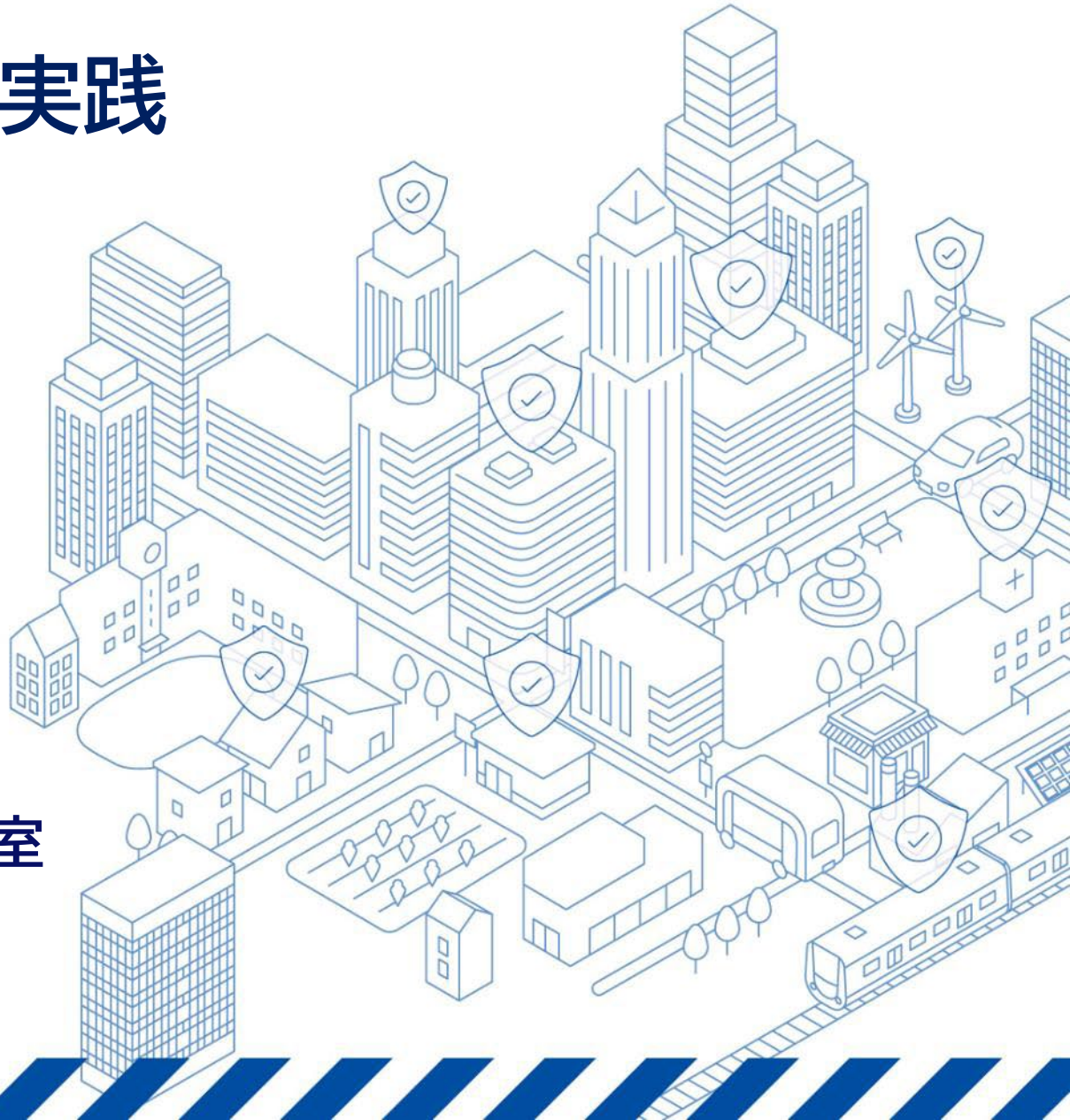
リスクアセスメント実践ラーニングキット

～自己学習、研修教材～



内閣官房 国家サイバー統括室

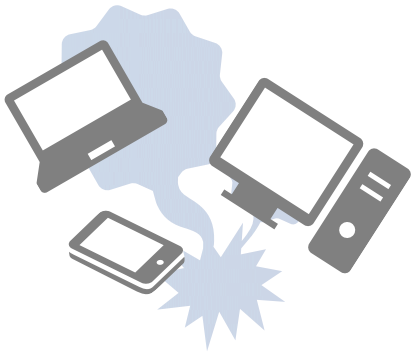
Agenda

00

はじめに

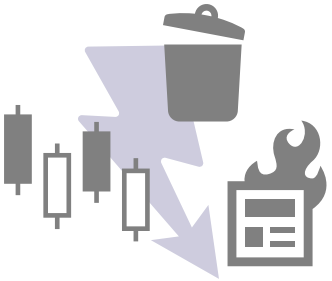
はじめに ①

近年、情報通信技術の活用場面が拡がる一方、サイバー攻撃やシステム障害による被害や損失も増加しています。



業務の停止

社会・経済活動への
重大な影響

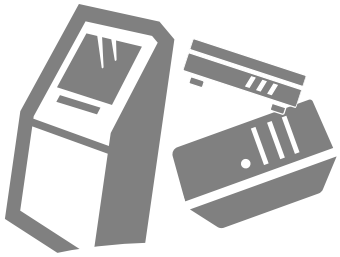


社会的信用の喪失

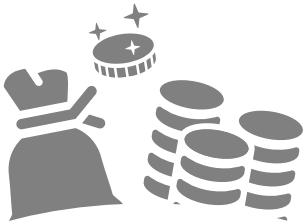
はじめに ②

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て対策することが重要となります。

人員の割当



追加対策の実施



予算の割当

はじめに ③

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て対策することが重要となります。

が

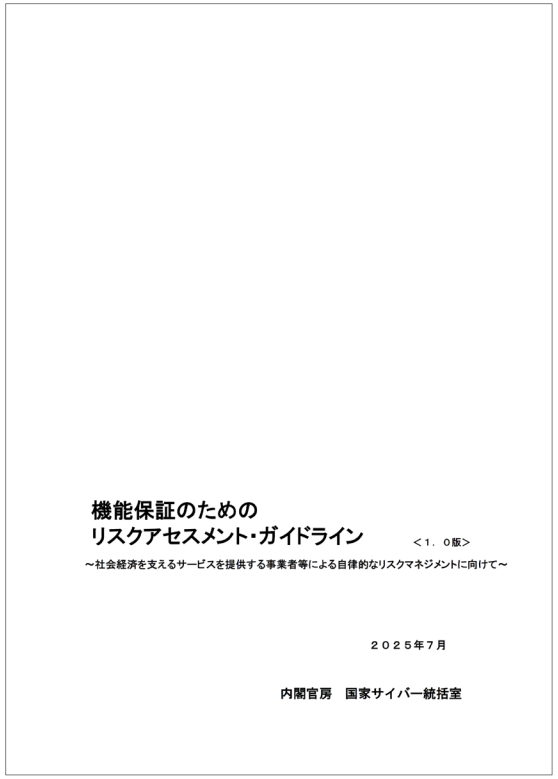
対策の実施には限度があり、
過剰な対策は業務効率を損なう

はじめに ④

自組織の実情に応じた戦略的なリスク対応と、
継続的に機能するリスクマネジメント体制の構築により
サイバー攻撃やシステム障害のリスクの低減と、
経営資源の適切な割当の実現に向けて、
本コンテンツをお役立てください。

機能保証に向けたリスクアセスメント

本コンテンツでは、「機能保証のためのリスクアセスメント・ガイドライン※」の考え方に基づいて、**「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「機能保証」の観点から、リスクアセスメントの手順を紹介します。

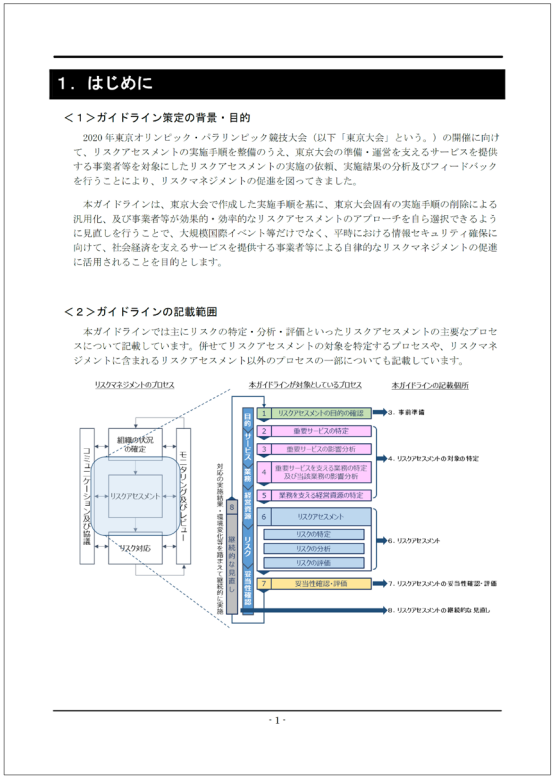


機能保証のための
リスクアセスメント・ガイドライン　＜1．0版＞

～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～

２０２５年７月

内閣官房　国家サイバー統括室



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「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。

