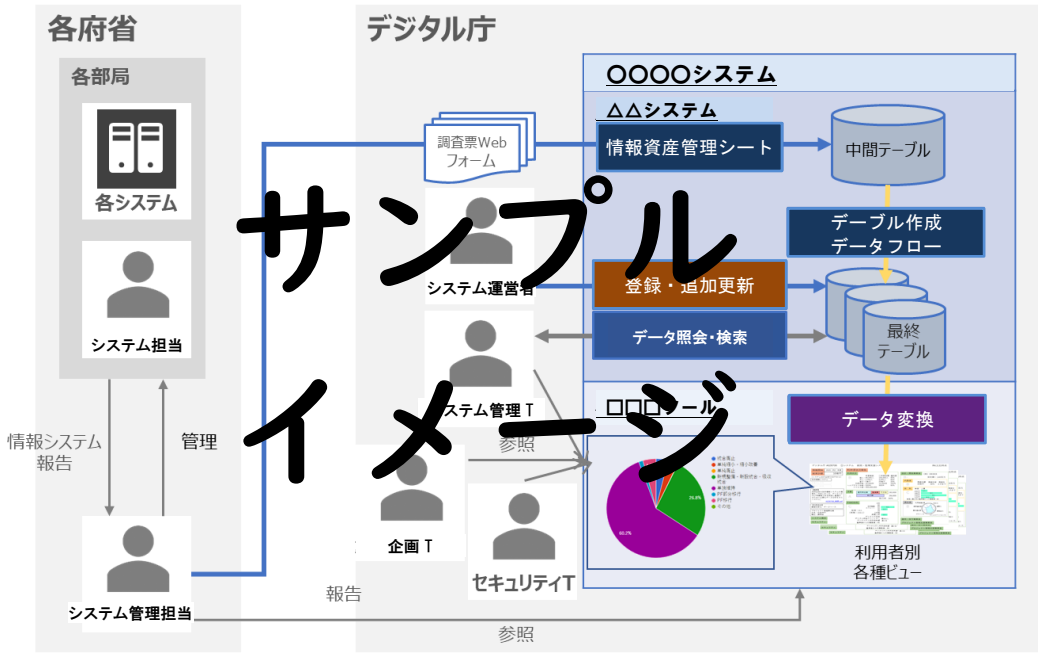
上記で求めた影響度をフロー上にマーキングする。



◆システム・プロファイル（システムの意図する使用）

項目	説明・内容
システムの概要・機能	システム名：〇〇〇〇システム 政府情報システムの情報資産管理シートとデジタル庁が保有するデータを〇〇〇社の△△システムで取込し、利用者のニーズに沿って□□□□ツールで可視化し提供する。
意図する使用者 想定する利用者数	デジタル庁職員　システム管理Ｔ　約〇名 企画Ｔ　約〇名 セキュリティＴ　約〇名 各府省　システム管理担当　約〇名 システム運営者　約〇名 ※システム管理に関わらない政府職員は利用しない
意図する使用環境、アクセス方法	デジタル庁職員　庁内ネットワーク 各府省　庁内ネットワークにゲストアカウントを登録して各府省ネットからの接続 システム運営者　庁内ネットワーク
ネットワークの構成と設定条件	既存のデジタル庁内ネットワーク内で構成 （この記載事例は省略する。 対象システムのネットワーク構成図とアクセス制限やセキュリティ機能・機器があれば記載すること。）

◆システム概要図



◆システム・プロファイル（システムの特質）

項目	説明・内容
情報資産	システム基本情報（管理番号、システム名、所管部門） システム利用情報（利用開始年度、利用対象者） システム構成（プラットフォーム、アクセス、連携先） 開発・改修履歴（開発名、開始／終了、委託先） 運用実績（登録ユーザ数、アクセス数）
システムの機能と権限、認証方法	機能と権限：下記に別途記載 認証方法：　庁内認証基盤でのＳＳＯ（ＭＦＡ）
システムのアーキテクチャモデル	○○○社（△△システム）で構成
システムの相互運用性（システム連携）	認証のため　□□□と連携 データの初期セットに EXCEL を使用
使用シナリオ またはデータフロー	１）庁内でデータ登録する ２）各府省からデータを登録する ３）登録データを確認・メンテナンスする ４）庁内でデータ照会する ５）庁内ユーザの権限設定をする ６）各府省のユーザ登録・アクセス権設定をする ７）各府省からのアクセスを有効／無効の設定をする （入力期間の制御処理）

