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＞

～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～

２０２３年３月

内閣官房　内閣サイバーセキュリティセンター

（空白ページ）

目次

1．はじめに

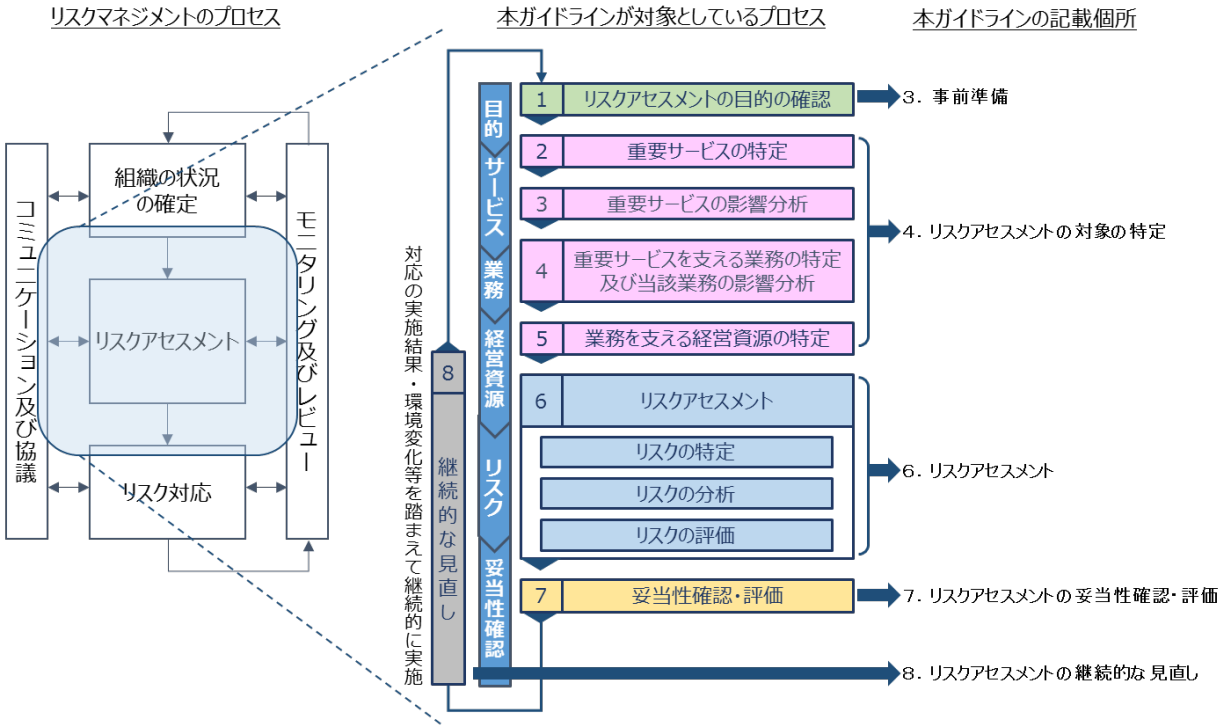
＜1＞ガイドライン策定の背景・目的

内閣サイバーセキュリティセンター（以下「NISC」という。）では、2020 年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）の開催に向けて、リスクアセスメントの実施手順を整備のうえ、東京大会の準備・運営を支えるサービスを提供する事業者等を対象にしたリスクアセスメントの実施の依頼、実施結果の分析及びフィードバックを行うことにより、リスクマネジメントの促進を図ってきました。

本ガイドラインは、東京大会で作成した実施手順を基に、東京大会固有の実施手順の削除による汎用化、及び事業者等が効果的・効率的なリスクアセスメントのアプローチを自ら選択できるように見直しを行うことで、大規模国際イベント等だけでなく、平時における情報セキュリティ確保に向けて、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の促進に活用されることを目的とします。

＜2＞ガイドラインの記載範囲

本ガイドラインでは主にリスクの特定・分析・評価といったリスクアセスメントの主要なプロセスについて記載しています。併せてリスクアセスメントの対象を特定するプロセスや、リスクマネジメントに含まれるリスクアセスメント以外のプロセスの一部についても記載しています。



＜３＞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、大規模国際イベント等及び平時における社会経済を支えるサービスを提供する事業者等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、社会経済を支えるサービスを提供する事業者等が、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（※）。