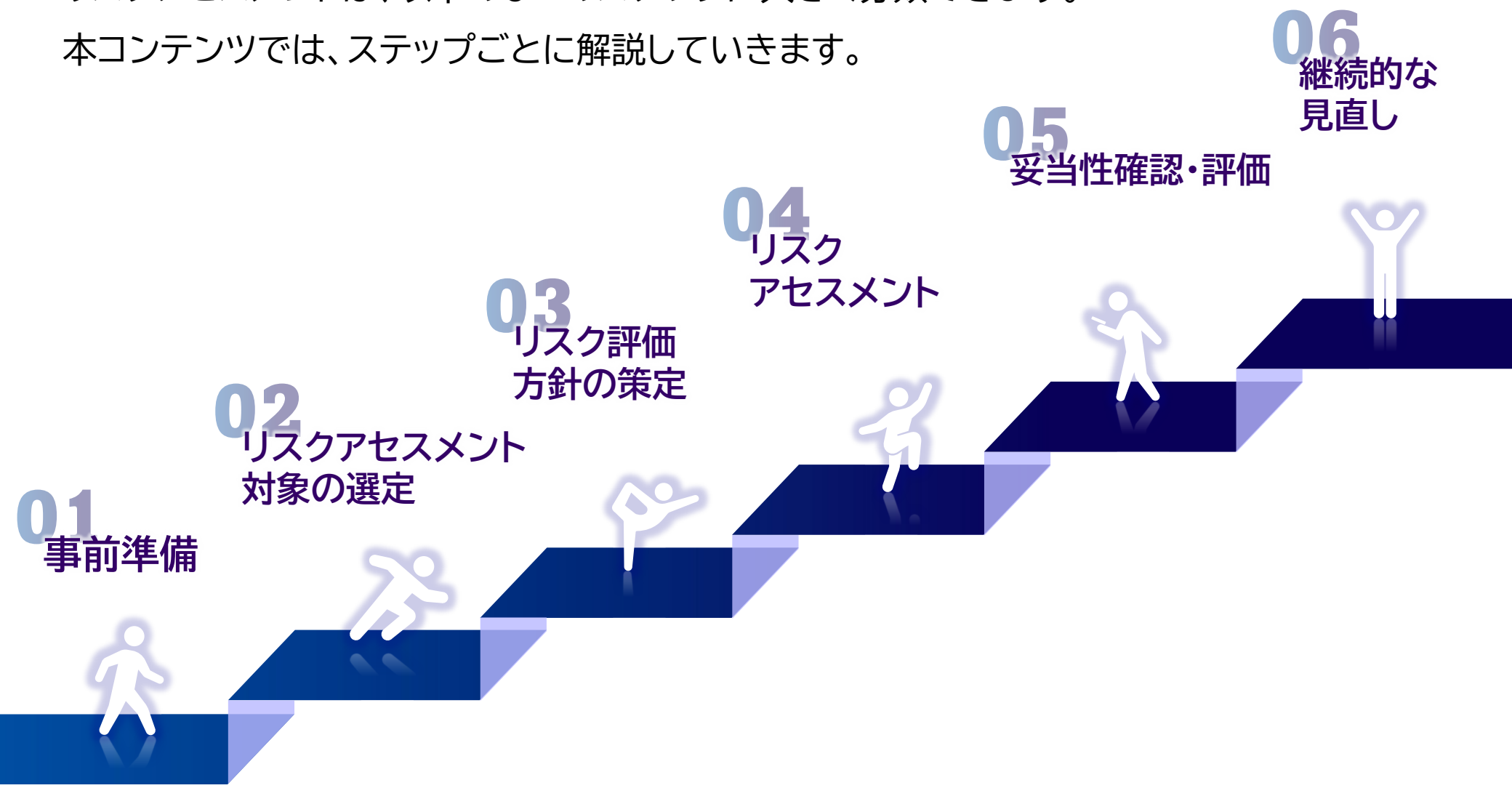
- 1 -

※ https://www.cyber.go.jp/policy/group/cyber/policy.html

リスクアセスメントの全体像

リスクアセスメントは、以下の6つのステップに大きく分類できます。

本コンテンツでは、ステップごとに解説していきます。



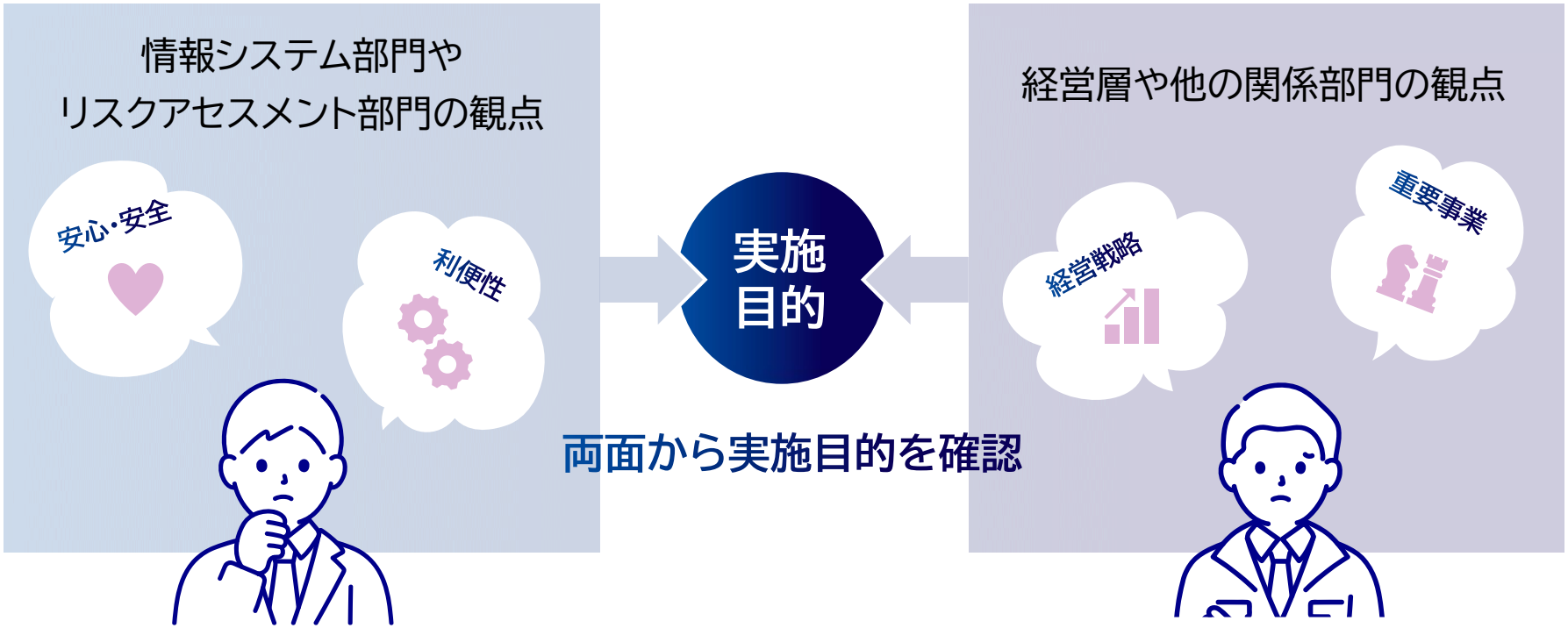
01

事前準備

リスクアセスメントの実施目的の確認

リスクアセスメントは、自組織の経営戦略を踏まえて実施することが重要となります。

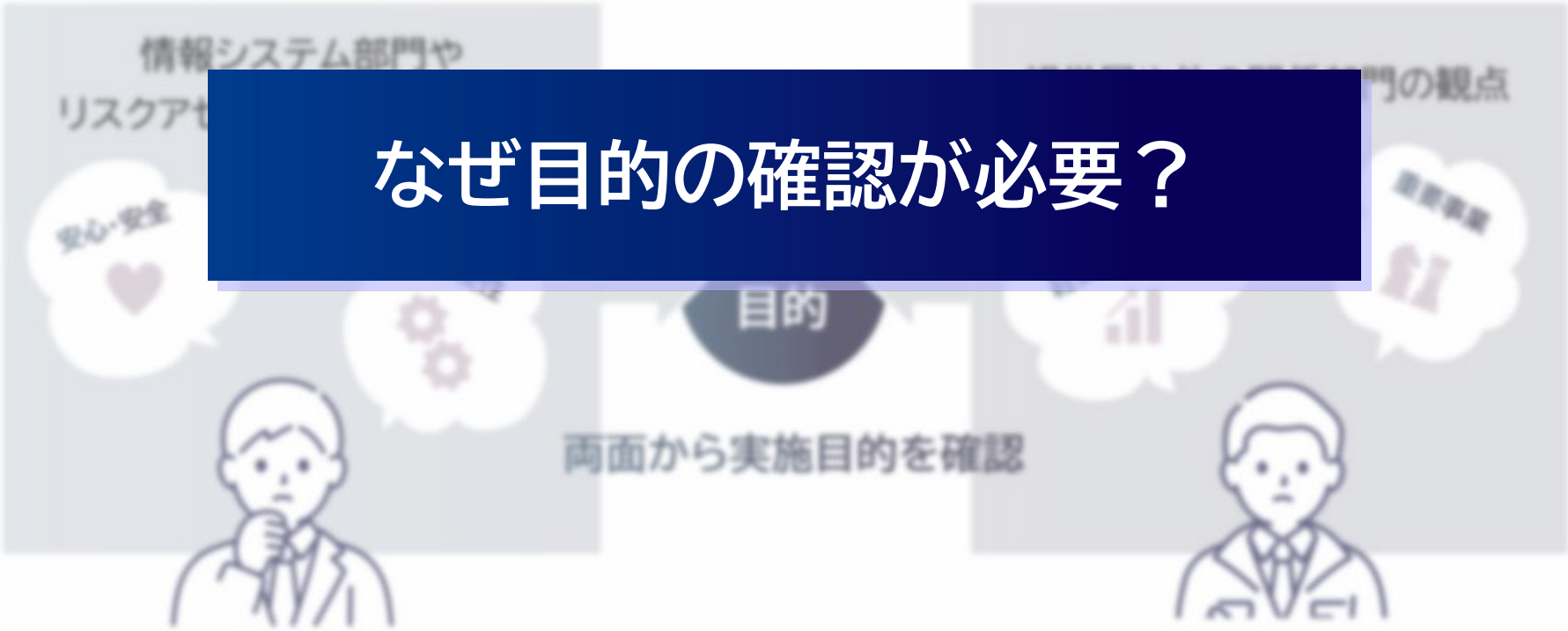
そのためには、情報システム部門やリスクマネジメント部門だけではなく、**経営層及びその他関係部門を含めて、リスクアセスメントの実施目的を確認**する必要があります。



リスクアセスメントの実施目的の確認

リスクアセスメントは、自組織の経営戦略を踏まえて実施することが重要となります。

そのためには、情報システム部門やリスクマネジメント部門だけではなく、経営層及びその他関係部門を含めて、リスクアセスメントの実施目的を確認する必要があります。



なぜ目的の確認が必要？

Answer

組織の提供サービスの維持・継続のため

経営戦略との整合が行われないままリスクアセスメントを実施した場合、組織にとってのリスクが正しく把握できず、対策が行われないおそれがあります。

組織として提供すべきサービスの維持・継続を目的として、適切に評価を行うためにも、必要な関係者を含めて目的を共有しましょう。

様式1 リスクアセスメントの実施目的の確認

「機能保証のためのリスクアセスメント・ガイドライン」では、実施目的の確認のための様式として様式1を提供しています。様式1は「リスクアセスメントの実施目的」と「自組織の活動目標」を記載する様式です。この様式を、関係者に目的・目標を共有する際に活用いただけます。

STEP1：リスクアセスメントの実施目的の確認

［様式１］

リスクアセスメントの実施目的	（1）自組織の活動目標 （左記の目的を踏まえて設定）	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
		【実施目的・方針の例】 （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。

Question

少しだけ時間をとって、考えてみましょう。

情報システム部門のみで、

リスクアセスメントの実施目的を決めると

リスクアセスメントの結果には

どんな影響がありそうでしょうか。

回答例

- 「情報システム」を中心にリスクアセスメントが実施され、
  ステークホルダーからの要求等の
  事業や業務固有の要件を見落とすおそれがある。
- リスクへの対策が技術的対策中心となり、
  業務継続の視点等や人的・組織的対策の観点での
  考慮が不足するおそれがある。
- 経営上の重要サービス・業務以外の
  サービス・業務へ過剰に対策が実施されるおそれがある。

**特定の部門の視点だけでは
組織としてのリスクを
適切に把握できないおそれがある。**

Answer

スケジュールの策定と実施体制の構築

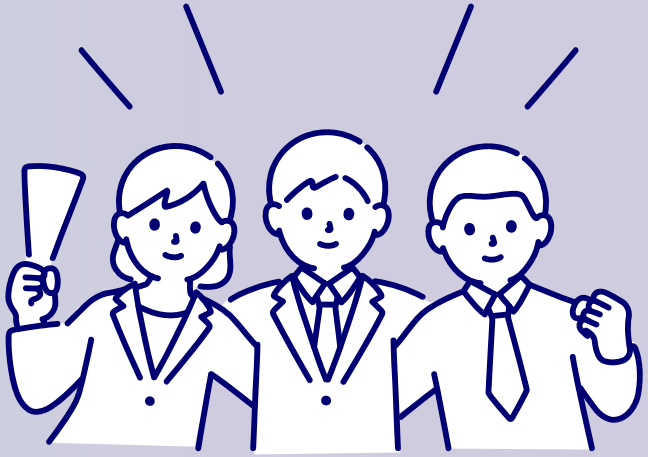
組織内で実施目的が共有出来たら、目的達成に向け、リスクアセスメントの実施スケジュールと実施体制を整備します。

スケジュールの策定

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たリスクアセスメントのスケジュールを策定します。

実施体制の構築

各作業の責任主体を定めた上で、経営層及びその他関係部門を含めた実施体制を構築し、組織としてリスクアセスメントに取り組みましょう。
有識者や専門家なども含めることが有効です。



02

リスクアセスメントの対象の特定

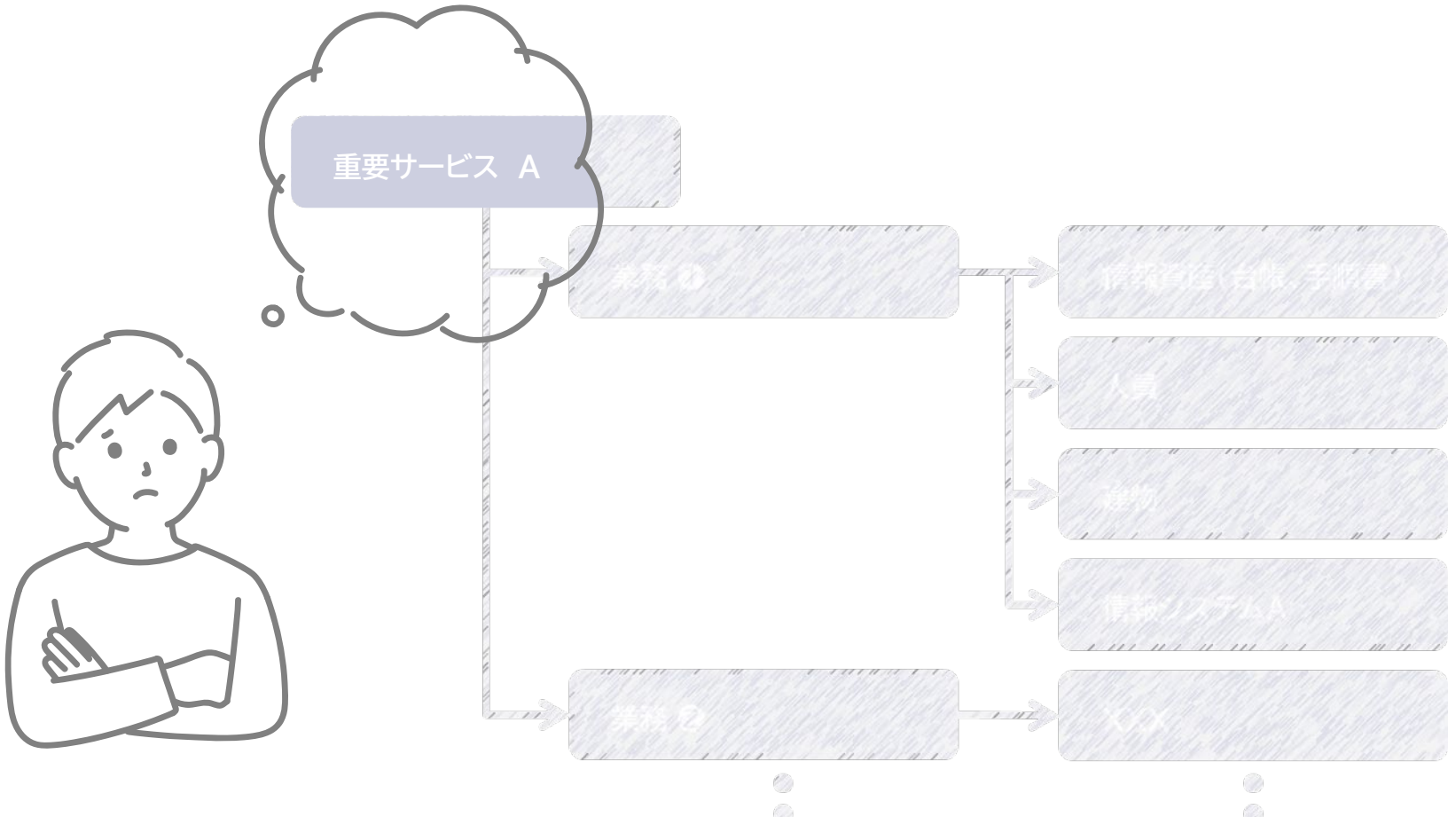
重要サービスの特定

リスクアセスメントは社会から期待されている役割・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優先して実施することが効果的です。

