資料３

2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況

資料３－１　2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況

資料３添付資料　2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価資料一式

2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況

◆ 重要インフラ事業者を含む、東京大会の円滑な運営に不可欠なサービスを提供する事業者等を選定。NISCが作成した手順に基づき、東京23区内の事業者等を対象に第1回目のリスク評価を実施。
◆ 来年度以降は、東京圏、地方会場に関連する事業者等に拡大しつつ、2020年までにリスク評価を計６回実施予定。

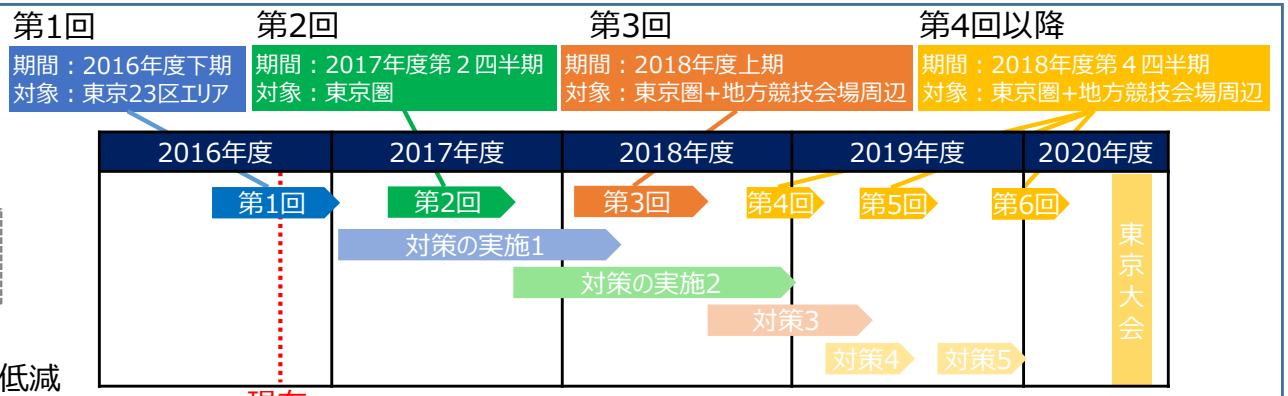
リスク評価の取組概要

○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成（添付資料を参照）

○ 東京大会の開催・運営に影響に与えうる重要サービス分野を、関連する所管省庁と調整の上で選定

通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給　計19分野

○ 東京大会に向けて、継続的に複数回実施することを想定
- 事業者等：PDCAサイクルを繰り返すことで、リスクを継続的に低減
- NISC：対象とする事業者等の拡大、手順の充実化



東京大会に向けたリスク評価の取組スケジュール

2016年度の取組状況

＜これまで（第１回）の取組状況＞

○ 東京23区エリアの事業者等がリスク評価を実施
- これまでに約70組織から実施結果を受領
  このほかの事業者等は、組織の事情に応じた時期に実施を予定
- ９月に説明会を６回に分け開催。所管省庁・事業者等から計215名が参加
- 11月に情報交換会を開催。事業者等の担当者ら51名が参加

＜今後の予定＞

○ リスク評価により明らかになったリスクへの対策実施を依頼

○ 第２回以降の取組に向けて準備と改善を実施
- 第１回で受領したレポートをもとにしたリスク評価の手順の見直し
- リスク評価を実施する事業者等の拡大
  - 対象地域を拡大し、東京23区外の地方競技会場周辺を追加
  - 大会計画の更新をもとに、対象の重要サービス分野を見直し
- 組織委員会等との継続的な意見交換により、大会開催時に要求されるサービス提供レベルを明確化
- 事業者等との情報交換を継続的に実施

第１回目（2016年度）の実施スケジュール


事業者等向けの説明会（9月）の様子


事業者等との情報交換会（11月）の様子

2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの全体像

資料３添付資料

基本的な考え方

全世界からの注目を集める2020年東京オリンピック・パラリンピック競技大会を直接的・間接的に支える重要なサービスを提供する事業者の皆様には、その**サービスを安全かつ継続的に提供**することが期待されます。そのために必要な措置を皆様自身で講じられるようにするためには、リスクを特定・分析・評価することが必要です。

（イメージ）

2020年東京オリンピック・パラリンピック競技大会の成功

成功のためには…

（要件）大会開催に必要なサービスが安全かつ継続的に提供されること
⇒ **大会開催に向けた各関係主体の活動目的**

機能を保証するためには…

活動目的に対する不確実さ（＝リスク）を特定・分析・評価し、必要な対処につなげることが重要

各関係主体が、

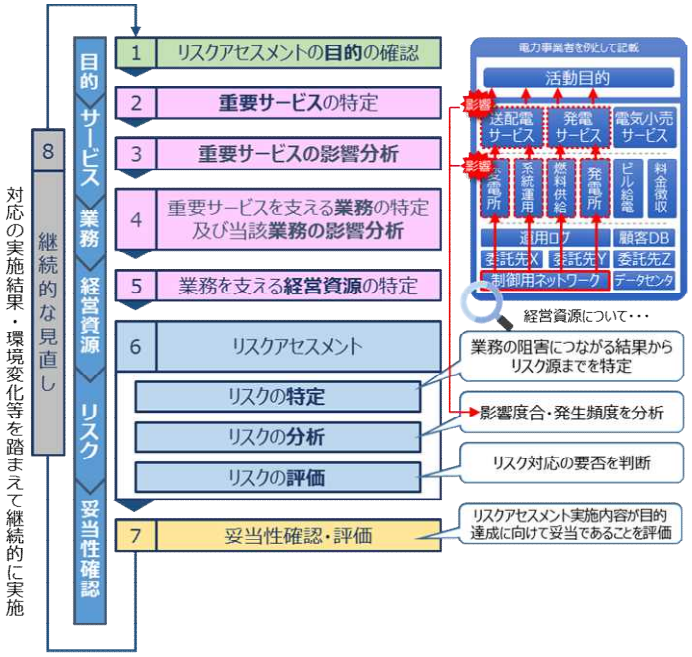
① 大会開催を支える重要なサービス及び必要なサービスレベルを特定し、

② その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

ことが重要です。（機能保証のためのリスクアセスメント）

機能保証のためのリスクアセスメントの枠組み

「機能保証の観点から、事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために**維持・継続することが必要なサービスを特定**」し、その「サービス提供の維持・継続に必要な**業務や経営資源に係る要件を分析・評価**」した上、これらに影響する「**事象の結果からリスク源までを分析**」していきます。



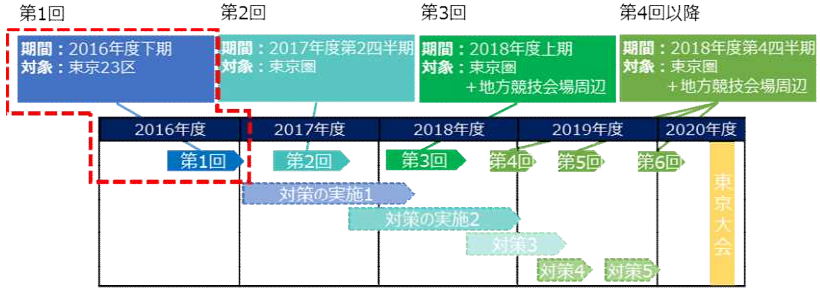
対象とするリスク

情報、情報システム、制御システム等の情報資産に係る事象の結果（自然災害やサイバー攻撃等に起因するＩＴ障害）から認識されるリスクを対象とします。

大会に向けたリスクアセスメントのスケジュール

●2020年まで継続的に複数回の実施を想定
- ➢事業者は、前回からのリスクアセスメントの見直しや、リスク対応の実施状況などを確認
- ➢NISCは、得られた知見を基に、コンテンツの拡充や支援策などを検討

●第1回（2016年度）：
- ➢東京23区エリアの事業者が対象
- ➢品質担保のため、NISCはリスク評価の結果として、事業者からレポートを受領
- ➢NISCは、事業者が自主的にリスク対策の実施を行えるように支援



リスクアセスメントの実施手順（例）

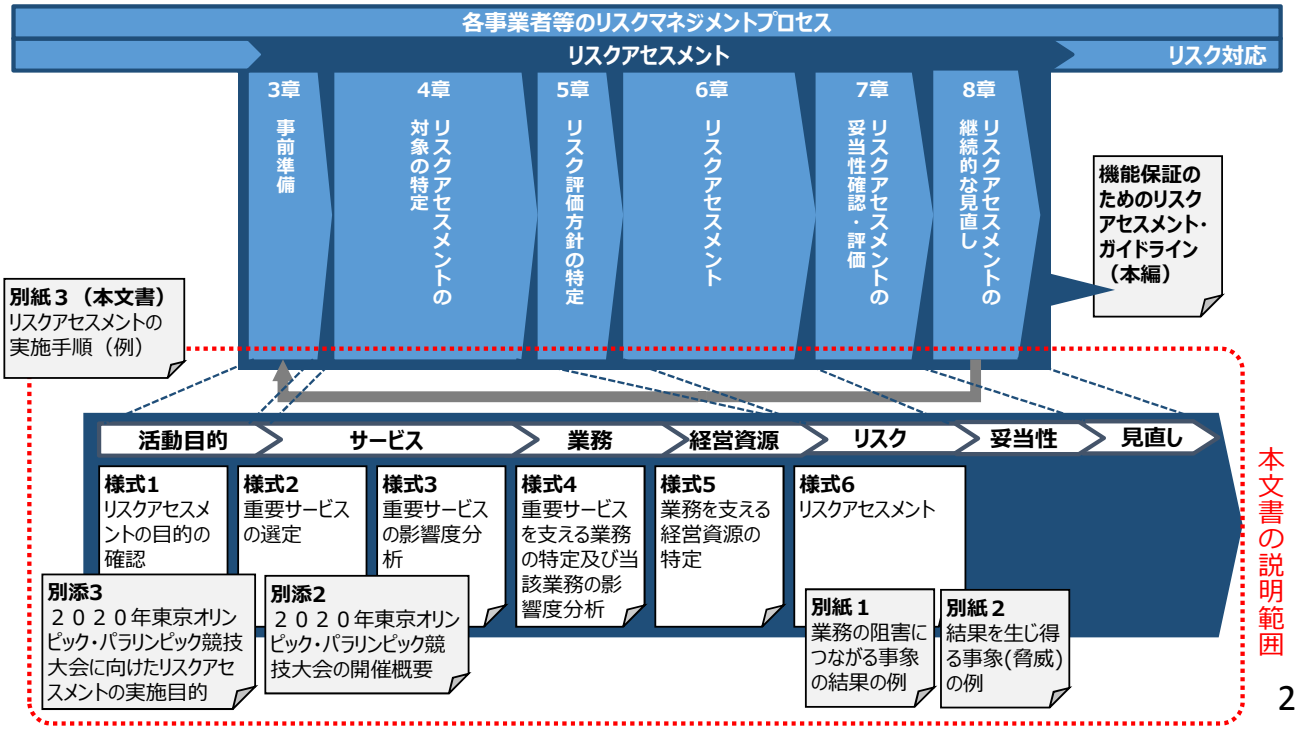
～2020年東京オリンピック・パラリンピック競技大会に向けて～

内閣官房 内閣サイバーセキュリティセンター
重要インフラグループ

2016年９月

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。



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

『2020年東京オリンピック・パラリンピック競技大会に向けた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的を設定します。

別添３
２０２０年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的

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。

2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的	自組織の活動目的
会場設営が予定どおり実施できること	会場設営に必要な通信サービスを十分な品質で提供する。
開閉会式のプログラム、各競技が予定どおり安全に実施できること	開閉会式、各競技に選手、スタッフ、来賓、観客等の関係者が予定どおり参加できるための通信サービスを十分な品質で提供する。
⋮	⋮
会場にいなくても大会を楽しむために必要な環境を提供すること	大会の情報を配信するための通信サービスを十分な品質で提供する。

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。

3 4 5 6 7 8

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**
  ３．事前準備
- **別紙３（様式集）**
  （様式１）リスクアセスメントの目的の確認
- **（付録）様式記載要領**
  Step1: リスクアセスメントの目的の確認
- **別添３ ２０２０年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的**

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、大会開催面での期待やその他の期待・要求事項の観点で分析し、重要サービス※1を特定します。

※1 リスクアセスメントの実施対象とするサービス

別添2
２０２０年東京オリンピック・パラリンピック競技大会の開催概要

自組織の活動目的に照らして、サービスが大会開催に関し、どのように期待されているのかを整理して記載します。

経営上の位置付け、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。

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。

参考 事業	参考 サービス	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					分析を踏まえた重要サービスの選定
		大会開催面での期待				その他の期待・要求事項	
		会場設営が予定どおり実施できること					
		⋮					
		会場にいなくても大会を楽しむために必要な環境を提供すること					
		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	○	…	○	大会の関係者が円滑に大会関連業務を遂行するためには、大会用のインフラサービスが高い品質で維持されることが必要である。	事業経営上、重要なサービスであり、大会開催に直接影響しない部分であっても、サービス継続が必要である。	○
	マスユーザ向けネットワークサービス	－	…	○	海外からの観光客を含め、パソコンやモバイルアプリから大会の情報を取得するために、重要である。	事業経営上、重要なサービスであり、大会開催に直接影響しない部分であっても、サービス継続が必要である。	○
…	…	…	…	…	…	…	…
付帯事業	法人SI	－	…	－	直接的な影響はない	－	－

以降の評価対象

3 4 5 6 7 8

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**
  4．リスクアセスメントの対象の特定
- **別紙３（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
- **別添2 ２０２０年東京オリンピック・パラリンピック競技大会の開催概要**

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。

大会期間中においては、ステークホルダーからの期待・要求が高まる可能性があることについても考慮が必要です。

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	大会開催面での期待、その他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	
		大会開催面	その他	大会開催面	その他	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	開催中、大会の関係者が円滑に大会関連業務を遂行するためには、インフラサービスの品質が片時も損なわれない事が必要である。	－	リアルタイム性を求められるデータ通信（映像や音声など）の遅延や消失により、大会運営へ直接的な影響があることが想定される。	自社のレピュテーションに対して重大なダメージが想定される。	瞬時	

各リスクの影響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**
  4．リスクアセスメントの対象の特定
- **別紙３（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大会運営、大会放送等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**
  4．リスクアセスメントの対象の特定
- **別紙３（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。

本取組においては、情報、情報システム、制御システム等の情報資産を対象とします。

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。

事業	サービス	重要サービスの提供に必要な業務	業務を支える経営資源の要件・必要数量	
			情報、データ	システム
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	サービス用システム
		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
		ポータルサイト系サービス提供	申込情報 工事情報	サービス用システム

3 4 5 6 7 8

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**
  4．リスクアセスメントの対象の特定
- **別紙３（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

3 4 5 6 7 8

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

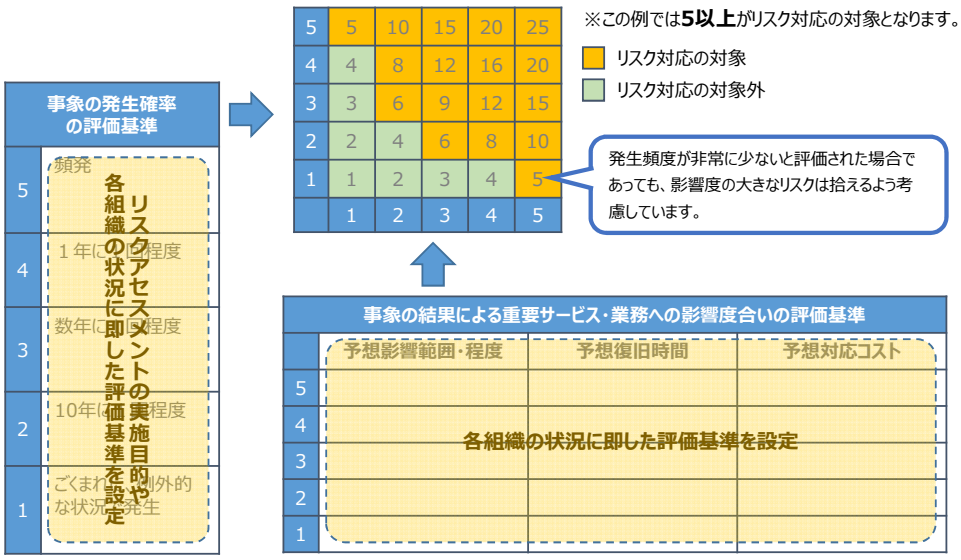
- **ガイドライン本編**
  5．リスク評価方針の特定

リスク評価方針の策定 2/2

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



リスク基準は、リスクアセスメントの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。

3 4 5 6 7 8

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
  5. リスク評価方針の策定

リスクアセスメント 1/3

リスクの特定

使用する様式	様式6	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 P18「帰納的なアプローチと演繹的なアプローチ」を参照

別紙1 業務の阻害につながる事象の結果(例) 参考
別紙2 結果を生じ得る事象(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	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。

3 4 5 6 7 8

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
  6. リスクアセスメントの対象の策定
- 別紙1 業務の阻害につながる結果（例）
- 別紙2 結果を生じる事象（例）
- 別紙3（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 2/3