（※）社会経済を支えるサービスを提供する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。

＜４＞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	事業・重要サービス・経営資源（情報資産）の例（重要サービス分野毎）	リスクアセスメントの対象とする「事業」、「重要サービス」及び「経営資源（情報資産）」を、重要サービス分野毎に例示した参考資料
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	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」、「結果を生じ得る事象」及び「リスク源」を例示した参考資料
別紙３	結果を生じ得る事象（脅威）及びリスク源に対する対策例	リスク源に対して整備すべき対策及び運用すべき「対策」を例示した参考資料
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	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」、「結果を生じ得る事象」及び「リスクシナリオ」を例示した参考資料
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	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	利害関係者のニーズ・期待／法規制面での要求事項を分析し、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 （様式６－１）リスク源 （様式６－２）リスクシナリオ	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。）
	自己評価レポート	リスクアセスメントの実施主体自らが、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（設定シートを含む）。
	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。
別紙６	自己評価レポートの利用要領	リスクアセスメントの実施主体自らが、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、「自己評価レポート」の利用方法を解説した文書。

（※）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。

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、社会経済を支えるサービスを提供する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、「各社会経済を支えるサービスを提供する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。

社会経済を支えるサービスを提供する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、各社会経済を支えるサービスを提供する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、重要サービスの継続性を確保するための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、各社会経済を支えるサービスを提供する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、社会経済を支えるサービスを提供する事業者等に限らず、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

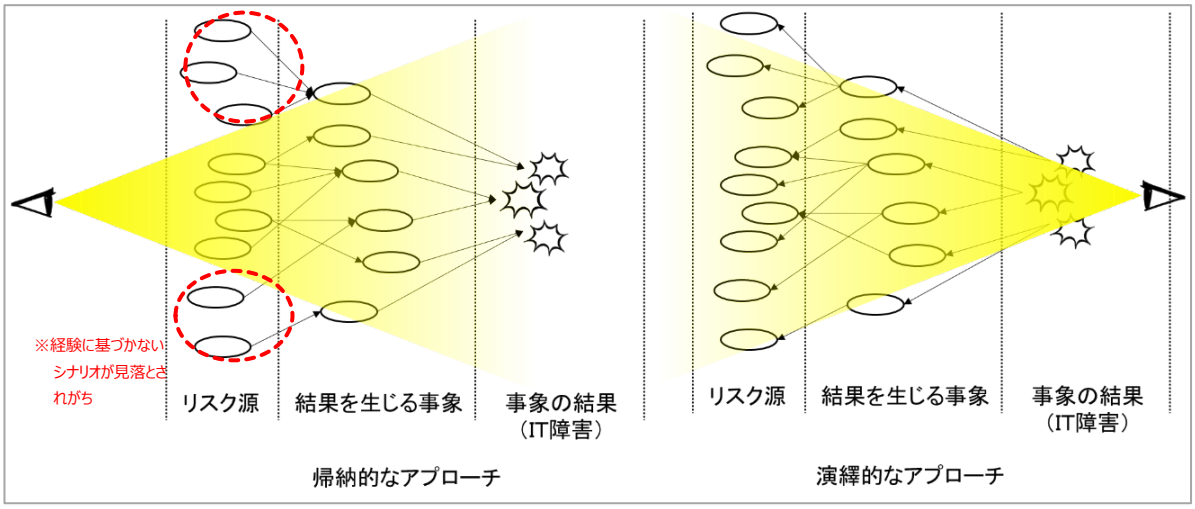
発生確率の低い事象から目を背けた（発生した場合には危機的状況につながる可能性がある事象であっても、過去に経験していない、又は発生確率が低いためにリスクとして想定しなかった）ことにより、その事象の結果が想定外となって大きな混乱を招くこととなった東日本大震災での教訓を踏まえ、上記①によるリスクの捉え方を前提として、機能保証の観点から、「事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定し、そのサービス提供の維持・継続に必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを演繹的に特定・分析・評価」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

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「事業・重要サービス・経営資源（情報資産）の例」（重要サービス分野ごと）（別紙１）、「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２）、及び「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４）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）事業・重要サービス・経営資源（情報資産）の例（重要サービス分野毎） （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
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