自組織が提供するサービスについて、**経営面や法制面等を総合的に評価して、リスクアセスメントの対象とする「重要サービス」を特定**しましょう。

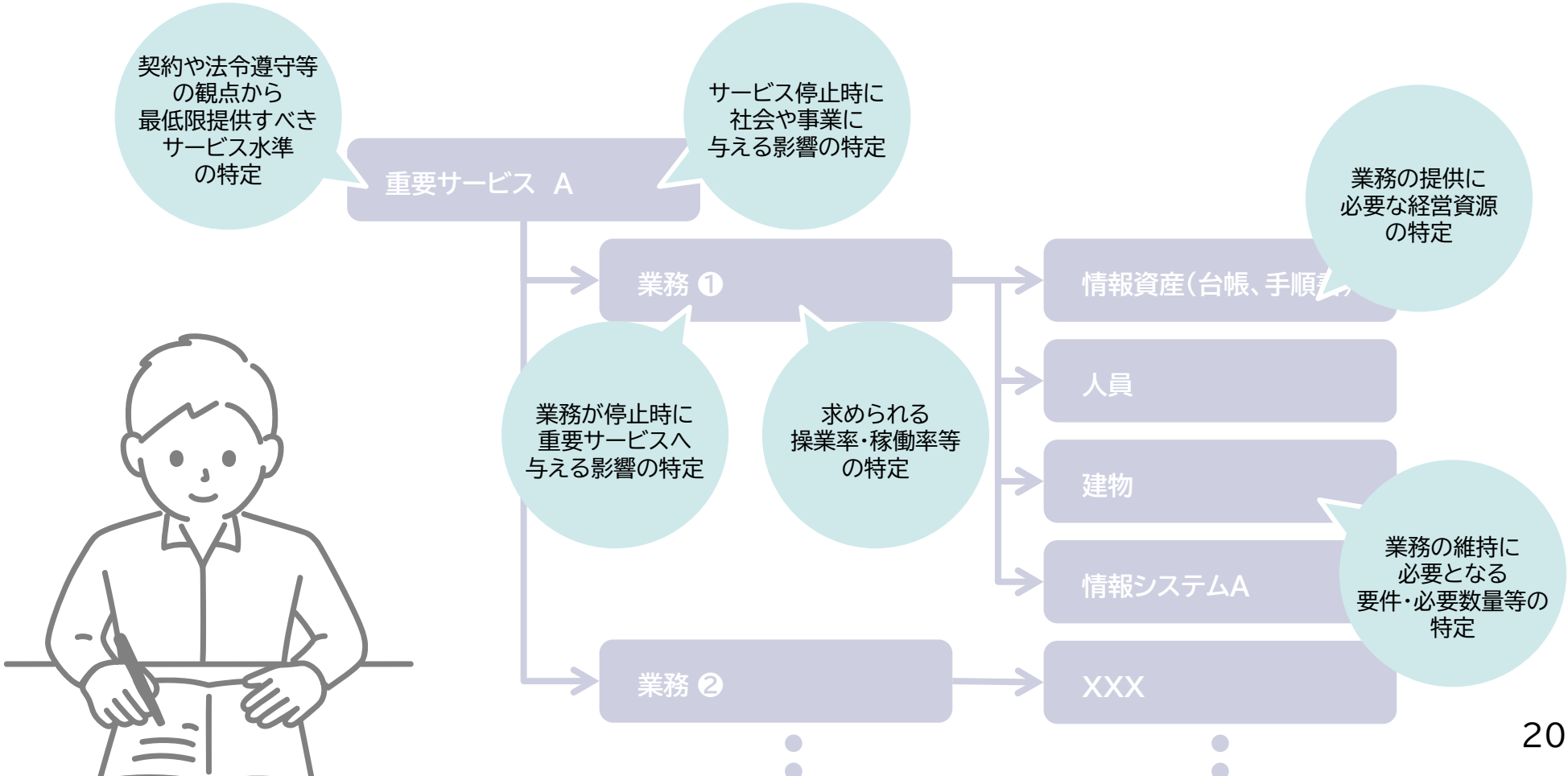
リスクアセスメントの対象の特定

特定した「重要サービス」に対し、「重要サービス」を一括りにリスク評価、するのではなく…



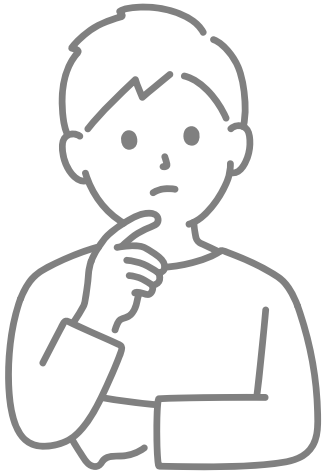
リスクアセスメントの対象の特定

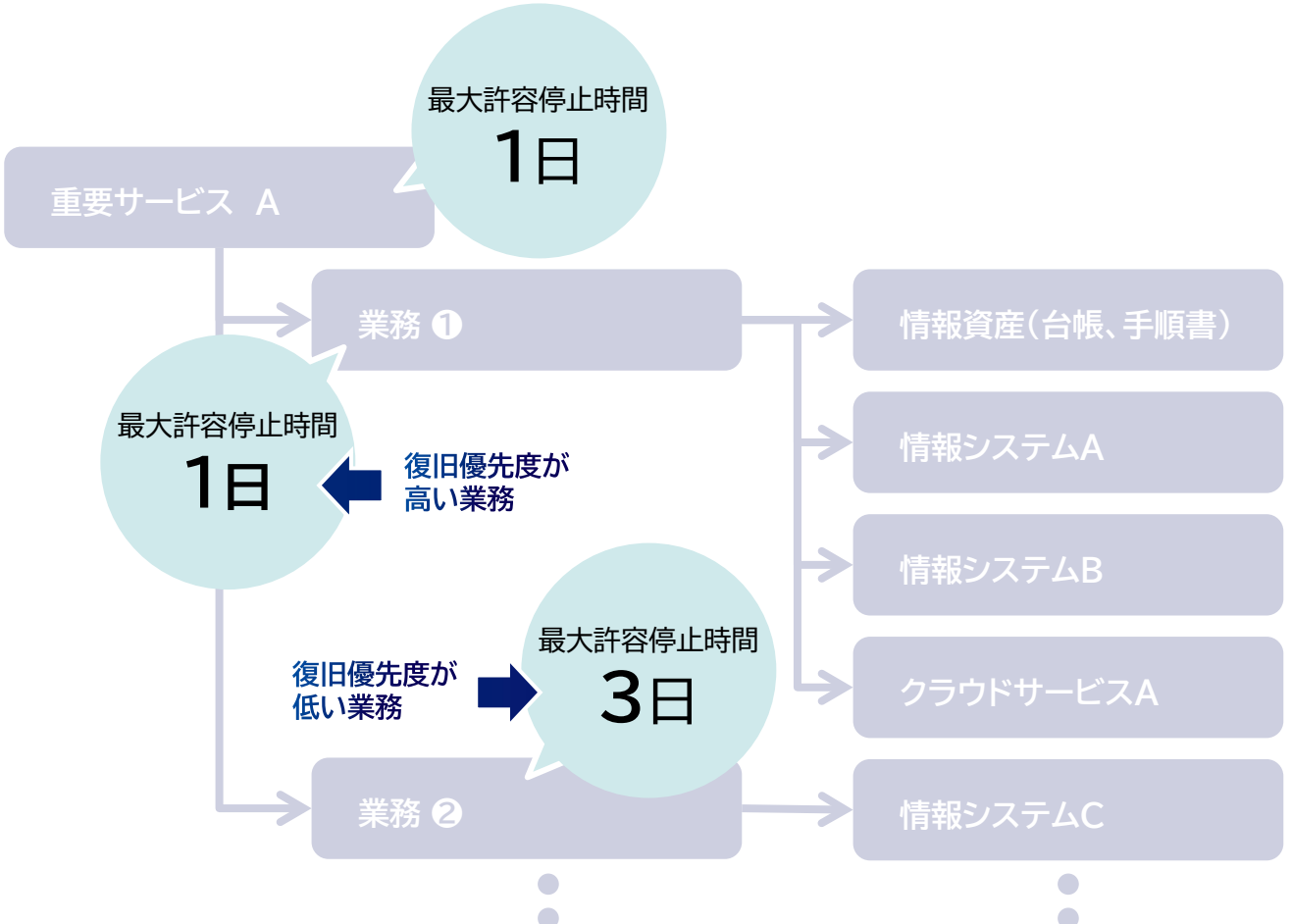
特定した「重要サービス」に対し、「重要サービス」を一括りにリスク評価、するのではなく…
「重要サービス」に求められている**最低限許容されるサービスの範囲や水準を特定**し、**重要サービスの提供に必要となる業務や経営資源まで詳細化**して、リスク評価を行いましょう。



リスクアセスメントの対象の特定

これらの作業を通じて、**リスク選好・リスク許容度が明確になり、リスク評価基準が設定できるようになります。**





様式2 重要サービスの選定

「機能保証のためのリスクアセスメント・ガイドライン」では、重要サービス選定のための様式として　様式2を提供しています。

事業・サービスごとに、**利害関係者や法規則面の要求や経営面での位置づけを整理し、重要サービスの特定**にお役立ていただけます。

STEP2：サービスの期待等を分析した上、重要サービスを選定する。　[様式2]

(1) 事業	(2) サービス	(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 サービスに関する利害関係者の期待 1．＊＊＊＊＊＊できること／すること 2．＊＊＊＊＊＊できること／すること 3．＊＊＊＊＊＊できること／すること 4．＊＊＊＊＊＊できること／すること 5．＊＊＊＊＊＊できること／すること コメント	その他の期待・要求事項	(4) 製品・サービスの経営面での位置づけ□ 業績面 売上	ROI	戦略面 市場成長性	相対市場シェア	(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

自組織における
事業・サービスの特定

事業・サービスごとに利害関係者や
法制度面での要求事項の整理

業績・経営戦略などの
経営面での位置づけを整理

実施した整理をもとに
重要サービスの決定

様式3 重要サービスの影響分析

さらに、重要サービスの影響分析のための様式として、様式3を提供しています。

最低限要求されるサービス水準・範囲とサービスが停止した際に事業に与える影響を可視化し、重要業務の優先順位づけにお役立ていただけます。

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。 ［様式３］

(1)事業	(2)サービス	(3)利害関係者のニーズ・期待／法規制面での要求事項等を満たすために最低限許容されるサービスの範囲・水準		(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)	
					時間経過に伴う影響度合いの評価								
		契約責任、法令遵守	社会的責任（CSR）	最低限許容されるサービスの範囲・水準が満たされない場合に生じる事態	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

自組織における
事業・サービスの特定

事業・サービスごとに利害関係者や
法制度面での要求事項の整理

サービスの提供が停止した時及び
時間経過に伴う影響度合いの評価

最大許容停止時間の
特定

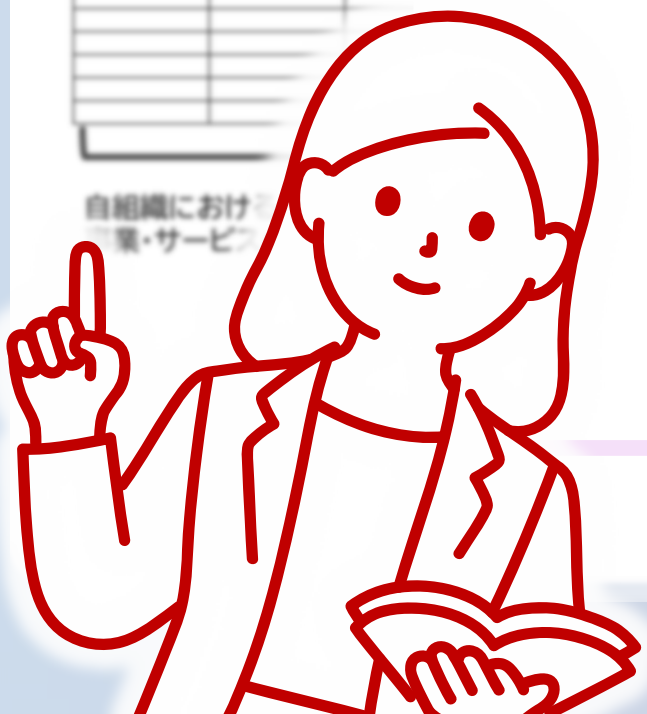
様式3 重要サービスの影響分析

さらに、重要サービスの影響分析のための様式として、様式3を提供しています。

最低限要求される
重要業務の優先順

ワンポイントアドバイス

組織の持続可能な発展や社会からの信頼の維持の観点から、財務的損失だけではなく、評判・信頼などの無形の資産や社会的責任も含めて、総合的に評価しましょう。



様式4 業務の洗い出し・業務が停止した場合の影響

続いて、重要サービスの提供に必要な業務ごとの評価を行うための様式として、様式4を提供しています。

業務ごとに、**業務停止時に生じるサービス提供・事業に与える影響を可視化し、重要業務の優先順位づけと復旧方針の策定に資する情報を整理**することができます。

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。 ［様式４］

（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

重要サービスの提供に必要な業務と業務の最低水準の整理

業務の提供が停止した時及び時間経過に伴う影響度合いの評価

最大許容停止時間の特定

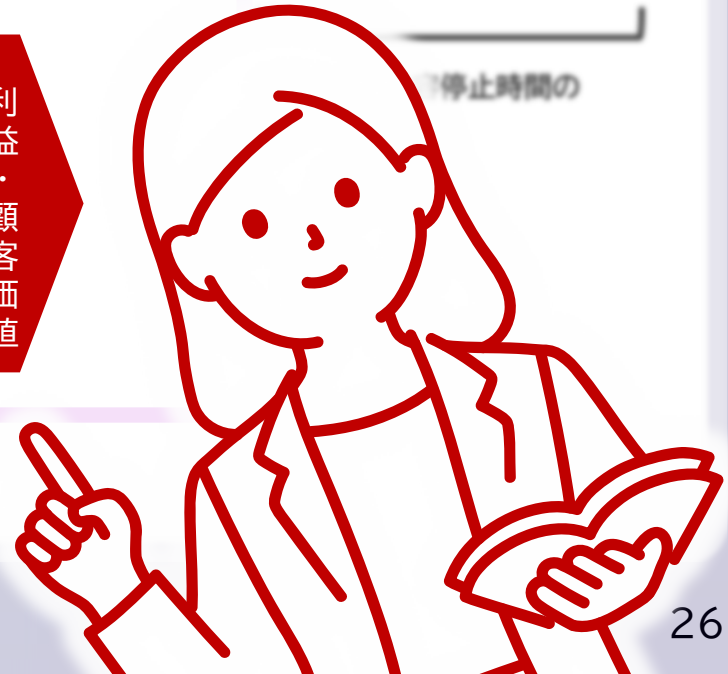
様式4　業務の洗い出し・業務が停止した場合の影響

続いて、重要サービスの提供に必要な業務ごとの評価を行うための様式として、様式4を提供し

ワンポイントアドバイス

製品やサービスを市場に提供するまでの一連の流れ（バリューチェーン）に着目して洗い出すと、業務間のつながりや依存関係を把握しやすくなり、リスク評価や影響分析の精度の向上が期待できます。

一般的なバリュー・チェーンの例



リスクアセスメントの対象の特定

リスクアセスメントの対象の特定にあたっては、経営層を含め、多角的な観点で評価を行うことで、効果的・効率的な実施が可能となります。

評価観点の例

- 財務的影響　：直接的な損失、コスト増加
- 社会的責任　：社会や利害関係者に対する義務・責任
- 評判・信用への影響　：ブランド価値、利害関係者からの信頼
- 人命への影響　：従業員、顧客、地域住民の安全
- 環境への影響　：生態系、気候変動、資源利用

様式5 業務を支える経営資源の要件・必要数量

リスクアセスメントの対象の特定として、最後に用いる様式が様式5です。

重要サービスに求められる水準を維持するために必要な経営資源の要素や必要数量を特定することで、**経営資源ごとにどのような脅威・リスクがあるかを評価**することができます。

また、**対策の優先度を判断する基礎情報**としてもご活用いただけます。

STEP5:重要サービスの提供について、最低許容水準を満たすために必要な業務及び資源の洗出し

［様式5］

(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の要件・必要数量							
				人	情報、データ	建物、作業環境、関連ユーティリティ	設備、機器、消耗品	情報通信技術(ICT)システム、制御システム	交通機関、ライフライン（例：電気、水、ガス）	資金	その他（例：取引先、サプライヤ）

(5)業務を支える経営資源の要件・必要数量							
人	情報、データ	建物、作業環境、関連ユーティリティ	設備、機器、消耗品	情報通信技術(ICT)システム、制御システム	交通機関、ライフライン（例：電気、水、ガス）	資金	その他（例：取引先、サプライヤ）