リスクの分析

使用する様式	様式6	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「残存リスク値」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			残存リスク値
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	9

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）

3 4 5 **6** 7 8

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**
  6．リスクアセスメントの対象の特定
- **別紙３（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 3/3

リスクの評価

使用する様式	様式6	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存リスク値のリスクを抽出します。

② リスク基準未満の残存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	残存リスク値	リスク基準	リスク評価	リスクオーナー
			8	5	●	○○部門
			2	5	－	－
			4	5	●	××部門

リスク基準未満の残存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。

3 4 5 **6** 7 8

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**
  6．リスクアセスメントの対象の特定
- **別紙３（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

（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

使用する様式	様式6	想定する作業部門	システム部門

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 P19「リスク対応の選択肢」を参照

複数選択可能

リスクの特定			リスクの評価	リスク対応の選択肢					
				低減			回避	移転（共有）	保有（受容）
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	リスク評価	リスク源の除去	影響の低減	発生の低減			
			●	●	－	●	－	－	－
			－	－	－	－	－	－	－
			●	－	－	－	●	－	－

<発生頻度及び影響度に応じたリスク対応（例）>

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、『（別添１）実施結果提出様式』により、所管省庁に報告し、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、大会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

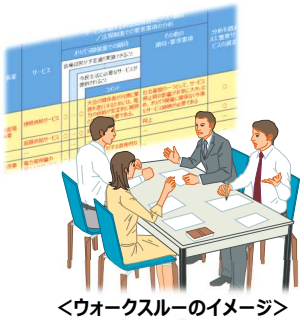
関連資料

- **ガイドライン本編**
  6．リスクアセスメントの対象の特定
- **別紙３（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

ウォークスルー

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。



<ウォークスルーのイメージ>

記録

ウォークスルー記録票

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・ウォークスルーにおける役割、議事内容等を記録

記録

ウォ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

<ウォ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

<ウォ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）
- ウォークスルーの実施
- レビュー対象成果物の修正
- ウォ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

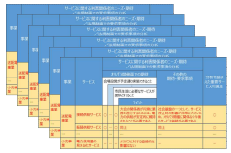
関連資料

- **ガイドライン本編**
  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。



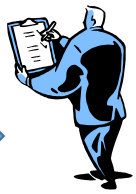
リスクアセスメントシート

ウォークスルー記録票

実施プロセスの証跡

ウォークスルー指摘事項一覧表

実施内容の証跡



評価担当者

<パフォーマンス評価のイメージ>

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。

ウォークスルー記録表

- 全てのリスクアセスメント推進部門がウォ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、有識者がウォ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ウォークスルーに参加し、レビューを実施しているか。

ウォークスルー指摘事項一覧表

- ウォ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観点の例>

3 4 5 6 7 8

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

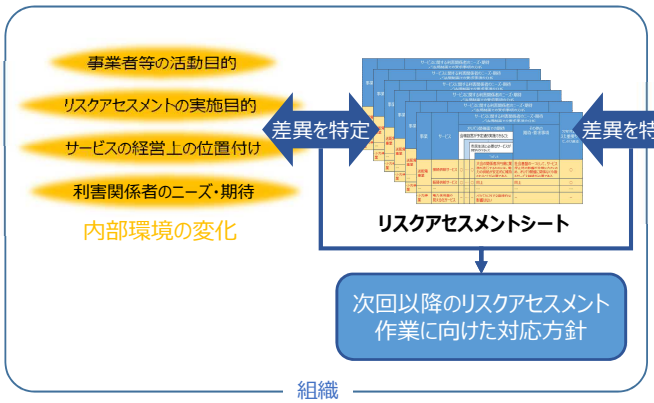
・ガイドライン本編
7. リスクアセスメントの妥当性確認・評価

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



3 4 5 6 7 8

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

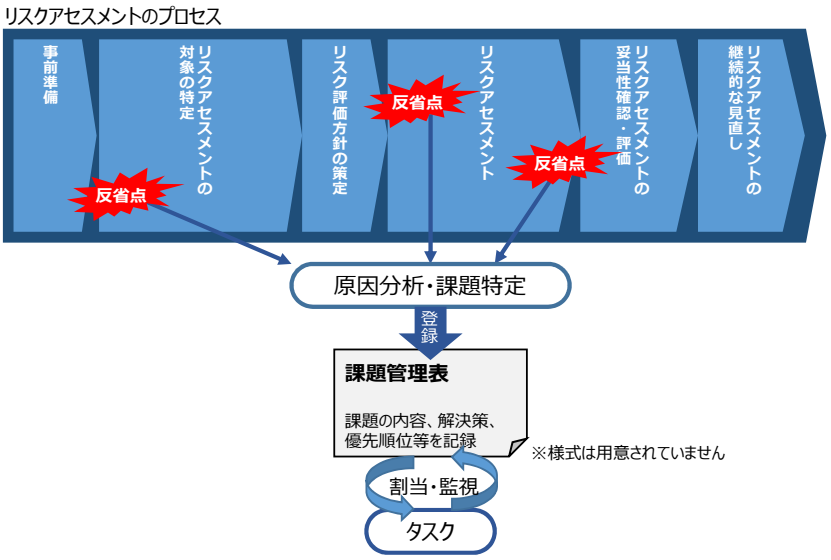
関連資料

・ガイドライン本編
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

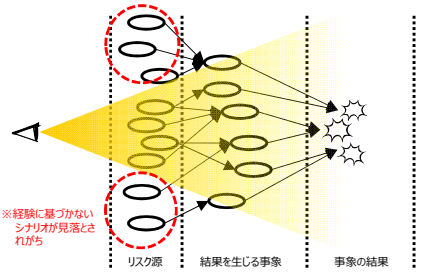
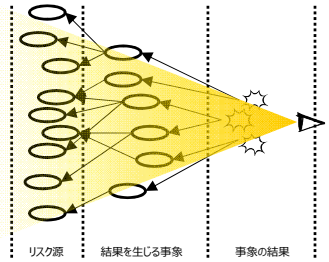
課題管理

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。



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** × **Y** → ？	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** ← ？ × ？
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、作業負荷が多大になる
イメージ		

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、どのような対処を、いつまでに行うかを明確にします。対処の方法には、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。

対処方法		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。	
＜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。）	リスク・ファイナンス
＜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

（付録）様式記載要領

Step1：リスクアセスメントの目的の確認

1. 作業の目的	**『2020年オリンピック・パラリンピック東京大会に向けたリスク評価の実施目的』を踏まえて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) 大会大会に向けた自組織の活動目標	『2020年オリンピック・パラリンピック東京大会に向けたリスク評価の実施目的』を踏まえて、自組織の活動目的を設定します。	■ 政府が設定する『2020年オリンピック・パラリンピック東京大会に向けたリスク評価の実施目的』を踏まえ、大会大会に向けて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。

（付録）様式記載要領

Step2：重要サービスの選定（1/2）

1. 作業の目的	**事業者が扱うサービスについて、大会開催面での期待やその他の期待・要求事項の観点で分析し、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。	■ 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。	■ 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「大会大会に向けて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。

（付録）様式記載要領

Step2：重要サービスの選定（2/2）

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、特に大会開催面での期待事項については、『2020年オリンピック・パラリンピック東京大会に向けたリスク評価の実施目的』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。	■「大会開催面での期待」については、Step1で設定した大会大会期間中の自組織の活動目的に照らして、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大会開催に関し、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、大会開催時は平常どおりでないことを想定し、大会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、大会開催面以外で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ことが必要です。 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) 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。	■ これまで整理してきた大会開催面での期待等を踏まえ、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)「大会開催面での期待」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（ブレーンストーミング）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。

（付録）様式記載要領

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) 大会開催面での期待その他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	大会開催面での期待その他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「大会開催面での期待」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ウォ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。

（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（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。

（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 （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。

（付録）様式記載要領

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。	■ 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と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・作業環境及び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、交通機関・ライフライン（電気・水道・ガス）、資金等が挙げられます。2020年東京オリンピック・パラリンピックに向けてのIT障害に係る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、情報通信システムやデータ等の情報資産に観点を絞ってもよいでしょう。 ■ 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と、Step6においてリスクを特定しやすくなります。

（付録）様式記載要領

Step6：リスクアセスメント（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。 先ず「結果」を想定し、その結果を生じうる「事象」と「リスク源」とを演繹的に洗い出すアプローチにより、リスクの特定を行います。	■ 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）
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。	■ 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

（付録）様式記載要領

Step6：リスクアセスメント（2/3）

4. 項目	5. 項目の概要	6. 記載方法
④ リスク源	上記③の事象を生じさせうるリスク源を記載します。	■ 上記③の事象を生じさせう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。	■「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。	■ 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、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。※ ■ 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こと、「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。

（付録）様式記載要領

Step6：リスクアセスメント（3/3）

4. 項目	5. 項目の概要	6. 記載方法
③残存リスク値	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存リスクの評価値を記載します。	■ 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、リスク源ごとの残存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。	■ 上記③で求めた「残存リスク値」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。	■ 残存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。	■ 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。

STEP1：リスクアセスメントの実施目的の確認

v1.0.0

2020年オリンピック・パラリンピック東京大会に向けた目的	（1）大会に向けた自組織の活動目標 （左記の目的を踏まえて設定）
1. 会場設営が予定どおり実施できること	
2. 開閉会式のプログラム、各競技が予定どおり安全に実施できること	
3. 選手の能力の発揮に必要な環境を提供すること	
4. 来賓・観客の不満なく安全な観戦に必要な環境を提供すること	
5. 会場にいなくても大会を楽しむために必要な環境を提供すること	

情報セキュリティ・リスクに係るリスクアセスメントの実施目的・方針

（リスクアセスメント実施目的）

左記活動目的に対する情報セキュリティ・リスクに対し、適切にリスク対応を行うために、当該リスクを特定、分析及び評価し、並びに残留リスクを可視化することをリスクアセスメントの実施目的とする。

（リスクアセスメント実施方針）

前記実施目的を達成するため、リスクアセスメントの対象とすべきサービス及びこれに必要な業務・経営資源を特定した上、これらの最低限許容される水準及び停止時間を推定し、IT障害に関するリスクを特定、分析及び評価する。

なお、具体的な手順は、次のとおり。

①

活動目的に係るサービスを重要サービス（リスクアセスメントの対象とすべきサービス）として選定する。

②

最低限許容される重要サービスの範囲・水準を明らかにした上、重要サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を推定する。

③

重要サービスの提供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を分析した上、当該業務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、業務の最大許容停止時間を推定する。

④

重要なサービスに必要な業務について、事態発生時に最低限満たすべき業務水準を維持するために必な経営資源を洗い出し、その経営資源が満たすべき要件・必要数量について把握する。

⑤

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、制御システム、データ等の情報資産に限定する。）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、分析及び評価を行う。

STEP1：リスクアセスメントの実施目的の確認

v1.0.0

2020年オリンピック・パラリンピック東京大会に向けた目的	（1）大会に向けた自組織の活動目標 （左記の目的を踏まえて設定）
1. 会場設営が予定どおり実施できること	■オリンピック関連契約の事故受付、事故対応、保険金支払等の保険金サービス業務を円滑に実行する。
2. 開閉会式のプログラム、各競技が予定どおり安全に実施できること	■オリンピック関連契約の事故受付、事故対応、保険金支払等の保険金サービス業務を円滑に実行する。
3. 選手の能力の発揮に必要な環境を提供すること	－
4. 来賓・観客の不満なく安全な観戦に必要な環境を提供すること	－
5. 会場にいなくても大会を楽しむために必要な環境を提供すること	－

情報セキュリティ・リスクに係るリスクアセスメントの実施目的・方針
（リスクアセスメント実施目的） 左記活動目的に対する情報セキュリティ・リスクに対し、適切にリスク対応を行うために、当該リスクを特定、分析及び評価し、並びに残留リスクを可視化することをリスクアセスメントの実施目的とする。 （リスクアセスメント実施方針） 前記実施目的を達成するため、リスクアセスメントの対象とすべきサービス及びこれに必要な業務・経営資源を特定した上、これらの最低限許容される水準及び停止時間を推定し、IT障害に関するリスクを特定、分析及び評価する。 なお、具体的な手順は、次のとおり。 ① 活動目的に係るサービスを重要サービス（リスクアセスメントの対象とすべきサービス）として選定する。 ② 最低限許容される重要サービスの範囲・水準を明らかにした上、重要サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を推定する。 ③ 重要サービスの提供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を分析した上、当該業務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、業務の最大許容停止時間を推定する。 ④ 重要なサービスに必要な業務について、事態発生時に最低限満たすべき業務水準を維持するために必な経営資源を洗い出し、その経営資源が満たすべき要件・必要数量について把握する。 ⑤ 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、制御システム、データ等の情報資産に限定する。）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、分析及び評価を行う。

STEP2：サービスの大会開催面での期待等を分析した上、重要サービスを選定する。

v1.0.0

（1）事業※1	（2）サービス※1	（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 顧客、仕入先、地域社会、経営 大会開催面での期待 1. 会場設営が予定どおり実施できること 2. 開閉会式のプログラム、各競技が予定どおり安全に実施できること 3. 選手の能力の発揮に必要な環境を提供すること 4. 来賓・観客の不満なく安全な観戦に必要な環境を提供すること 5. 会場にいなくても大会を楽しむために必要な環境を提供すること コメント	その他の期待・要求事項	（4）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） 重要	コメント

＜凡例＞
－（非関連）　：サービスに係る活動目的と関連しない

※ Step1で設定した「大会に向けた自組織の活動目的」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。

（1）事業※1	（2）サービス※1	（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 顧客、仕入先、地域社会、経営 大会開催面での期待 1. 会場設営が予定どおり実施できること	2. 開閉会式のプログラム、各競技が予定どおり安全に実施できること	3. 選手の能力の発揮に必要な環境を提供すること	4. 来賓・観客の不満なく安全な観戦に必要な環境を提供すること	5. 会場にいなくても大会を楽しむために必要な環境を提供すること	コメント	その他の期待・要求事項	（4）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） 重要	コメント
損害保険事業	自動車保険	○	○	－	○	－	大会の関係者が円滑に大会関連業務を遂行するためには、大会期間中の事故受付件数増加に備えたシステム改修を実施した上、自動車保険の保険金支払業務が維持されることが必要である。	自動車保険は事業収入に占める割合が極めて大きく、大会開催に直接影響しない部分であっても、サービス継続が必要である。	○	大会開催面での影響を踏まえ、重要サービスであると判断する。
	自賠責保険	－	－	－	－	－	大会開催に対する直接的な影響はない。	自動車損害賠償保障法に基づく強制保険であり、引受義務がある。	○	大会開催面での直接影響はないが、法令に基づく強制保険であることから、当該サービスの継続維持は経営上の優先度が高い。このため、当該サービスの継続において重大な支障が生じた場合には、間接的に大会開催に影響を及ぼすことも想定されるため、重要サービスであると判断する。
	ペット保険	－	－	－	－	－	大会開催に対する直接的な影響はない。	一般的な個人マスマーケット向け商品であり、法制面等の要求はない。また、収入規模その他財務上のインパクトも小さい。	－	大会開催面及びその他の期待・要求事項を踏まえ、リスクアセスメントを行うべき重要サービスには該当しないと判断する。
	地震保険									
	傷害保険・医療保険									
	賠償責任保険									
	⋮									
生命保険事業	生命保険	－	－	－	－	－	大会開催に対する直接的な影響はない。		－	大会開催面及びその他の期待・要求事項を踏まえ、リスクアセスメントを行うべき重要サービスには該当しないと判断する。
資産運用事業	資産運用	－	－	－	－	－	大会開催に対する直接的な影響はない。		－	大会開催面及びその他の期待・要求事項を踏まえ、リスクアセスメントを行うべき重要サービスには該当しないと判断する。

<凡例>
－（非関連）　：サービスに係る活動目的と関連しない

※ Step1で設定した「大会に向けた自組織の活動目的」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。

STEP3：最低限許容されるサービスの範囲・水準を明らかにした上、サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定する。 v1.0.0

（1）事業	（2）サービス	(3)大会開催面での期待その他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		(4)サービスの提供が完全停止した場合の影響										(5）サービスの提供に係る最大許容停止時間(MTPD)	
				サービスの提供が完全停止した場合に生じる事態		時間経過に伴う影響度合いの評価									
		大会開催面	その他	大会開催面	その他	瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント

<凡例>
－（影響なし） ：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明） ：活動目的の阻害につながる影響があるかどうかわからない

STEP3：最低限許容されるサービスの範囲・水準を明らかにした上、サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定する。