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。

＜重要サービスの継続性を確保するための対応＞

『（様式１）リスクアセスメントの実施目的の確認』を用いて、重要サービスの継続性を確保する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。また、大規模国際イベント等に向けては、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。

＜重要サービスの継続性を確保するための対応＞

『（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）マススター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（マススタースケジュール）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、マススター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、マススタースケジュールは、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

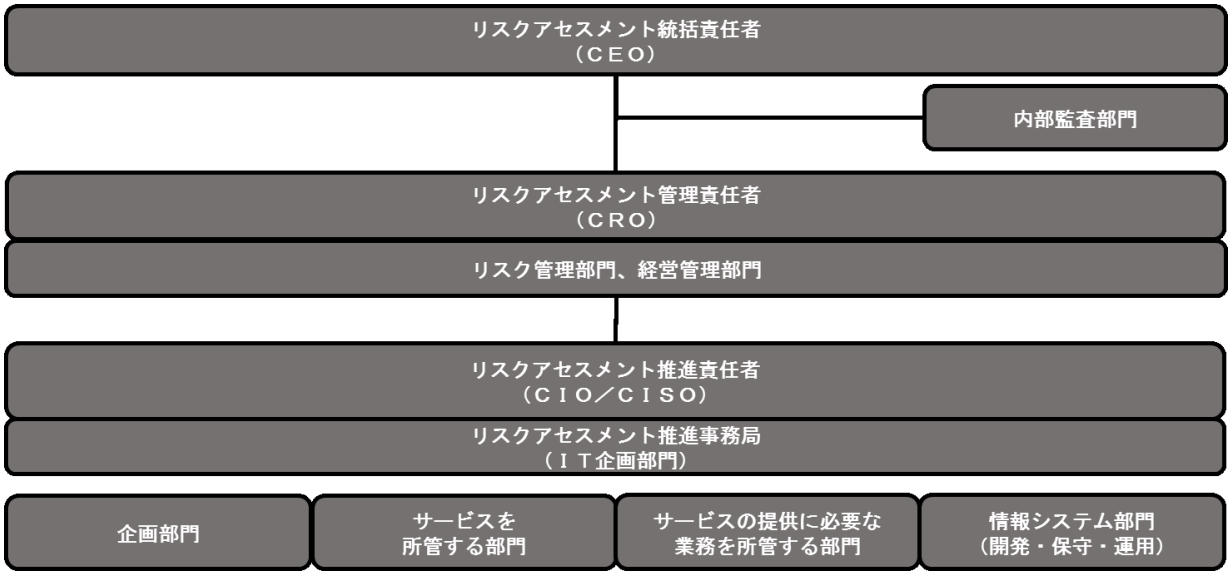
リスクアセスメントの実施方針及びマススタースケジュールを踏まえ、実施体制を構築します。実施体制の構築に際し、機能保証に向けたリスクアセスメントが経営戦略上の重要な活動であることを踏まえ、経営層が、リスクアセスメントの最高責任者として、推進及び管理を主導することが重要です。

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.〇〇事業部門	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）

（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。

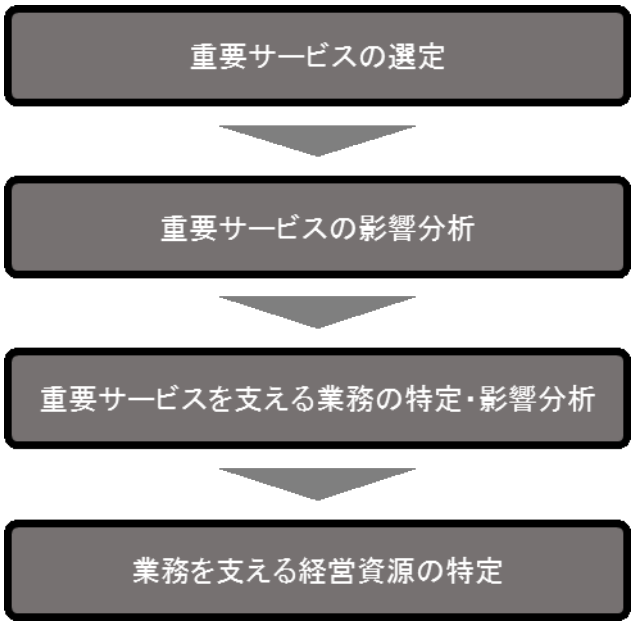
４．リスクアセスメントの対象の特定

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。

＜重要サービスの継続性を確保するための対応＞

『（様式２）重要サービスの選定』を用いて、利害関係者のニーズ・期待／法規制面で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、「事業・重要サービス・経営資源（情報資産）の例」（別紙１）等を参考に、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限許容される範囲・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。