業務を支える経営資源の洗い出し

Question

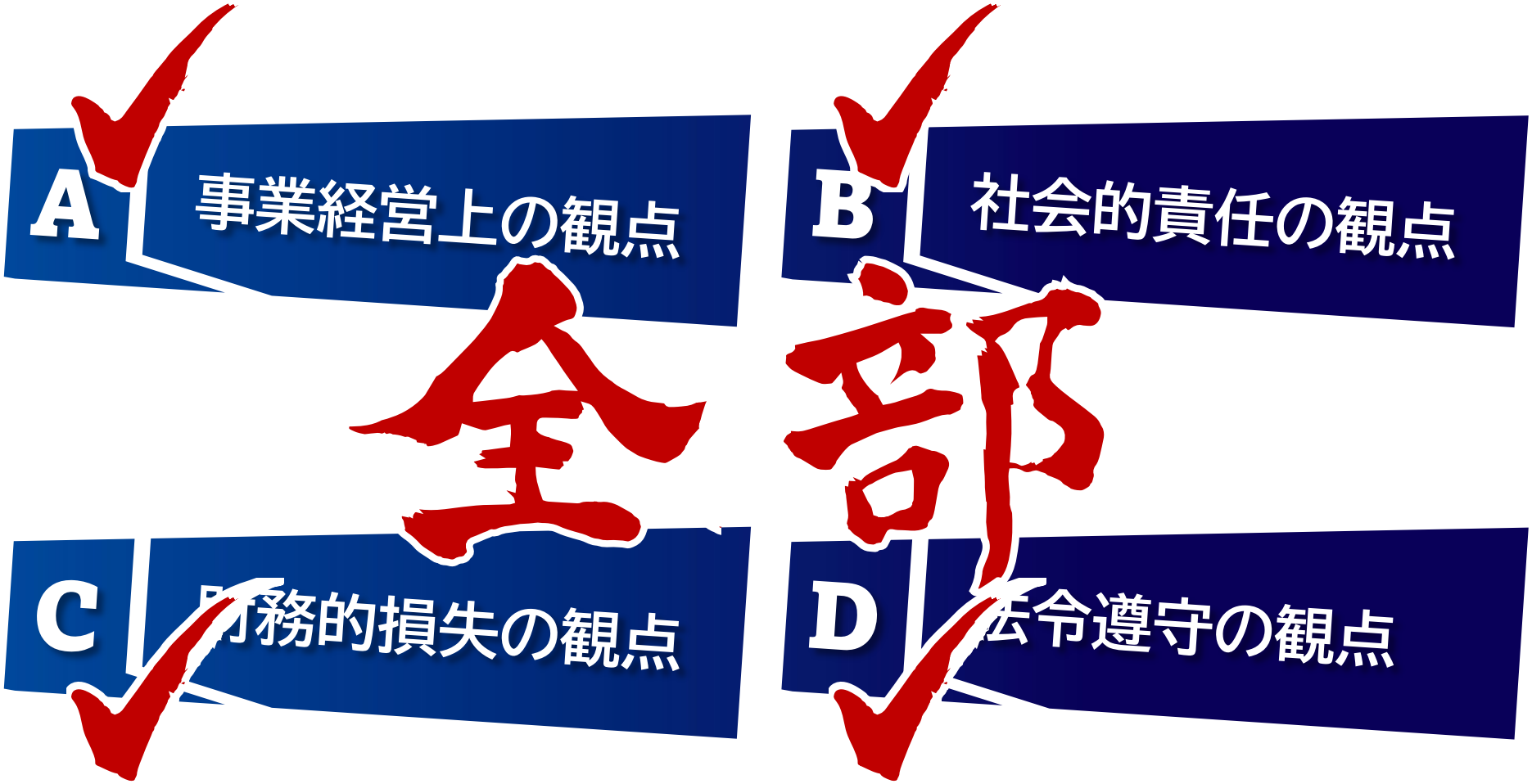
重要サービスの選定にあたって必要となる観点を選びましょう。

A 事業経営上の観点

B 社会的責任の観点

C 財務的損失の観点

D 法令遵守の観点



経営層を含めて様々な観点から
総合的に評価して、対象を選定しましょう。

Answer

03

リスク評価方針の策定

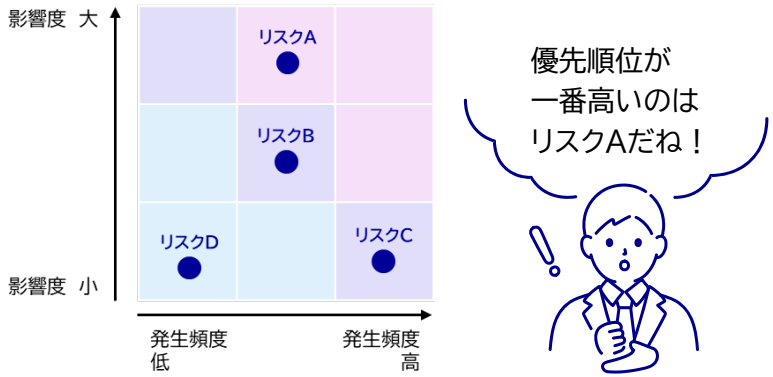
リスク分析手法の検討

リスクアセスメントの対象が特定出来たら、いよいよリスク評価を行うための「リスク分析手法」を決めていきます。リスク分析手法には、様々な手法がありますが、多くの事業者等により採用されている手法をご紹介します。

リスクマップ

「影響度」と「発生頻度」等の2つの評価軸で作成したマトリクスにリスクを配置し、優先順位を視覚的に把握する手法

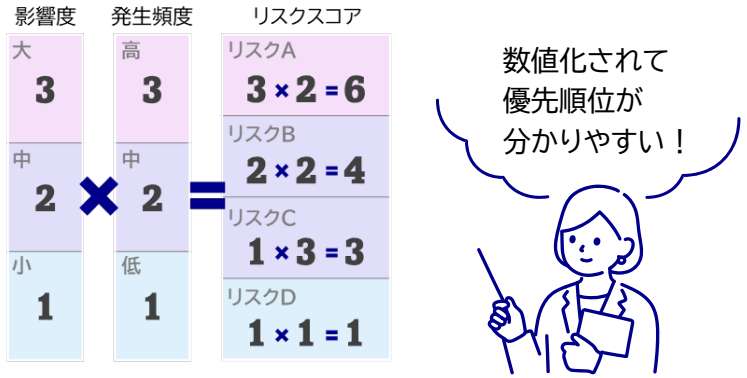
リスクマップの例



リスク・スコアリング

「影響度」と「発生頻度」等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て、優先して対応すべきリスクを明確にする分析手法

リスク・スコアリングの例



リスク分析手法の検討

機能保証に向けたリスクアセスメントでは「組織が果たすべき役割を継続するために、リスクを特定・分析・評価して残留リスクの可視化、戦略的な対応につなげること」を目的に、以下を評価の軸としています。

事象の結果による重要サービス・業務への影響度合い

重要サービス・業務への影響は以下のような要素等を総合的に評価します。

- 予想影響範囲・程度
- 予想復旧時間
- 予想対応コスト

事象の発生頻度（発生可能性、起こりやすさ）

上記の評価の軸を用いることで、情報システム部門や業務部門の視点に留まらず、「組織の果たすべき役割の継続」に向けたリスクの評価を支援しています。

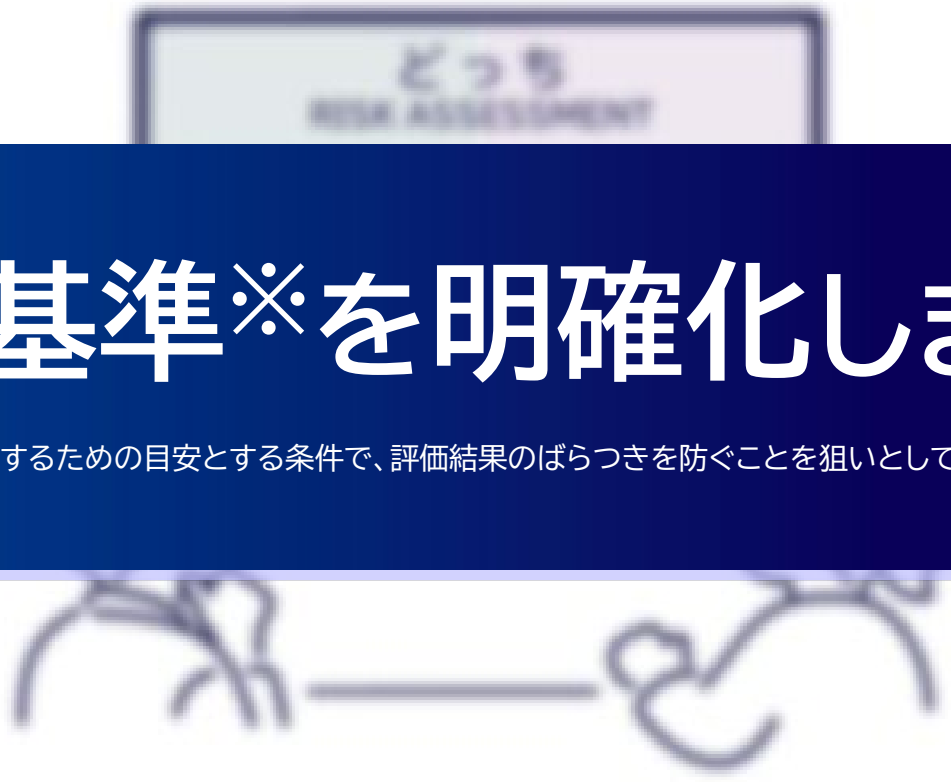
リスク基準の決定

リスクアセスメントの対象とリスク分析手法が決まったら、リスク評価ができそうです。

しかし、その前に――

リスク基準の決定

リスクアセスメントの対象とリスク分析手法が決まったら、リスク評価ができそうです。
しかし、その前に――



リスク基準※を明確化しましょう

※ リスクの重大さを評価するための目安とする条件で、評価結果のばらつきを防ぐことを狙いとして設定する判断指標のこと

リスク基準の決定

リスク評価は担当者ごとの主観に左右されやすく、組織として一貫した評価を行うための基準を用意する必要があります。

評価にばらつきが生じてしまい
組織として一貫した評価ができなくなる。

本コンテンツ33ページで示した機能保証に向けたリスクアセスメントで採用している評価の軸を用いた場合の判断指標の例です。

事象の結果による重要サービス・業務への影響度合い

example

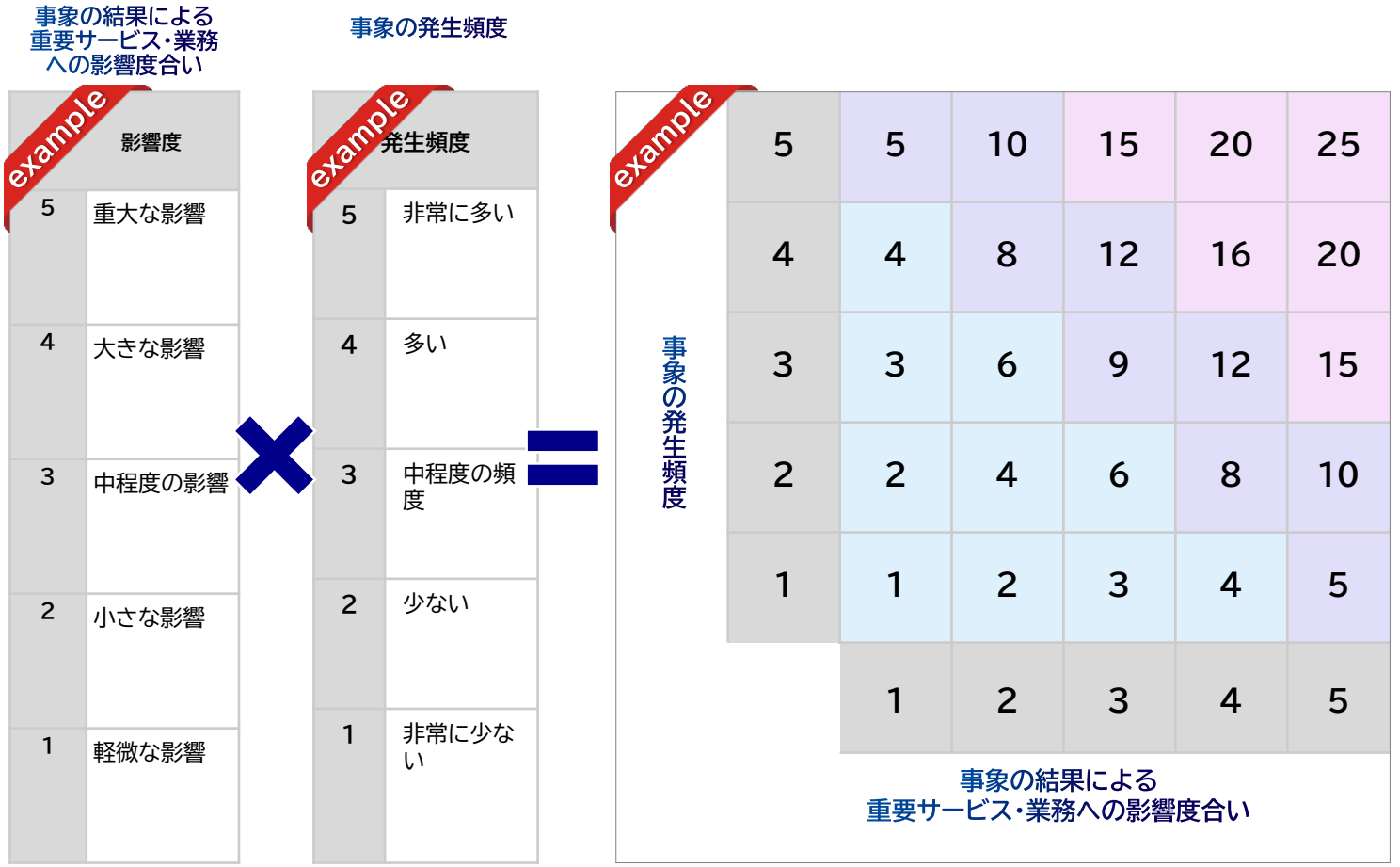
影響度		影響度合い		
		業務に対する影響の範囲・程度	予想復旧時間	対応に要するコスト
5	重大な影響	当該業務が**停止**する。	業務の**復旧自体が困難**である。	業務の復旧や事象の結果の対処のために要するコストの**負担が、事業者にとって甚大**である。
4	大きな影響	当該業務が阻害され、**業務の最低水準の維持が困難**である。	業務の**最大許容停止時間内での業務の復旧が困難**である。	業務の復旧や事象の結果の対処のために要するコストの**負担が、事業者にとって大きい**。
3	中程度の影響	当該業務が阻害され、**業務の最低水準を維持できないおそれ**がある。	業務の**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、**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	ー	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との**負担が、事業者にとって軽微**である。

事象の発生頻度

example

発生頻度		事象の予想発生頻度
5	非常に多い	頻発 **ほぼ確実に発生する**
4	多い	1年に1回程度発生 **通過する確率が高い**
3	中程度の頻度	数年に1回程度発生 **通過する確率と止められる確率が拮抗**
2	少ない	10年に1回程度発生 **止められる確率が高い**
1	非常に少ない	ごくまれに、例外的な状況で発生 **ほとんどの場合止められる**

判断指標をもとにリスクを数値化(リスク値を算出)し、リスク対応の対象となるリスク値(リスク基準)を超えているか定量的な評価ができます。また、判断指標やリスク基準は、リスクアセスメントの目的や業務・システムの特性に応じて、設定することが大事です。



