

リスクアセスメントの実施手順（例）

**～社会経済を支えるサービスを提供する事業者等による
自律的なリスクマネジメントに向けて～**

本文書の目的・位置づけ

「機能保証のためのリスクアセスメント・ガイドライン」（以下「ガイドライン」といいます。）に沿ったリスクアセスメントの実施手順について、各プロセスに対応した様式の記載例等を用いて、主に作業担当者に向けて解説するものです。

各事業者等のリスクマネジメントプロセス

リスクアセスメント

リスク対応

3章
事前準備

4章
リスクアセスメントの
対象の特定

5章
リスク評価方針の特定

6章
リスクアセスメント

7章
リスクアセスメントの
妥当性確認・評価

8章
リスクアセスメントの
継続的な見直し

機能保証の
ためのリスク
アセスメント・
ガイドライン
(本編)

別紙5 (本文書)
リスクアセスメントの
実施手順 (例)

活動目的

様式1
リスクアセスメントの実施目的
の確認

サービス

様式2
重要サービスの
選定

業務

様式4
重要サービスを
支える業務の
特定及び当該
業務の影響度
分析

経営資源

様式5
業務を支える
経営資源の特
定

リスク

様式6
リスクアセスメント
6-1 リスク源
6-2 リスクシナリオ

妥当性

自己評価
レポート

見直し

別紙1

事業・重要サービス・経営資源（情報資産）の例（重要サービスごと）

別紙3

結果を生じ得る事象
（脅威）及び対策例

別紙4

業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスクシナリオの例

別紙6

自己評価レポートの利用要領

本文書の説明範囲

事前準備



リスクアセスメントの実施目的の確認

使用する様式

様式1

想定する作業部門

経営企画部門、サービス管理部門 など

平時又は大規模国際イベント等に向けた「リスクアセスメントの実施目的」を定め、それを踏まえた自組織の活動目標を設定します。

リスクを考慮する上での前提になります。
各関係者で認識を共有しておくことが重要です。

リスクアセスメントの実施目的	自組織の活動目標
サービスをストレスなく、快適に利用できること。	利用者が、業務や情報の取得、コミュニケーション等に必要なネットワークサービスを必要な速度で安定的かつ継続的に提供する。
安全・安心なネットワークサービスを提供すること。	ネットワークサービスを提供することにより、セキュアなアクセスを実現する。
自然災害、管理不良、サイバー攻撃などの発生時にも必要最低限のサービスが利用できること	自然災害、管理不良、サイバー攻撃などサービスへの脅威が発生した際にも必要最低限のネットワークサービスが提供できるようにする。

作業ステップ

リスクアセスメントの実施目的の確認

実施方針の確認

マスタースケジュールの策定

実施体制の構築

詳細スケジュールの策定
及び要員計画

本資料の説明範囲

関連資料

- ・ ガイドライン本編 [9～12ページ]
3. 事前準備
- ・ 別紙5 (様式集)
(様式1) リスクアセスメントの実施目的の確認
- ・ (付録) 様式記載要領
Step1: リスクアセスメントの実施目的の確認

実施方針の確認

使用する様式

様式1

想定する作業部門

経営企画部門、サービス管理部門 など

自組織におけるリスクアセスメントの実施方針※1を設定し、経営層及び関係部門において、これを確認します。

※1 リスクアセスメントの実施目的を達成するために必要な活動の範囲や進め方。
本ガイドラインに沿った「リスクアセスメントの実施方針」(例)を様式1に記載してありますので、参考としてください。

リスクアセスメントの対象の特定 1/4



重要サービスの選定

使用する様式

様式 2

想定する作業部門

経営企画部門、サービス管理部門 など

事業者等が扱うサービスについて、利害関係者からの期待、その他の期待・要求事項、経営面からの位置づけを分析し、重要サービス※1を特定します。

別紙 1

事業・重要サービス・経営資源（情報資産）の例（重要サービスごと）

※1 リスクアセスメントの実施対象とするサービス

自組織の活動目的に照らして、サービスが利害関係者から、どのように期待されているのかを整理して記載します。

利害関係者からのニーズ・期待、社会的責任（CSR）、法制面の要求（コンプライアンス）等の観点からの期待や要求を記載します。

サービスに関する利害関係者のニーズ・期待
／法規制面での要求事項の分析

製品・サービスの経営面での位置づけ

事業

サービス

サービスに関する利害関係者の期待

その他の
期待・要求事項

売上

...

分析を
踏まえた
重要
サービスの
選定

後続の作業を考慮して、
必要以上に細分化しないよう
留意が必要です。

自然災害・・・などの発生時にも
サービスが利用できること

コメント

売上高等の業績・戦略面の数値を
記載し、経営上の位置付けを明確に
します。

通信事業	企業向けプライベートネットワークサービス	○	…	○	企業が円滑にビジネスを遂行するためには、各拠点を結ぶネットワークサービスが高い品質で維持されることが必要である。	安全かつ高品質なネットワークサービスを、継続的に提供することが必要である。	XXX億円/年	…	○
	一般ユーザ向けネットワークサービス	○	…	○	国民生活を支える重要なサービスであり、パソコンやモバイルアプリから情報を取得するために、重要である。	安全かつ高品質なネットワークサービスを、継続的に提供することが必要である。	XXX億円/年	…	○
…	…	…	…	…	…	…	…	…	…
付帯事業	法人SI	—	…	—	直接的な影響はない	—	X億円/年	…	—

以降の
評価対象

作業ステップ

重要サービスの選定

重要サービスの影響分析

重要サービスを支える業務の
特定・影響分析

業務を支える経営資源の特定

本資料の説明範囲

関連資料

- ・ガイドライン本編 [13ページ]
4. リスクアセスメントの対象の特定
- ・別紙 1 事業・重要サービス・経営資源（情報資産）の例（重要サービスごと）
- ・別紙5（様式集）
（様式2）重要サービスの選定
- ・（付録）様式記載要領
Step2: 重要サービスの選定

リスクアセスメントの対象の特定 2/4



重要サービスの影響分析

使用する様式

様式3

想定する作業部門

経営企画部門、サービス管理部門 など

事業者等が扱うサービスの最低限許容される範囲・水準を明らかにした上、その提供が完全に停止した場合の影響及び時間経過に伴う影響度合いを評価し、サービスの最大許容停止時間を推定します。

直接の取引先だけでなく、エンドユーザ等も視野に入れてその影響を推測します。

事業	サービス	利害関係者のニーズ・期待／法規制面での要求事項等を満たすために最低限許容されるサービスの範囲・水準		サービスの提供が完全停止した場合の影響		サービスの提供に係る最大許容停止時間	
		契約責任、法令遵守	社会的責任 (CSR)	最低限許容されるサービスの範囲・水準が満たされない場合に生じる事態	時間経過に伴う影響度合いの評価	時間	コメント
通信事業	企業向けプライベートネットワークサービス	企業が円滑にビジネスを遂行するためには、各拠点を結ぶネットワークサービスの品質が片時も損なわれない必要がある。	高品質なネットワークサービスを提供し、日本経済の発展に貢献する。	データ通信の遅延や消失により、事業者の業務に直接的な影響があることが想定される。		瞬時	

リスクの影響度を評価する際の参考情報として活用します。

作業ステップ

重要サービスの選定

重要サービスの影響分析

重要サービスを支える業務の特定・影響分析

業務を支える経営資源の特定

本資料の説明範囲

関連資料

- ・ガイドライン本編 [14ページ]
4. リスクアセスメントの対象の特定
- ・別紙5 (様式集)
(様式3) 重要サービスの影響分析
- ・(付録) 様式記載要領
Step3: 重要サービスの影響分析

リスクアセスメントの対象の特定 3/4



重要サービスを支える業務の特定・影響分析

使用する様式

様式4

想定する作業部門

サービス管理部門、業務管理部門 など

重要サービス（リスクアセスメントの対象とすべきサービス）の提供のために必要な業務を洗い出し、当該業務について最低限許容される水準（操業率、稼働率等）を明らかにした上、当該業務が停止した場合の影響及び停止に係る最大許容時間を推定します。

バリューチェーンを意識し、重要サービスの提供のために必要な業務を洗い出します。

事業	サービス	重要サービスの提供に必要な業務	重要サービスの最低許容範囲・水準を満たすために必要な業務の最低水準	業務が完全停止した場合に重要サービスの提供に及ぼす影響	業務に係る最大許容停止時間
通信事業	企業向けプライベートネットワークサービス	アクセス系サービス提供	通信サービスの利用不可は基本的に許されない。	お客様プライベートネットワーク利用不可によるビジネスへの重大な影響。	瞬時
		アクセス系故障復旧機能	故障発生時のみ、影響あり。故障復旧の着手は迅速に、復旧完了までも短時間で済ませることが必要。	故障発生時の修理対応が不可となる。	1 時間
		ポータルサイト系サービス提供	お客様による細部設定変更や契約情報の閲覧などが24時間・安全・快適にできること。	お客様のサービス利用の利便性が損なわれる。営業対応による代替は一定可能である。	1 営業日