＜重要サービスの継続性を確保するための対応＞

『（様式３）重要サービスの影響度分析』を用いて、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、大規模国際イベント等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＞

＜重要サービスの継続性を確保するための対応＞

『（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、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。

＜重要サービスの継続性を確保するための対応＞

『（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、「事業・重要サービス・経営資源（情報資産）の例」（別紙１）等を参考に、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（下記のような要素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、大規模国際イベント等の開催期間及び平時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（下記のような要素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

リスクの特定は、リスク源又はリスクシナリオのどちらの手法を用いても行うことができます。事業者等において、業界団体等から公表されている基準やガイドライン等に基づいたリスクの特定・分析・評価を既に継続的に実施している場合は、事業者等の環境や昨今のインシデント事例に基づいたリスクシナリオを用いる（リスクシナリオによるアプローチ）ことで、効率的にリスクアセスメントを実施することが可能と考えられます。

a)リスク源の場合

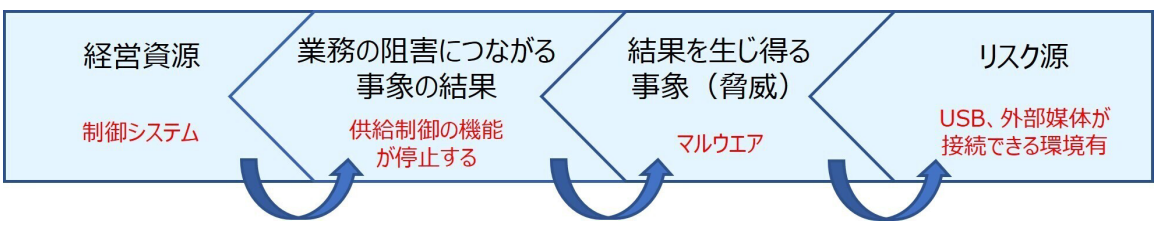
次のステップに沿って、演繹的にリスク源を洗い出します。

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（脅威）」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＞制御システムを経営資源とした際の作業イメージ



＜重要サービスの継続性を確保するための対応＞

『(様式６－１）リスクアセスメント（リスク源)』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、「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２）等を参考に、特定します。

b)リスクシナリオの場合

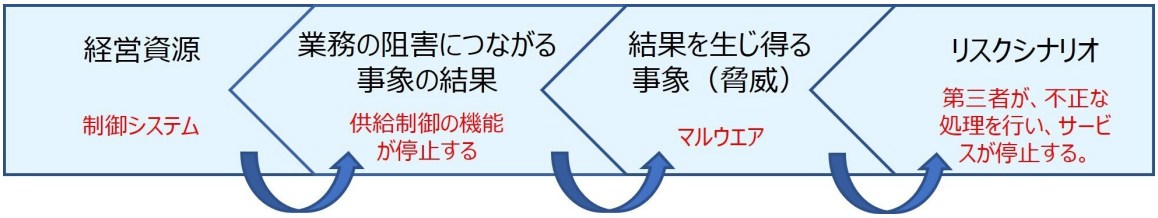
次のステップに沿って、リスクシナリオを洗い出します。

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（脅威）」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「リスクシナリオ」を書き出します。

＜例＞制御システムを経営資源とした際の作業イメージ



＜重要サービスの継続性を確保するための対応＞

『(様式６－２）リスクアセスメント（リスクシナリオ)』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シナリオを、「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４）等を参考に、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（※）。