Question

リスク基準を利用して、リスク評価をしてみましょう。

最近、偽広告による感染被害が報道されているけれど、もし当社の業務端末でこの攻撃による感染被害が生じた場合の**「重要サービス・業務への影響度合い」は、どの程度だろう。**

以下の前提・基準を基に「業務に対する影響の範囲・程度」を評価してみましょう。

前提情報

- 業務端末と重要サービスのネットワークは分離されており、業務端末が感染しても重要サービスまで侵入されることは考えにくい。
- 同一ネットワーク内の業務端末に感染拡大するおそれは十分にある。
- 注意喚起等や必要な対応などの周知はしていないため、1台感染しただけであっても、報告や対応がされず感染が拡がるおそれがある。
- 代替端末の数を考慮すると、業務端末の3割が感染してしまうと業務の最低水準の維持は困難となる。

リスク基準

影響度		業務に対する影響の範囲・程度
5	重大な影響	当該業務が**停止**する。
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。
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。
2	小さな影響	当該業務が阻害され、**業務の最低水準は維持**される。
1	軽微な影響	ー

- 業務端末と重要サービスのネットワークは分離されており、業務端末が感染しても重要サービスまで侵入されることは考えにくい。

重要サービスへの直接的な影響は生じない見込み

- 同一ネットワーク内の業務端末に感染拡大するおそれは十分にある。
- 注意喚起等や必要な対応などの周知はしていないため、1台感染しただけであっても、報告や対応がされず感染が拡がるおそれがある。
- 代替端末の数を考慮すると、業務端末の3割が感染してしまうと業務の最低水準の維持は困難となる。

数台の感染であれば、業務影響も大きくない。

でも

感染拡大しやすい（感染拡大を防ぐ対策が不十分な）環境と

更に

3割の感染拡大で、最低水準を維持できない状況を踏まえて評価すると…

影響度		業務に対する影響の範囲・程度
5	重大な影響	当該業務が**停止**する。
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。
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。
2	小さな影響	当該業務が阻害され、**業務の最低水準は維持**される。
1	軽微な影響	―

感染拡大を防ぐための
追加の対策を考えないと…！

業務環境や社員への教育状況を踏まえると「3」と評価できます。

システム・サービスだけではなく、業務や人員等を総合的に評価することが重要です。

Answer

04

リスクアセスメント

機能保証の観点からのリスクの特定

過去に経験していない、又は発生確率が低い事象がリスクとして想定されず、対策や備えができなかったことにより、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て、「機能保証のためのリスクアセスメント・ガイドライン」では、「**事象の結果からリスク源までを演繹的に特定・分析・評価**」するアプローチを採用しています。

様式は2種類あり、リスク源となる経営資源からのアプローチと、リスクが顕在化する過程ごとに評価するリスクシナリオベースのアプローチ両方に対応しています。

様式6-1 リスクアセスメント(リスク源)

経営資源ごとに、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するための様式

経営資源	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
制御システム	供給制御の機能が停止する	マルウェア	外部媒体が接続できる環境

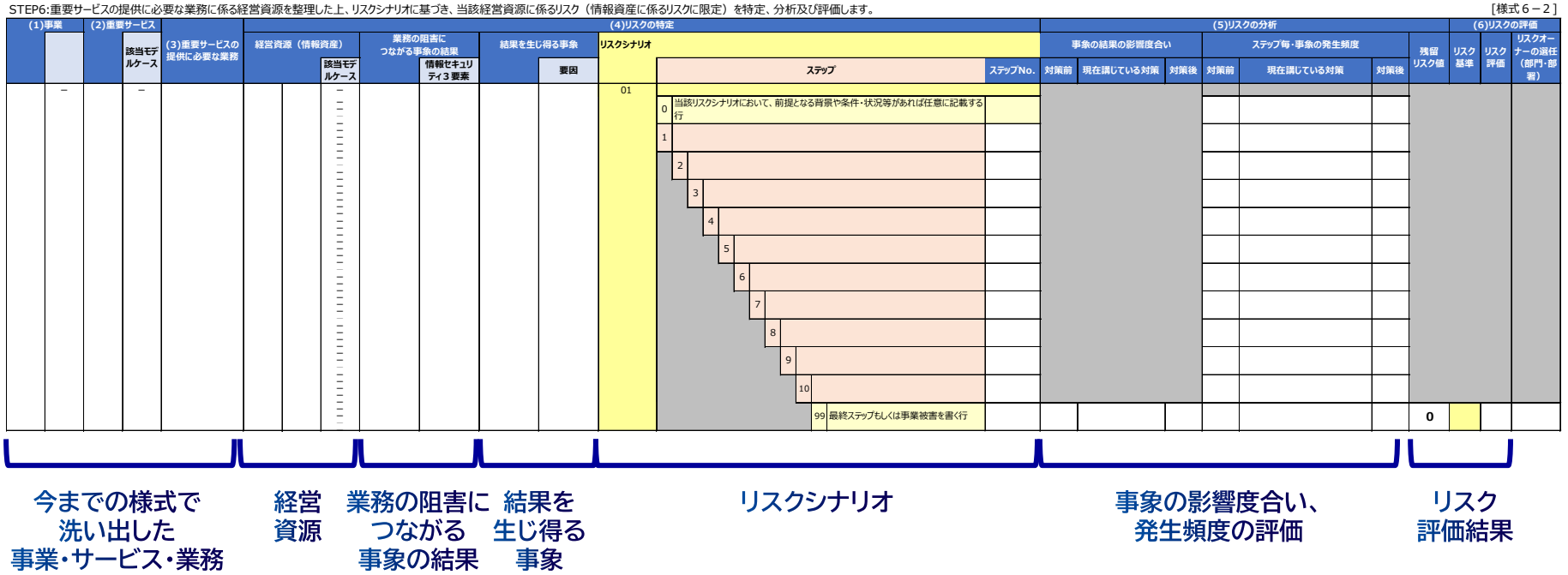
様式6-2 リスクアセスメント(リスクシナリオ)

経営資源ごとに、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、リスクが顕在化する過程ごとに生じ得るリスクを特定するための様式

経営資源	業務の阻害につながる事象の結果	結果を生じ得る事象	リスクシナリオ
制御システム	供給制御の機能が停止する	マルウェア	第三者が不正な処理を行い、サービスが停止

様式6-2 リスクアセスメント(リスクシナリオ)

本コンテンツでは、リスクシナリオベースのアプローチを行う様式6-2を用いたリスク評価手法をご紹介します。

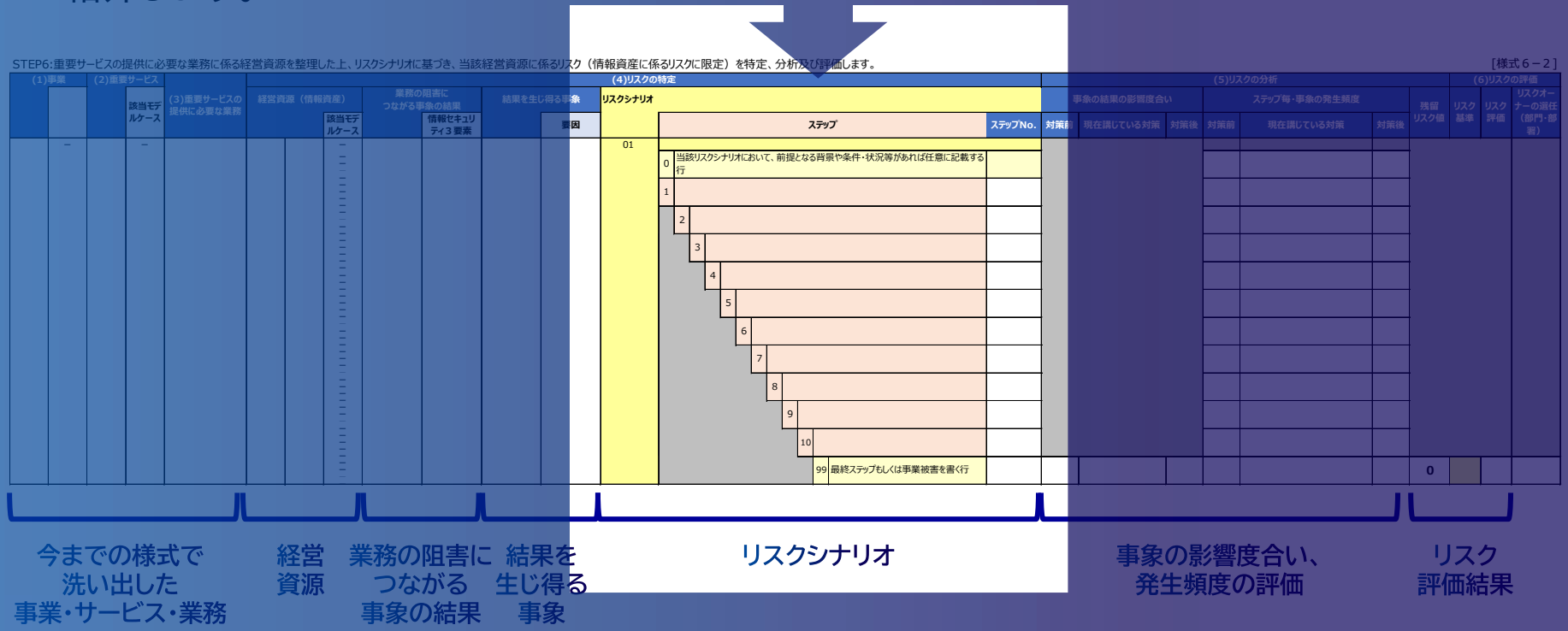


各組織における事業・重要サービス・重要サービスを支える業務を洗い出し、業務を支える経営資源ごとに、リスクシナリオを用いてリスクの特定を行っていく様式となります。

まずは、様式6-2 リスクアセスメント(リスクシナリオ)

リスクシナリオの作り方を体験してみましょう。

本ワークショップでは、リスクシナリオの作成方法について、様式6-2を用いたリスク評価手法をご紹介します。

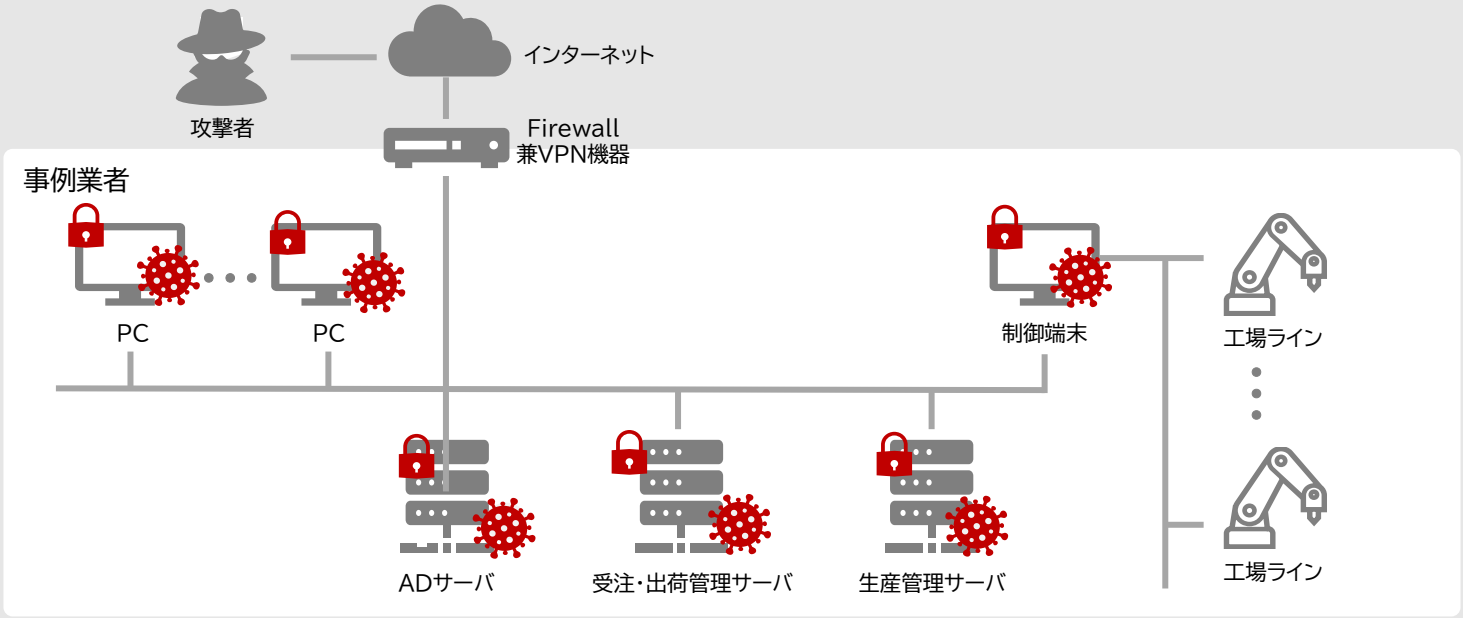


各組織における事業・重要サービス・重要サービスを支える業務を洗い出し、業務を支える経営資源ごとに、リスクシナリオを用いてリスクの特定を行っていく様式となります。

Case Study

インシデント事例からのリスクシナリオの作成

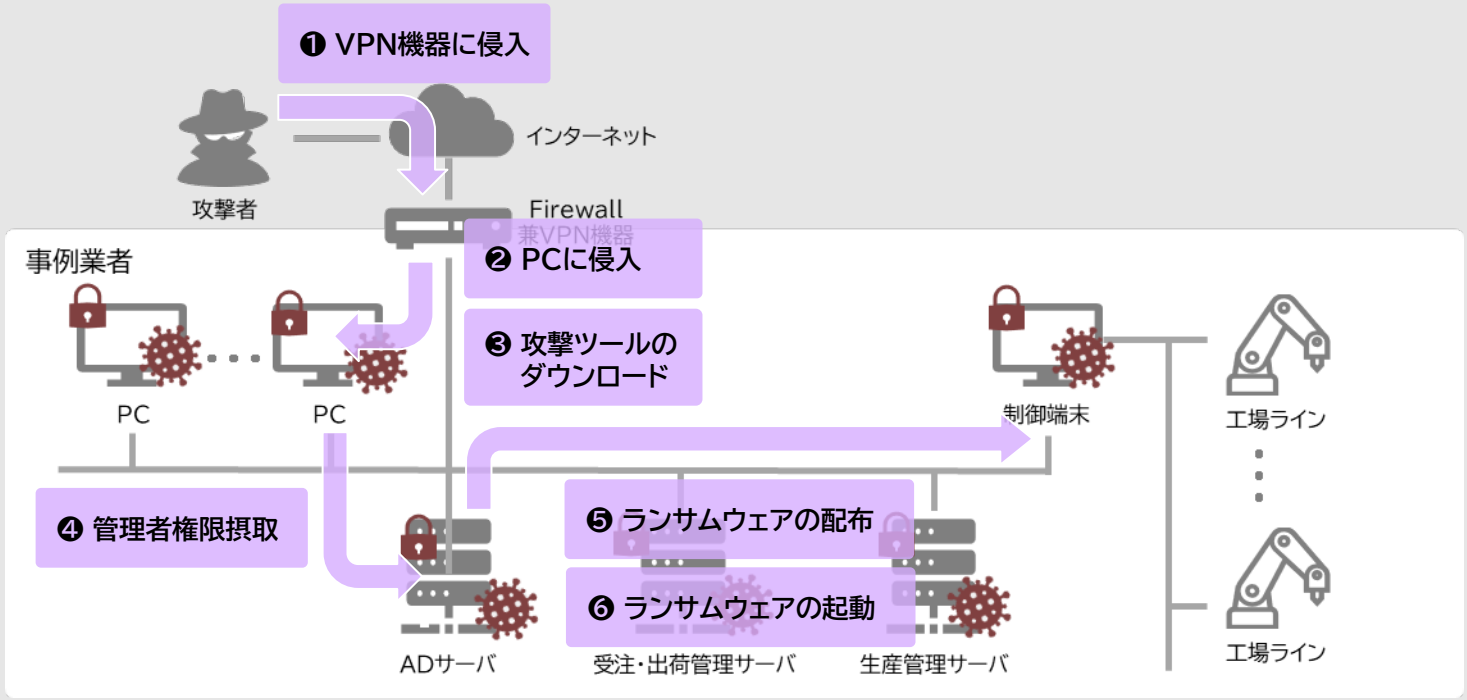
ある製造業者（以下、「事例業者」という。）において、ランサムウェアにより、サーバに保存されていたファイルが暗号化され、業務継続が困難となった事例が公表されました。
この事例をもとに、攻撃者の流れを考えてみましょう。