◆システムの機能と権限（業務上の機能と使用者の関係）

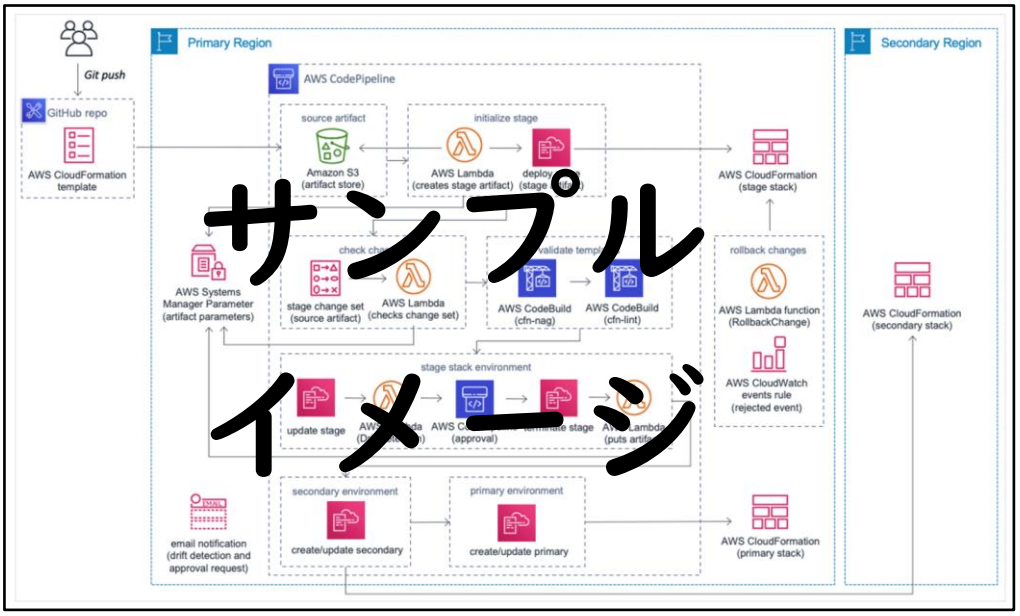
業務	機能	使用者	システムの機能権限
システム情報登録・更新	登録・更新機能（庁内）	システム管理Ｔ	システム情報登録
	調査票 Web エントリー（登録、結果確認、履歴）	各府省システム管理担当	調査票 Web アクセス
	情報メンテナンス	システム運営者	システム情報更新
システム情報検索	一般情報ビューの照会	システム管理Ｔ 企画Ｔ セキュリティＴ	システム情報照会
	システム構成情報の照会	システム管理Ｔ セキュリティＴ	システム構成照会
	各府省からの情報照会	各府省システム管理担当	システム情報照会（自省）
維持管理	ゲストユーザ登録	システム運営者	（基盤担当へ申請）
	権限設定	システム運営者	（基盤担当へ申請）
	入力期間の設定登録	システム運営者	入力期間設定
	ログ取得・確認機能	システム運営者	アクセスログ出力

◆システムの機能と権限（ロール定義）

ユーザグループ		権限						
		登録	調査票 Web アクセス	情報 更新	照会 （全部）	照会 （自省）	入力期間 設定	アクセス ログ出力
	システム管理Ｔ	✔						
	企画Ｔ				✔			
	セキュリティ Ｔ				✔			
	各府省システム 管理担当		✔			✔		
	システム運営者			✔	✔		✔	✔

◆システムのアーキテクチャモデル

・ Structure



・ ミドルウェア・ＯＳＳ

コンポーネント名	Ver	提供元	パッチ レベル	サポート 期限
○○○○○○	1.0	○○○社		2029.12
△△△△△△	2.0	○○○社		2029.12
□□□□□□	3.0	□□□社		2029.12