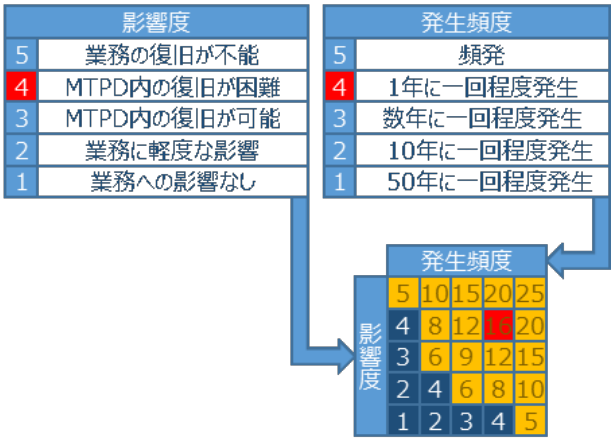
②事象の発生可能性について、「５．リスク評価方針の策定」において定めた評価軸に基づく評価を行います（※）。

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、リスク源又はリスクシナリオごとの残留リスク値を導出します。

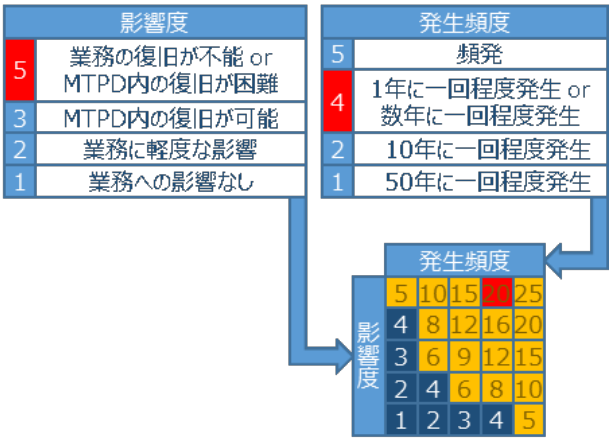
（※）何らかの対策を講じている場合であっても、技術の進歩により対策の有効性が陳腐化しやすいという情報セキュリティ対策の性質を考慮し、対策前の評価（固有リスク）及び対策後の評価（残留リスク）の両方を行います。また、リスク源の場合は「結果を生じ得る事象（脅威）及びリスク源に対する対策例」（別紙３）を参考に、現在講じている対策がリスク源に対して有効なものであるかを確認します。

＜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



＜重要サービスの継続性を確保するための対応＞

『(様式６－１）リスクアセスメント（リスク源)』又は『(様式６－２）リスクアセスメント（リスクシナリオ)』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。

＜重要サービスの継続性を確保するための対応＞

『(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」のリスク源又はリスクシナリオを抽出し、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。

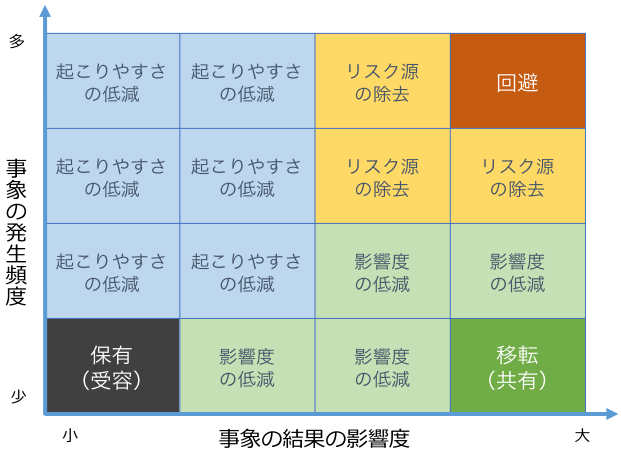
＜リスク対応の選択肢＞

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。特に社会経済を支えるサービスを提供する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（リスクアセスメントの実施内容の妥当性確認）」による分析結果の検証及び「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）」による実施体制や活動内容の評価を紹介します。また、リスクアセスメントの実施主体自らが、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』を参照）。

＜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（リスクアセスメントの実施内容の妥当性確認）

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、大規模国際イベント等の開催等経営環境の変化、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（リスクアセスメント作業の妥当性確認）