Case Study

インシデント事例からのリスクシナリオの作成

事例業者の公表内容を読み取ると、以下の流れで攻撃が行われたことが分かりました。



Case Study

インシデント事例からのリスクシナリオの作成

様式6-2の「リスクシナリオ」に記載できるように書き直したものが以下の内容となります。

01	**悪意のある第三者によるランサムウェアの起動により、重要サービスが停止する。**
1	攻撃者は、VPN機器の**初期パスワードでログインし、侵入する**
2	攻撃者は、VPN利用者のアカウント一覧を入手し、 社内ネットワーク内の**推測しやすいパスワードを使用していた**PCに侵入する
3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**
4	攻撃者は、ADサーバの脆弱性を悪用し**ADサーバの管理者アカウント情報を窃取し、不正にログインする**
5	攻撃者は、ADサーバから**各端末・サーバにRDPでログインし、ランサムウェアを設置する**
6	攻撃者は、**ランサムウェアを起動し、保存されていたファイルを暗号化**

インシデントを踏まえたリスクシナリオの考察

次はその攻撃ステップを自組織に当てはめてリスクシナリオを作成していきます。

しかし、自組織の環境は事例業者と環境や対策が異なるため、事例業者で行われた攻撃を参考に、リスクシナリオをカスタマイズする必要があります。

インシデント事例

原因

VPN機器が**初期パスワードのまま運用**されている。

攻撃ステップ

攻撃者は、**初期パスワードのまま運用されていた**VPN機器の管理画面に対しログインを試行、VPN機器に侵入する。

自組織の環境を踏まえて
攻撃ステップをカスタマイズ

カスタマイズ例

原因

VPN機器の**パッチ適用を半期に1回のみ実施**している。

攻撃ステップ

攻撃者は、**パッチが未適用のVPN機器に対し、公開されている脆弱性を悪用**し、認証回避の攻撃を試行、VPN機器に侵入する。

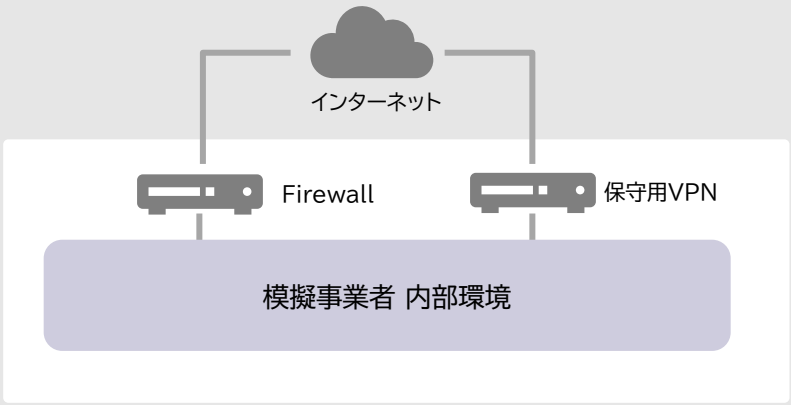
本コンテンツでは、学習用の模擬事業者（A社）の環境で、リスクアセスメントを簡易にご体験いただきます。

Question

模擬事業者（A社）における リスクシナリオの検討1

事例業者で生じたリスクシナリオが、模擬事業者（A社）において発生した場合に、最初に行われる攻撃（ステップ1）を考えてみましょう。

模擬事業者（A社）の環境



模擬事業者（A社）における対策状況

- Firewall、保守用VPNは、複雑なパスワードが設定されており、認証失敗が一定回数発生した際にアカウントのロックが発動する
- Firewallは、週1回、パッチの適用や設定内容の棚卸確認を実施、さらに緊急度の高い脆弱性の公表時に、適宜のパッチ適用を実施
- 保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施
- メールセキュリティゲートウェイを導入し、メール経由でのスパム・マルウェア対策を実施
- 委託先を含め、年1回、標的型攻撃メール訓練を実施

事例業者のステップ1

1	攻撃者は、VPN機器の初期パスワードでログインし、侵入する

模擬事業者の環境を踏まえて ステップ1をカスタマイズ

模擬事業者（A社）におけるステップ1

1	？？？

Question

模擬事業者（A社）における リスクシナリオの検討1

事例業者で生じたリスクシナリオが、模擬事業者（A社）において発生した場合に、最初に行われる攻撃（ステップ1）を以下の4つから選択してみましょう。

A Firewall への総当たり攻撃による認証の突破

B 保守用VPNに残存していた脆弱性の悪用

C フィッシングメールによるFirewallの認証情報の窃取

D Firewallで、誤ってアクセス制限が解除された時機を狙った不正アクセス

A　Firewall への総当たり攻撃による認証の突破

Firewallは、認証失敗が一定回数発生した際にアカウントのロックが発動するため、総当たり攻撃での突破は困難、と考えられる。

B　保守用VPN に残存していた脆弱性の悪用

保守用VPNは緊急度の高い脆弱性が公表された場合の適宜のパッチ適用は実施していないため、侵入し得る余地がある、と考えられる。

C　フィッシングメールによるFirewallの認証情報の窃取

年1回の標的型攻撃メール訓練とメールセキュリティゲートウェイの導入により、一定のフィッシングメール耐性がある、と考えられる。

D　Firewallで、誤ってアクセス制限が解除された時機を狙った不正アクセス

Firewallは週1回、設定内容の棚卸確認を行っていることから、発生頻度は低い、と考えられる。

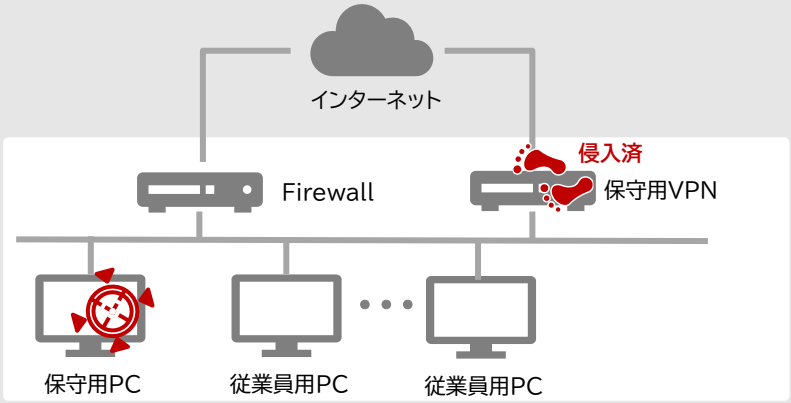
自組織における環境・対策状況を踏まえて、
リスクシナリオが発生し得る攻撃手法を
ステップ毎に検討しながら、リスクシナリオを作成していきます。

Answer

模擬事業者(A社)における リスクシナリオ｜ステップ2

保守用VPNから内部侵入拡大を行うステップです。
事例業者では、VPN機器内に保存されていたアカウント一覧が利用されましたが、模擬事業者（A社）ではパスワード管理が脆弱であった保守用PCが標的になったと考えました。

模擬事業者(A社)の環境



模擬事業者(A社)の環境情報

- 従業員用PCでは、従業員用のアカウントは従業員ごとに個別に払い出し、共有アカウントの利用を禁止している
- 従業員用PCでは、認証失敗が一定回数続くとアカウントのロックが発動する
- 保守用PCでは、共通の保守アカウントを複数担当者で共有しており、**パスワードは覚えやすい簡易なパスワードを設定している**
- 保守用PCでは、認証失敗が一定回数続くとアカウントをロックする設定を行っているが、保守作業の利便性のため、**従業員用PCよりアカウントのロックに必要な認証失敗回数が多い**

事例業者のステップ2

2	攻撃者は、VPN利用者のアカウント一覧を入手し、社内ネットワーク内の**推測しやすいパスワードを使用していた**PCに侵入する

模擬事業者の環境を踏まえて ステップ2をカスタマイズ

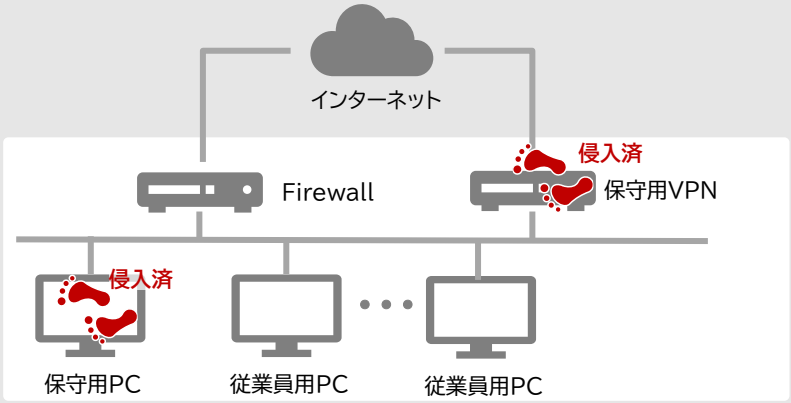
模擬事業者(A社)におけるステップ2

2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する

模擬事業者(A社)における リスクシナリオ｜ステップ3

侵入したPCに攻撃ツールをダウンロードし、攻撃のための基盤構築を行うステップです。
事例業者で用いられた攻撃が、模擬事業者(A社)においても実行可能か対策状況を確認した結果、同じ攻撃が成立し得る、と評価しました。

模擬事業者(A社)の環境



模擬事業者(A社)の環境情報

- Firewallでは、URLフィルタリングを設定し、各PCからのインターネットのアクセスを制限
- Firewallでは、各PCからのインターネットへのファイルのアップロードおよびダウンロードは特定のWebサイトに制限
- 保守用VPNは、**保守用PCのみインターネットに接続可能**となるよう制限
- 保守用ツールや各種パッチ取得のため、**保守用VPN経由では様々なWebサイトへのアクセスおよびファイルのダウンロードが可能**

事例業者のステップ3

3	攻撃者は、侵入したPCに攻撃ツールをダウンロードする

模擬事業者の環境を踏まえて
ステップ3はそのまま適用

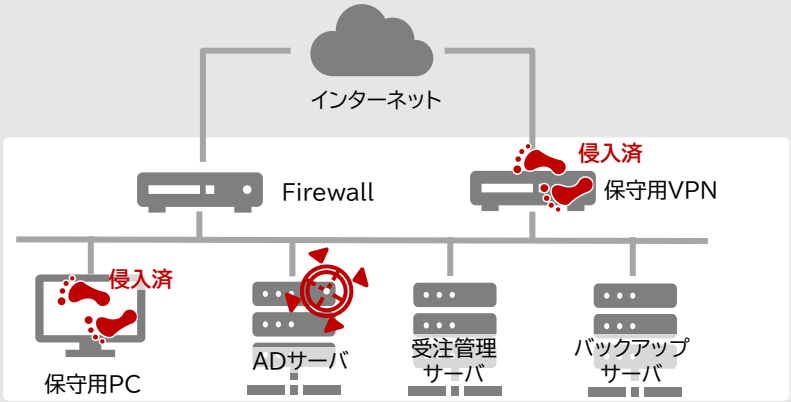
模擬事業者(A社)におけるステップ3

3	攻撃者は、侵入したPC(保守用PC)に攻撃ツールをダウンロードする

模擬事業者(A社)における リスクシナリオ｜ステップ4

内部侵入拡大が行われるステップです。事例業者ではADサーバの脆弱性が悪用されています。しかし、模擬事業者(A社)では、適宜のパッチ適用が実施されているため、同様の攻撃はできず、保守用PCに保存された認証情報を攻撃ツールを用いて窃取が行われたシナリオとしました。

模擬事業者(A社)の環境



模擬事業者(A社)の環境情報

- 攻撃者は最初の侵入時に保守用PCの管理者権限を窃取している
- 保守用PCでは、**ADサーバの管理者アカウントを用いて当該PCにログインして障害調査を実施**しており、**ログイン情報へのアクセスを制限する保護機能が無効化されている**
- ADサーバは、各PCやサーバの設定を変更可能な強い管理者権限(ドメイン管理者アカウント)が存在する
- ADサーバは、月1回、パッチの適用や設定内容の棚卸確認を実施、さらに緊急度の高い脆弱性の公表時に、適宜のパッチ適用を実施

事例業者のステップ4

4	攻撃者は、ADサーバの脆弱性を悪用し**ADサーバの管理者アカウント情報を窃取し、不正にログインする**

模擬事業者の環境を踏まえて ステップ3はそのまま適用

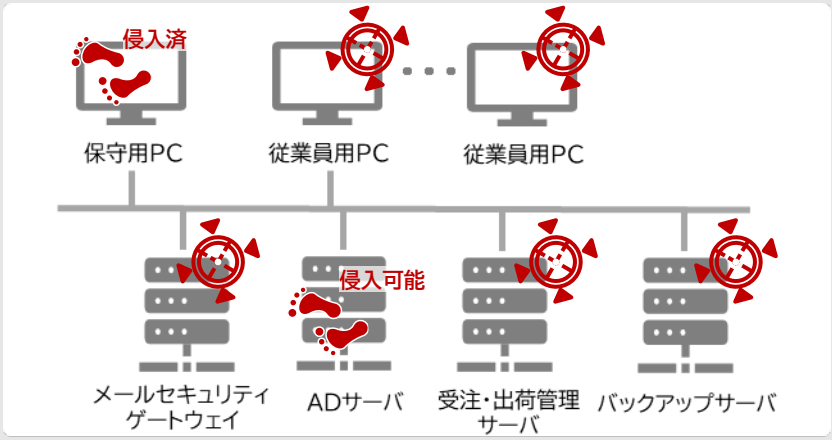
模擬事業者(A社)におけるステップ4

4	攻撃者は、**攻撃ツールを用いて保守用PCに保存されていたADサーバの管理者アカウントの情報を窃取し、ADサーバに不正にログインする**

Question 模擬事業者（A社）における リスクシナリオの検討2

模擬事業者（A社）の環境において、模擬事業者（A社）の各端末・サーバにランサムウェアを配布する攻撃手法を考えてみましょう。

模擬事業者（A社）の環境



模擬事業者（A社）の環境情報

- 攻撃者はADサーバの管理者アカウントの認証情報を窃取済みで、ADサーバにログイン可能
- ADサーバは、ネットワーク上の全てのサーバ・端末に、設定・ファイルを一括配布する機能（グループポリシーオブジェクト）を持つ
- 全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入しており、EDRの設定はADサーバの機能（グループポリシーオブジェクト）で管理
- 全てのサーバ・端末へのRDP（ネットワーク越しに端末へログインする機能）は禁止