参考資料 D）ベースラインアプローチの記載例と様式

セキュリティリスク分析　ベースライン管理策 （記載例）

選択したセキュリティ管理策　：　CIS Controls V8

“セキュリティ管理策の選択”の項目を追加する

“管理策のアセスメント”の項目を追加する

【ステップ3】　【ステップ5】【ステップ6】

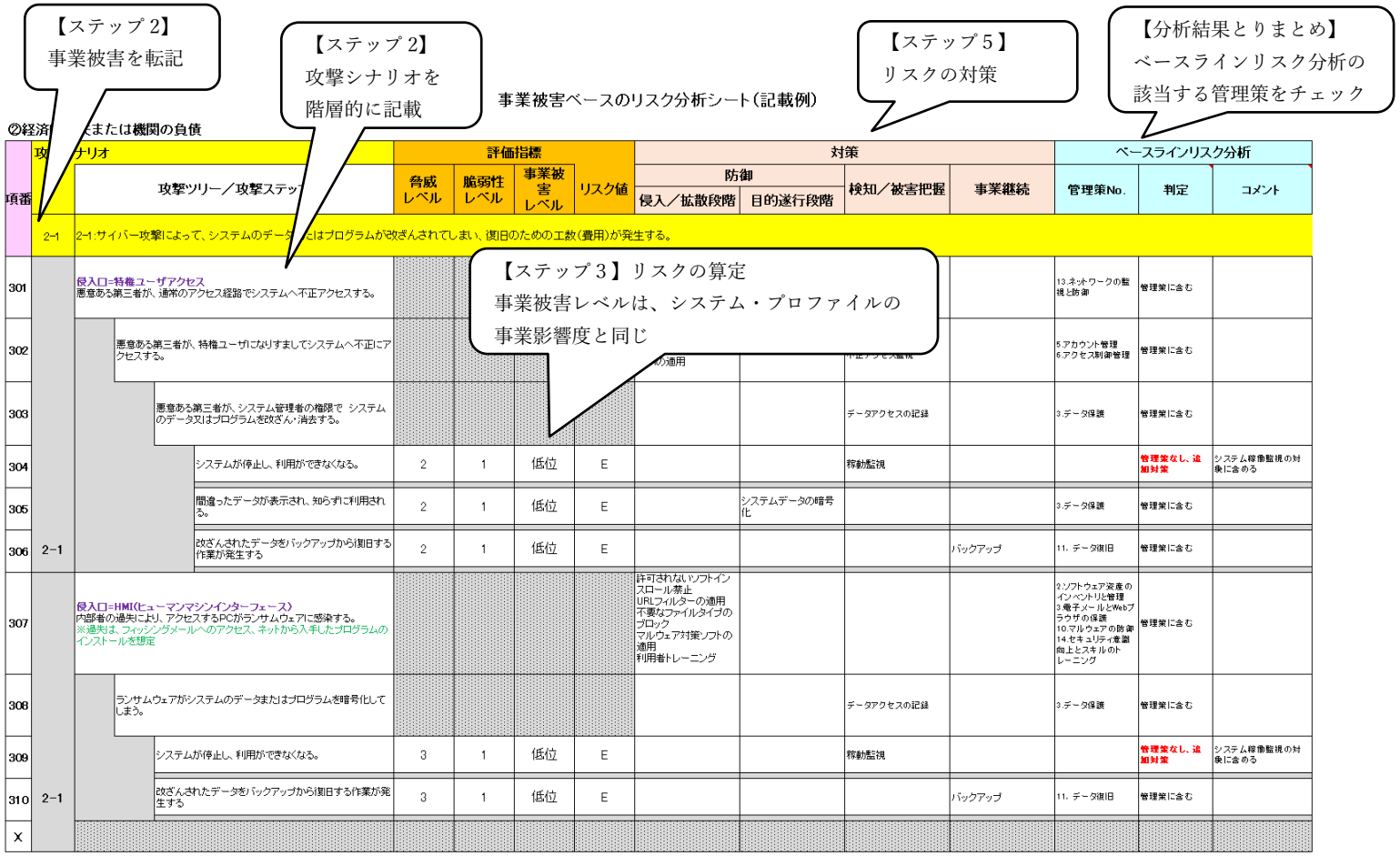
CIS Controls V8要求事項									セキュリティ管理策の選択				管理策のアセスメント	
juusok	CIS Safeguard	Asset Type	Security Function	Title(jp)	Description(jp)	IG1	IG2	IG3	要否判定	判定の理由	不要としたために発生するリスク	実装検証のタイミング	実施の有無 検証結果	実施エビデンス
3				データ保護	*データの特定、分類、安全な取り扱い、保持、および廃棄のためのプロセスおよび技術的管理手法を策定します。*									
3	3.10	Data	Protect	送受信中の機密データを暗号化する	送受信中の機密データの暗号化実装例としては、次のようなものがあります。TLSやOpenSSHなど		x	x	対策済み	庁内MS365上でのセキュリティ対策に含め、本アプリ個別の対応はしない				
3	3.12	Network	Protect	機密度に応じてデータ処理・保管を分離する	データの機密度に応じて、データの処理と保管を分離します。機密データを、機密度の低いデータ用の組織の資産で処理しません。		x	x	必要（内部で実装）			受入テスト	PASS	データ保管とアクセス制御のテストレポート
3	3.14	Data	Detect	機密データへのアクセスを記録する	変更や廃棄を含む、機密データへのアクセスを記録します。			x	不要・非該当	本システムの保証レベルはAAL2(IG2相当)のためIG3要求は含めない	庁内インフラに依存。本システムへの直接の影響は少ない			
5				アカウント管理	*プロセスとツールを使用して、管理者アカウントやサービスアカウントなどのユーザー アカウントの資格情報に、組織の資産やソフトウェアへの認可を割り当てま*									
5	5.3	Users	Respond	休止アカウントを無効にする	設定可能であれば、45日間非アクティブ状態が 続く休止アカウントを削除または無効にします。	x	x	x	対策済み	庁内インフラ上でのセキュリティ対策に含め、本アプリ個別の対応はしない				
5	5.4	Users	Protect	管理者権限を専用の管理者アカウントに制限する	管理者権限を組織の資産専用の管理者アカウントに制限します。 ユーザーのプライマリの非特権アカウントから、インターネットブラウジング、電子メール、各製品の使用など、一般的なコンピューティング アクティビティを実行します。	x	x	x	対策済み	庁内インフラ上でのセキュリティ対策に含め、本アプリ個別の対応はしない				
8				監査ログ管理	*攻撃の検知、理解、あるいは攻撃からの復旧に役立つイベント監査ログを収集し、警告を発し、分析し、保存します。*									
8	8.2	Network	Detect	監査ログを収集する	監査ログを収集します。監査ログ管理プロセスに基づいて、組織の資産全体でログの収集が有効になっていることを確認します。	x	x	x	必要（調達先が実装）			運用および保守	PASS	監査ログ収集手順書 監査ログ確認報告
10				マルウェアの防御	*組織の資産に悪意のあるアプリケーション、コード、スクリプトがインストール、拡散、実行されることを防止または制御します。*									
10	10.1	Devices	Protect	マルウェア対策ソフトウェアを導入し維持する	すべての組織の資産にマルウェア対策ソフトウェアを導入し、維持します。	x	x	x	対策済み	庁内インフラ上でのセキュリティ対策に含め、本アプリ個別の対応はしない				