リスクの影響度を評価する際の参考情報として活用します。

作業ステップ

重要サービスの選定

重要サービスの影響分析

重要サービスを支える業務の特定・影響分析

業務を支える経営資源の特定

本資料の説明範囲

関連資料

- ガイドライン本編 [14ページ]
4. リスクアセスメントの対象の特定
- 別紙5（様式集）
（様式4）重要サービスを支える業務の特定及び当該業務の影響分析
- （付録）様式記載要領
Step4:重要サービスを支える業務の特定及び当該業務の影響分析

リスクアセスメントの対象の特定 4/4



業務を支える経営資源の特定

使用する様式

様式5

想定する作業部門

サービスを担当する事業部門など

事業者等が扱う重要なサービスに必要な業務について、最低限満たすべき業務水準を維持するために必要な経営資源及びその経営資源が満たすべき要件・必要な数量等について明らかにします。

後続の作業を考慮し、同一の管理を実施している資産をまとめる等の工夫が必要です。

別紙 1

事業・重要サービス・経営資源（情報資産）の例（重要サービスごと）

参考

参考

業務を支える経営資源の要件・必要数量

事業	サービス	重要サービスの提供に必要な業務								
			人	情報、データ	建物、作業環境、関連ユーティリティ	設備、機器、消耗品	情報通信技術（ICT）システム、制御システム	交通機関、ライフライン（例：電気、水、ガス）	資金	その他
通信事業	企業向けプライベートネットワークサービス	アクセス系サービス提供		設定情報		機器 約○台	サービス用システム	電気		
		アクセス系故障復旧機能		設備情報			専用システム 専用NW 予備機	電気		
		ポータルサイト系サービス提供		申込情報 工事情報	サービスセンター		サービス用システム	電気		業務委託先A社

本書のリスクアセスメントにおいてはIT障害に係るリスクを対象としていますので、これ以降の作業ステップについては、「情報、データ」や「情報通信技術（ICT）システム、制御システム」等の情報資産が対象となります。

作業ステップ

重要サービスの選定

重要サービスの影響分析

重要サービスを支える業務の
特定・影響分析

業務を支える経営資源の特定

本資料の説明範囲

関連資料

- ガイドライン本編 [15ページ]
4. リスクアセスメントの対象の特定
- 別紙 1 事業・重要サービス・経営資源（情報資産）の例（重要サービスごと）
- 別紙 5（様式集）
（様式5）業務を支える経営資源の特定
- （付録）様式記載要領
Step5:業務を支える経営資源の特定

リスク評価方針の策定 1/2



リスク分析手法の検討

リスクの重大さを把握するための分析手法を決定します。ガイドラインでは、サービス提供を全うすることに対するリスクを特定・分析・評価するという観点から、「事象の結果による重要サービス・業務への影響度合い」と「事象の発生確率」を評価の軸とし、リスクマップ※1及びリスク・スコアリング※2を用いてリスクを分析する手法を参考例として紹介しています。

※1 「影響度」及び「発生頻度」等の評価軸をそれぞれ縦横の軸にしたマトリクスにリスクを配置して、そのリスクの相対的な優先関係を把握する手法です。

※2 それぞれの要素に重大さに応じた一定のスコアを付して掛け合わせることによって、優先すべきリスクを明確にする手法です。

事象の発生確率	5	5	10	15	20	25
	4	4	8 リスク	12	16	20
	3	3	6	9	12	15
	2	2	4	6 リスク	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		事象の結果による重要サービス・業務への影響度合い				

リスクマップ及びリスク・スコアリングのイメージ

作業ステップ

リスク分析手法の検討

リスク基準の決定

■ 本資料の説明範囲

関連資料

- ガイドライン本編 [16～17ページ]
5. リスク評価方針の策定

リスク評価方針の策定 2/2



作業ステップ

リスク分析手法の検討

リスク基準の決定

リスク基準の決定

リスクの重大さを評価するための判断指標を決定します。

ガイドラインで紹介する分析手法においては、「各評価軸の評価基準」及び「リスク・スコアリング結果の何点以上をリスク対応※¹の対象とするかの基準値」を決定します。

※¹ リスクを修正するプロセス

事象の発生確率の評価基準	
5	頻発 各組織の状況に即した評価基準を設定
4	1年に1回程度
3	数年に1回程度
2	10年に1回程度
1	ごくまれな状況発生

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

※この例では**5以上**がリスク対応の対象となります。

■ リスク対応の対象

□ リスク対応の対象外

発生頻度が非常に少ないと評価された場合であっても、影響度の大きなリスクは拾えるよう考慮しています。

事象の結果による重要サービス・業務への影響度合いの評価基準		
	予想影響範囲・程度	予想復旧時間
5		
4		
3		
2		
1		

各組織の状況に即した評価基準を設定

リスク基準は、リスクアセスメントの実施目的に応じた設定にすることが必要です。

また、リスクアセスメントの継続的な見直しにおいて、環境変化等に応じて設定の見直しを行うことも重要です。

■ 本資料の説明範囲

関連資料

- ガイドライン本編 [17～18ページ]
- 5. リスク評価方針の策定

リスクアセスメント (リスク源) 1/3



リスクの特定 (リスク源)

使用する様式

様式6-1

想定する作業部門

システム部門

経営資源（情報資産）ごとに、業務の阻害につながる事象の結果、その結果を生じ得る事象及びリスク源※1を演繹的なアプローチ※2により特定します。

※1 それ自体又はほかとの組合せによって、リスクを生じさせる力を本来潜在的にもっている要素。

※2 P22「帰納的なアプローチと演繹的なアプローチ」を参照

別紙2

業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスク源の例

参考

参考

参考

事業	サービス	重要サービスの提供に必要な業務	経営資源（情報資産）	業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源
通信事業	企業向けプライベートネットワークサービス	営業活動	顧客情報	顧客情報の情報流出	内部持ち出し	情報を持ち出せる環境（記録媒体） ・USBメモリ 業務の社会的重要性を理解していない人物や悪意ある人物による情報/システムの使用
				⋮	⋮	⋮

以降、リスク源から発生する事象及び結果の連なり（リスク）について、分析・評価を行います。

作業ステップ

リスクの特定

リスクの分析

リスクの評価

本資料の説明範囲

関連資料

- ・ガイドライン本編 [19～20ページ]
6. リスクアセスメントの対象の策定
- ・別紙2 業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスク源の例
- ・別紙5（様式集）
（様式6-1）リスクアセスメント(リスク源用)
- ・（付録）様式記載要領
Step6:リスクアセスメント

リスクアセスメント (リスク源) 2/3



リスクの分析 (リスク源)

使用する様式

様式6-1

想定する作業部門

システム部門

「事象の結果による重要サービス・業務への影響度合い」と「事象の発生可能性」を分析し、リスク評価のインプットとなる「残留リスク値」を導出します。

- 何らかの対策を講じている場合であっても、対策の有効性が陳腐化しやすいという情報セキュリティ対策の性質を考慮し、対策前の評価及び対策後の評価を行います。
- 「別紙3：対策例」を参考に、現在講じている対策がリスク源に対して有効なものであるかを確認します。

リスクの特定			事象の結果による重要サービス・業務への影響度合い			事象の発生確率			残留リスク値
業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	事象の結果の影響	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後
顧客情報の情報流出	内部持ち出し	悪意ある人物による情報/システムの使用	業務停止に直結するものではないが、調査や説明対応に追われることにより、通常業務の遂行を大きく阻害する。	4	顧客情報を扱うシステムの操作者は制限され、操作できるサービスレベルも操作者ごとに必要最低限に制限されている。	3	4	社員教育の実施	3

事象の結果による重要サービス・業務への影響度合いの評価基準

5	...
4	...
3	...
2	...
1	...

事象の発生確率の評価基準

5	...
4	...
3	...
2	...
1	...