事例業者のステップ5

5	撃者は、ADサーバから各端末・サーバにRDPでログインし、ランサムウェアを設置する

模擬事業者の環境を踏まえて ステップ5をカスタマイズ

模擬事業者（A社）におけるステップ5

5	？？？

Question

模擬事業者（A社）における リスクシナリオの検討2

模擬事業者（A社）の環境において、模擬事業者（A社）の各端末・サーバにランサムウェアを配布する攻撃手法を以下の4つから選択してみましょう。

A 全社員にランサムウェア添付メールを送信する

B 各端末・サーバにRDPでログインしランサムウェアを設置する

C 各端末・サーバのEDRを無効化しランサムウェアを配布する

D ADサーバで全ユーザのパスワードを強制変更する

A　全社員にランサムウェア添付メールを送信する

年1回の標的型攻撃メール訓練とメールセキュリティゲートウェイの導入により、一定のフィッシングメール耐性がある、と考えられる。

B　各端末・サーバにRDPでログインしランサムウェアを設置する

全てのサーバ・端末へのRDPは禁止されており、まずRDPの禁止設定を解除した上で、サーバ・端末個別にログインを行う必要があるため、攻撃に時間を要する、と考えられる。

C　各端末・サーバのEDRを無効化しランサムウェアを配布する

ADサーバが持つ機能（ネットワーク上の端末・サーバに対して設定・ファイルを一括配布する機能）を利用して、EDRの無効化及びランサムウェアの配布が可能、と考えられる。

D　ADサーバで全ユーザのパスワードを強制変更する

各端末・サーバのパスワードを強制的に変更したとしても、ランサムウェアを配布することはできない、と考えられる。

リスクシナリオの検討にあたっては、
実施している対策が有効に機能しない場合も想定して、
評価を行っていきましょう。

Answer

Case Study

インシデント事例からのリスクシナリオの作成

ここまで整理した模擬事業者（A社）における攻撃ステップを、様式6-2の「リスクシナリオ」に記載できるように書き直したものが以下の内容となります。

01	悪意のある第三者によるランサムウェアの起動により、重要サービスが停止する。	
	1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する
	2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する
	3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**
	4	攻撃者は、**攻撃ツールを用いて保守用PCに保存されていたADサーバの管理者アカウントの情報を窃取し、ADサーバに不正にログインする**
	5	攻撃者は、ネットワーク上のサーバと端末に対して、ADサーバの設定を一括配布する機能（グループポリシーオブジェクト）を悪用し、**EDRの無効化命令とランサムウェアを配布**する
	6	攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**

完成したリスクシナリオに対して、ステップごとに実施している対策状況を踏まえリスク評価を行っていきます。

様式6-2 リスクアセスメント(リスクシナリオ)

このコンテンツでは、リスクシナリオのアプローチ手法における評価手法をご紹介します。

各組織における事業・重要サービス・重要サービスを支える業務を洗い出し、業務を支える経営資源ごとに、リスクシナリオを用いてリスクの特定を行っていく様式となります。

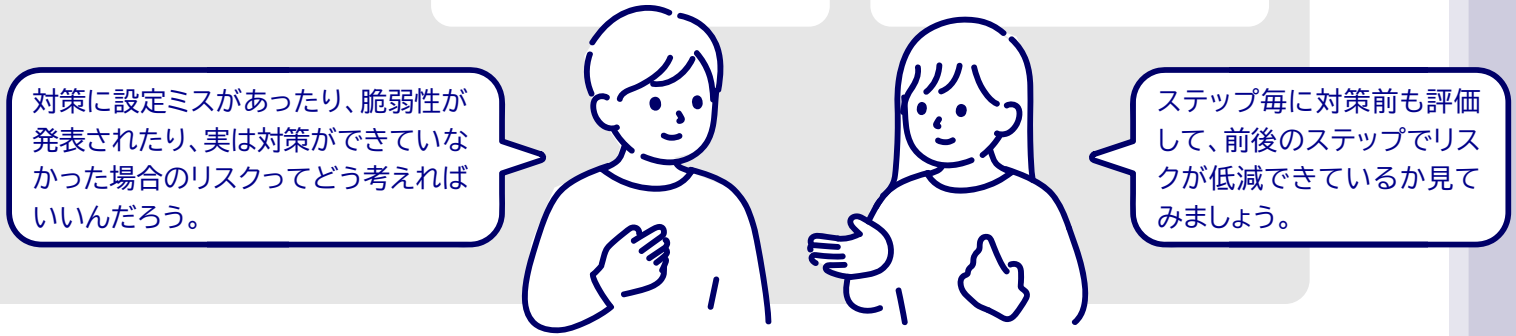
ステップ毎・事象の発生頻度の評価

様式6-2 では、リスクシナリオのステップ毎に対策前と対策後のリスクを評価します。

		対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する		講じている対策を記載	
2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する			
3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**			

対策が実施されていない場合又は対策が陳腐化した場合のリスク値

講じている対策が想定通り、機能している場合のリスク値



Question

模擬事業者（A社）における ステップ1の対策状況

リスクシナリオのステップ1の攻撃に対し、模擬事業者（A社）が講じている対策について考えてみましょう。

模擬事業者の環境情報

- 保守用VPNは、認証失敗が一定回数発生した際にアカウントのロックが発動する
- 保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施
- メールセキュリティゲートウェイを導入し、メール経由でのスパム・マルウェア対策を実施
- 委託先を含め、年1回、標的型攻撃メール訓練を実施

様式6-2上での記載

回答箇所

	攻撃ステップ	対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する			

Question

模擬事業者（A社）における ステップ1の対策状況

保守用VPNの脆弱性悪用が行われる攻撃に対し、模擬事業者（A社）で現在、講じている対策を以下から選んでください。

A 保守用VPNの認証失敗が一定回数発生した際に、アカウントのロックが発動する

B 保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施

C メールセキュリティゲートウェイを導入

D 委託先を含め、年1回、標的型攻撃メール訓練を実施

A

保守用VPNの認証失敗が
一定回数発生した際に、
アカウントのロックが発動する

アカウントのロックによって保守用VPNの脆弱性を悪用した攻撃の発生頻度を低減できる効果は、非常に限定的である。

B

保守用VPNは、
四半期に1回、パッチの適用や
設定内容の棚卸確認を実施

パッチの適用により脆弱性の解消が図られ、設定内容の棚卸を通じて設定ミス等への対応が行われ得ることから、保守用VPNの脆弱性を悪用した攻撃への対策と言える。

C

メールセキュリティゲートウェイ
を導入

メールセキュリティゲートウェイは、メール経由でのスパム・マルウェアへの対策であり、保守用VPNの脆弱性を悪用した攻撃への対策ではない。

D

委託先を含め、年1回、
標的型攻撃メール訓練を実施

年1回の標的型攻撃メール訓練は、メール経由での標的型攻撃への対策であり、保守用VPNの脆弱性を悪用した攻撃への対策ではない。

攻撃を検知、防御するために講じている対策を
ステップ毎に整理を行い、
リスクが低減されているのか評価していきます。

Answer

Question

模擬事業者（A社）における ステップ1の発生頻度の評価

先ほどの回答を踏まえて、様式6-2には「現在講じている対策」を記載しました。対策後のリスク値を評価基準を使って評価してみましょう。

なお、対策前は脆弱性への対応（パッチ適用）が行われておらず、攻撃を防ぐための対策が講じられていないことから、「発生頻度 ：５　頻発（ほぼ確実に発生する）」と評価しています。

様式6-2上での記載

回答箇所

攻撃ステップ		対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に１回、パッチの適用や設定内容の棚卸確認を実施	

事象の発生頻度の評価基準

発生頻度		事象の予想発生頻度
5	非常に多い	頻発（ほぼ確実に発生する）
4	多い	1年に1回程度発生（通過する確率が高い）
3	中程度の頻度	数年に1回程度発生（通過する/止められる確率が拮抗）
2	少ない	10年に1回程度発生（止められる確率が高い）
1	非常に少ない	ごくまれに、例外的な状況で発生（ほとんどの場合止められる）

Question

模擬事業者（A社）における ステップ1の発生頻度の評価

保守用VPNの脆弱性悪用が行われる攻撃に対し、模擬事業者（A社）が講じている対策を踏まえて、どの程度発生頻度が低減できているか、考えてみましょう。

A 発生頻度：5
頻発（ほぼ確実に発生する）

B 発生頻度：4
1年に1回程度発生

C 発生頻度：3
数年に1回程度発生。

D 発生頻度：1
ごくまれに、例外的な状況で発生

A

発生頻度：5
頻発（ほぼ確実に発生する）

四半期に1回のパッチ適用により、既知の脆弱性に対しては一定程度対策はできているため、攻撃が「ほぼ確実に発生する」とは評価できない。

B

発生頻度：4
1年に1回程度発生

四半期に1回のパッチ適用では、公開後に短時間で悪用され得る脆弱性への対応が間に合わないおそれがあり、インターネットから直接アクセス可能な場所に設置されていることから、発生頻度は一定に高いと評価できる。

C

発生頻度：3
数年に1回程度発生。

悪用され得る緊急度の高い脆弱性が発見・公表される頻度は機器・メーカにより異なるものの、数年に1回程度よりは高い頻度であることが多い。

D

発生頻度：1
ごくまれに、例外的な状況で発生

悪用され得る緊急度の高い脆弱性が発見・公表される頻度は機器・メーカにより異なるものの、ごくまれに、と言える頻度ではないことが多い。

評価基準を用いて、定量的な評価を行いましょう。
また、「攻撃が行われる前提」で評価してください。

Answer

Case Study

ステップ毎・事象の発生頻度の評価

ステップ1と同様に、ステップ2以降もステップ毎の攻撃内容に対して講じている対策を整理し、同じ評価基準を用いて、事象の発生頻度の評価を行いました。

攻撃ステップ	対策前	現在講じている対策	対策後
1 攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2 攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3 攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	4
4 攻撃者は、**攻撃ツールを用いて保守用PCに保存されていたADサーバの管理者アカウントの情報を窃取し、ADサーバに不正にログインする**	5	ー	5
5 攻撃者は、ネットワーク上のサーバと端末に対して、ADサーバの設定を一括配布する機能（グループポリシーオブジェクト）を悪用し、**EDRの無効化命令とランサムウェアを配布**する	5	グループポリシーオブジェクトが変更された場合のログを取得	5
6 攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

Case Study

ステップ毎・事象の発生頻度の評価

ステップ2では、パスワードの試行に対しアカウントロックの設定が行われていました。
しかし、推測しやすい脆弱なパスワードが利用されているため、多くない回数で特定可能であると評価しました。

攻撃ステップ	対策前	現在講じている対策	対策後
1 攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2 攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3 攻撃者は、侵入したPCに**攻撃ツールを**			
4 攻撃者は、**攻撃ツールを用いて保守** **の管理者アカウントの情報を窃取し**			
5 攻撃者は、ネットワーク上のサー 定を一括配布する機能（グループポリシーオブジェクト）を悪用し、 **EDRの無効化命令とランサムウェアを配布**する	5	グループポリシーオブジェクトが変更された場合のログを取得	5
6 攻撃者は、ネットワーク上のサーバ（バックアップサー む）や端末で**ランサムウェアを起動し、保存されていたファイ** **ルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

アカウントロックはパスワード試行に一定の効果があると考えられるが、推測しやすいパスワードを利用していること、またアカウントのロックに必要な認証失敗回数が多くなっていることから、事象の発生頻度は低減できない、と評価した。

POINT
対策が講じられていても、対策前とリスク値が変わらない場合もある

Case Study

ステップ毎・事象の発生頻度の評価

ステップ3では、ウイルス対策ソフト・EDRが導入されているため、攻撃ツールを検知できる可能性はあるものの、正規ツールを用いられる場合などの検知ができない場合を想定して対策後も「4」としています。

	攻撃ステップ	対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	4
4	攻撃者は、**攻撃ツールを用いて保守用PCに保存されていたADサーバの管理者アカウントの情報を窃取し、ADサーバに不**			
5	攻撃者は、ネットワーク上のサーバと端末に対し 定を一括配布する機能（グループポリシーオブジ **EDRの無効化命令とランサムウェアを配布**する			
6	攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

攻撃ツールには、Windowsの正規ツール等も含まれており、ウイルス対策ソフトでは検知できないおそれがある。また、EDRによる振る舞い検知も必ず検知が可能、とは評価できなかった。

Case Study

ステップ毎・事象の発生頻度の評価

ステップ4は、保守用PC内に保存されていたADサーバの管理者アカウント情報の窃取となりますが、攻撃を防ぐための対策は模擬事業者（A社）ではとられていなかったことから、対策前・後ともに「5」と評価しています。

攻撃ステップ	対策前	現在講じている対策	対策後
1 攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2 攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3 攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	4
4 攻撃者は、**攻撃ツールを用いて保守用PCに保存されていたADサーバの管理者アカウントの情報を窃取し、ADサーバに不正にログインする**	5	－	5
5 攻撃者は、ネットワーク上のサーバと端末に対して、ADサーバの設定を一括配布する機能（グループポリシーオブジェクト）を悪用し、**EDRの無効化命令とランサムウェアを配布**する	5	グループポリシーオブジェクトが変更された場合のログを取得	5
6 攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

Case Study

ステップ毎・事象の発生頻度の評価

ステップ5では、検知のための対策として「ログの取得」が行われていましたが、攻撃を検知可能な対策となっているか確認したところ、リアルタイム監視の対象外であったことから対策前後変わらず「5」と評価した。

	攻撃ステップ	対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードす**			
4	攻撃者は、**攻撃ツールを用いて保守用PCに保存さ** **の管理者アカウントの情報を窃取し、ADサーバに不正にログインする**			
5	攻撃者は、ネットワーク上のサーバと端末に対して、ADサーバの設定を一括配布する機能（グループポリシーオブジェクト）を悪用し、**EDRの無効化命令とランサムウェアを配布**する	5	グループポリシーオブジェクトが変更された場合のログを取得	5
6	攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