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。

＜パフォーマンス評価における確認観点（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

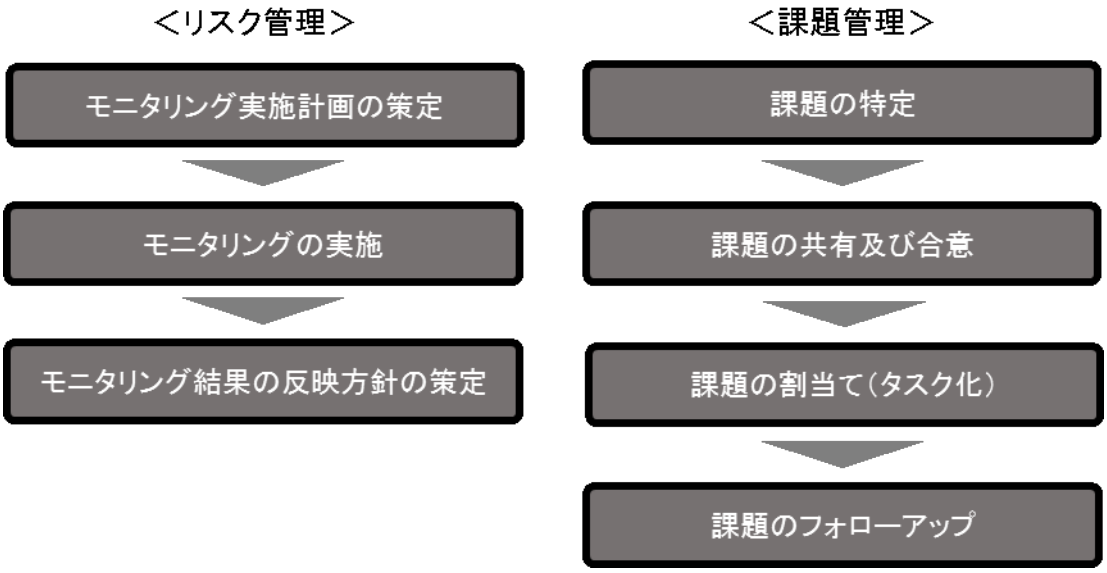
リスクアセスメントの結果として認識された状態は、経時的に変化すると予想されます。リスクアセスメントを変更又は無効なものとするおそれのある状況及びその他の要因を特定し、リスクの変動に適切に対処するためには、「リスクアセスメント結果を継続的にモニタリング（リスクアセスメントの結果として認識された状態との差異を特定するために、状態を継続的に点検し、監督し、要点を押さえて観察し、又は決定する取組）を実施し、必要に応じて適宜にリスクアセスメント結果の見直しを実施する」など、リスクを適切に管理し、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要です。

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
IT 障害	情報、情報システム、制御システム等が期待通りの機能を発揮しない又は発揮できない状態となる事象のうち、重要サービスの提供水準が最低限許維持されるべき水準を下回る事象。
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。 本ガイドラインのリスクアセスメントにおいては、重要サービス又はそれを支える業務の中断が許容できる時間の最大値を指し、重要サービスの中断による影響を、サービスに関する利害関係者の期待、その他の期待・要求事項等を踏まえ評価・分析した上で判断される。
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、組織又はステークホルダーが負う準備ができている残留リスクの程度。 本ガイドラインのリスクアセスメントにおいては、社会経済を支えるサービスを提供する事業者等が設定した活動目的を達成するために、自組織又はステークホルダーが許容可能な残留リスクの水準を指す。リスクが発現した際にその穴埋めが可能かといった観点等から判断される。
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。
リスクシナリオ	どのような経営資源（情報資産）に対して、何に起因して何が起こるかを時系列に整理し、最終的にリスクが顕在化することを示したシナリオ。
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。 本ガイドラインのリスクアセスメントにおいては、社会経済を支えるサービスを提供する事業者等が設定した活動目的を達成するために、自組織が許容することを選択したリスクの水準を指し、経営層の意思が反映される。
リスク対応	リスクを修正するプロセス。 リスク対応には、リスクを修正するために一つ以上の選択肢を選び出すこと及びそれらの選択肢を実践することが含まれる。リスク対応は本書の対象ではないが、リスクアセスメントに続くプロセスとしてリスク対応の選択肢の同定について、P22 に参考情報を記載している。
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る。
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。

用語	説明
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。 本ガイドラインのリスクアセスメントにおいては、特定したリスクについて事象の結果の影響度とその起こりやすさ（発生頻度）を決定し、その組み合わせでリスクレベルを決定するプロセスを指す。
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う。

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＞

[11] 独立行政法人情報処理推進機構（2020）『制御システムのセキュリティリスク分析ガイド（第２版）』,＜https://www.ipa.go.jp/files/000080712.pdf＞