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

リスク評価の方針 (例)

作業ステップ

リスクの特定

リスクの分析

リスクの評価

本資料の説明範囲

関連資料

- ・ ガイドライン本編 [21~22ページ]
6. リスクアセスメントの対象の特定
- ・ 別紙5 (様式集)
(様式6-1) リスクアセスメント(リスク源用)
- ・ (付録) 様式記載要領
Step6:リスクアセスメント

リスクアセスメント (リスク源) 3/3



リスクの評価 (リスク源)

使用する様式

様式6-1

想定する作業部門

システム部門

次のステップにより、経営層による全社的な意思決定に基づくリスク対応の実施対象とするリスクを特定します。

- ① リスク対応の実施対象として、リスク基準以上の残留リスク値のリスクを抽出します。
- ② リスク基準未満の残留リスク値のリスクのうち、個別事情を勘案してリスク対応の実施対象とするものを抽出します。
- ③ リスク対応の実施対象として抽出されたリスクに対し、リスクオーナー（そのリスクの管理に関する責任を負担する部門又は役職員）を定めます。

リスクの特定			リスクの分析	リスクの評価		
業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	残留リスク値	リスク基準	リスク評価	リスクオーナー
			8	5	●	〇〇部門
			2	5	—	—
			4	5	●	××部門

「リスク評価方針の特定」において
定めた「リスク基準」を転記

凡例

- ：リスク対応の実施対象
- ：リスク対応が不要

リスク基準未満の残留リスク値のリスクであっても、個別事情によっては、リスク対応の対象とします。

(注)本ステップにおいてリスク対応の実施対象として抽出されなかったリスクについては、リスクとして認識しないということではなく、通常の業務又は職務上の分掌に基づく管理対象として、所管する部署・部門又は役職員の責任において管理します。

作業ステップ

リスクの特定

リスクの分析

リスクの評価

本資料の説明範囲

関連資料

- ・ガイドライン本編 [22ページ]
6. リスクアセスメントの対象の特定
- ・別紙5 (様式集)
(様式6-1) リスクアセスメント(リスク源用)
- ・(付録) 様式記載要領
Step6:リスクアセスメント

リスクアセスメント (リスクシナリオ) 1/3



リスクの特定 (リスクシナリオ)

使用する様式

様式6-2

想定する作業部門

システム部門

経営資源（情報資産）ごとに、業務の阻害につながる事象の結果、その結果を生じ得る事象を洗い出し、当該事象が顕在化するリスクシナリオ※1を策定します。

※1 業務の阻害につながる事象が起きる過程をステップごとに記載したもの

- 別紙4の例を参考に、自社を取り巻く内外の環境を踏まえて、リスクシナリオを策定します。

別紙4 業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスクシナリオの例

参考

事業	サービス	重要サービスの提供に必要な業務	経営資源（情報資産）	業務の阻害につながる事象の結果	情報セキュリティ3要素	結果を生じ得る事象	要因	リスクシナリオ
								ステップ
通信事業	企業向けプライベートネットワークサービス	営業活動	顧客情報	顧客情報の情報流出	機密性	ベンダーによる不正	内部不正	悪意のあるベンダーがデータを不正にアクセスし、USBメモリにより、機密情報が組織外に流出する。
								悪意のあるベンダー関係者が、リモート保守端末を操作し、保守用アカウントでリモートアクセスする。
								悪意のあるベンダー関係者が、機密情報を保守作業以外の目的で端末に不正にダウンロードする。
								悪意のあるベンダー関係者が、USBメモリを端末に接続し、機密情報をUSBメモリに保存する。

情報セキュリティ3要素は複数の記載が可能です。

以降、策定したリスクシナリオに対して分析・評価を行います。

作業ステップ

リスクの特定

リスクの分析

リスクの評価

本資料の説明範囲

関連資料

- ガイドライン本編 [20ページ]
6. リスクアセスメントの対象の策定
- 別紙4 業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスクシナリオの例
- 別紙5（様式集）
（様式6-2）リスクアセスメント(リスクシナリオ用)
- （付録）様式記載要領
Step6: リスクアセスメント

リスクアセスメント (リスクシナリオ) 2/3



リスクの分析 (リスクシナリオ)

使用する様式

様式6-2

想定する作業部門

システム部門

「事象の結果による重要サービス・業務への影響度合い」と「事象の発生可能性」を分析し、リスク評価のインプットとなる「残留リスク値」を導出します。

- 何らかの対策を講じている場合であっても、対策の有効性が陳腐化しやすいという情報セキュリティ対策の性質を考慮し、対策前の評価及び対策後の評価を行います。

リスクの特定			事象の結果の影響度合い		事象の発生確率		残留 リスク値	
業務の阻害につながる事象の結果	結果を生じ得る事象	リスクシナリオ	対策前	現在講じている対策	対策後	現在講じている対策		
		ステップ						
顧客情報の情報流出	ベンダーによる不正	悪意のあるベンダーがデータを不正にアクセスし、USBメモリにより、機密情報が組織外に流出する。	4	顧客情報を扱うシステムの操作者は制限され、操作できるサービスレベルも操作者ごとに必要最低限に制限されている。	3	4	3	9
		悪意のあるベンダー関係者が、リモート保守端末を操作し、保守用アカウントでリモートアクセスする。						
		悪意のあるベンダー関係者が、機密情報を保守作業以外の目的で端末に不正にダウンロードする。						
		悪意のあるベンダー関係者が、USBメモリを端末に接続し、機密情報をUSBメモリに保存する。						
					<div>・ 事象の発生確率では、ステップごとに現在講じている対策が当該ステップにおける対策として有効なものであると認めます。なお、複数の対策を記載することも可能です。</div>			
					アクセス権限の管理			
					外部記憶媒体の管理			

- 事象の発生確率では、ステップごとに現在講じている対策が当該ステップにおける対策として有効なものであるかを確認します。なお、複数の対策を記載することも可能です。

アクセス権限の管理

外部記憶媒体の管理

事象の結果による重要サービス・業務への影響度合いの評価基準	
5	...
4	...
3	...
2	...
1	...

事象の発生確率の評価基準	
5	...
4	...
3	...
2	...
1	...

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
1	2	3	4	5	

- 評価基準を何段階にするかは、任意に設定できます。

リスク評価の方針 (例)

作業ステップ

リスクの特定

リスクの分析

リスクの評価

本資料の説明範囲

関連資料

- ガイドライン本編 [21~22ページ]
6. リスクアセスメントの対象の特定
- 別紙 5 (様式集)
(様式6-2) リスクアセスメント(リスクシナリオ用)
- (付録) 様式記載要領
Step6: リスクアセスメント

リスクアセスメント (リスクシナリオ) 3/3

作業ステップ

リスクの特定

リスクの分析

リスクの評価

リスクの評価 (リスクシナリオ)

使用する様式

様式6-2

想定する作業部門

システム部門

次のステップにより、経営層による全社的な意思決定に基づくリスク対応の実施対象とするリスクを特定します。

- ① リスク対応の実施対象として、リスク基準以上の残留リスク値のリスクを抽出します。
- ② リスク基準未満の残留リスク値のリスクのうち、個別事情を勘案してリスク対応の実施対象とするものを抽出します。
- ③ リスク対応の実施対象として抽出されたリスクに対し、リスクオーナー（そのリスクの管理に関する責任を負担する部門又は役職員）を定めます。

リスクの特定			リスクの分析	リスクの評価		
業務の阻害につながる事象の結果	結果を生じ得る事象	リスクシナリオ	残留リスク値	リスク基準	リスク評価	リスクオーナー
			8	5	●	〇〇部門
			2	5	—	—
			4	5	●	××部門

「リスク評価方針の特定」において
定めた「リスク基準」を転記

凡例
●：リスク対応の実施対象
—：リスク対応が不要

リスク基準未満の残留リスク値のリスクであっても、個別事情によっては、リスク対応の対象とします。

(注)本ステップにおいてリスク対応の実施対象として抽出されなかったリスクについては、リスクとして認識しないということではなく、通常の業務又は職務上の分掌に基づく管理対象として、所管する部署・部門又は役職員の責任において管理します。

本資料の説明範囲

関連資料

- ・ガイドライン本編 [22ページ]
6. リスクアセスメントの対象の特定
- ・別紙5 (様式集)
(様式6-2) リスクアセスメント(リスクシナリオ用)
- ・(付録) 様式記載要領
Step6: リスクアセスメント

(参考)

リスクアセスメントの次ステップ（リスク対応の選択肢の同定）

リスク対応の選択肢の同定

様式 6 において、リスク対応の実施対象とした各リスクについて、リスク対応の選択肢（低減・回避・移転・保有）※1のいずれを採用するかを同定することにより、リスク対応の方針を明らかにします。

※1 P23「リスク対応の選択肢」を参照

複数選択可能

リスク源	リスク対応の選択肢					
	低減			回避	移転 (共有)	保有 (受容)
	リスク源の 除去	影響の 低減	発生の 低減			
インターネットへの接続 環境有	●	—	●	—	—	—
冗長化の不採用	—	●	—	—	—	—
周辺システムとの連携有	—	—	—	●	—	—

＜発生頻度及び影響度に応じたリスク対応（例）＞

多 事象の発生頻度	起こりやすさ の低減	起こりやすさ の低減	リスク源 の除去	回避
	起こりやすさ の低減	起こりやすさ の低減	リスク源 の除去	リスク源 の除去
	起こりやすさ の低減	起こりやすさ の低減	影響度 の低減	影響度 の低減
	保有 (受容)	影響度 の低減	影響度 の低減	移転 (共有)
小		事象の結果の影響度		大