ログの取得は行われているものの、模擬事業者（A社）では、リアルタイム監視が行われていなかったため、速やかな検知と対応ができないことから、事象の発生頻度は低減できない、と評価した。

Case Study

ステップ毎・事象の発生頻度の評価

ステップ6では、ランサムウェアの起動です。
ウイルス対策ソフト・EDRは導入されていますが、既にステップ5で無効化されていることをふまえた評価をしました。

	攻撃ステップ	対策前	現在講じている対策	対策後
1	攻撃者は、保守用VPNの**脆弱性を悪用**し、当該機器に侵入する	5	保守用VPNは、四半期に1回、パッチの適用や設定内容の棚卸確認を実施	4
2	攻撃者は、**推測しやすい脆弱なパスワードを使用していた**保守用PCに侵入する	5	PCにアカウントロックを設定	5
3	攻撃者は、侵入したPCに**攻撃ツールをダウンロードする**			
4	攻撃者は、**攻撃ツールを用いて保守用PCに保存さ の管理者アカウントの情報を窃取し、ADサーバにネ**			
5	攻撃者は、ネットワーク上のサーバと端末に対 定を一括配布する機能（グループポリシーオブ **EDRの無効化命令とランサムウェアを配布**する			
6	攻撃者は、ネットワーク上のサーバ（バックアップサーバを含む）や端末で**ランサムウェアを起動し、保存されていたファイルを暗号化する**	5	全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入	5

POINT
リスクシナリオの中で無効化された対策は、その後のステップでは対策が機能していない対策として評価する

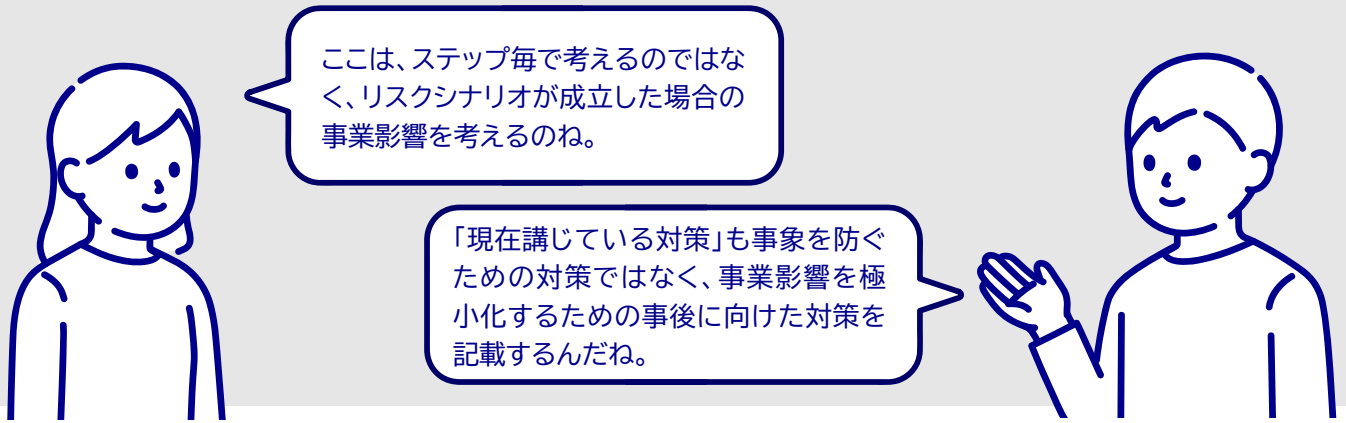
ウイルス対策ソフトやEDRが導入されているものの、ステップ5で無効化されており、既にこのステップでは有効に機能していないため、事象の発生頻度は低減できない、と評価した。

重要サービス・業務への影響度合いの評価

様式6-2 では、リスクシナリオの最終行に「事業被害」を記載する欄を用意しています。

この行を利用して、重要サービス・業務への影響度合いの評価を行います。

		対策前	現在講じている対策	対策後
99	作成したリスクシナリオを踏まえ、本シナリオが発生した際の事業被害（又は最終ステップ）を記載する。		事象の結果の影響度合いを小さくするための対策状況について記載します。	



Case Study

重要サービス・業務への影響度合いの評価

模擬事業者（A社）では、以下のような記載となりました。

様式6-2上での記載

		対策前	現在講じている対策	対策後
99	VPN機器の脆弱性を悪用した侵入を端緒としてランサムウェア感染が発生し、従業員PCに加え、受発注システム等の業務システムを含む複数サーバが暗号化被害を受けた。 バックアップは取得していたものの、整備していた復旧手順書に不備があり手順どおりに復旧できず、システム復旧までに3カ月を要した。 また、手動による業務再開を試みたが、最大許容停止時間（1日）以内に再開できず、当該期間中の受発注業務が著しく低下した結果、業績に多大な影響を及ぼした。	5	日次でバックアップを取得	4

重要サービス・業務への影響度合いの評価基準

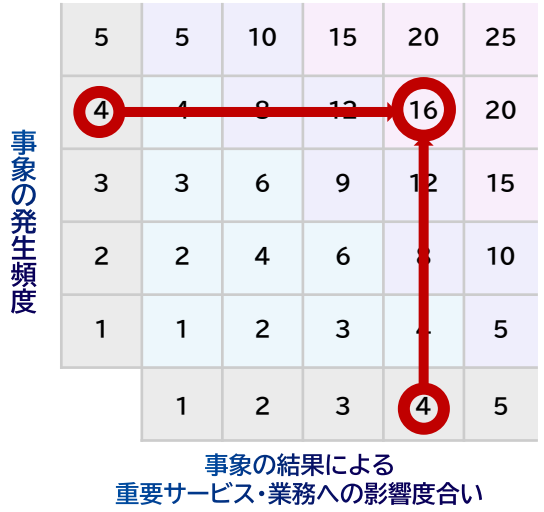
影響度		業務に対する影響の範囲・程度
5	重大な影響	業務の**復旧自体が困難**である。
4	大きな影響	業務の**最大許容停止時間内での業務の復旧が困難**である。
3	中程度の影響	業務の**最大許容停止時間内での業務の復旧が可能**である。
2	小さな影響	業務の阻害が軽度で**収まる時間内での復旧**が可能である。
1	軽微な影響	業務の**阻害が生じない時間内での復旧**が可能である。

模擬事業者（A社）の残留リスク値の算出

「事象の発生頻度」と「事象の結果による重要サービス・業務への影響度合い」を掛け合わせ、残留リスク値を算出できます。

残留リスク値がリスク基準を下回った場合や特性等を踏まえ、対応が必要と判断した場合は、リスク対応が必要なリスクとして、リスクオーナを選出し、残留リスクの低減等の取組に繋げてください。

今回のリスクシナリオにおけるリスク値



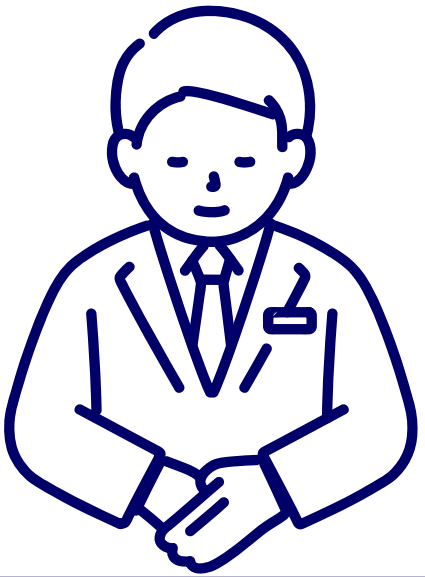
リスクオーナの役割

リスクの対処に関する責任を負担する部署・部門又は役職員のことを「リスクオーナ」と呼び、以下のような役割を担っています。

- **リスクへの対応方針（回避・低減・移転・保有）の検討**
- **経営層、リスクアセスメント実施体制への対応方針や対応状況の報告**
- **対応状況のモニタリング**

リスクアセスメント

ご紹介したリスクアセスメントの手法は、
様々なある中でのひとつの手法にすぎません。
組織・環境、状況等によって
効果的・効率的な手法・手順は異なり、
手法や手順には、唯一の正解はありません。
「事業継続」の確保に向け、
少しでも参考になれば幸いです。



05

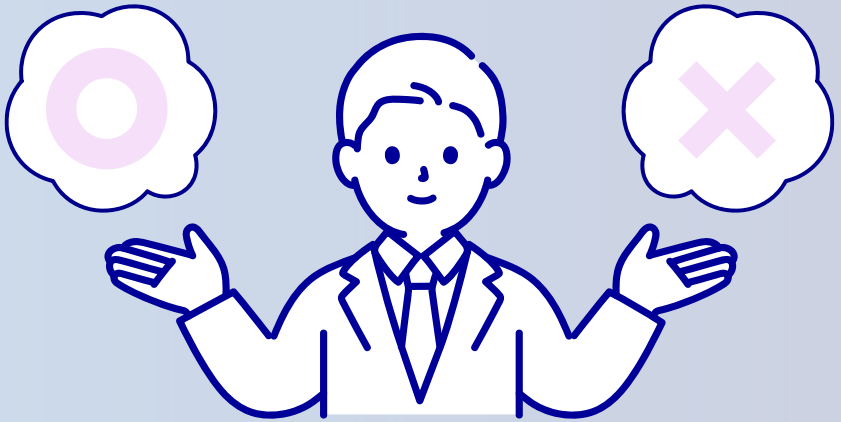
リスクアセスメントの妥当性確認・評価

リスクアセスメントの妥当性確認・評価

リスクアセスメントを実施した後に、その取組や結果の妥当性を評価し、「作業者による偏りやばらつきの解消」や「フィードバック・改善」に繋げていきます。

作業者による偏りやばらつきの解消

作業者の知識や経験による偏り、分担作業による精度のばらつきが生じていないか、複数の関係主体が連携して妥当性を検証します。



フィードバック・改善

リスクアセスメントを実施する体制、実施手順及び活動状況が適切・十分であったかを評価し、関係者にフィードバック・改善につなげます。

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）

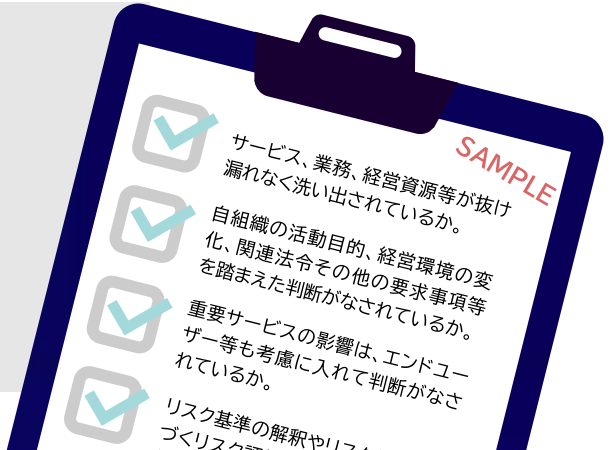
リスクアセスメントの実施目的の確認からリスクアセスメント（リスクの評価）までの一連の取組を対象として、指摘事項を出し合い、互いが持っているリスクに対する認識をすり合わせ、必要な修正事項を導き出します。

担当者の選任及び役割分担

リスクアセスメントを実施した担当者だけでなく、関連業務の所管部門や経営資源の利用・管理部門等にも参画いただくことで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ための指摘や意見交換が実現できます。
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も効果的です。

確認観点の策定と修正の反映

参加者がリスクアセスメントの結果の正当性を確認し、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ます。
ウォークスルーを通じて、確認観点を踏まえた指摘事項を出し合い、互いの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、リスクアセスメントの成果物への反映を行います。

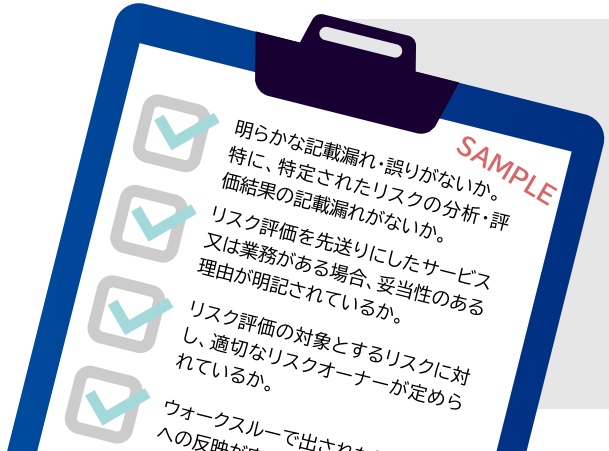


パフォーマンス評価(リスクアセスメント作業の妥当性確認)

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です。
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。

評価担当者の選任

会計監査や業務監査等と同様、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、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。
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るため、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。



評価の実施と各関係主体へのフィードバック

パフォーマンス評価の結果は、改善すべき事項等を含め、後続で検討するリスク対応の最終責任者である経営層を含めた各関係主体と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。

06

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

リスクアセスメントを通じて確認できた状態は、不変ではなく、内外の環境変化などにより変化してしまうことが予想されます。また妥当性評価等の取組を通じて検出できた改善すべき点が適切に対応されるための管理も重要です。

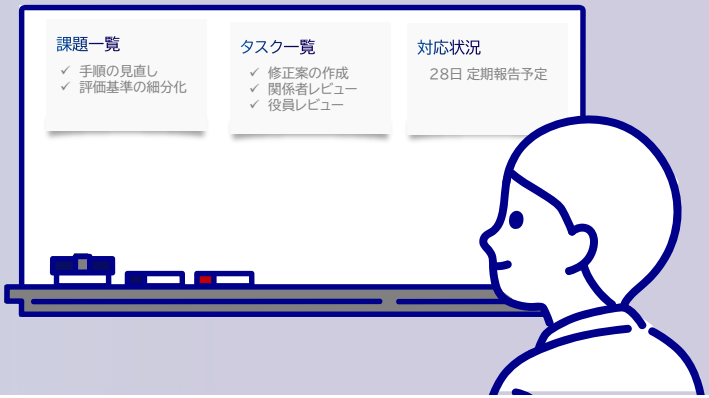
以下の2つの取組を行い、リスクアセスメントの継続的な見直し・改善を図りましょう。

リスク管理

リスクアセスメントを実施した際に前提としていた内外の環境に、変化が生じていないかモニタリングを実施し、次回以後のリスクアセスメント作業に向けた対応方針へ反映を行います。

課題管理

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、対応を行っていきます。



リスクアセスメントの継続的な見直し

リスク管理や問題管理を通じて、
適宜、リスクアセスメント結果の見直しを実施し、
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しましょう。

99

おわりに

組織のリスクを正しく把握して、効率的に対策を講じましょう

ランサムウェア、標的型攻撃、内部不正　－　サイバー環境における脅威は日々変化しています。リスクアセスメントで最新の脅威を把握し、技術・人・プロセス等の観点から対策を講じることが、デジタル時代におけるサービスを提供し続ける組織にとって必要不可欠な取組です。