対象のシステムの特性にあったセキュリティ管理策を選択する。

セキュリティ管理策の要否判定を行い記載する。

セキュリティ管理策の実施結果を確認し記載する。

参考資料 E）事業被害ベースアプローチのリスク分析の記載例と様式[8]



項番	攻	ナリオ 攻撃ツリー／攻撃ステッ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	目的遂行段階	検知／被害把握	事業継続	ベースラインリスク分析 管理策No.	判定	コメント
	2-1	2-1:サイバー攻撃によって、システムのデータまたはプログラムが改ざんされてしまい、復旧のための工数（費用）が発生する。											
301		侵入口=特権ユーザアクセス 悪意ある第三者が、通常のアクセス経路でシステムへ不正アクセスする。									13.ネットワークの監視と防御	管理策に含む	
302		悪意ある第三者が、特権ユーザになりすましてシステムへ不正にアクセスする。					の適用		不正アクセス監視		5.アカウント管理 6.アクセス制御管理	管理策に含む	
303		悪意ある第三者が、システム管理者の権限で システムのデータ又はプログラムを改ざん・消去する。							データアクセスの記録		3.データ保護	管理策に含む	
304		システムが停止し、利用ができなくなる。	2	1	低位	E			稼動監視			管理策なし、追加対策	システム稼働監視の対象に含める
305		間違ったデータが表示され、知らずに利用される。	2	1	低位	E		システムデータの暗号化			3.データ保護	管理策に含む	
306	2-1	改ざんされたデータをバックアップから復旧する作業が発生する	2	1	低位	E				バックアップ	11. データ復旧	管理策に含む	
307		侵入口=HMI(ヒューマンマシンインターフェース) 内部者の過失に起因、アクセスするPCがランサムウェアに感染する。 ※過失は、フィッシングメールへのアクセス、ネットから入手したプログラムのインストールを想定					許可されないソフトインスロール禁止 URLフィルターの適用 不要なファイルタイプのブロック マルウェア対策ソフトの適用 利用者トレーニング				2.ソフトウェア資産のインベントリと管理 9.電子メールとWebブラウザの保護 10.マルウェアの防御 14.セキュリティ意識向上とスキルのトレーニング	管理策に含む	
308		ランサムウェアがシステムのデータまたはプログラムを暗号化してしまう。							データアクセスの記録		3.データ保護	管理策に含む	
309		システムが停止し、利用ができなくなる。	3	1	低位	E			稼動監視			管理策なし、追加対策	システム稼働監視の対象に含める
310	2-1	改ざんされたデータをバックアップから復旧する作業が発生する	3	1	低位	E				バックアップ	11. データ復旧	管理策に含む	
X													