どうしてもリスク回避せざるを得ない（分野内又は分野横断的にリスクを共有すべき）との判断に至ったリスクがある場合には、関係各所と共有し、その対応を協議します。

例えば運輸業における振替輸送のように、同種のサービスを提供する事業者間での協力に基づく代替措置を講ずるなど、大規模国際イベント等の準備期間及び開催期間における時限的な措置としてのリスクの共有についても、顧客保護の観点から考慮することが重要です。

作業ステップ

リスクの特定

リスクの分析

リスクの評価

リスク対応の選択肢の同定

本資料の説明範囲

関連資料

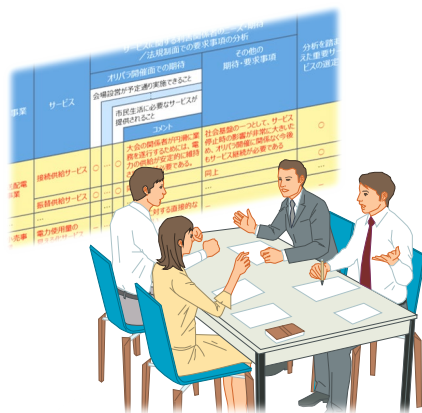
- ・ガイドライン本編 [23ページ]
6. リスクアセスメントの対象の特定
- ・別紙 5（様式集）
（様式6）リスクアセスメント
- ・（付録）様式記載要領
Step6:リスクアセスメント

リスクアセスメントの妥当性確認・評価 1/2



ワークスルー（リスクアセスメントの実施内容の妥当性確認）

リスクアセスメントの結果における偏りやばらつきを解消するため、複数の関係主体が連携してリスクアセスメントの実施内容を検証し、その正当性を確認するとともに、検証結果を共有・合意します。



＜ワークスルーのイメージ＞



ワークスルー記録票

実施プロセスの証跡
開催日、レビュー対象、
参加者の所属・氏名・
ワークスルーにおける役割、
議事内容等を記録



ワークスルー指摘事項一覧表

実施内容の証跡
指摘内容、指摘者、
指摘に対する対応方針、
指摘に基づく修正内容等を記録

＜ワークスルーに係る証跡の例＞

※様式は用意されていません

リスクアセスメントの実施内容の妥当性を確認する際に参考となる、リスクアセスメントの集計結果やグラフ等を表示する『自己評価レポート』を提供しています
(利用方法等の詳細は『別紙6 自己評価レポートの利用要領』をご参照)

リスクアセスメントシートに記載された内容が正当であること

- サービス、業務、経営資源等が抜け漏れなく洗い出されているか。また、その洗出作業の際に参照した内部資料等の根拠が客観的に成果物から読み取れるか。
- 各ステップでの判断が、前ステップの結果を踏まえて論理的に説明可能であるか（整合性が確保されているか）。また、その判断根拠が客観的に成果物から読み取れるか。

リスクアセスメントシートに記載された内容についての認識が共有及び合意されていること

- リスクアセスメントシートの記載内容が、読み手に誤解を与えるような記述となっていないか。また、特定の部門内、とりわけ情報システム部門内でしか通じないような記述となっていないか。
- リスクアセスメントシートの記載の粒度や精度にばらつきがないか。
- リスク基準の解釈やリスク基準に基づくリスク評価の判断について、関係主体間の認識齟齬はないか。

＜ワークスルーの観点の例＞

作業ステップ

担当者の選任及び役割分担

事前準備（確認観点等の周知）

ワークスルーの実施

レビュー対象成果物の修正

ワークスルー結果のまとめ

各関係主体へのフィードバック

本資料の説明範囲

関連資料

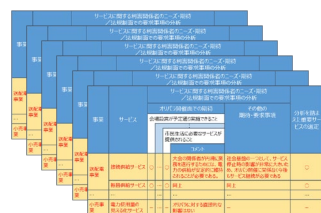
- ガイドライン本編 [25～28ページ]
7. リスクアセスメントの妥当性確認・評価

リスクアセスメントの妥当性確認・評価 2/2



パフォーマンス評価（リスクアセスメント作業の妥当性確認）

リスクアセスメントを実施するための体制 並びに リスクアセスメントの実施手続及び活動状況が適切かつ十分であったかを評価することにより、リスクアセスメント実施内容が目的達成に向けて妥当であったかを確認します。



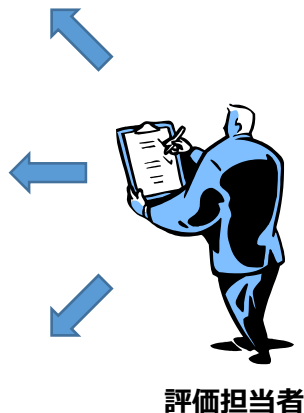
リスクアセスメントシート

ワークスルー記録票

実施プロセスの証跡

ワークスルー指摘事項一覧表

実施内容の証跡



評価担当者

リスクアセスメントシート

- 明らかな記載漏れがないか。特に、特定されたリスクの分析・評価結果の記載漏れやリスクオーナーの設定漏れがないか。
- 明らかな記載誤りがないか。例えば、既に何らかの対策を講じているにも関わらず、その対策を講じる前に比べ、リスクが高い評価数値となっているようなことはないか。

ワークスルー記録表

- 全てのリスクアセスメント推進部門がワークスルーに参加し、レビューを実施しているか。特に、評価結果の精度向上の観点から、有識者がワークスルーに参加し、レビューを実施しているか。
- 評価結果の客観性を確保する観点から、法務部門やリスク管理部門等の間接部門がワークスルーに参加し、レビューを実施しているか。

ワークスルー指摘事項一覧表

- ワークスルーで出された指摘事項に対して、漏れなく対応方針が整理されているか。また、整理された対応方針は、リスクアセスメントシートに確実に反映されているか。

<パフォーマンス評価のイメージ>

<パフォーマンス評価の観点の例>

作業ステップ

評価担当者の選任

パフォーマンス評価の実施

パフォーマンス評価結果のまとめ

各関係主体へのフィードバック

■ 本資料の説明範囲

関連資料

- ・ ガイドライン本編 [29～30ページ]
7. リスクアセスメントの妥当性確認・評価

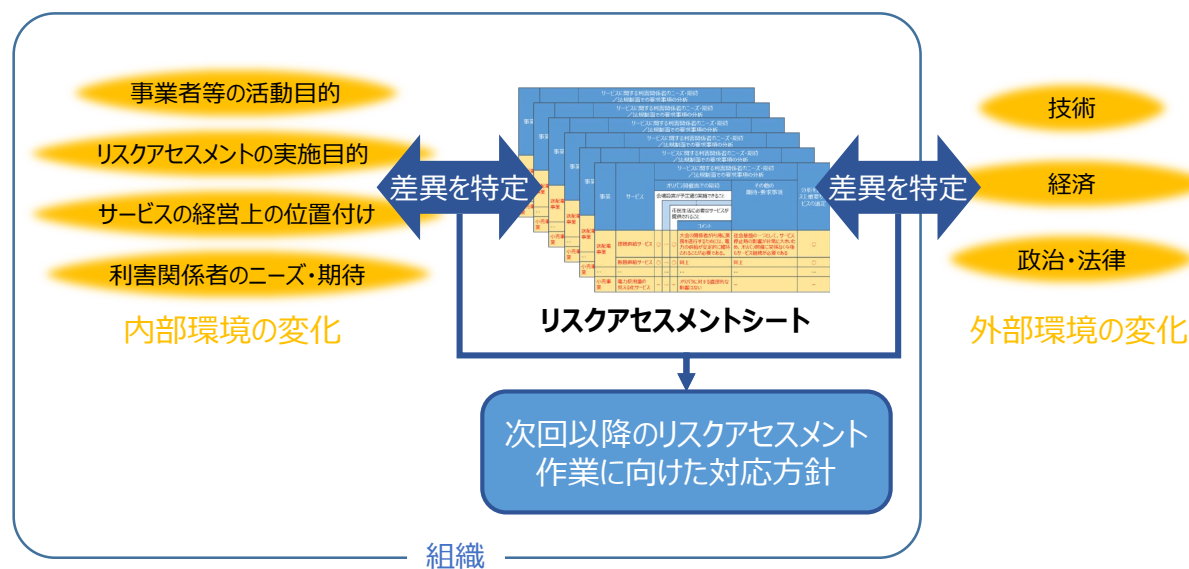
リスクアセスメントの継続的な見直し 1/2



リスク管理

リスクアセスメントの結果として認識された状態は、経時的に変化すると予想されます。リスクアセスメントを変更又は無効なものとするおそれのある状況及びその他の要因を特定し、リスクの変動に適切に対処するためには、「リスクアセスメント結果を継続的にモニタリング※1し、必要に応じて適宜にリスクアセスメント結果の見直しを実施する」など、リスクを適切に管理し、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要です。