（1）事業	（2）サービス	(3)大会開催面での期待その他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		(4)サービスの提供が完全停止した場合の影響									(5）サービスの提供に係る最大許容停止時間(MTPD)	
				サービスの提供が完全停止した場合に生じる事態		時間経過に伴う影響度合いの評価								
		大会開催面	その他	大会開催面	その他	瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント
損害保険事業	自動車保険	オリンピック関連の契約に係る事故対応業務（事故受付、照会対応、保険金支払）を遅滞なく実行する。	既存契約に係る契約者からの照会対応や事故対応業務（事故受付、照会対応、保険金支払）を遅滞なく実行する。	契約者からの照会対応や示談代行その他の事故対応が停止するため、大会関係の契約車両で事故が生じた場合、スタッフ業務の円滑な遂行を阻害する可能性がある。	自動車保険は契約数や事故件数が極めて大きく、契約者からの照会対応を含む営業活動や示談代行その他の事故対応が停止することにより、事業の継続に大きな影響を及ぼす可能性がある。	－	－	－	－	×	×	×	×	1営業日	保険金支払については、1営業日までのサービス停止であれば許容可能と判断した。
	自賠責保険	－	店頭や代理店での保険引受業務を遅滞なく実行する。	大会開催に対する直接的な影響はない。	自動車損害賠償保障法に基づく強制保険であるが、引受義務を果たすことができない。	－	－	－	－	－	×	×	×	5営業日	引受義務に係るサービスレベルについて法令で定められていないが、1週間を超えるサービス停止は許容できないと判断した。
	火災保険														
	地震保険														
	傷害保険・医療保険														
	賠償責任保険														
	⋮														
生命保険事業															
資産運用事業															

＜凡例＞
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない
×（影響あり）　：活動目的の阻害につながる影響がある

STEP4：重要サービスの提供に必要な業務を洗い出し、当該業務について許容される最低限の水準（操業率、稼働率等）を決定する。また、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決定する。 v1.0.0

（1）事業	（2）重要サービス	（3）重要サービスの提供に必要な業務 （重要サービスを構成する業務）	（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）	（5)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								（6）業務に係る最大許容停止時間(MTPD)	
				業務が完全停止した場合に生じる事態	時間経過に伴う影響度合いの評価								
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント

＜凡例＞
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない

STEP4：重要サービスの提供に必要な業務を洗い出し、当該業務について許容される最低限の水準（操業率、稼働率等）を決定する。また、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決定する。 v1.0.0

（1）事業	（2）重要サービス	（3）重要サービスの提供に必要な業務（重要サービスを構成する業務）	（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）	（5)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								（6）業務に係る最大許容停止時間(MTPD)	
				業務が完全停止した場合に生じる事態	時間経過に伴う影響度合いの評価								
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント
損害保険事業	自動車保険	顧客応対、募集（営業部門）	営業店における稼働率が50%程度であれば、既存契約者への対応が可能。	保険契約に係る契約者からの照会対応や募集を行うことができなくなる。	－	－	－	－	－	×	×	×	1営業日	営業店業務については、1営業日までのサービス停止であれば許容可能と判断した。
		引受、商品開発（商品部門）	商品部門が停止しても重要サービスの提供に直接の影響は生じない。ただし、商品改定等の業務が滞った場合、中長期的に事業に与える悪影響が大きい。	特殊契約の引き受けや商品開発・改定業務を行うことができなくなる。	－	－	－	－	－	－	－	×	2週間	業務停止期間が2週間を超えると、中長期的な改定作業に影響が生じると判断した。
		契約計上事務（事務部門・システム部門）	顧客対応上、契約の反映や保険証券の発行を遅滞なく行う必要がある。	契約計上が停止すると、その間に締結された契約照会や証券発行ができなくなる。	－	－	－	－	－	－	×	×	1週間	業務停止期間が1週間を超えると、顧客対応上問題が生じると判断した。
		保険金支払（SC部門）	大会関連契約の担当SCにおいて、稼働率が50%程度であれば、既存契約者への対応が可能。	事故対応や保険金支払いができなくなる。	－	－	－	－	×	×	×	×	1営業日	保険金支払については、1営業日までのサービス停止であれば許容可能と判断した。
		コールセンター（コールセンター部門）	顧客対応上、応答率90%以上、平均処理時間30分以下を維持する必要がある。	顧客からの照会対応ができなくなる。	－	－	－	－	－	×	×	×	1営業日	コールセンター業務については、1営業日までのサービス停止であれば許容可能と判断した。
	自賠責保険	顧客応対、募集（営業部門）	営業店における稼働率が50%程度であれば、既存契約者への対応及び店頭窓口での対応が可能。	保険契約に係る照会対応や募集を行うことができなくなる。	－	－	－	－	－	×	×	×	5営業日	引受義務に係るサービスレベルについて法令で定められていないが、1週間を超えるサービス停止は許容できないと判断した。
		引受、商品開発（商品部門）	商品部門が停止しても重要サービスの提供に直接の影響は生じない。ただし、商品改定等の業務が滞った場合、中長期的に事業に与える悪影響が大きい。	特殊契約の引き受けや商品開発・改定業務を行うことができなくなる。	－	－	－	－	－	－	－	×	2週間	業務停止期間が2週間を超えると、中長期的な改定作業に影響が生じると判断した。
		契約計上事務（事務部門・システム部門）	顧客対応上、契約の反映や保険証券の発行を遅滞なく行う必要がある。	契約計上が停止すると、その間に締結された契約照会や自賠責証明書の発行ができなくなる。	－	－	－	－	－	－	×	×	1週間	業務停止期間が1週間を超えると、顧客対応上問題が生じると判断した。
		保険金支払（SC部門）	SCにおいて、稼働率が50%程度であれば、既存契約者への対応が可能。	事故対応や保険金支払いができなくなる。	－	－	－	－	×	×	×	×	1営業日	保険金支払については、1営業日までのサービス停止であれば許容可能と判断した。
		コールセンター（コールセンター部門）	顧客対応上、応答率90%以上、平均処理時間30分以下を維持する必要がある。	顧客からの照会対応ができなくなる。	－	－	－	－	－	×	×	×	1営業日	コールセンター業務については、1営業日までのサービス停止であれば許容可能と判断した。
	火災保険													
	地震保険													
	傷害保険・医療保険													
	賠償責任保険													
	⋮													
生命保険事業														
資産運用事業														

＜凡例＞
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない

(1)事業	(2)重要サービス	(3) 重要サービスの提供に必要な業務 （重要サービスを構成する業務）	(4)前提とする業務水準（許容できる最低稼働率等） ※Step4の（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）を転記		(5)業務を支える経営資源							
			大会開催面	その他	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(電気、水、ガス)	資金	その他

(1)事業	(2)重要サービス	(3) 重要サービスの提供に必要な業務 （重要サービスを構成する業務）	(4)前提とする業務水準（許容できる最低稼働率等） ※Step4の（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）を転記		(5)業務を支える経営資源							
			大会開催面	その他	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（電気、水、ガス）	資金	その他
損害保険事業	自動車保険	顧客応対、募集（営業部門）	–	営業店における稼働率が50%程度であれば、既存契約者への対応が可能。	営業職員：XXX人 代理店従業員：XXX人	顧客DB 自動車保険契約データ 帝国データバンク企業情報	○○支店ビル、…	職員用端末：○台 インターネット専用端末：○台 電話設備（外線：○回線、電話機：○台） 複合機：○台	保険募集システム 代理店システム	電力：X	店頭での現金払の釣銭：●万円 交通費：●万円	
		引受、商品開発（商品部門）	–	商品部門が停止しても重要サービスの提供に直接の影響は生じない。ただし、商品改定等の業務が滞った場合、中長期的に事業に与える悪影響が大きい。	内勤職員：XXX人	自動車保険リザルト管理用データ	本社ビル	職員用端末：○台 インターネット専用端末：○台 電話設備（外線：○回線、電話機：○台）	本社共用サーバ	電力：X,…		
		契約計上事務（事務部門・システム部門）	–	顧客対応上、契約の反映や保険証券の発行を遅滞なく行う必要がある。	事務職員：XXX人	顧客DB 自動車保険契約データ	事務本部	職員用端末：○台 インターネット専用端末：○台 電話設備（外線：○回線、電話機：○台） 複合機：○台	申込書計上システム 証券発行システム	電力：X,…		
		保険金支払（SC部門）	大会関連契約の担当SCにおいて、稼働率が50%程度であれば、既存契約者への対応が可能。	SCにおいて、稼働率が50%程度であれば、既存契約者への対応が可能。	SC職員：XXX人 （うち、決裁権者○人）	顧客DB 自動車保険契約データ 自動車保険事故データ	○○支店ビル、…	職員用端末：○台 インターネット専用端末：○台 電話設備（外線：○回線、電話機：○台）	SCシステム	電力：X,…		
		コールセンター（コールセンター部門）	–	顧客対応上、応答率90%以上、平均処理時間30分以下を維持する必要がある。	コールセンター職員：XXX人 （SV：○人、OP：○人）	顧客DB 自動車保険契約データ インバウンド管理DB	本社ビル	職員用端末：○台 インターネット専用端末：○台 電話設備（外線：○回線、電話機：○台）	コールセンターシステム	電力：X,…		
	自賠責保険	顧客応対、募集（営業部門）	–	営業店における稼働率が50%程度であれば、既存契約者への対応及び店頭窓口での対応が可能。								
		引受、商品開発（商品部門）	–	商品部門が停止しても重要サービスの提供に直接の影響は生じない。ただし、商品改定等の業務が滞った場合、中長期的に事業に与える悪影響が大きい。								
		契約計上事務（事務部門・システム部門）	–	顧客対応上、契約の反映や保険証券の発行を遅滞なく行う必要がある。								
		保険金支払（SC部門）	–	SCにおいて、稼働率が50%程度であれば、既存契約者への対応が可能。								
		コールセンター（コールセンター部門）	–	顧客対応上、応答率90%以上、平均処理時間30分以下を維持する必要がある。								
	火災保険											
	地震保険											
	傷害保険・医療保険											
	賠償責任保険											
	：											

(1)事業	(2)重要サービス	(3)重要サービスの提供に必要な業務	(4)リスクの特定					(5)リスクの分析								(6)リスクの評価		
			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	事象の結果の影響度合い				事象の発生頻度			残存リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部署）
								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				
			情報・データ															
			情報システム，制御システム															

STEP6:重要サービスの提供に必要な業務に係る経営資源を整理した上、当該経営資源に係るリスク（情報資産に係るリスクに限定）を特定、分析及び評価します。

(1)事業	(2)重要サービス	(3)重要サービスの提供に必要な業務	(4)リスクの特定					(5)リスクの分析								(6)リスクの評価		
			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	事象の結果の影響度合い				事象の発生頻度			残存リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部署）
								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				
損害保険事業	自動車保険	顧客応対、募集（営業部門）	情報・データ	顧客DB	顧客DB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	業務停止に直結するものではないが、営業部門を中心とする全社員が全顧客に対する所要の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。	5	顧客DBにクレジットカード番号等のセンシティブ情報を含まない設計としている。	3	3	全てのクライアント端末に対し、物理的にUSBメモリを使用不能としている	1	3	8	－	－
							情報を持ち出せる環境（外部接続）・電子メール						特段の対策を講じていない	3	9		●	自動車商品業務部
							情報を持ち出せる環境（その他）・用紙管理						特段の対策を講じていない	3	9		●	自動車商品業務部
							業務の社会的重要性を理解していない派遣社員の使用						派遣社員のIDからは顧客DBにアクセスできないようにコントロールしている	2	6		－	－
						外部からの情報搾取	インターネットに接続しているサーバに保管されている					2	ファイヤーウォールを設置し、セキュリティソフトを導入している	1	3		－	－
					顧客DBの改ざん	外部からの不正アクセス	インターネットに接続しているサーバに保管されている	顧客応対、募集活動に係る全ての業務が顧客DB復旧まで停止する。	4	特段の対策を講じていない	4	2	ファイヤーウォールを設置し、セキュリティソフトを導入している	1	4		－	－
					顧客DB消失													
			情報システム，制御システム	保険募集システム	保険募集システムの未認証													
					保険募集システムのバグ													
					保険募集システムの停止													
				代理店システム	代理店システムの未認証													
					代理店システムのバグ													
					代理店システムの停止													
		引受、商品開発（商品部門）	情報・データ															
			情報システム，制御システム															

機能保証のための
リスクアセスメント・ガイドライン ＜１．０版＞

－２０２０年東京オリンピック・パラリンピック競技大会に向けて－

平成２８年９月

内閣官房　内閣サイバーセキュリティセンター
重要インフラグループ

（空白ページ）

目次

１．はじめに

＜１＞ガイドライン策定の背景・目的

２０２０年東京オリンピック・パラリンピック競技大会（以下「大会」といいます。）は国際的なビッグイベントであり、世界各国から多くのアスリートや観客が来日することが予想されます。また、開催国である我が国の動向は、２０２０年に向けて、テレビ放送、インターネット等のマスメディアを通じて、世界中の注目を集めることになります。

一方、日本企業を対象とした国際的なサイバー攻撃の脅威の高まりなど、とりわけ情報セキュリティをめぐる情勢は日々刻々と変化しています。大会運営の成功のためには、政府機関等だけでなく、大会を直接的又は間接的に支えるサービスを提供する事業者等が、自らのサービス提供の継続に対するリスクを自律的に評価した上、適切に情報セキュリティを確保し、サービス提供の継続に必要な体制を整えていくことが不可欠です。

本ガイドラインは、こうした情勢を踏まえ、情報セキュリティ確保に向けてのリスクアセスメントの参考になる手法を示すことにより、大会を直接的又は間接的に支えるサービスを提供する事業者等による自律的な情報セキュリティ対策を促進することを目的とします。

＜２＞ガイドラインの適用範囲

（１）対象とする事業者等

本ガイドラインは、大会を直接的又は間接的に支えるサービスを提供する事業者等、とりわけサービスの提供が停止又は品質が低下した場合に大会の運営等に多大な影響を及ぼす可能性のある事業者等（以下「重要サービス事業者等」といいます。）による利活用を想定しています。

（２）リスクアセスメントの対象

本ガイドラインにおけるリスクアセスメントでは、重要サービス事業者等が、そのサービス提供に必要な業務の遂行のために所有、使用又は管理する情報、情報システム、制御システム等の情報資産に係る事象の結果（自然災害やサイバー攻撃等に起因するＩＴ障害）から認識されるリスク（以下「情報セキュリティ・リスク」といいます。）を対象とします（※）。

（※）重要サービス事業者等においては、情報セキュリティ・リスク以外のリスクがあることも考えられます。本ガイドラインでは、情報セキュリティ・リスクにスコープを限定したリスクアセスメントの手法を紹介していますが、実際にリスクの評価やリスク対応の選択肢の同定に係る意思決定を行う際には、情報セキュリティ・リスク以外のリスクについても勘案し、総合的に考慮することが重要です。

＜３＞ガイドラインの構成

本ガイドラインは、次に掲げるドキュメントにより構成されます。

ドキュメント名称		概要
機能保証のためのリスクアセスメント・ガイドライン		本文書
別紙１	業務の阻害につながる事象の結果の例	業務の維持のために経営資源に求められる観点を踏まえた「業務の阻害につながる事象の結果」（ＩＴ障害）を例示した参考資料
別紙２	結果を生じ得る事象（脅威）の例	結果を生じ得る事象について、基本的な分類と併せて主な例示を掲載した参考資料
別紙３ （様式集） （※）	（様式１）リスクアセスメントの実施目的の確認	組織の活動目標の設定及びリスクアセスメントの実施目的・方針の確認のためのワークシート（記載例を含む。）
	（様式２）重要サービスの選定	大会開催面その他の期待事項・要求事項を分析し、重要サービス（リスク評価の対象とするサービス）を選定するためのワークシート（記載例を含む。）
	（様式３）重要サービスの影響度分析	重要サービスの影響分析として、重要サービスの最低許容範囲・水準及びサービス提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定するためのワークシート（記載例を含む。）
	（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	重要サービスの提供のために必要な業務を洗い出し、その業務について最低限維持すべき状態を明らかにした上、その業務が停止した場合の影響及び最大許容停止時間を推定するためのワークシート（記載例を含む。）
	（様式５）業務を支える経営資源の特定	重要なサービスの提供に必要な業務について、最低限維持すべき状態を維持するために必要な経営資源を明らかにするためのワークシート（記載例を含む。）
	（様式６）リスクアセスメント及びリスク対応方針の決定	重要サービスの提供に必要な業務に係る経営資源を整理した上、その業務継続に対するリスクの特定、分析及び評価を行うためのワークシート（記載例を含む。）
	リスクアセスメントの実施手順（例）	主に作業担当者に向けて、本ガイドラインに沿った詳細な作業手順を解説した文書。リスクアセスメントシートの記載要領を含みます。

（※）本ガイドラインにおいて、様式１から様式６までの様式を総称して「リスクアセスメントシート」といいます。

＜大会に向けての対応＞

上記ドキュメントに加え、次に掲げるドキュメントを別添します。

ドキュメント名称	
別添１	実施結果提出様式
別添２	２０２０年東京オリンピック・パラリンピック競技大会の開催概要
別添３	２０２０年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的

２．リスクアセスメントの全体像

＜１＞リスクアセスメントの重要性等

情報通信技術は、社会経済システムに広く普及し、事業者等が事業活動を行う上で欠かせないものとなっています。近年では、センサーデバイス等のハードウェアの進化、低廉かつ高速なインターネットの普及、ビッグデータ解析技術の進歩等を背景として、制御システムに情報通信技術を融合させた新たな制御技術が導入されるなど、いわゆるＩｏＴシステムを活用した事業活動の高度化・高付加価値化が進展し、事業活動における情報通信技術への依存度も高まりつつあります。