[8] ＩＰＡ　「制御システムのセキュリティリスク分析ガイド第２版」　　の　様式を元に作成

◆事業被害ベースアプローチでのリスクの算定基準[9]

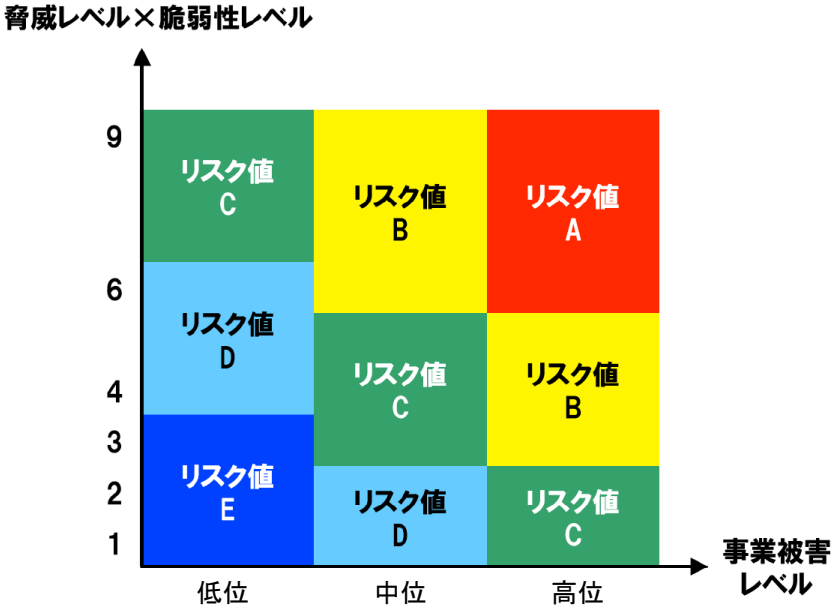
・脅威レベル

脅威レベル	判断基準（技術的要素）	判断基準（時間的要素）
3	脅威が発生する可能性が高い。 ・攻撃実現に必要な知識は限定的。 ・攻撃実現に必要な技術の入手は容易。	脅威が発生する可能性が高い。 ・攻撃実施に必要な時間は短い。 ・攻撃実施可能な時間帯は無制限。
2	脅威が発生する可能性が中程度である。 ・攻撃実現に必要な知識は中程度。 ・攻撃実現に必要な技術の入手容易性は中程度。	脅威が発生する可能性が中程度である。 ・攻撃実施に必要な時間は中程度。 ・攻撃実施可能な時間帯に制約がある。
1	脅威が発生する可能性が低い。 ・攻撃実現に必要な知識は膨大。 ・攻撃実施に必要な技術の入手は困難。	脅威が発生する可能性が低い。 ・攻撃実施に必要な時間は長い。 ・攻撃実施可能な時間帯は極めて限定的。

・脆弱性レベル

脆弱性レベル	判断基準
3	脅威に対するセキュリティ対策が実施されておらず、攻撃が成功する可能性は高い。
2	脅威の対策が実施されているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 一般的な対策を実施しており、攻撃が成功するか否かは攻撃者のレベルに依る。
1	脅威の対策が十分実施されており、攻撃が成功する可能性は低い。 効果的な対策や、多層的な対策を実施しており、攻撃が成功する可能性は低い。

・リスク値の算定基準



[9] ＩＰＡ　「制御システムのセキュリティリスク分析ガイド第２版」を元に作成
事業被害レベルの区分について、本ガイドラインの事業影響度の表現に変更している。