※1 リスクアセスメントの結果として認識された状態との差異を特定するために、状態を継続的に点検し、監督し、要点を押さえて観察し、又は決定する取組



作業ステップ

モニタリング実施計画の策定

モニタリングの実施

モニタリング結果の反映方針の策定

本資料の説明範囲

関連資料

- ガイドライン本編 [32ページ]
8. リスクアセスメントの継続的な見直し

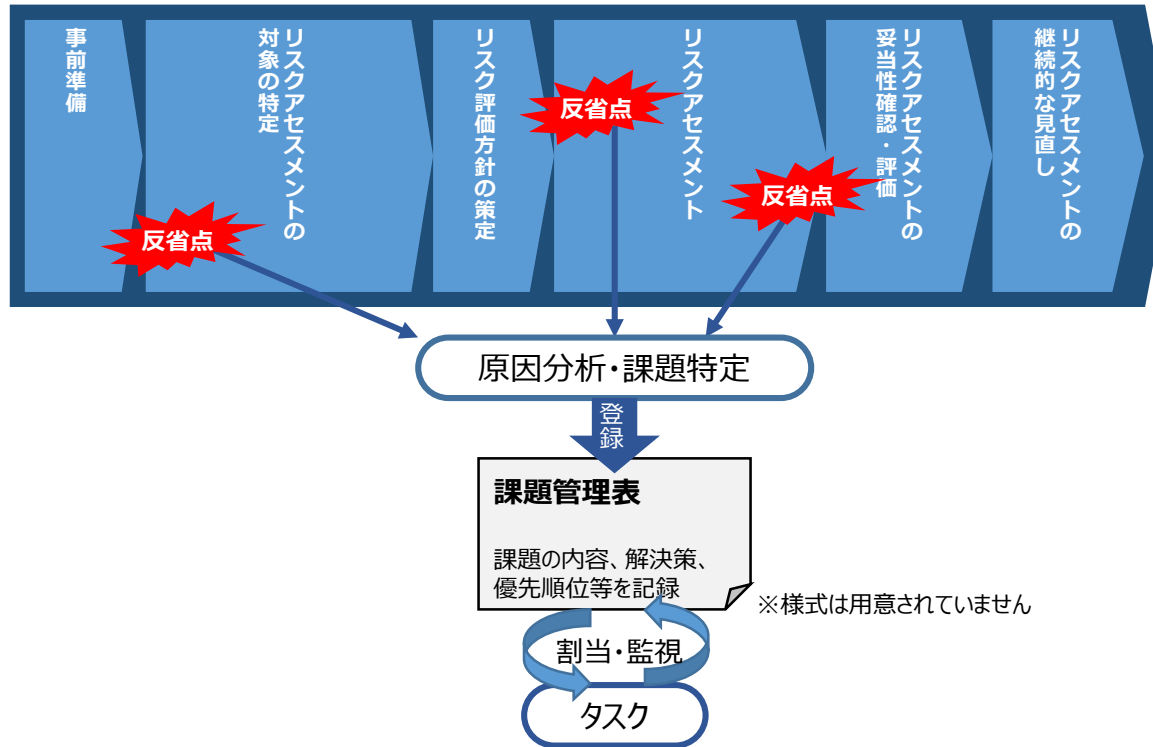
リスクアセスメントの継続的な見直し 2/2



課題管理

リスクアセスメントの見直しを継続的に実施していくためには、リスクアセスメント作業や妥当性確認により明らかとなった体制面や実行面での課題等を踏まえて、これを改善する取組を見直しに係るプロセスに組み入れることが重要です。

リスクアセスメントのプロセス



作業ステップ

課題の特定

課題の共有及び合意

課題の割当て（タスク化）

課題のフォローアップ

本資料の説明範囲

関連資料

- ガイドライン本編 [33ページ]
8. リスクアセスメントの継続的な見直し

帰納的なアプローチと演繹的なアプローチ

リスクの洗い出しには、リスク源を想定し、そのリスク源から派生する様々な事象及び事象の結果を明らかにする「帰納的なアプローチ」と、結果を想定し、その結果に至る様々な事象及びリスク源を明らかにする「演繹的なアプローチ」があります。ガイドラインでは演繹的なアプローチを基本とし、帰納的なアプローチを組み合わせることにより、効率的な作業ができるよう配慮しています。

	帰納的なアプローチ	演繹的なアプローチ
概要	リスク源を想定し、そのリスク源から派生する様々な事象及び事象の結果がどうなるかを明らかにする手法 (イメージ) $X \times Y \rightarrow ?$	事象の結果を想定し、その結果に至る様々な事象及びリスク源を明らかにする手法 (イメージ) $Z \leftarrow ? \times ?$
主な手法	イベントツリー分析	フォールトツリー分析
メリット	個別のシナリオ分析に優れており、各シナリオに応じた対処事項についての有効な知見を得ることができる	事象の結果に関するシナリオを演繹的に分析することにより、網羅的に全容を知ることができる
デメリット	リスク源を網羅することが難しい	提供するサービスや業務の構成が複雑な場合、分析結果の組合せが爆発的に増加し、作業負荷が多くなる
イメージ	<p>The diagram illustrates the inductive approach using an event tree. It starts from a single point on the left (Risk Source) and branches out into multiple paths (Intermediate Events) as they move towards the right (Event Results). A yellow cone highlights the expanding range of possibilities. Two red dashed circles at the start indicate specific initial conditions. A red note states: 「※経験に基づかないシナリオが見落とされがち」 (※ Scenarios not based on experience are often overlooked). The stages are labeled: リスク源 (Risk Source), 結果を生じる事象 (Intermediate Events), and 事象の結果 (Event Results).</p>	<p>The diagram illustrates the deductive approach using a fault tree. It starts from a single point on the right (Event Results) and branches out into multiple paths (Intermediate Events) as they move towards the left (Risk Sources). A yellow cone highlights the expanding range of possibilities. The stages are labeled: リスク源 (Risk Source), 結果を生じる事象 (Intermediate Events), and 事象の結果 (Event Results).</p>

リスク対応の選択肢

リスク対応では、対象とするリスクに対して、どのような対応を、いつまでに行うかを明確にします。対応の方法には、大きく分けて「リスクの低減」「リスクの回避」「リスクの移転」「リスクの保有」の4つがあります。

対応方法	概要	分類
< 1 > 低減（最適化）	リスクに対して適切な管理策を適用する。	リスク・コントロール
①リスク源の除去	リスクの起こりやすさ及び結果に与える影響の源を除去する。	
②影響度の低減	事業者等への影響度を低減させる。	
③起こりやすさの低減	発生頻度や起こりやすさを下げる。	
< 2 > 回避	リスクを生じさせる活動を開始又は継続しないことを決定することにより、リスクを回避する。	リスク・ファイナンス
< 3 > 移転（共有）	一つ以上の他者とリスクの全部又は一部を共有する。（契約によるリスクの分散及び保険加入等による金銭面でのリスク対策を含む。）	
< 4 > 保有（受容）	情報に基づく意思決定により、リスクを保有（受容）する。	

（注）ISO 31000:2009において、リスクの低減には、「ある機会を追求するために、リスクを取る、又は増加させる」という概念も含まれていますが、本ガイドラインでは、目的に対する負の影響をリスクと捉える考え方に基づくため、表中には記載していません。

(付録) 様式記載要領

Step1: リスクアセスメントの実施目的の確認

1. 作業の目的	平時又は大規模国際イベント等に向けた「リスクアセスメントの実施目的」を定め、それを踏まえた自組織の活動目標を設定し、自組織のリスク評価の目的を確認します。		
2. 使用する様式	様式1	3. 想定する主な作業部門	経営企画部門、サービス管理部門 など

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) リスクアセスメントの実施目的	平時又は大規模国際イベント等に向けた「リスクアセスメントの実施目的」を設定します。	■ 自組織の活動目標を踏まえた上で、リスクアセスメントの実施目的を設定します。
(2) 自組織の活動目標	「リスクアセスメントの実施目的」を踏まえて、自組織の活動目標を設定します。	■ 「リスクアセスメントの実施目的」を踏まえ、重要サービスの継続性を確保するために自組織が目指す事業活動（サービスの提供）の目標を設定します。 ■ 活動目標を明らかにし、部門・関係者間でこれを共有することにより、各部門・関係者が事業活動に対して有する価値観を、これから実施するリスクアセスメントの実施目的・方針に関する組織の価値観に合致させる（＝ベクトルを合わせ、利害の対立を極小化する）ことを目指します。