他方、情報通信技術の普及に伴い、サイバー攻撃や情報システムの不具合に起因する個人情報の漏えいやサービス提供の中断による経済的損失等の事例が頻繁に報告されており、実社会への被害が深刻化しています。事業経営においては、ひとたび情報セキュリティを脅かす事例が顕在化すると、業務の遂行に大きな影響が出るだけでなく、社会的信用の喪失やブランドイメージの毀損につながるおそれもあります。特にサイバー攻撃に関しては、攻撃者に踏み台として利用された場合など、自らが被害者になると同時に第三者にとっては加害者になり得るという特性があることから、どのような事業者等でも重大なセキュリティ事件の当事者となり、事業者等の存亡に関わるような深刻なダメージを被る可能性があります。加えて、未公開の脆弱性を狙ったゼロデイ攻撃のような高度化したサイバー攻撃や内部不正に関しては、もはや「未然に防ぎきることは不可能である」ということを認識する必要があります。

こうした中、事業経営においては、製品・サービスへのセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることが必要です。特に、近年では、前述のような情報通信技術の高度化や事業者等を標的とするサイバー攻撃の増加などを背景として、事業者等を取り巻く環境が「ＶＵＣＡ」と呼ばれる不安定（Volatility）で不確実性（Uncertainly）が高く、複雑（Complexity）かつ曖昧（Ambiguity）な状況となっており、こうした状況において敏捷かつ適切に対処できるように、情報セキュリティ・リスクへの備えを経営戦略として位置付けることが重要になってきます。しかしながら、いざ情報セキュリティ対策を講じようとした場合、その実施範囲や程度には限度がありません。また、行き過ぎた対策は、業務の効率を低下させることになります。真に有効な情報セキュリティ体制を構築し、これを適切にマネジメントするには、事業経営・事業活動における目的、その目的に照らした製品・サービスの経営上の位置付け、利害関係者からの期待、社会的責任（ＣＳＲ）、法制面の要求（コンプライアンス）等を分析した上、保有する経営資源の重要性の尺度に基づくリスクの特定・分析・評価（リスクアセスメント）を行い、各事業者等の実情や風土に応じたリスク対応を戦略的に講じることが必須の要件となります。あわせて、こうした活動全体（リスクマネジメント）が継続的かつ有効に機能する仕組みを構築することも必要です。

リスクアセスメントの重要性については、既に多くの事業者等の認識するところとなり、その実施についても、事業者等の掲げる情報セキュリティ基本方針に記載されることなどが増えています。他方、リスクアセスメントの重要性を認識しながらも、具体的にどのように進めたらよいかが分からないなどの理由により、実施できていない事業者等も多く存在しており、リスクアセスメントの考え方や実施方法がしっかりと定着しているとは言い難い状況です。

本ガイドラインでは、こうした状況を踏まえ、情報セキュリティに係るリスクアセスメントの実施方法についての具体的な手順を含む基礎的なフレームワークを提供することにより、リスクアセ

スメントの考え方や実施方法を普及・定着させ、ひいては我が国におけるセキュリティマインドを持った事業経営の推進に寄与することを期待しています。

＜２＞機能保証に向けたリスクアセスメントの観点・考え方

リスクアセスメントの手法には、既に確立されており、多くの運用実績を有するものが多数存在しますが、その手法の採用や実施手順において唯一の正解というものはありません。このため、事業者等がリスクアセスメントを実践する際には、どの手法を採用すれば、自組織にとって、より効果的・効率的にリスクの特定・分析・評価を行うことができるかを十分に検討した上、自らの判断でこれを決定することが必要です。この検討・決定に際しては、重要インフラ事業者等を含め、その提供するサービスが社会経済システムにおいて不可欠な役割・機能を担う事業者等においては、機能の発揮やサービスの提供を全うするという観点でのリスクアセスメントを行い、経営層による総合的な判断を踏まえたリスク対応を進めていくことにより、事業継続を確保していくという「機能保証」の考え方を踏まえることが重要となります。

本ガイドラインでは、前述のとおり、重要サービス事業者等により利活用されることを想定していることから、機能保証の考え方に立脚したリスクアセスメントとして、「各重要サービス事業者等が大会を取り巻く社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために必要なサービスの提供を維持・継続する」という観点から、情報セキュリティ・リスクの特定・分析・評価を実践するための手順を紹介します。

重要サービス事業者等にあっては、リスクアセスメントを主体的かつ自律的に取り組むことが必要です。ただし、その取組の精度や水準については、各重要サービス事業者等の力量に依存することから、本ガイドラインでは、大会の開催に向けたリスクアセスメントの考え方や参考になる作業手順を示すことにより、各重要サービス事業者等における取組が一定以上の精度や水準を確保されることを狙いとしています。

なお、本ガイドラインで紹介するリスクアセスメントの手順は、重要サービス事業者等や重要インフラ事業者等に限らず、中堅・中小企業を含む様々な分野の事業者等においても準用することができます。

＜３＞機能保証に向けたリスクアセスメントの方針

本ガイドラインでは、「２．＜２＞機能保証に向けたリスクアセスメントの観点・考え方」に記載したとおり、「事業者等が、機能保証の考え方に立脚し、リスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びにリスク対応の選択肢の同定を行うとともに、残留リスクを可視化すること」を志向します。このことを踏まえ、本ガイドラインで紹介するリスクアセスメントの手法は、次に掲げる方針に従うものとします。

①リスクの捉え方

「社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続すること」を事業者等における経営戦略上の目的とし、「目的に対する不確かさの影響」をリスクと捉えます（ISO 31000:2009 における定義に準拠。）。ただし、機能保証が目的となることから、本ガイドラインで対象とするリスクは、「負の影響：純粋リスク」に限定します。

②機能保証の観点からの演繹的なリスクアセスメント

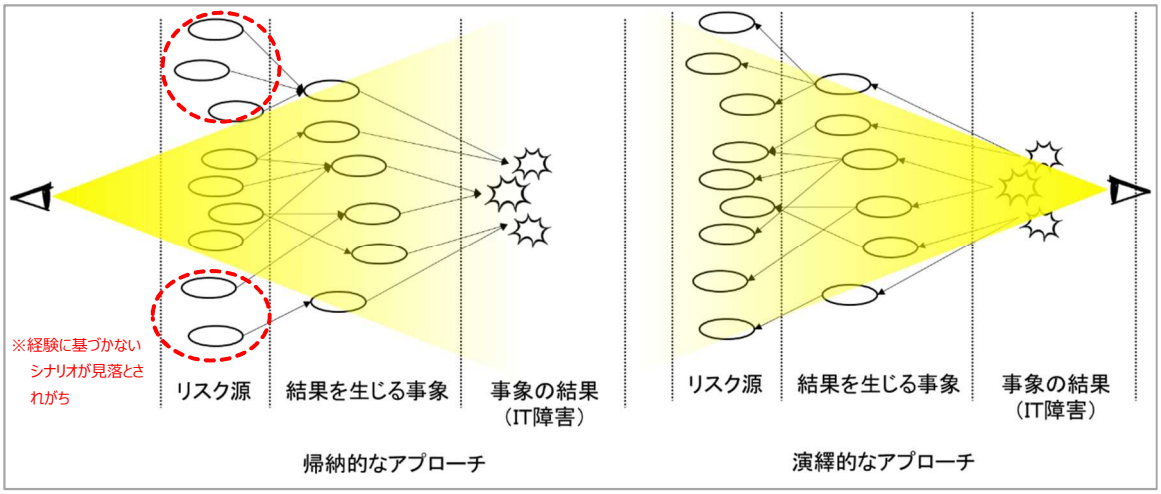
発生確率の低い事象から目を背けた（発生した場合には危機的状況につながる可能性がある事象であっても、過去に経験していない、又は発生確率が低いためにリスクとして想定しなかった）ことにより、その事象の結果が想定外となって大きな混乱を招くこととなった東日本大震災での教訓を踏まえ、上記①によるリスクの捉え方を前提として、機能保証の観点から、「事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定し、そのサービス提供の維持・継続に必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを演繹的に特定・分析・評価」するアプローチとします。

③効率的な作業への配慮（帰納的なアプローチとの組合せ）

演繹的な詳細リスク分析のアプローチを採用しますが、多くの事業者等により実施されているイベントツリー分析等の帰納的なアプローチによって、想定される脅威（事象）及び脆弱性（リスク源）の組合せを書き出していくやり方も、事業者等が想定するリスクについての分析には一定の効果があることから、こうした実績のある帰納的な手法を組み合わせることにより、効率的な作業を行うことができるように配慮します。具体的には、事業者等における作業負荷や、作業者の知識・経験が浅い場合などに結果を生み出す事象を見逃してしまう可能性があることについても考慮し、リスク分析における気付きとなるような「業務の阻害につながる事象の結果（例）」（別紙１）及び「結果を生じ得る事象（例）」（別紙２）を提供することにより、作業の効率化や網羅性の確保に資するように配慮します。

＜アプローチ手法の比較＞

	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） $\mathscr{X} \times \mathscr{Y} \rightarrow$?	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） $\mathscr{Z} \leftarrow$? × ?
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、作業負荷が多大になる



④妥当性確認

リスクアセスメントにおいては、唯一の絶対的な正解というものがなく、その判断結果には、作業者の立場や知識・経験に基づく偏り（バイアス）を含むことがあります。また、多くの作業者が分担して作業を行う場合には、作業者ごとにリスクアセスメント結果の粒度や精度にばらつきが生じることがあります。こうした特性を踏まえ、「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ること」を検証するための妥当性確認（Validation）のプロセスを組み入れます。この妥当性確認のプロセスには、サービス提供を支える業務や経営資源に係る職務分掌の確認や部門間の連係状況の相互理解を目的とする関係主体間のコミュニケーションを含みます。

⑤リスクアセスメントの継続的な見直し

ＶＵＣＡと呼ばれる不透明な環境においては、事業者等が環境の変化に敏捷かつ適切に対応するために、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となることから、妥当性確認を踏まえたリスクアセスメント結果の見直しを継続的に実施するために必要な体制を整備するプロセスを組み入れます。

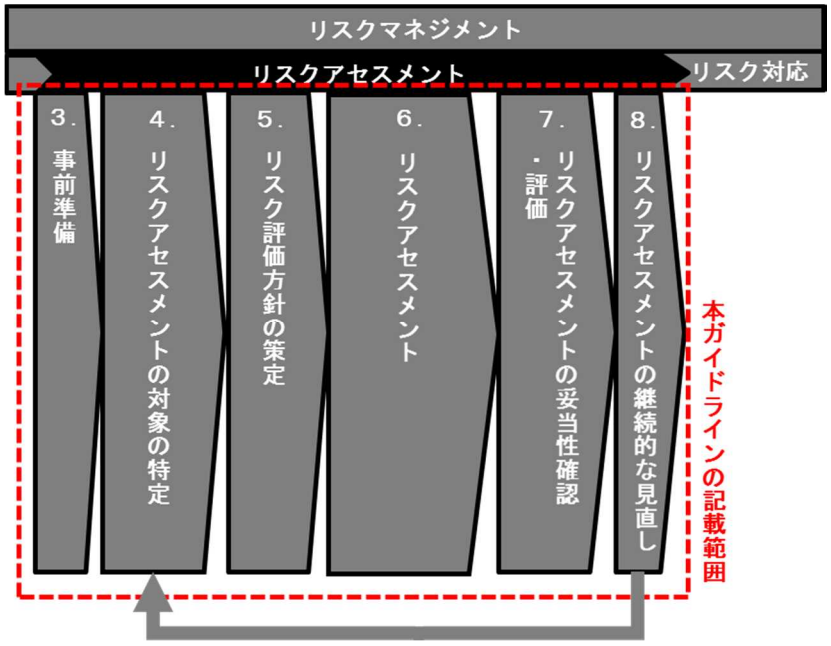
＜４＞機能保証に向けたリスクアセスメントのフレームワーク

「２．＜３＞機能保証に向けたリスクアセスメントの方針」に記載された方針に基づき、次のとおり、機能保証に向けたリスクアセスメントの枠組みを示します。

方針	リスクアセスメントのプロセス
①リスクの捉え方、リスクアセスメントの実施目的	３．＜２＞（１） リスクアセスメントの実施目的の確認
②機能保証の観点からの演繹的なリスクアセスメント	４．リスクアセスメントの対象の特定 ６．リスクアセスメント
③効率的な作業への配慮 （帰納的なアプローチとの組合せ）	（別紙１）業務の阻害につながる事象の結果（例） （別紙２）結果を生じる事象（例）
④妥当性確認	７．リスクアセスメントの妥当性確認・評価
⑤リスクアセスメントの継続的な見直し	８．リスクアセスメントの継続的な見直し

＜５＞リスクアセスメントの位置付け（俯瞰図）

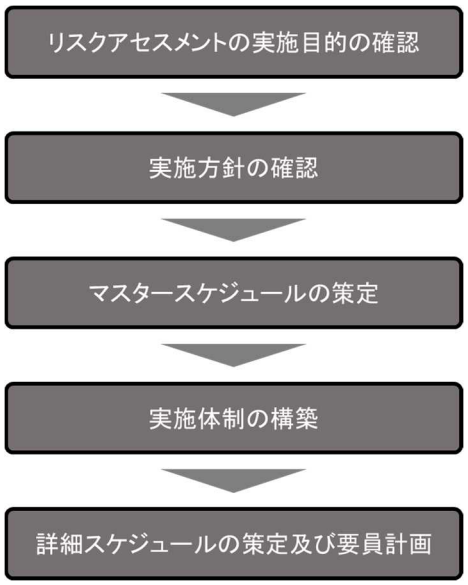
リスクマネジメント活動全体の中におけるリスクアセスメントの位置付け（本ガイドラインの記載範囲）は、下図のとおりです。



３．事前準備

本章では、機能保証に向けたリスクアセスメントの実施のための事前準備作業の実施手順を記載します。

＜１＞作業ステップ



＜２＞実施内容

（１）リスクアセスメントの実施目的の確認

自組織の活動目的を設定し、これを踏まえた自組織のリスクアセスメントの目的を確認します。機能保証に向けたリスクアセスメントでは、「自組織が社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続するという活動目的に対するリスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びに残留リスクを可視化すること」が、基本的なリスクアセスメントの実施目的になります。

＜大会に向けての対応＞

『（様式１）リスクアセスメントの実施目的の確認』を用いて、大会の成功のために自組織が利害関係者から期待されている役割・機能を整理するプロセスを通じ、リスクアセスメントの実施目的の確認を行います。この際、大会に向けては、大会の準備期間及び開催期間における時限的な外部環境の変化や利害関係者からの期待の高まりなどを十分に考慮することが重要です。

（２）実施方針の確認

自組織におけるリスクアセスメントの実施方針（※）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。この際、本ガイドラインで紹介する機能保証に向けたリスクアセスメントの枠組みを参考として、自組織における実施方針を定めることができます。

（※）本ガイドラインにおいて、リスクアセスメントの実施方針とは、「リスクアセスメントの目的を達成するために必要な活動の範囲や進め方について、経営層において合意されたもの」をいいます。

＜大会に向けての対応＞

『（様式１）リスクアセスメントの目的の確認』を用いて、リスクアセスメントの実施目的の確認と合わせて実施方針の確認を行います。

（３）マススケジュールの策定

リスクアセスメントの実施方針が定まったら、実施方針として定めた各作業の実施時期を定め、リスクアセスメント活動全体の作業スケジュール（マススケジュール）を策定します。

リスクアセスメントには経営層による承認が要求されるプロセスも含まれており、マススケジュールの策定においては、このような進捗管理上の重要な節目となる局面をマイルストーンに設定し、これを踏まえたスケジュールとなるように調整することが重要です。

なお、マススケジュールは、進捗管理の前提である重要なベースラインであり、後続の作業手順である実施体制の構築や各作業部門での詳細スケジュールの策定及び要員手配の前提となります。

（４）実施体制の構築

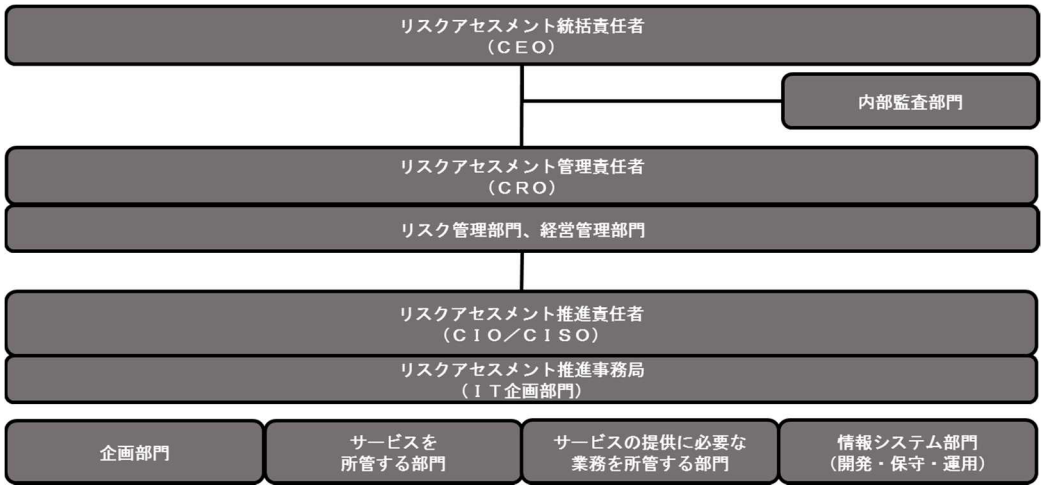
リスクアセスメントの実施方針及びマススケジュールを踏まえ、実施体制を構築します。実施体制の構築に際し、機能保証に向けたリスクアセスメントが経営戦略上の重要な活動であることを踏まえ、経営層が、リスクアセスメントの最高責任者として、推進及び管理を主導することが重要です。