Step2：重要サービスの選定（1/3）

1. 作業の目的	事業者が扱うサービスについて、利害関係者からの期待、その他の期待・要求事項、経営面からの位置づけを分析し、当該事業者にとって重要な（リスクアセスメントを実施し、必要なリスク対応を講じることを検討すべき）サービスを特定します。		
2. 使用する様式	様式2	3. 想定する主な作業部門	経営企画部門、サービス管理部門 など

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	<ul style="list-style-type: none"> ■ 事業部制を採用している事業者においては事業部単位で分類するなど、後続の作業（事業に紐づくサービスを、業務、経営資源、リスクに段階的に分解していく作業を行います。）を実施するに際して、作業の分担や管理を行いやすい区切り方を事業者の状況に応じて設定します。
(2) サービス	サービスを記載します。	<ul style="list-style-type: none"> ■ 事業者のサービスの管理台帳等を参考にして、事業者が扱うサービスを洗い出します。後続の作業を踏まえ、必要以上に細分化してしまわないように留意します。※

※ Step1で設定した「重要サービスの継続性を確保するために自組織が目指す事業活動（サービスの提供）の目標」に照らして、事業単位で関連がないものについては、サービスを洗い出さなくても構いません。

Step2 : 重要サービスの選定 (2/3)

4. 項目	5. 項目の概要	6. 記載方法
(3) サービスに関する利害関係者のニーズ・期待／法規制面での要求事項の分析	サービスが、利害関係者からどのように期待されているのか、また法令や契約等によりどのような要求（又は制約）があるのかを記載します。 なお、特にサービスに関する利害関係者の期待については、「リスクアセスメントの実施目的」のいずれに関連するかを紐付けた上、その詳細を記載します。	<ul style="list-style-type: none"> ■ 「サービスに関する利害関係者の期待」については、Step1で設定したリスクアセスメントの実施目的に照らして、各サービス及び当該サービスの供給を受けて提供されているサービスが利害関係者に対し、どのように必要とされているのか（期待されているのか）を整理して記載します。なお、大規模国際イベント等開催時は平常どおりでないことを想定し、大規模国際イベント等開催に伴う海外からの旅行者増加などの社会情勢や経営環境の変化についての把握に努め、その変化に基づく期待や要求事項を整理することが重要です。 ■ 「その他の期待・要求事項」については、サービスが、リスクアセスメントの実施目的以外に利害関係者にとってどのように必要とされているのか（期待されているのか）、また法令・各種基準（事業者が遵守している業界団体による安全基準ガイドライン等を含みます。）やSLA等の契約上の要求事項等を洗い出します。特に法律上の要求事項などは、リスク対応や事業継続計画に関する意思決定において最も重要になるポイントの一つであることから、経営者がしっかりと把握できるように整理しておく必要があります。また、本項目では、社会的責任（CSR）の観点や経営上の位置づけ（事業収益に占める当該サービスの比重が高く、当該サービスの阻害が事業全体に影響を及ぼすケースなども想定）についても考慮します。
(4) 製品・サービスの経営面での位置づけ	サービス毎に経営指標となる値を記載し、経営面での位置づけを把握します。	<ul style="list-style-type: none"> ■ 業績面（売上高、ROI）や戦略面（市場成長性、相対的シェア）を必要に応じて、サービス毎に記載します。これらの値からサービスが経営上どのような位置づけであるかを把握し、重要サービス選定の参考とします。

Step2 : 重要サービスの選定 (3/3)

4. 項目	5. 項目の概要	6. 記載方法
(5) 分析を踏まえた重要サービスの選定 (重要サービスの決定)	サービスについて、経営上の位置づけ、利害関係者のニーズ、法的制約等の観点を踏まえ、事業者にとって重要な（リスクアセスメントを実施し、必要なリスク対応やBCPの構築を講じることを検討すべき）サービスを決定します。	<ul style="list-style-type: none">■ これまで整理してきた利害関係者の期待等を踏まえ、事業者にとって重要な（リスクアセスメントの対象とすべき）サービスを選定します。上記(3)「サービスに関する利害関係者のニーズ・期待／法規制面での要求事項の分析」において、自組織の活動目標と関連する期待事項を記載しているサービスについては、その影響の大きさを勘案し、重要サービスとして選定し、Step3以後の分析を行うことが望ましいです。■ なお、重要であるか否かは、利害関係者のニーズ・期待といった定性的な要素を事業者がどう評価するかにも依存することになります。このため、事業者にとっての重要であるかの判定基準を予め定めておくことが望ましいといえますが、これまで同様の分析を行ったことがなく、重要であるかの判定基準を事前に定めることが難しい事業者においては、事前に基準を定めずに、上記(3)までの作業を終えた上で、関係者間で協議（ブレンストーミング）等を行い評価するというやり方でも差し支えありません。

Step3 : 重要サービスの影響分析

1. 作業の目的	事業者が扱うサービスの最低許容される範囲・水準を明らかにした上、その提供が完全に停止した場合の影響及び時間経過に伴う影響度合いを評価し、サービスの最大許容停止時間（MTPD, Maximum Tolerable Period of Disruption）を推定します。		
2. 使用する様式	様式3	3. 想定する主な作業部門	経営企画部門、サービス管理部門 など

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	■ 前Stepの「重要サービス」として選定されたサービスについて、前Stepの「事業」を転記します。
(2) サービス	サービスを記載します。	■ 前Stepの「重要サービス」として選定されたサービスについて、前Stepの「重要サービス」を転記します。
(3) 利害関係者のニーズ・期待／法規制面での要求事項等を満たすために最低限許容されるサービスの範囲・水準	利害関係者のニーズ・期待／法規制面での要求事項等を満たすために最低限許容されるサービスの範囲・水準を記載します。	■ 前Step(3)において洗い出された「サービスに関する利害関係者の期待」及び「その他の期待・要求事項」について、その期待・要求を満たすために「契約責任、法令遵守」及び「社会的責任（CSR）」ごとに必要な（最低限許容される）サービスの範囲・水準を記載します。
(4) サービスが完全停止した場合の影響	サービスが完全停止した場合に生じる事態及び時間経過に伴う影響度合いを記載します。	■ サービスの提供が完全停止した場合、直接の取引先だけでなくエンドユーザー等も視野に入れ、どういった事態が想定されるのかを明らかにした上、その事態が時間の経過に伴ってどの程度の悪影響を及ぼしていくかを想定します。実際にサービスの提供が停止した経験がある場合には、直近の環境変化等を考慮しつつ、その経験に基づいて想定を記載することが可能ですが、停止実績がない場合には、関連部門の担当者を集めて、日次、週次又は月次といった定例の業務を想定したワークスルーを実施し、実務において影響が生じると思われる業務手順を特定するなどにより、その影響が及ぶ範囲を推測します。
(5) サービスの提供に係る最大許容停止時間(MTPD)	サービスの提供に係る最大許容停止時間及びその設定の根拠を記載します。	■ (4)で評価したサービスが完全に停止した場合の影響を踏まえ、当該サービスの最大許容停止時間を推定します。最大許容停止時間の決定に際しては、考慮した観点及び根拠を明記し、妥当性の検証や今後の見直しのために残しておくことが重要です。

Step4：重要サービスを支える業務の特定及び当該業務の影響分析（1/2）

1. 作業の目的	重要サービス（リスクアセスメントの対象とすべきサービス）の提供のために必要な業務を洗い出し、当該業務について最低限許容される水準（操業率、稼働率等）を明らかにした上、当該業務が停止した場合の影響及び停止に係る最大許容時間を推定します。		
2. 使用する様式	様式4	3. 想定する主な作業部門	サービス管理部門、業務管理部門 など

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	■ 前Stepの「事業」を転記します。
(2) 重要サービス	重要サービスを記載します。	■ 前Stepで決定した重要サービスを記載します。
(3) 重要サービスの提供に必要な業務	重要サービスの提供のために必要な業務を記載します。	■ 前Stepで決定した重要サービスについて、事業者がこれを提供するために必要となる業務を洗い出します。直接的に顧客との接点のある業務に限らず、サービスに係る開発・製造からアフターサービス等までの一連の業務やサービス提供に欠かせない品質管理等の間接業務についても、事業者が当該サービスを提供するために必要な業務については全て洗い出します。
(4) 重要サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）	重要サービスを提供するために必要な業務について、当該重要サービスの提供のために必要な最低限の業務水準を記載します。	■ 利害関係者のニーズ・期待や法規制面での要求事項に適うように重要サービスの提供を継続するためには、一定の業務水準が維持される必要があります。本項目では、最低限維持されるべき業務水準を明らかにすることを目的として、最低限維持すべき業務の状態（可能であれば操業率、稼働率、品質基準等の目安）を明らかにし、その根拠を記載します。
(5) 業務が完全停止した場合の影響	重要サービスの提供のために必要な業務が完全停止した場合に生じる事態及び時間経過に伴う影響度合いを記載します。	■ 重要サービスの提供のために必要な業務が完全停止した場合、重要サービスの提供に関し、どういった事態が想定されるのかを明らかにした上、その事態が時間の経過に伴ってどの程度の悪影響を及ぼしていくかを想定します。

Step4：重要サービスを支える業務の特定及び当該業務の影響分析（2/2）

4. 項目	5. 項目の概要	6. 記載方法
(6) 業務に係る最大許容停止時間 (MTPD)	業務に係る最大許容停止時間及びその設定の根拠を記載します。	■ 上記(5)で評価した業務が完全に停止した場合の影響を踏まえ、当該業務の最大許容停止時間を推定します。最大許容停止時間の決定に際しては、考慮した観点及び根拠を明記し、妥当性の検証や今後の見直しのために残しておくことが重要です。

Step5 : 業務を支える経営資源の特定

1. 作業の目的	事業者が扱う重要なサービスに必要な業務について、最低限満たすべき業務水準を維持するために必要な経営資源及びその経営資源が満たすべき要件・必要な数量について明らかにします。		
2. 使用する様式	様式5	3. 想定する主な作業部門	サービスを担当する事業部門など

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	■ 前Stepの「事業」を転記します。
(2) 重要サービス	重要サービスを記載します。	■ 前Stepの「重要サービス」を転記します。
(3) 重要サービスの提供に必要な業務	重要サービスの提供に必要な業務を記載します。	■ 前Stepの「重要サービスの提供に必要な業務」を転記します。
(4) 前提とする業務水準（許容できる最低稼働率等）	経営資源の要件等を記載する上での前提となる業務水準を記載します。	■ 前Stepの「重要サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）」を転記します。
(5) 業務を支える経営資源の要件・必要数量	各業務を求められる水準で遂行するために必要な経営資源について記載します。	<ul style="list-style-type: none"> ■ 当該業務を上記(4)で規定した水準で遂行する際に必要な経営資源について考えます。経営資源について、数量等の要件がある場合には合わせて記載します。 ■ 作業を行う前に着目する観点を整理しておくことで考慮漏れを軽減できます。主な観点として、人、情報・データ、建物・作業環境・関連ユーティリティ、設備・機器・消耗品、情報通信技術（ICT）システム・制御システム、交通機関・ライフライン（例：電気・水道・ガス）、資金等が挙げられます。 ■ なお、経営資源には自社資産として位置づけられるものと、委託契約等により外部から供給されるものに分けて記載しておくこと、Step6においてリスクを特定しやすくなります。

Step6 : リスクアセスメント (リスク源) (1/3)

1. 作業の目的	事業影響度分析により決定した重要サービスの提供に必要な業務に係る経営資源（IT障害に関するリスクを対象にするため、情報通信システムやデータ等の情報資産に限定します。）を整理した上、当該業務の継続を目的とした場合の当該経営資源に係るリスクを特定、分析及び評価を行います。		
2. 使用する様式	様式6	3. 想定する主な作業部門	システム部門

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	■ 前Stepの「事業」を転記します。
(2) 重要サービス	重要サービスを記載します。	■ 前Stepの「重要サービス」を転記します。
(3) 重要サービスの提供に必要な業務	重要サービスの提供に必要な業務を記載します。	■ 前Stepの「重要サービスの提供に必要な業務」を転記します。
(4) リスクの特定 ① 経営資源	重要サービスの提供に必要な業務に係る経営資源のうち、情報通信システムやデータ等の情報資産を洗い出して記載します。	■ 本リスクアセスメントでは、IT障害に係るリスクを対象とするため、事業影響度分析により洗い出した重要サービスの提供に必要な業務に係る経営資源のうち、情報通信システムやデータ等の情報資産を抽出して記載します。
② 業務の阻害につながる事象の結果	重要サービスの提供に必要な業務の阻害につながる事象の結果を記載します。	<ul style="list-style-type: none"> ■ 本リスクアセスメントでは、重要サービスの提供に必要な業務を継続すること（期待に合う業務運営を行うこと）を事業者の目的とし、当該目的に対する不確かさの影響（負の影響）をリスクと捉えます。 ■ 本項目では、業務の阻害につながる事象の結果を記載します。なお、情報セキュリティの三要件である機密性(Confidentiality)、完全性(Integrity)及び可用性(Availability)の観点で踏まえて整理します。 (例) 経営資源 : 顧客データベース 事象の結果 : 顧客データベースの改ざん（完全性の欠如）
③ 結果を生じうる事象	上記②の結果を生じうる事象を記載します。	<ul style="list-style-type: none"> ■ 上記②の結果を生じうる事象を洗い出します。 (例) 事象 : 内部犯行による情報の不正持出

Step6 : リスクアセスメント (リスク源) (2/3)

4. 項目	5. 項目の概要	6. 記載方法
④ リスク源	上記③の事象を生じさせるリスク源を記載します。	<ul style="list-style-type: none"> ■ 上記③の事象を生じさせる要素をリスク源として洗い出します。リスク源は、それ自体又は他との組合せによって、リスクを生じさせる力を本来潜在的に持っている要素をいい、必ずしも有形に限らず、無形（規定、慣習、職場の雰囲気等）の要素を含みます。 (例) リスク源 : ①顧客データベースにアクセス可能な端末でUSBメモリの使用が可能である。 ②業務の社会的重要性を理解していない派遣社員が顧客データベースにアクセス可能なIDを使用している。
(5) リスクの分析 ①事象の結果の影響度合い	前記(4)②の事象の結果が重要サービスの提供に必要な業務に与える影響の度合いを記載します。	<ul style="list-style-type: none"> ■ 「事象の結果の影響」については、前記(4)②で特定された事象の結果が生じた場合において、重要サービスの提供に必要な業務に与える影響を記載します。 ■ 「対策前」については、上記影響に対して何らかの対策を講じている場合に、その対策を講じる前の影響の度合いの評価を記載します。「現在講じている対策」については、影響度合いを低減、回避又は移転するために講じている対策を記載します。「対策後」については、上記対策を講じた後の影響の度合いの評価を記載します。※ ■ 影響の度合いについては、影響の範囲・程度、予想復旧時間、対応に要するコスト等を総合的に勘案して決定します。リスクマップに基づくリスク評価を行う場合には、例えばP.9のような評価基準を設定し、これに基づき評価するなどのやり方があります。
②事象の発生頻度	前記(4)③の事象の発生頻度を記載します。	<ul style="list-style-type: none"> ■ 前記(4)③で特定された事象について、予想される発生頻度を評価します。 ■ 「対策前」については、事象の発生頻度を低減するための何らかの対策を講じている場合に、その対策を講じる前の発生頻度の評価を記載します。「現在講じている対策」については、発生頻度を低減するために講じている対策を記載します。「対策後」については、上記対策を講じた後の発生頻度の評価を記載します。※ ■ 発生頻度について、例えばP.9のような評価基準を設定し、これに基づき評価するなどのやり方があります。

※「対策前」と「対策後」を分けて分析しておく、「評価の過程を説明できる」及び「対策の陳腐化に気付くことができる」といったメリットがあります。

Step6 : リスクアセスメント (リスク源) (3/3)

4. 項目	5. 項目の概要	6. 記載方法
③残留リスク値	事象の結果の影響度合い及び事象の発生頻度を斟酌したリスク源ごとの残留リスクの評価値を記載します。	<ul style="list-style-type: none"> ■ 上記①及び②で評価した「事象の結果の影響度合い」及び「事象の発生頻度」の対策後の評価値を踏まえ、リスク源ごとの残留リスクの評価値を決定します。「事象の結果の影響度合い」及び「事象の発生頻度」のそれぞれの評価値を掛け合わせて算定した値をリスク値とするなどのやり方が一般的です。
(6) リスクの評価 ①リスク基準	リスク対応の実施対象を選定するための基準となるリスク値の閾値を記載します。	<ul style="list-style-type: none"> ■ 上記③で求めた「残留リスク値」に基づきリスク対応の実施対象を選定するための基準値（閾値）を決定します。 ■ 一般的に、リスクの受容基準としてのリスク基準については、組織のリスク選好等を踏まえて決定されるべきであるため、組織がこれを定めるための意思決定を行うことが難しい場合がありますが、この手順では「リスク対応を優先して実施する対象を選別するための基準」と捉えます。 ■ リスクマップに基づくリスク評価を行う場合には、例えばP.9のような基準を定めるやり方があります。
②リスク評価	リスク対応の対象とするリスクを選定します。	<ul style="list-style-type: none"> ■ 残留リスク及びリスク基準に基づき、リスク対応の対象とするリスクを選定します。
③リスクオーナーの選任	リスクオーナーとして選任された部門・部署を記載します。	<ul style="list-style-type: none"> ■ リスク対応の対象として抽出されたリスクに対し、リスクオーナー（そのリスクの対処に関する責任を負担する部署・部門又は役職員）を定めます。 ■ リスク対応の実施対象として抽出されたリスクについては、経営層による全社的な意思決定の対象として取り扱われます。このため、リスク分析の結果、特に大きなリスクとして認識されたリスクについては、部門や部署を越えて、担当役員がリスクオーナーとして管理することも考えられます。