リスクアセスメントを円滑かつ効果的に推進するためには、ある特定の部門が閉鎖的に取り組むのではなく、各作業ステップにおいて責任主体となる部門を定めた上、関連部門が、適宜にコミュニケーションを取りながら、連携して取り組むことが必要です。

なお、本ガイドラインにおいて想定する実施体制及び作業ステップ別の作業担当部門は、次のとおりです。

＜リスクアセスメント実施体制（例）＞

体制		役割	主な担当部門
統括	リスクアセスメント統括責任者	リスクアセスメントの目的達成に係る最終的な責任を負います。	ＣＥＯ
監査	リスクアセスメント監査部門	リスクアセスメントの管理・推進の妥当性を第三者的立場から確認し、リスクアセスメント統括責任者による意思決定を補助します。	内部監査部門
管理	リスクアセスメント管理責任者	リスクの運用管理の責任者であり、リスクアセスメントの結果等をリスクアセスメント統括責任者に報告する責任を負います。	ＣＲＯ
	リスクアセスメント管理担当部門	リスクアセスメント管理責任者を補助し、リスクの運用管理を担当します。	リスク管理部門 経営管理部門
推進	リスクアセスメント推進責任者	リスクアセスメントの推進に係る責任を負います。	ＣＩＯ／ＣＩＳＯ
	リスクアセスメント推進事務局	リスクアセスメント推進担当部門をとりまとめ、部門横断的なリスクアセスメントの全体調整を行います。	ＩＴ企画部門
	リスクアセスメント推進担当部門	リスクアセスメントの実施主体となります。	企画部門 サービス部門 業務部門 情報システム部門



＜作業ステップ別の作業担当部門（例）＞

STEP	評価対象	経営企画を所管する部門 Ex.経営企画部門、リスク管理部門	サービスを所管する部門 Ex.○○事業部門	サービスの提供に必要な業務を所管する各部門 Ex.営業部門、技術開発部門、研究開発部門、システム部門	
STEP1：活動目的の決定	目的	◎			
STEP2：重要サービスの選定	サービス	◎	○		
STEP3：重要サービスの影響分析	サービス	○	◎		
STEP4：重要サービスを支える業務の特定・影響分析	サービス⇒業務		◎	○	
STEP5：業務を支える経営資源の特定	業務⇒経営資源			◎	
STEP6：リスクアセスメント	経営資源⇒リスク	○	○	○ （ユーザ部門）	◎ （システム部門）

◎：主担当（取りまとめ等）
○：副担当（結果の確認等）

#42

（５）詳細スケジュールの策定及び要員計画

実施体制が定まり、各作業ステップの推進担当部門が決定したら、各推進担当部門において、詳細スケジュールの策定及び要員計画（作業担当者の選任及び作業の割当て）を行います。

要員計画に際しては、サービス、業務、システム等に係る有識者を確保するほか、組織で決められたレポートラインを踏まえた関連部門との連絡窓口となる担当者等の確保も考慮する必要があります。

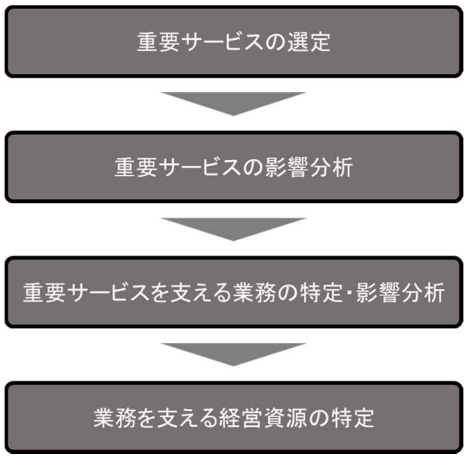
４．リスクアセスメントの対象の特定

本章では、「リスクアセスメントの対象の特定」に係る作業の実施手順を記載します。

リスクアセスメントの対象は、機能保証の観点から、事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定し、そのサービス提供の維持・継続に必要な業務や経営資源に係る要件を分析・評価した結果を踏まえて、見極めます。

なお、この一連の作業は、バリュー・チェーン及びサプライ・チェーンの把握並びに事業影響度の把握を通じて、後続のリスク評価を行う上での評価基準（リスク基準）の前提となるリスク選好及びリスク許容度を分析する作業でもあります。

＜１＞作業ステップ



＜２＞実施手順

（１）重要サービスの選定

事業者等が扱うサービスについて、経営上の位置付け（業績への寄与度や事業上の依存度等の事業経営上の位置付け）、利害関係者（顧客、仕入先、株主、地域社会等）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）等を総合的に勘案した上、機能保証の観点からサービスの重要度（優先度）を評価し、リスクアセスメントの対象とするサービス（重要サービス）を特定します。

＜大会に向けての対応＞

『（様式２）重要サービスの選定』を用いて、大会開催面での期待事項とその他の要求事項を勘案し、事業者等にとって重要なサービスを特定します。

（２）重要サービスの影響分析

重要サービスについて、前ステップ「（１）重要サービスの選定」で分析した要求事項等を満たすために最低許容される範囲・水準を明らかにします。また、重要サービスの提供が完全に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分析・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。

＜大会に向けての対応＞

『（様式３）重要サービスの影響度分析』を用いて、大会開催面での期待その他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・水準を明らかにし、またサービスの提供が完全停止した場合の影響を分析・評価した上でサービスの最大許容停止時間（ＭＴＰＤ）を推定します。

なお、とりわけ大会の開催期間中においては、世界中からの注目が高まっている特異な状況に置かれており、利害関係者からの期待・要求が通常よりも高まる可能性があることについても想定した上で影響分析することが必要です。

（３）重要サービスを支える業務の特定・影響分析

重要サービスの提供に必要な業務を洗い出し、その業務について許容される最低限の水準（操業率、稼働率等）を明らかにします。この際、自組織のバリュー・チェーンを意識して作業を行うことを推奨します。また、その業務が完全に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分析・評価し、業務の最大許容停止時間を推定します。

＜一般的なバリュー・チェーンの例＞

＜大会に向けての対応＞

『（様式４）重要サービスを支える業務の特定・影響度分析』を用いて、大会開催面での期待その他要求事項等を満たすための重要サービス提供に必要な業務の範囲・水準を明らかにし、また業務が完全停止した場合の影響を分析・評価した上で業務の最大許容停止時間（ＭＴＰＤ）を推定します。

（４）業務を支える経営資源の特定

前ステップ「（３）重要サービスを支える業務の特定・影響分析」で洗い出した業務を遂行するために必要な経営資源を特定し、その必要な要件（条件や数量など）を分析します。

＜大会に向けての対応＞

『（様式５）業務を支える経営資源の特定』を用いて、『（様式４）重要サービスを支える業務の特定・影響度分析』で洗い出した業務を支える経営資源（重要サービス提供に必要な業務の遂行のために所有、使用又は管理する情報、情報システム、制御システム等の情報資産）を洗い出します。

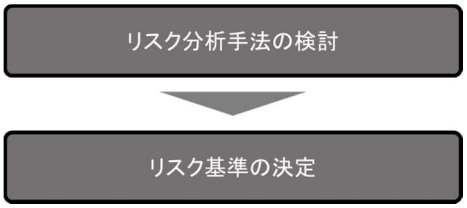
５．リスク評価方針の策定

本章では、「リスク分析の手法及びリスク評価の基準（リスク基準）の策定」に係る作業の実施手順を記載します。

リスク評価のための手法には様々なものがありますが、従来型の情報セキュリティ・リスクの評価においては、「情報資産の価値（機密性・完全性・可用性の観点から評価）×脅威の大きさ×脆弱性の度合い」といった算式により、情報資産保護の観点からリスクの重大さを測ることが一般的でした。この手法では、まず情報資産を洗い出した後、その情報資産に自らが想定する事象（セキュリティ・インシデント）を当てはめるという帰納的なアプローチでリスクの特定・分析・評価が行われます。この帰納的なアプローチは、過去の経験の中から事象を当てはめるという経験的な作業を伴いやすく、再発防止型のアプローチであるともいえます。また、この手法は、情報資産の洗出しから最終的なリスクの評価までが情報システム部門内で完結してしまい、機能保証の観点からサービス提供への影響を十分に分析・評価されにくいことも懸念されます。

従来型の情報セキュリティ・リスクの評価において、こうした課題があることを踏まえ、本ガイドラインでは、特定されたリスクに対し、機能保証の観点から重要サービスに要求されるサービスレベル・業務要件を踏まえた影響度合い等を考慮したリスク評価方針（分析手法及び評価基準）に基づくリスクの分析・評価を行うことを志向します。

＜１＞作業ステップ



＜２＞実施手順

（１）リスク分析手法の検討

本ガイドラインでは、多くの事業者等により採用されているリスクマップ及びリスク・スコアリングの手法を用いたリスク分析を紹介します。

リスクマップは、一般的に、「影響度」及び「発生頻度（発生可能性、起こりやすさ）」又は「情報資産の価値」及び「脅威の大きさ×脆弱性の度合い」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分析手法です。また、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、優先して対応すべきリスクを明確にする分析手法をリスク・スコアリングといいます。

機能保証に向けたリスクアセスメントでは、「自組織が社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続するという活動目的に対するリスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びに残留リスクを可視化すること」が基本的なリスクアセスメントの実施目的となることから、「事象の結果による重

要サービス・業務への影響度合い」と「事象の発生頻度（発生可能性、起こりやすさ）」を評価の軸とします。

「事象の結果による重要サービス・業務への影響度合い」については、「４．リスクアセスメントの対象の特定」において分析した結果を踏まえ、例えば、次に掲げる要素等を用いて総合的に評価します。

＜主な影響度合いの評価要素＞

影響度合いの評価要素	概要
予想影響範囲・程度	事象の結果が重要サービスを支える業務に及ぼすと予想される影響の範囲及び程度を評価します。業務に及ぼす影響には、「４．リスクアセスメントの対象の特定」において分析した各要求事項への影響についても考慮します。
予想復旧時間	事象の結果により重要サービスを支える業務が停止又は阻害された場合における予想復旧時間を評価します。
予想対応コスト	事象の結果により重要サービスを支える業務が停止又は阻害された場合において、その業務の復旧や事象の結果の対処に要する予想コストを評価します。

（２）リスク基準の決定

リスク基準とは、リスクの重大さを評価するための目安とする条件であり、リスクアセスメント作業担当者によって評価結果にばらつきを生じさせないことを狙いとして、あらかじめ設定される判断指標をいいます。

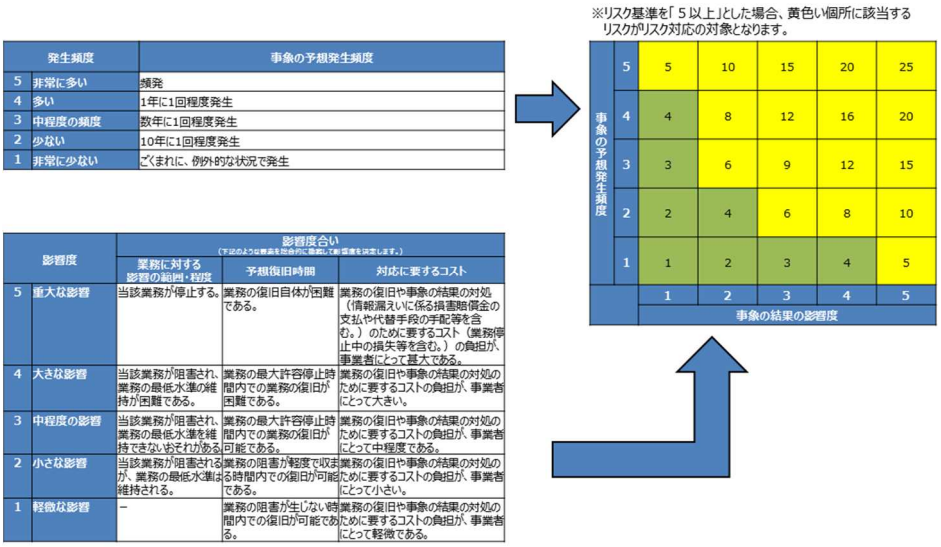
機能保証の考え方に立脚すると、リスク基準は、重要サービスの許容最低水準を満たすことや、許容停止時間内での復旧が可能であることが目安となります。「事象の結果による重要サービス・業務への影響度合い」と「事象の発生頻度（発生可能性、起こりやすさ）」を評価の軸とする場合におけるリスク基準の設定イメージは、次ページのとおりです。

なお、リスク基準は、リスクアセスメントの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。

＜リスク基準の設定イメージ＞

（例１）

事象の結果として、重要サービスを支える業務が停止する場合や業務の復旧が困難になる場合を重大な影響として評価し、この場合においては、発生頻度が非常に少ないと評価されるときであっても、リスク対応の対象となるようにリスク基準を「５以上」と設定しています。



発生頻度		事象の予想発生頻度
5	非常に多い	頻発
4	多い	1年に1回程度発生
3	中程度の頻度	数年に1回程度発生
2	少ない	10年に1回程度発生
1	非常に少ない	ごくまれに、例外的な状況で発生

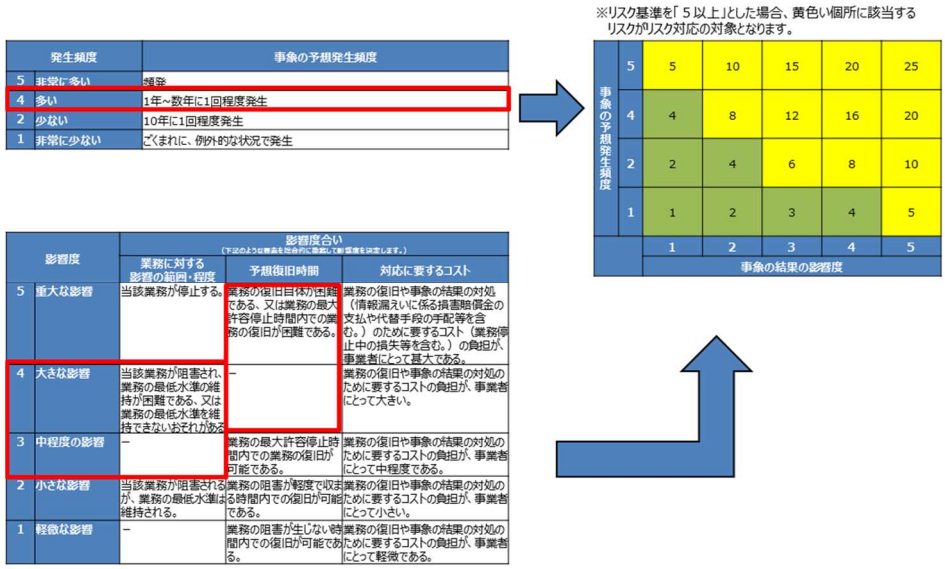
影響度		影響度合い（下記のような影響度を総合的に勘案して影響度を決定します。）		
		業務に対する影響の範囲・程度	予想復旧時間	対応に要するコスト
5	重大な影響	当該業務が停止する。	業務の復旧自体が困難である。	業務の復旧や事象の結果の対処（情報漏えいに係る損害賠償金の支払や代替手段の手配等を含む。）のために要するコスト（業務停止中の損失等を含む。）の負担が、事業者にとって甚大である。
4	大きな影響	当該業務が阻害され、業務の最低水準の維持が困難である。	業務の最大許容停止時間内での業務の復旧が困難である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって大きい。
3	中程度の影響	当該業務が阻害され、業務の最低水準を維持できないおそれがある。	業務の最大許容停止時間内での業務の復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって中程度である。
2	小さな影響	当該業務が阻害されるが、業務の最低水準は維持される。	業務の阻害が軽度で収まる時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって小さい。
1	軽微な影響	－	業務の阻害が生じない時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって軽微である。

※リスク基準を「５以上」とした場合、黄色い個所に該当するリスクがリスク対応の対象となります。

事象の予想発生頻度 ＼ 事象の結果の影響度	1	2	3	4	5
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

（例２）

（例１）のリスク基準をベースとして、大会開催期間における事象の発生が過小評価されないように、「数年に１回程度発生」を「１年に１回程度発生」と同等の基準とするように修正しています。また、影響度合いにおいて、「業務の最低水準を維持できないおそれがある」及び「業務の最大許容停止時間内での業務の復旧が困難である」場合についても、過小評価されないように修正しています。



発生頻度		事象の予想発生頻度
5	非常に多い	頻発
4	多い	1年～数年に1回程度発生
2	少ない	10年に1回程度発生
1	非常に少ない	ごくまれに、例外的な状況で発生

影響度		影響度合い（下記のような影響度を総合的に勘案して影響度を決定します。）		
		業務に対する影響の範囲・程度	予想復旧時間	対応に要するコスト
5	重大な影響	当該業務が停止する。	業務の復旧自体が困難である、又は業務の最大許容停止時間内での業務の復旧が困難である。	業務の復旧や事象の結果の対処（情報漏えいに係る損害賠償金の支払や代替手段の手配等を含む。）のために要するコスト（業務停止中の損失等を含む。）の負担が、事業者にとって甚大である。
4	大きな影響	当該業務が阻害され、業務の最低水準の維持が困難である、又は業務の最低水準を維持できないおそれがある	－	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって大きい。
3	中程度の影響	－	業務の最大許容停止時間内での業務の復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって中程度である。
2	小さな影響	当該業務が阻害されるが、業務の最低水準は維持される。	業務の阻害が軽度で収まる時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって小さい。
1	軽微な影響	－	業務の阻害が生じない時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって軽微である。

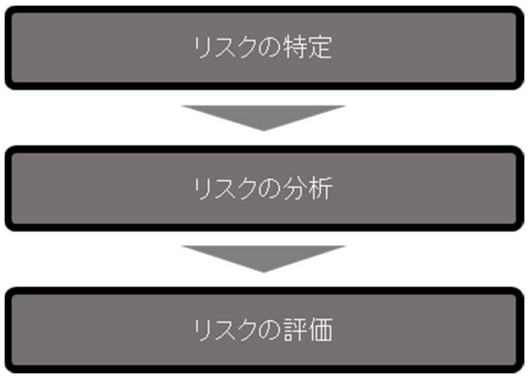
※リスク基準を「５以上」とした場合、黄色い個所に該当するリスクがリスク対応の対象となります。

事象の予想発生頻度 ＼ 事象の結果の影響度	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
2	2	4	6	8	10
1	1	2	3	4	5

６．リスクアセスメント

本章では、「重要サービスの提供に必要な業務に係る経営資源を整理した上、その経営資源に係るリスクを特定、分析及び評価」するための作業の実施手順を記載します。

＜１＞作業ステップ



＜２＞実施手順

（１）リスクの特定

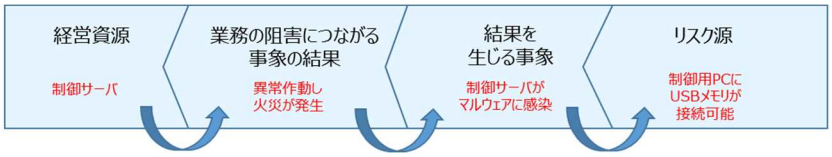
次のステップに沿って、演繹的にリスク源を洗い出します。

①重要サービスの提供に必要な業務に係る経営資源に対し、「業務の阻害につながる事象の結果」を書き出します。

②上記①の「結果を生じ得る事象」を書き出します。

③上記②の事象と合わせて上記①の結果を生じ得る「リスク源」を書き出します。

＜例＞制御サーバを経営資源とした際の作業イメージ



＜２０２０年オリンピック・パラリンピック東京大会に向けての対応＞

『（様式６）リスクアセスメント』を用いて、『（様式５）業務を支える経営資源の特定』で洗い出した経営資源（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を特定します。

（２）リスクの分析

次のステップに沿って、「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。

①事象の結果が重要サービス・業務に及ぼし得る影響について、その内容を書き出し、「５．リスク評価方針の策定」において定めた評価軸に基づく評価を行います（※）。

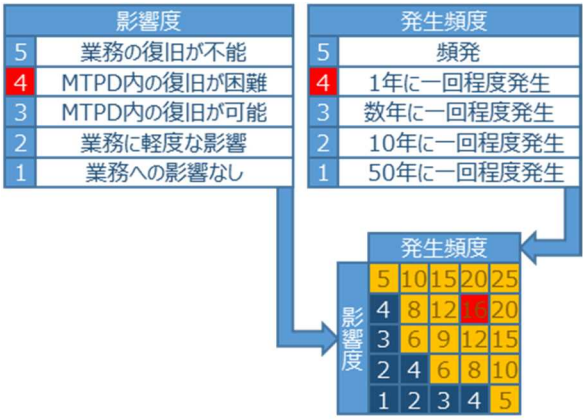
②事象の発生可能性について、「５．リスク評価方針の策定」において定めた評価軸に基づく評価を行います（※）。

③上記①及び②の結果を踏まえ、「５．リスク評価方針の策定」において定めた評価マトリクスに基づき、リスク源ごとの残留リスク値を導出します。

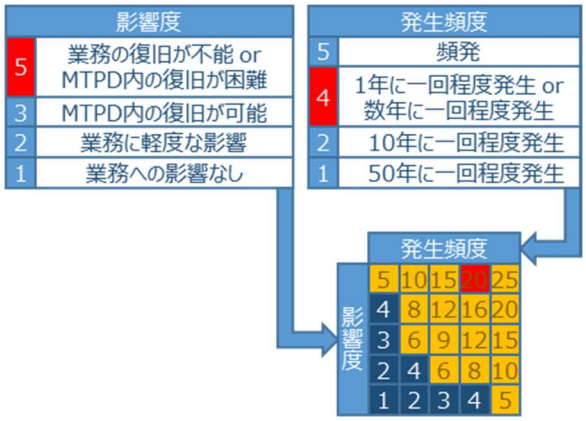
（※）何らかの対策を講じている場合であっても、技術の進歩により対策の有効性が陳腐化しやすいという情報セキュリティ対策の性質を考慮し、対策前の評価（固有リスク）及び対策後の評価（残留リスク）の両方を行います。

＜例＞リスク分析のイメージ

（Ａ）Ｐ．１７の（例１）のリスク基準を用いたリスク分析



（Ｂ）Ｐ．１７の（例２）のリスク基準を用いたリスク分析



＜大会に向けての対応＞

『（様式６）リスクアセスメント』を用いて、「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・評価し、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。

（３）リスクの評価

次のステップに沿って、「リスク対応の実施対象とするリスクを特定」します。ここでは、洗い出されたリスクから、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選別し、そのリスクに係る組織内の責任主体を明確化することが作業目的となります。

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、個別事情についても勘案（※）した上、リスク対応の実施対象とするものを抽出します。

（※）リスク基準は、あくまでリスク対応の優先度に係る判断の目安であり、実際のリスク評価の際には、個別の事情に応じて適宜に判断します。

③上記①及び②で抽出されたリスク（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）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。

（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、定期的にモニタリングを行い、リスクアセスメントの継続的な見直しの中で再評価を行います。
なお、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。

＜大会に向けての対応＞

『（様式６）リスクアセスメント及びリスク対応方針の決定』を用いて、「リスク基準」以上の「残留リスク値」のリスク源を抽出し、そのリスクのリスクオーナーを定めます。

＜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）

リスク対応では、対象とするリスクに対して、どのような対処を、いつまでに行うかを明確にします。対処の方法には、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。各リスクについて、これらの対処方法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。

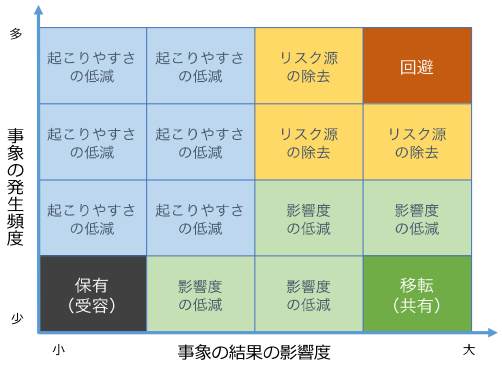
＜リスク対応の選択肢＞

対処方法	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。	
＜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。）	リスク・ファイナンス
＜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。

効果的なリスク対応を実現するためには、事象の発生可能性や事象の結果の影響度合いなどに応じて、適切な対策を講じることが必要です。事象の発生頻度及び事象の結果の影響度合いのいずれも大きいと判断されたリスクについては、そのリスクの大きさを小さくするための努力をするよりも、むしろリスク回避をした方が望ましいという考え方もあります。また、発生頻度が低いものの、影響度が大きいといった場合には、サイバー保険等を活用したリスク移転（共有）が望ましいという考え方もあります。こうした考え方を整理すると、発生可能性と影響度に応じて、一般的には、下図のように表すことができます。

＜発生頻度及び影響度に応じたリスク対応（例）＞



なお、リスク対応の選択肢の同定は、必ずしも択一ではなく、複数の選択肢に跨る対処を実施することがあります。特に重要サービス事業者等における機能保証の観点からは、リスクの低減若しくは分散又はこれらの組合せにより、リスクの回避を選択しないための最大限の努力を払うことも必要です。

また、例えば情報漏えいのような事象においては、事象の結果の影響度が低く、かつ、事象の発生頻度が高いと分析された場合であっても、起こりやすさの低減が必ずしも合理的なリスク対応でなく、セキュリティパッチの適用等のリスク源の除去を講じた方が費用や効果の面でより合理的なリスク対応であるケースもあります。

最終的には、事業者等の活動目的や利害関係者からの要求事項等を勘案して意思決定することになりますが、こうした考え方を念頭に置きながら、リスク対応の選択肢の同定について検討することが重要です。

7．リスクアセスメントの妥当性確認・評価

本章では、「リスクアセスメントの妥当性確認・評価」の実施手順を記載します。

リスクアセスメントの結果には、作業者の立場や知識・経験に基づく偏り（バイアス）や、複数の作業者で作業を分担することなどによる粒度や精度のばらつきが生じることがあります。こうした偏りやばらつきを解消し、リスクアセスメントの実施主体において、その実施内容が目的達成に向けて妥当であることを保証するためには、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、その結果を共有することが必要です。

また、効果的なリスクアセスメントの実現には、リスクアセスメント作業が適切かつ十分に実施されたかどうかを客観的に評価した上、その結果を関係者にフィードバックし、改善につなげることが重要です。一般的に、ある取組に対して評価を行う場合、ストラクチャー（構造）、プロセス（過程）及びアウトカム（成果）の各観点から実施されますが、リスクアセスメントの評価においては、成果の有効性（リスクアセスメントの目的がどれだけ達成されたか）を評価することが困難であることから、「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順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の妥当性を確認します。

こうした妥当性確認のための取組として、本ガイドラインでは、「ウォークスルー」による分析結果の検証及び「パフォーマンス評価」による実施体制や活動内容の評価を紹介します。

＜妥当性確認の手法＞

妥当性確認の手法	概要	主な実施主体
ウォークスルー	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・合意するための取組。サービス提供を支える業務や経営資源に係る職務分掌の確認や部門間の連係状況の相互理解を目的とする関係主体間のコミュニケーションを含みます。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門） （注）関連業務の所管部門、経営資源の利用部門、法務部門、リスク管理部門等もレビュー役として参画する
パフォーマンス評価	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の妥当性を確認する取組 （※）本ガイドラインでは、ISO22301、ISO27001 等で採用されているＩＳＯマネジメントシステムの上位構造（High Level Structure：ＨＬＳ）を参考として、この取組を「パフォーマンス評価」（Performance Evaluation）と称します。	・リスクアセスメント監査部門（内部監査部門等のリスクアセスメントの管理・推進の妥当性を第三者的立場から確認する部門）

＜１＞作業ステップ

＜２＞実施手順

（１）ウォークスルー

ウォークスルーは、複数の関係主体を交えたリスクアセスメントの妥当性確認のための取組として、前ステップ「６．リスクアセスメント」に係る作業が完了した後、リスクアセスメントの実施目的の確認からリスクアセスメント（リスクの評価）までの一連の取組を対象として、次のような流れで実施します。ただし、対象範囲及び実施のタイミングについては、例えば規模の大きな組織において効率的に作業を進めるため、作業の中途で担当者の範囲を限定した簡易的なウォークスルーを実施するなどの工夫を行うことが望ましいです。

①担当者の選任及び役割分担

ウォークスルーを実施する担当者（以下「ウォークスルー担当者」と総称します。）を選定します。ウォークスルーを円滑に実施するためには、役割分担した上、役目に応じた適切な担当者がウォークスルーに参画することが重要です。

＜ウォークスルーにおける主な役割・役目＞

役割	役目	担当部門（例）
まとめ役	ウォークスルーの推進役として、ウォークスルーを実施する担当者の選任に係る調整、スケジュールの調整、確認観点の整理、レビュー対象成果物の手配等を行います。また、ウォークスルーの結果を踏まえたリスクアセスメント結果の修正等について、リスクアセスメント推進担当部門のフォローアップを行います。	・リスクアセスメントの推進事務局
説明役	ウォークスルーを実施する各担当者に対し、レビュー対象成果物の記載により可視化されたリスクアセスメントの実施目的並びに重要サービスを支える業務・経営資源及びリスクの関係性についての説明を行います。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門）
レビュー役	説明役からの説明を踏まえ、レビュー対象成果物の記載内容に対し、確認観点に基づく指摘を行います。 リスクアセスメント結果の粒度や精度のばらつきを抑えるという観点から、リスクアセスメントシートの作成者（リスクアセスメント推進担当部門）だけでなく、リスクアセスメントシートの作成者の所属部門以外の者、とりわけ関連業務の所管部門や経営資源の利用・管理部門等の参画が必要です。また、総合的な判断に基づき重要サービスの選定やリスク評価がなされていることを確認する観点から、必要に応じて、経営企画部門、法務部門、リスク管理部門、広報（ＩＲ）部門等の間接部門からもレビュー役を任命することが重要です。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門） ・企画部門 ・サービスを所管する部門 ・サービスの提供に必要な業務を所管する部門
記録役	ウォークスルーの議事内容、指摘事項等の記録を行います。	・リスクアセスメントの推進事務局

（※）同一の担当者が複数の役割を務めたり、ここに記載されていない役割を設置したりすることがあります。

②事前準備（確認観点等の周知）

各関係主体がリスクアセスメントの結果（リスクアセスメントシートの記載内容）の正当性を確認し、結果についての認識を正しく共有及び合意するために、事前に、ウォークスルーにおける確認観点を策定した上、ウォークスルーを実施する各担当者に周知しておくことが必要です。

＜ウォークスルーにおける確認観点（例）＞

確認の目的	確認観点（例）
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。 ・重要サービスの選定に当たり、自組織の活動目的、大会の開催に伴う経営環境の変化、関連法令その他の要求事項等を踏まえた判断がなされているか。また、その判断根拠が客観的に成果物から読み取れるか。 ・重要サービスが完全停止した場合の影響について、直接の取引先だけでなく、エンドユーザー等も考慮に入れて判断がなされているか ・重要サービスの提供に必要な業務について、直接的に顧客との接点がある業務に限らず、間接業務についても考慮されているか ・リスクの分析において、固有リスクの評価がなされているか
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、共有認識の醸成を妨げるような記述（主語や目的語が明確でない、複数の解釈が可能な書き振りとなっているなど）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（専門性の高い用語を用いているにもかかわらず、対外的に通用する補足説明がないなど）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

③ウォークスルーの実施

ウォークスルーを実施する各担当者が、それぞれの役割に基づき、確認観点を踏まえた指摘事項を出し合い、互いが持っているリスクに対する認識をすり合わせ、必要な修正事項を導き出します。

また、次回以後の取組における効率性の向上に向けて、リスクアセスメント作業において体制面や実行面での反省点（改善すべき点）を確認します。

④レビュー対象成果物の修正

ウォークスルーで出された指摘事項を踏まえた修正事項について、レビュー対象成果物の作成者が修正を行います。

⑤ウォークスルー結果のまとめ

ウォークスルーの実施結果については、各関係主体間で共有されるだけでなく、「（2）パフォーマンス評価」において、一連のリスクアセスメント活動に係るプロセスの妥当性を評価するためのレビュー対象成果物となります。このため、まとめ役は、ウォークスルーの実施に係る証跡として、次の成果物を作成します。

＜ウォークスルーの実施に係る証跡（例）＞

証跡となる成果物	概要
ウォークスルー記録票	ウォークスルーの実施プロセスに係る証跡として、開催日時、レビュー対象、参加者の所属・氏名・ウォークスルーにおける役割、議事内容等を記録します。
ウォークスルー指摘事項一覧表	ウォークスルーの実施内容に係る証跡として、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します。

⑥各関係主体へのフィードバック

まとめ役は、ウォークスルーに係る一連の作業が完了した後、『ウォークスルー記録票』及び『ウォークスルー指摘事項一覧表』を各関係主体と共有します。

（２）パフォーマンス評価

パフォーマンス評価は、独立した担当者によるリスクアセスメントの妥当性確認の取組として、ウォークスルーの完了後、次のような流れで実施します。

①評価担当者の選任

パフォーマンス評価の一連の作業を実施する評価担当者を選任します（担当者数については、自組織の規模等に応じて判断します）。評価担当者の選任に当たっては、次に掲げる観点を考慮することが重要です。