Step6 : リスクアセスメント (リスクシナリオ) (1/4)

1. 作業の目的	事業影響度分析により決定した重要サービスの提供に必要な業務に係る経営資源（IT障害に関するリスクを対象にするため、情報通信システムやデータ等の情報資産に限定します。）を整理した上、当該業務の継続を目的とした場合の当該経営資源に係るリスクを特定、分析及び評価を行います。		
2. 使用する様式	様式6	3. 想定する主な作業部門	システム部門

以下、様式に沿って説明します。

4. 項目	5. 項目の概要	6. 記載方法
(1) 事業	サービスを所管する事業を記載します。	<ul style="list-style-type: none"> ■ 前Stepの「事業」を転記します。 ■ 「該当モデルケース」には、別紙 1「事業・重要サービス・経営資源（情報資産）の例」（事業分野毎）に該当する「事業」がある場合、その項目を転記します。
(2) 重要サービス	重要サービスを記載します。	<ul style="list-style-type: none"> ■ 前Stepの「重要サービス」を転記します。 ■ 「該当モデルケース」には、別紙 1「事業・重要サービス・経営資源（情報資産）の例」（事業分野毎）に該当する「重要サービス」がある場合、その項目を転記します。
(3) 重要サービスの提供に必要な業務	重要サービスの提供に必要な業務を記載します。	<ul style="list-style-type: none"> ■ 前Stepの「重要サービスの提供に必要な業務」を転記します。
(4) リスクの特定 ① 経営資源	重要サービスの提供に必要な業務に係る経営資源のうち、情報通信システムやデータ等の情報資産を洗い出して記載します。	<ul style="list-style-type: none"> ■ 本リスクアセスメントでは、IT障害に係るリスクを対象とするため、事業影響度分析により洗い出した重要サービスの提供に必要な業務に係る経営資源のうち、情報通信システムやデータ等の情報資産を抽出して記載します。 ■ 「該当モデルケース」には、別紙 1「事業・重要サービス・経営資源（情報資産）の例」（事業分野毎）に該当する経営資源（情報資産）がある場合、その項目を転記します。

Step6 : リスクアセスメント (リスクシナリオ) (2/4)

4. 項目	5. 項目の概要	6. 記載方法
② 業務の阻害につながる事象の結果	重要サービスの提供に必要な業務の阻害につながる事象の結果を記載します。	<ul style="list-style-type: none"> ■ 本リスクアセスメントでは、重要サービスの提供に必要な業務を継続すること（期待に適う業務運営を行うこと）を事業者の目的とし、当該目的に対する不確かさの影響（負の影響）をリスクと捉えます。 ■ 本項目では、業務の阻害につながる事象の結果を記載します。なお、情報セキュリティの三要件である機密性(Confidentiality)、完全性(Integrity)及び可用性(Availability)の観点を踏まえて整理します。 (例) 経営資源 : 顧客データベース 事象の結果 : 顧客データベースの改ざん（完全性の欠如） ■ 特定した「情報セキュリティ3要素」を入力します。
③ 結果を生じうる事象	上記②の結果を生じうる事象を記載します。	<ul style="list-style-type: none"> ■ 上記②の結果を生じうる事象を洗い出します。 (例) 事象 : 内部犯行による情報の不正持出 ■ 「要因」には、別紙4「業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスクシナリオの例」を参考に事象が生じる要因を入力します。
④ リスクシナリオ	上記③の事象が顕在化するリスクシナリオを記載します。	<ul style="list-style-type: none"> ■ 上記③の事象が顕在化するリスクシナリオを策定します。経営資源（情報資産）に対して、システムや運用等の不備からどのような脅威をもたらし、その結果、どのような業務の阻害につながるかを検討します。この際、過去のインシデントの事例を参考にすることも有効です。 ■ リスクシナリオの策定に当たっては、上記③の事象を生じさせるまでの一連のステップを、各事業者等の環境に応じて書き出します。リスクの顕在化が故意による場合、行為者が、どのような経営資源（情報システム及び/又は制御システム、データ）に対して、どのような手法で何を実施するかを時系列のステップとして整理します。リスクの顕在化が故意ではないものによる場合、どのような経営資源（情報システム及び/又は制御システム、データ）に対して、何に起因して何が起こるかを時系列のステップとして整理します。 ■ リスクシナリオの策定例として、別紙4が参考になります。

Step6 : リスクアセスメント (リスクシナリオ) (3/4)

4. 項目	5. 項目の概要	6. 記載方法
(5) リスクの分析 ① 事象の結果の影響度合い	前記(4)②の事象の結果が重要サービスの提供に必要な業務に与える影響の度合いを記載します。	<ul style="list-style-type: none"> ■ 「対策前」については、上記影響に対して何らかの対策を講じている場合に、リスクシナリオごとにその対策を講じる前の影響の度合いの評価を記載します。「現在講じている対策」については、リスクシナリオごとに影響度合いを低減、回避又は移転するために講じている対策を記載します。「対策後」については、リスクシナリオごとに上記対策を講じた後の影響の度合いの評価を記載します。※ ■ 影響の度合いについては、影響の範囲・程度、予想復旧時間、対応に要するコスト等を総合的に勘案して決定します。リスクマップに基づくリスク評価を行う場合には、例えばP.9のような評価基準を設定し、これに基づき評価するなどのやり方があります。
② 事象の発生頻度	前記(4)③の事象の発生頻度を記載します。	<ul style="list-style-type: none"> ■ 前記(4)③で特定された事象について、予想される発生頻度を評価します。 ■ 「対策前」については、事象の発生頻度を低減するための何らかの対策を講じている場合に、リスクシナリオごとにその対策を講じる前の発生頻度の評価を記載します。「現在講じている対策」については、ステップごとに発生頻度を低減するために講じている対策を記載します。「対策後」については、リスクシナリオごとに上記対策を講じた後の発生頻度の評価を記載します。※ ■ 発生頻度について、例えばP.9のような評価基準を設定し、これに基づき評価するなどのやり方があります。
③ 残留リスク値	事象の結果の影響度合い及び事象の発生頻度を斟酌したリスク源ごとの残留リスクの評価値を記載します。	<ul style="list-style-type: none"> ■ 上記①及び②で評価した「事象の結果の影響度合い」及び「事象の発生頻度」の対策後の評価値を踏まえ、リスクシナリオごとの残留リスクの評価値を決定します。「事象の結果の影響度合い」及び「事象の発生頻度」のそれぞれの評価値を掛け合わせて算定した値をリスク値とするなどのやり方が一般的です。

※「対策前」と「対策後」を分けて分析しておく、「評価の過程を説明できる」及び「対策の陳腐化に気付くことができる」といったメリットがあります。

Step6 : リスクアセスメント (リスクシナリオ) (4/4)

4. 項目	5. 項目の概要	6. 記載方法
(6) リスクの評価 ①リスク基準	リスク対応の実施対象を選定するための基準となるリスク値の閾値を記載します。	<ul style="list-style-type: none">■ 上記③で求めた「残留リスク値」に基づきリスク対応の実施対象を選定するための基準値（閾値）を決定します。■ 一般的に、リスクの受容基準としてのリスク基準については、組織のリスク選好等を踏まえて決定されるべきであるため、組織がこれを定めるための意思決定を行うことが難しい場合がありますが、この手順では「リスク対応を優先して実施する対象を選別するための基準」と捉えます。■ リスクマップに基づくリスク評価を行う場合には、例えばP.9のような基準を定めるやり方があります。
②リスク評価	リスク対応の対象とするリスクを選定します。	<ul style="list-style-type: none">■ 残留リスク及びリスク基準に基づき、リスク対応の対象とするリスクを選定します。
③リスクオーナーの選任	リスクオーナーとして選任された部門・部署を記載します。	<ul style="list-style-type: none">■ リスク対応の対象として抽出されたリスクに対し、リスクオーナー（そのリスクの対処に関する責任を負担する部署・部門又は役職員）を定めます。■ リスク対応の実施対象として抽出されたリスクについては、経営層による全社的な意思決定の対象として取り扱われます。このため、リスク分析の結果、特に大きなリスクとして認識されたリスクについては、部門や部署を越えて、担当役員がリスクオーナーとして管理することも考えられます。