＜評価担当者の選任に当たり考慮すべき主な観点＞

考慮すべき観点	趣旨
評価担当者の独立性	会計監査や業務監査等と同様、パフォーマンス評価は、前ステップまでのリスク評価作業から独立した担当者が行うことによって公正性・客観性が確保され、ひいてはリスクアセスメントの品質向上に寄与すると考えられます。このため、事業部門から独立した内部監査部門等を有しない中小規模の事業者等においては、コンサルタント企業等の外部の専門家を活用することも有効です。
必要な能力・知識	パフォーマンス評価では、ストラクチャー及びプロセスの評価を行うことから、担当者には基本的なドキュメント読解力やフィードバック時の関係者への説明力等が要求されます。後述の観点を参考に評価を行う限りにおいては、ＩＴや情報セキュリティに関する高度な専門知識は不要と考えます。

②パフォーマンス評価の実施

パフォーマンス評価では、公正性・客観性の確保やリスクアセスメント推進担当部門の負担軽減といった観点から、前ステップ及びウォークスルーまでの作業における各成果物を確認することを基本とします。具体的には、「リスクアセスメントシート」の記載に係る品質の確認を行い、あわせて「ウォークスルー記録票」及び「ウォークスルー指摘事項一覧表」を参照することにより、リスクアセスメントシートの記載内容について関連部門間で認識が共有され、リスク対応の実施対象とするリスクについて合意がとれていること（合意形成のプロセスが適切であること）などを確認します。

なお、各成果物の確認作業は、次に例示したような観点を踏まえて実施することを推奨します。

＜ウォークスルーにおける確認観点（例）＞

対象成果物	確認観点（例）
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。 ・全ての記載項目について、回答者（記入者）及びその責任者の名前が漏れなく明記されているか ・リスク評価を先送りにした（リスク評価の対象としなかった）サービス又は業務がある場合、コメント欄等に妥当性のある理由が明記されているか。また、責任者が先送りを承認していることが確認できるか。

	・リスク評価の対象とするリスクに対し、リスクオーナーが定められているか。また、リスクオーナーとして、そのリスクの影響範囲等を踏まえた適切な部門や役職員が選任されているか。
ウォークスルー記録票	・全てのリスクアセスメント推進部門がウォ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（サービスの提供、サービスの提供に必要な業務及び業務に係る経営資源に関し、一定の職務経験や知識を有する者）がウォ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ウォークスルーに参加し、レビューを実施しているか。 ・ウォークスルーの実効性（形骸化していないこと）を確認する観点から、各ウォークスルー担当者が、それぞれの役割に基づき、確認観点を踏まえた指摘事項を出しているか。また、リスクアセスメントシートに記載された内容のボリュームに照らし、適当な時間・回数で実施されているか。 ・ウォークスルーの実施結果は、経営層に対し適切に報告されているか（又は経営層がウォークスルーに参加し、レビューを実施しているか）
ウォークスルー指摘事項一覧表	・ウォ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。

③パフォーマンス評価結果のまとめ

パフォーマンス評価の結果として、反省点（改善すべき事項）等が発見された場合には、各関係主体へのフィードバックに備え、リスト化しておきます。

④各関係主体へのフィードバック

評価担当者は、パフォーマンス評価に係る一連の作業が完了した後、パフォーマンス評価結果を各関係主体と共有します。その際、後続で検討するリスク対応の最終責任者である経営層に対しても、同結果を共有することを推奨します。

また、リスクアセスメントに係る取組において良かった点についても共有することが望ましいと考えます。良かった点が各関係主体に認識され、水平展開されることによって、リスクアセスメントの更なる品質向上が期待できます。

８．リスクアセスメントの継続的な見直し

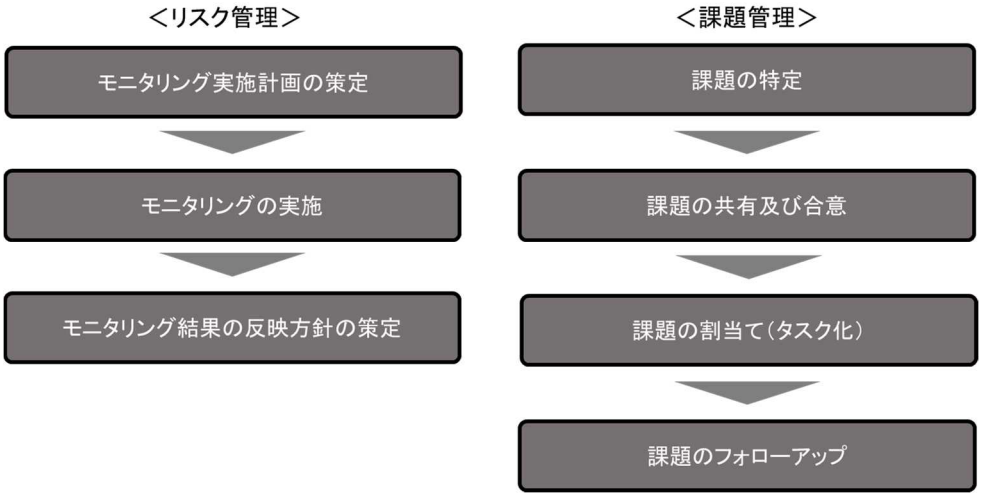
リスクアセスメントの結果として認識された状態は、経時的に変化すると予想されます。リスクアセスメントを変更又は無効なものとするおそれのある状況及びその他の要因を特定し、リスクの変動に適切に対処するためには、「リスクアセスメント結果を継続的にモニタリング（リスクアセスメントの結果として認識された状態との差異を特定するために、状態を継続的に点検し、監督し、要点を押さえて観察し、又は決定する取組）を実施し、必要に応じて適宜にリスクアセスメント結果の見直しを実施する」など、リスクを適切に管理し、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要です。

また、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。

本章では、「リスクアセスメントの継続的な見直し」に向けたリスク管理及び課題管理について、参考になる実施手順を記載します。

なお、次回以後のリスクアセスメントの際には、モニタリングや課題等の確認の結果を踏まえ、必要な体制や運用の見直しを行います。

＜１＞作業ステップ



＜２＞実施手順

（１）リスク管理

①モニタリング実施計画の策定

リスクアセスメントシートに記載されたリスクアセスメント結果について、モニタリングを行うため、その実施計画を策定します。

なお、実施計画には、モニタリングの結果を踏まえた、次回以後のリスクアセスメント作業に向けた対応方針の策定に係る計画を含みます。

②モニタリングの実施

リスクオーナーは、モニタリング実施計画に基づき、モニタリングを実施します。モニタリングについては、リスク評価により特定されたリスク（リスク対応の実施対象とするリスク）に係るリスク対応のフォローアップに限らず、当該リスクの評価に至る一連の取組において洗い出された事項の全て（各リスクアセスメントシートに書き出された事項の全て）を対象として実施することを基本とします。

なお、モニタリングの実施に際しては、次に掲げる観点を踏まえることを推奨します。

・リスクアセスメントを実施した際に前提としていた外部環境の変化に起因する状態の変動。なお、技術的な環境の変化だけでなく、経済的、政治・法律的及び社会的な環境の変化についても考慮することが必要です。

・リスクアセスメントを実施した際に前提としていた内部環境の変化に起因する状態の変動。とりわけ、事業者等の活動目的、リスクアセスメントの実施目的、サービスの経営上の位置付け（業績への寄与度や事業上の依存度等の事業経営上の位置付け）、利害関係者（顧客、仕入先、株主、地域社会等）からのニーズ・期待等の変化を考慮することが重要です。

③モニタリング結果の反映方針の策定

モニタリングの結果を踏まえ、次回以後のリスクアセスメント作業に向けた対応方針を策定します。

（２）課題管理

リスクアセスメント推進部門は、次の手順で課題の管理を行います。

①課題の特定

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反省点（改善すべき点）等について、その原因を分析し、課題として特定します。この際、特定された課題については、課題管理表に登録します。

②課題の共有及び合意

特定された課題について、各関係主体間で共有し、その課題の内容、解決策、優先順位等を合意します。

③課題の割当て（タスク化）

課題の解決策を独力で解決可能な作業（タスク）単位に分割し、各タスクを作業担当者に対し、解決期限を定めて割り当てます。

④課題のフォローアップ

タスクが完了するまで継続的に監視し、経過及び結果を記録します。

また、期限を超過しても完了していないタスクがある場合、そのタスクの遅延による影響の範囲を分析し、課題として課題管理表に登録するなど、必要な対処を行います。

付録Ａ．用語の説明

用語	説明
イベントツリー分析	所与の単一の原因から生じる複数の潜在的な結果を分析する手法。ある初期事象からスタートして、いろいろな経路をとることにより結果がどうなるかを明らかにするもの。
経営層	最高位で組織を指揮し、管理する個人又は人々の集まり。 （会社の場合には、業務を執行する取締役、執行役等の機関及びこれらに準じる重要な使用人（執行役員等の役職に就いている者）などが該当する。）
固有リスク	リスク対応を講じる前又は講じていないと想定した状態における本来有するリスク。
最大許容停止時間	製品・サービスを提供しない、又は事業活動を行わない結果として生じる可能性のある悪影響が、許容不能な状態になるまでの時間。
サプライ・チェーン	組織の壁を越えたサービス提供に関わる一連の活動又は関係者。
残留リスク	リスク対応後に残るリスク。
事象	ある一連の周辺状況の出現又は変化。
事象の結果	目的に影響を与える事象の結末。
詳細リスク分析	資産ごとに関連するリスクの解析を実施するリスク分析のアプローチ。
バリュー・チェーン	サービスの提供に関係する事業活動を機能単位に分割して捉え、その役割と流れに沿って体系化するもの。
フォールトツリー分析	望ましくない結果をもたらす原因をトップダウンで体系的に探究する手法。事象の結果の発生原因、潜在的に発生の可能性がある原因又は発生の要因を抽出し、事象の結果の発生条件及び要因の識別及び解析を行うもの。
利害関係者	ある決定事項又は活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している個人又は組織。
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。
リスク許容度	自らの目的を達成するため、リスク対応の後のリスクを負う組織又はステークホルダーの用意している程度。
リスク源	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。 なお、リスク源は、有形の場合も無形の場合もある。
リスク選好	組織に追求する又は保有する意思があるリスクの量及び種類。
リスク対応	リスクを修正するプロセス。
リスク特定	リスクを発見、認識及び記述するプロセス。 なお、リスク特定には、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれます。
リスク評価	リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。
リスク分析	リスクの特質を理解し、リスクレベルを決定するプロセス。 なお、リスク分析は、リスク評価及びリスク対応に関する意思決定の基礎を提供する。
リスクレベル	事象の結果の影響度とその起こりやすさ（発生頻度）との組合せとして表わされるリスク又は組み合わさったリスクの大きさ。 なお、リスクレベルを定量化（数値化）した評価をリスク値といいます。

付録Ｂ．参考文献

[1] JIS Q 31000:2010, リスクマネジメント－原則及び指針.
（注）対応国際規格：ISO 31000:2009, Risk management－Principles and guidelines.

[2] JIS Q 31010:2012, リスクマネジメント－リスクアセスメント技法.
（注）対応国際規格：ISO 31010:2009, Risk management－Risk assessment techniques.

[3] JIS Q 0073:2010, リスクマネジメント－用語.
（注）対応国際規格：ISO Guide73 2009, Risk management－Vocabulary.

[4] ISO/IEC 27005:2011, Information technology－Security techniques－Information security risk management.

[5] JIS Q 22301:2013, 社会セキュリティ－事業継続マネジメントシステム－要求事項
（注）対応国際規格：ISO 22301:2012, Social security－Business continuity management systems－Requirements

[6] 勝俣良介著（2012）『ISO22301 徹底解説―BCP・BCMS の構築・運用から認証取得まで―』ニュートン・コンサルティング監修, オーム社.

[7] リスクマネジメント規格活用検討会編著（2014）『ISO 31000:2009 リスクマネジメント 解説と適用ガイド』日本規格協会.

[8] 佐藤学・羽田卓郎・中川将征（2013）『ISO 22301 で構築する事業継続マネジメントシステム』日科技連出版社.

[9] 畠中伸敏編著（2008）『情報セキュリティのためのリスク分析・評価 第２版―官公庁・金融機関・一般企業におけるリスク分析・評価の実践―』日科技連出版社.

[10] 内閣官房内閣サイバーセキュリティセンター(2015)『重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）』, ＜http://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf＞

資料３添付資料-別紙１　業務の阻害につながる事象の結果の例 v1.0.0

業務維持のために経営資源に求められる観点		業務の阻害につながる事象の結果の例 （経営資源：顧客データベース）
分類	考え方	
可用性	許可された利用者が、必要な時に経営資源を利用できること。	・顧客データベース上のデータが消失する ・顧客データベースの応答が滞る
完全性	経営資源及び経営資源に含まれる情報に誤りがなく（正確であり）、欠損や不整合がないこと（完全であること）。	・顧客データベースに誤ったデータが記録される ・顧客データベースから誤ったデータが応答される
機密性	正当な権限をもつ限られた者のみが、経営資源及び経営資源に含まれる情報を利用できること。	・顧客データベース上の機密データが社外に漏えいする
その他		

資料３添付資料-別紙２　結果を生じる事象（脅威）　v1.0.0

大分類	中分類	小分類		結果を生じうる事象（脅威）の例
環境に起因する脅威	災害	自然現象による災害		地震、火災、風水害、落雷、動物害、温度・湿度異常
	障害	設備障害		停電、瞬断、施設内火災、漏水、空調機器の故障、入退出管理装置の故障、監視カメラの故障
		ハードウェア障害		メモリ障害、ディスク障害、CPU障害、電源装置障害、ケーブル劣化、メモリやディスクの容量オーバー
		ソフトウェア障害		OSやアプリケーションの潜在的なバグ・過負荷等による異常
		ネットワーク障害		回線障害（専用回線・公衆回線の障害）、通信事業者（接続局、ISP、NOC、IDC等）内での障害、通信機器障害、構内配線の障害
人に起因する脅威	意図的	外部不正	不正侵入	SQLインジェクション、OSコマンドインジェクション
			なりすまし	パスワードクラック、ソーシャルハッキング
			マルウェア感染	スパイウェア、ランサムウェア
			妨害	DoS攻撃
			盗聴	ネットワーク盗聴
		内部不正	システムの不正利用	不正なデータ操作、機密情報の不正な閲覧
			データの不正持ち出し	機密情報の不正持ち出し、データの意図的な外部送信
			システムの破壊	データを破壊するマルウェアのインストール
	偶発的	操作ミス		メール誤送信、マルウェア付きメールの開封、重要データの消去、意図しないシステム停止
		遺失・紛失		持ち出し媒体の置き忘れ、管理不備による媒体の紛失
		不適切な廃棄		廃棄した媒体からの復元
		許可されない機器・媒体・プログラムの持ち込み		マルウェアに感染した機器を社内ネットワークに接続
		意図しない情報公開		Webサーバの設定不備による重要データの流出
		任務怠慢		既定の操作の実行忘れ

［資料３添付資料-別添１］　2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施結果提出様式（レポート） v1.0.1

会社名	記入日

報告者			責任者	
所属組織	氏名	連絡先	氏名	役職
		03-****-**** example1@example.co.jp		
		03-****-**** example2@example.co.jp		
		03-****-**** example3@example.co.jp		
		03-****-**** example4@example.co.jp		
		03-****-**** example5@example.co.jp		

A. 実施期間及び実施体制について

① 実施にあたり要した期間/稼働

開始時期（年/月/日）　～　終了時期（年/月/日）　　稼動 約　人日

② 実施にあたり関係した部門 （枠内に参加された人数を記入願います）

a) 経営企画部門　人　　b) 情報システム部門　人

c) 総務部門　人　　d) サービス主管部門　人

e) その他の部門 （参加された人数についても合わせて記入願います）

B. 実施手続き及び活動状況について

※実施状況を選択願います。実施しない場合や独自の方法で実施した場合は、『実施しない』を選択し、理由等を記入願います。

状況

① 『2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的』を踏まえ、自組織の活動目的を設定しましたか？

「実施した」とご回答いただいた方へ

①-1 「自組織の活動目的」に落とし込んだ実施目的を選択願います。　該当するものにチェック（複数選択）

- 会場設営が予定通り実施できること
- 開閉会式のプログラム、各競技が予定通り安全に実施できること
- 選手の能力の発揮に必要な環境を提供すること
- 会場で観戦する来賓・観客の不満なく安全な観戦に必要な環境を提供すること
- 会場にいなくても大会を楽しむために必要な環境を提供すること

①-2 上記の実施目的以外で、独自に設定したリスクアセスメントの実施目的がある場合は記入願います。

「実施予定」とご回答いただいた方へ

①-4 実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

①-5 理由を記入願います。

状況

② リスクアセスメントの実施方針を設定し、経営層及び関係部門において確認しましたか？

「実施した」とご回答いただいた方へ

②-1 リスクアセスメントの実施方針を決定した主体を記入願います。

「実施予定」とご回答いただいた方へ

②-2 実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

②-3 理由を記入願います。

状況

③　①の「自組織の活動目的」を踏まえ、重要サービスを特定しましたか？

「実施した」とご回答いただいた方へ

③-1　特定した重要サービスを**別紙A**に記入願います。

「実施予定」とご回答いただいた方へ

③-2　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

③-3　理由を記入願います。

状況

④　③の各重要サービスを支える業務を洗い出しましたか？

「実施予定」とご回答いただいた方へ

④-1　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

④-2　理由を記入願います。

状況

⑤　④の各業務を支える経営資源（情報資産）を洗い出しましたか？

「実施した」とご回答いただいた方へ

⑤-1　情報資産として、制御システムについても洗い出していますか？

「実施予定」とご回答いただいた方へ

⑤-2　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

⑤-3　理由を記入願います。

状況

⑥　⑤の各経営資源（情報資産）に係るリスクを特定、分析及び評価しましたか？

「実施した」とご回答いただいた方へ

⑥-1　特定したリスクを**別紙B**に記入願います。

⑥-2　リスクの分析において対策前の評価と対策後の評価の両方を行いましたか？

⑥-3　リスク基準に満たないリスクについてもリスク対応の要否を検討しましたか？

⑥-4　リスク対応の実施対象として抽出したリスクについてもれなくリスクオーナーを設定しましたか？

「実施予定」とご回答いただいた方へ

⑥-5　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

⑥-6　理由を記入願います。

状況

⑦　リスク対応の選択肢を同定しましたか？

「実施予定」とご回答いただいた方へ

⑦-1　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

⑦-2　理由を記入願います。

状況

⑧　リスクアセスメントの実施内容の妥当性を確認しましたか？

「実施予定」とご回答いただいた方へ

⑧-1　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

⑧-2　理由を記入願います。

状況

⑨　リスクアセスメント作業の妥当性を確認しましたか？

「実施予定」とご回答いただいた方へ

⑨-1　実施予定時期を選択願います。

「実施しない」とご回答いただいた方へ

⑨-2　理由を記入願います。

C. 取組について

① 本取組を通じて得られたことがありましたら記入願います。

(例)大会に関連するサービスを会社横断的に検討し抽出することができた／日頃行っている対策に加え、大会に向けて注力すべき点が明確になった　等

② 本取組を通じて課題に感じられた点について該当する項目をチェック又は「その他」に理由を記入願います。

a) 実施担当者または関係主体がスキル不足している
b) 設定されている実施期間が短い
c) 実施のために費用が必要である
d) その他

③ 本取組を通じて洗い出されたリスクの中で、個別組織だけでは十分な対策を施すことが難しいリスクがありましたら記入願います。

④ その他実施いただいての感想や、本取組に対するご意見等ありましたら記入願います。

◆重要サービスと特定されたサービス

※「様式2」から、転記願います。

事業	サービス

◆想定したリスク

※「様式6」から、転記願います。

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

2020年東京オリンピック・パラリンピック競技大会の開催概要

v1.0.0

資料３添付資料-別添２

■ 大会の基本的な情報

項目	分類	2012ロンドン大会	2016リオ大会	2020東京大会
参加国・地域	オリンピック	204	206	未定
	パラリンピック	164	159	未定
競技数	オリンピック	26競技302種目	42競技306種目	33競技
	パラリンピック	20競技503種目	22競技528種目	22競技
チケット販売数	オリンピック	約880万枚	約750万枚	約780万枚
	パラリンピック	約270万枚	約330万枚	約230万枚
競技会場	オリンピック	34	37	34（一部調整中）
	パラリンピック	15	21	17（一部調整中）

【出典】https://www.olympic.org/london-2012、https://www.Paralympic.org/london-2012
https://www.rio2016.com/en、https://www.rio2016.com/en/paralympics
https://tokyo2020.jp/jp/games/plan/

- 2020年東京大会における参加国・地域は確定していないが、直近2大会と同等かそれ以上と想定される。
- 2016年8月3日に追加競技として「野球・ソフトボール」、「空手」、「スポーツクライミング」、「サーフィン」「スケートボード」の5競技18種目が決まったと発表された。これらの競技の会場は調整中である。
- 2020年東京大会ではオリンピック・パラリンピックで合わせて約1010万枚のチケット販売が計画されている。海外からの訪日客に限らず、多くの国民も含めた観客が国内を移動・宿泊施設等を利用することになる。
- 競技会場は東京の湾岸エリア中心であるが、サッカーの予選等、一部の競技は地方で開催される。

■ 選手や大会関係者

項目	分類	2012ロンドン大会	2016リオ大会	2020東京大会
選手数	オリンピック	約10,500人	約10,500人	–
	パラリンピック	約4,200人	約4,400人	–
大会関係者	組織委員会	約6,000人	約8,000人	約7,000人（予定）
	契約者等	約100,000人	約85,000人	–
	ボランティア	約70,000人	約70,000人	約80,000人（予定）
メディア関係者		約21,000人	–	–

【出典】https://www.olympic.org/london-2012、https://www.paralympic.org/london-2012
https://www.rio2016.com/en/athletes、https://www.rio2016.com/en/paralympics/athletes、
https://www.rio2016.com/transparencia/en/human-resources#processos-seletivos

- 2020年の東京大会における選手数は現時点では未定だが、IOCの定義もあるため直近2大会と同程度のなるものと予想される。ロンドン大会では選手を含めコーチ、大会役員を合わせて3万5千人を超える人数が英国に入国した。
- 多くのボランティア等が大会運営に携わるため、選手や観客のみならず、多くの人々が国内を移動・滞在することになる。
- 2012年のロンドン大会では、アクレディテーション（認定証）が発行されたメディア関係者だけで2万1千人だった。実際にはより大勢のメディア関係者が入国することになると想定される。

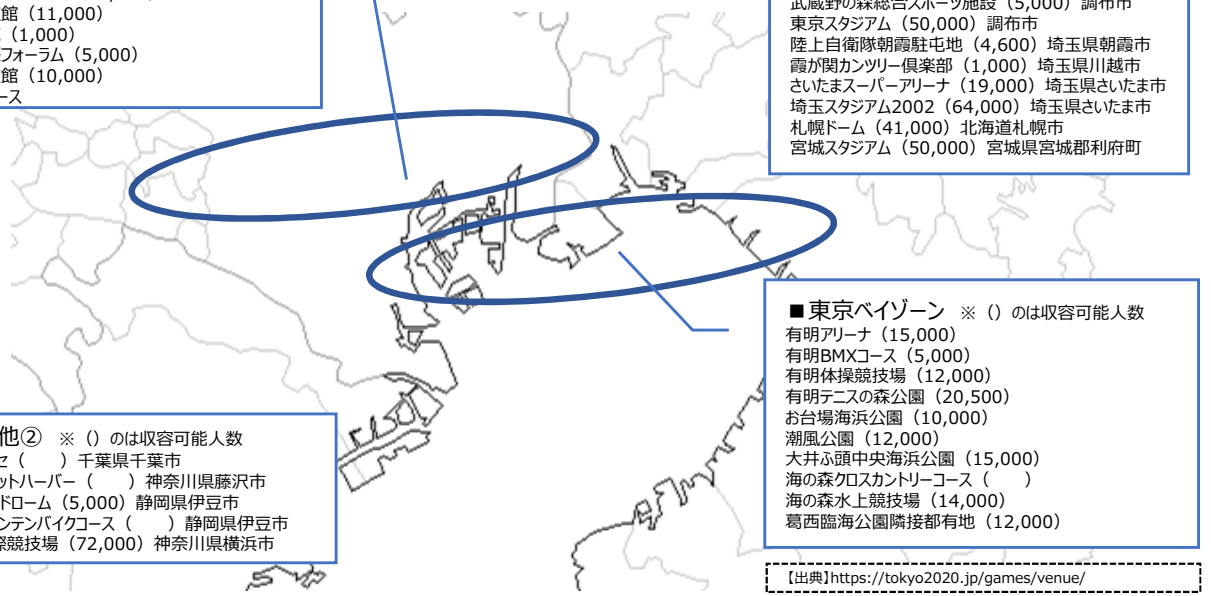
■ 観客・観光客

項目	2012ロンドン大会	2016リオ大会
観客・観光客	• ヒースロー空港の1日あたり最高到着人数 約12万7千人 • 大会期間中、最も多い日で300万人が英国に入国	• GIG空港では平均で4万人、閉会式当日は9万人の利用を予想

【出典】Oliver Hoare「LONDON2012: CYBER SECURITY」

- リオデジャネイロのGIG空港では、1日当たりの渡航者対応可能数を従来の2倍の9万人に対応可能となるように改装した模様である。
- 日本政府は2020年の訪日観光客数の目標値を2千万に設定している。大会期間中に限らず、多くの訪日客に対応可能な宿泊設備等の準備が必要になる。

2020年東京オリンピック・パラリンピック競技大会競技会場　2016年8月末時点



■ヘリテッジゾーン　※（）のは収容可能人数
オリンピック・スタジアム（68,000）
東京体育館（8,000）
国立代々木競技場（12,000）
日本武道館（11,000）
皇居外苑（1,000）
東京国際フォーラム（5,000）
両国国技館（10,000）
マラソンコース

■その他①　※（）のは収容可能人数
馬事公苑（　　）世田谷区
武蔵野の森総合スポーツ施設（5,000）調布市
東京スタジアム（50,000）調布市
陸上自衛隊朝霞駐屯地（4,600）埼玉県朝霞市
霞が関カンツリー倶楽部（1,000）埼玉県川越市
さいたまスーパーアリーナ（19,000）埼玉県さいたま市
埼玉スタジアム2002（64,000）埼玉県さいたま市
札幌ドーム（41,000）北海道札幌市
宮城スタジアム（50,000）宮城県宮城郡利府町

■東京ベイゾーン　※（）のは収容可能人数
有明アリーナ（15,000）
有明BMXコース（5,000）
有明体操競技場（12,000）
有明テニスの森公園（20,500）
お台場海浜公園（10,000）
潮風公園（12,000）
大井ふ頭中央海浜公園（15,000）
海の森クロスカントリーコース（　　）
海の森水上競技場（14,000）
葛西臨海公園隣接都有地（12,000）

■その他②　※（）のは収容可能人数
幕張メッセ（　　）千葉県千葉市
江の島ヨットハーバー（　　）神奈川県藤沢市
伊豆ベロドローム（5,000）静岡県伊豆市
伊豆マウンテンバイクコース（　　）静岡県伊豆市
横浜国際競技場（72,000）神奈川県横浜市

【出典】https://tokyo2020.jp/games/venue/

■ インターネット・放送・配信環境

2012年のロンドン大会におけるインターネットや配信状況
- 2012年のロンドン大会では220の地域でテレビ放送された
- ツイート数は1.5億回
- 公式サイトへのユニークユーザでの1日あたりの最高アクセス数は180万
- 公式サイトのページビューは47億件
- 大会期間中、イギリス各地に７０カ所以上のライブサイトが用意され、810万人が訪れた

- 公式サイト等大会の関連サイトに限らず、海外からの訪日予定者による国内サイトへのアクセスの増加が予想される。
- インターネットを利用したサービス提供は、2020年の東京大会まで拡大していくものと予想される。
- 2020年の東京大会においても東京大会に限らず、多くの場所でライブサイトを準備することが計画されている。

【出典】IOC「London 2012 Olympic Games Global Broadcast Report」
IOC [FACSHEET LONDON 2012 FACTS & FIGURES UPDATE – NOVEMBER 2012」
IET「Delivering London 2012: ICT implementation and operations」
The London Organising Committee of the Olympic Games and Paralympic Games Limited「London 2012 Report and accounts」

■ 調達

項目	2012ロンドン大会	2016リオ大会
調達	スポーツ関連設備：100万点	全体：3000万点 スポーツ関連設備：100万点 ベッド＆マットレス：4万 座席：約20万 馬：40頭

【出典】https://www.rio2016.com/transparencia/en/procurement

- 競技に関連するアイテムに限らず、大会を開催するために様々な物品が調達される。これらアイテムの調達の他、これらを運ぶ物流機能は大会の成功には欠かせない機能となる。

■ サイバーセキュリティ環境

2012年のロンドン大会において以下のサイバーセキュリティ事案が発見された。
- 23億5千万件のセキュリティ関連のログが記録された
- 2億件の悪意のある接続要求をブロック
- 構築時のウイルス検出
- 電力システムへの攻撃予告（直前で手動での対応へ切り替えた）

【出典】Oliver Hoare「LONDON2012: CYBER SECURITY」

- 世界的なビッグイベントであり注目度は高い。2016年のリオ大会でも、「Anonymous」と名乗る者らにより、大会や政府機関のWebサイトがサイバー攻撃の標的とされた。
- 攻撃手法等は刻々と変化し、脅威は深刻化する状況を鑑みると、2020年には現在以上に深刻な状況となっていることが予想される。
- 標的型攻撃やDDoS攻撃等、脅威の種類が増加。2020年に向けてIoT等の普及が進み、これら、脅威の範囲もさらに広まることが懸念される。

『2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの実施目的』

1. 会場設営が予定通り実施できること

予定通りに開閉会式及び競技を行うためには、会場設営が計画通り完了していなければなりません。

会場設営等の準備を計画通り実現していくためには、携わる人員等を確保し、円滑に業務を推進することはもちろんのこと、設営に関連する資機材等の円滑な輸送が適切に行われることも重要です。

具体的な例としては、必要な資機材等の調達を考えると、運送関連事業者によるサービス提供や関連するところとして、交通インフラ（道路・鉄道・空路・航路）及び海外からの輸入に関連する手続き等についてもサービスの継続的な提供が望まれます。

時期：主に開催前

2. 開閉会式のプログラム、各競技が予定通り安全に実施できること

大会に向けて多くのスタッフが準備に携わり、アスリートは、能力を最大限発揮するために競技に向けて準備を進めます。また、多くの観客が日本に集まり、海外メディアの報道により世界の注目が日本に集まる中で開催されることから、開閉会式や各競技は予定通り安全に実施されることが期待されます。

すべてのプログラムが予定通り安全に実施されるためには、それぞれの安全の確保や進行を支える大会組織委員会等が準備した競技システム等が安定して稼働すること及びスタッフがそれぞれの役割を果たすことが重要です。また、制御することが不可能な自然災害等に関する迅速且つ的確な情報の提供も重要です。

具体的な例としては、各会場へ供給する電力や通信等のインフラサービスや気象情報等の安定した提供、スタッフが業務に従事するために必要な移動のための交通インフラ（道路・鉄道）等の安全且つ安定したサービス提供が望まれます。

時期：期間中

3. 選手の能力の発揮に必要な環境を提供すること

世界各国の選手は、それぞれの持つ目標の達成を目指して、厳しいトレーニングや練習を通して能力を最大限に高めて大会に出場します。

選手が最高の舞台で能力を発揮するためには、競技に集中するための安全の確保はもちろんのこと、選手村における滞在及び移動等における快適な環境の提供も重要です。

具体的な例としては、各会場や選手村における電力、通信、ガス、上下水道等の日常生活においても不可欠と考えられるインフラサービス、選手の移動に関わるサービスの安全且つ安定した提供及び体調不良等が発生しても迅速に対応可能な医療サービス等の提供が望まれます。

時期：期間中

4. 来賓・観客の不満なく安全な観戦に必要な環境を提供すること

大会には各国の要人、観戦客等、多くの方々の来日が予想されるとともに、多くの国民が各会場へ足を運ぶことが予想されます。

これらの方々が目的地に予定通り安全に到着し目的の競技等に様々な形で参加するためには、計画されているインフラ整備が確実に実施されることに加え、円滑かつ安全に人員を輸送することが重要です。また、会場の各種設備はもちろん、快適な観戦環境を用意するために暑さ対策等が検討されており、それらが適切に機能することも重要です。

具体的な例としては、会場警備や防災はもちろんのこと、海外からの移動及び国内移動に欠かせない交通インフラ（道路・鉄道・空路・航路）、海外からの出入国に関連する手続き等についてもサービスの継続的な提供および各会場へ供給する電力、通信、上下水道、熱供給等のインフラサービスの安全且つ安定した提供が望まれます。

時期：開催前・期間中

5. 会場にいなくても大会を楽しむために必要な環境を提供すること

国内に限らず、世界中に大会を楽しみにしている方々がいます。会場での観戦に限らずテレビやパソコン、スマートフォン等を通じてオリンピック・パラリンピックの感動及び日本の魅力を世界中に伝えていくことになります。

この実現のためには、リアルタイムでの競技の配信や、用意するコンテンツの配信に必要な環境を整備することが重要です。

具体的な例としては、通信、放送サービスの安定したサービス提供が望まれます。

時期：期間中

注意事項

- 安定したサービス提供とは、自然災害やサイバー攻撃等に起因する IT 障害が可能な限り抑えられており、さらに IT 障害が発生した場合にも迅速な対応等により継続的にサービスが提供されることです。
- 情報セキュリティリスクに関しては、直接的には大会運営に関係しない事業者からの機微情報の漏えい等によって、大会運営を担うサービスを中断せざるを得ない事態につながるような可能性もあります。直接的に大会運営に関わらない事業者におかれても、間接的な影響についても勘案した上で、活動目標を検討してください。
- 大会に向けて、リスク低減策を講ずることは重要ですが、過剰な対策により市民生活に必要なサービスの提供が不当に制限・阻害されてしまっては本末転倒です。リスク対応にあたっては、こうした観点でも勘案し、市民生活に必要なサービスの安全且つ安定したサービス提供に影響を及ぼさないことが望まれます。