リスクアセスメント実践ラーニングキット解説・研修展開マニュアル

～自己学習、研修教材～

内閣官房 国家サイバー統括室

SLIDE 01

Agenda

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」に基づき、リスクアセスメントの手順を紹介しています。

「はじめに」と「おわりに」を除くと、大きく6つの章で構成されています。

SLIDE 02

はじめに

00

はじめに

まず、なぜリスクアセスメントを実施する必要があるのか、その背景について簡単にご説明します。

SLIDE 03

はじめに①

近年、私たちの生活においてさまざまな場面で情報通信技術が活用されており、情報システムやクラウドサービス、テレワーク環境など、今や情報通信技術は業務に欠かせない存在となっています。

一方で、情報通信技術の活用拡大に伴い、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。

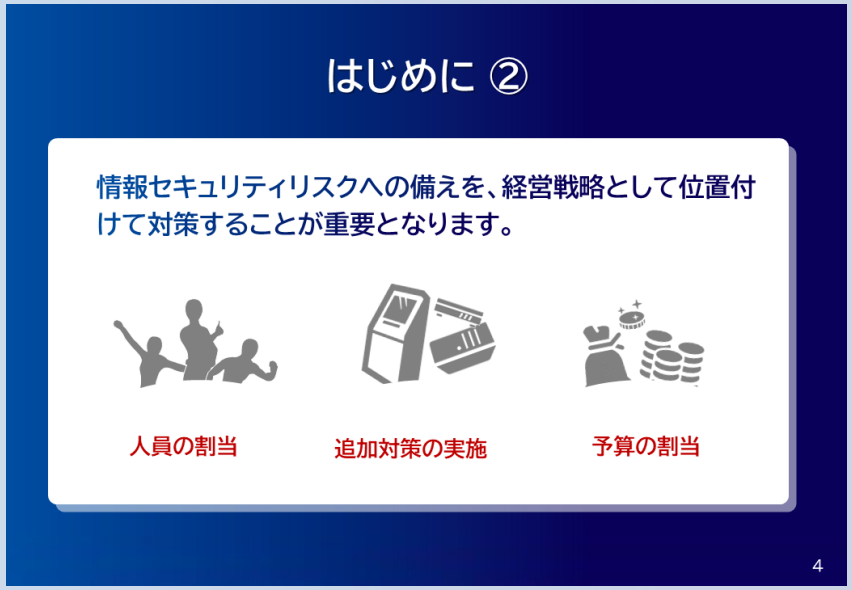
例えば、システム障害の影響で業務にも長期間の停止が発生したり、さらに業務の停止が社会や経済活動に大きな影響を及ぼしたりするケースも見られます。

また、情報漏えいや長時間のサービス停止が発生した場合、組織の社会的信用が大きく損なわれる可能性もあります。

このように、情報セキュリティリスクは、組織だけではなく社会経済全体に影響する重要な課題になっています。

SLIDE 04

はじめに②

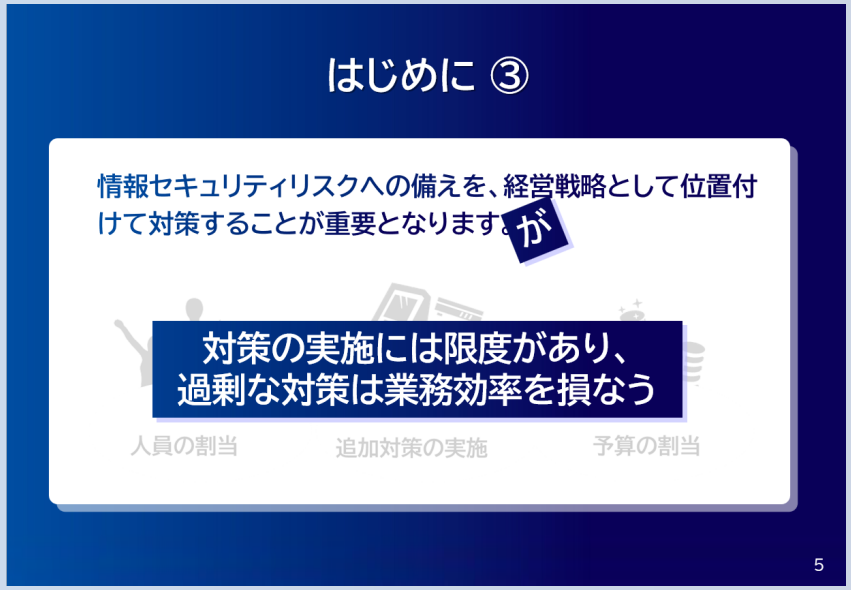


　こうした背景を踏まえると、情報セキュリティリスクへの備えは、技術的な対策だけでなく、経営戦略として位置付け、人やお金、時間といった経営資源を適切に配分することが必要となります。

　例えば、情報セキュリティを担当する人員をどの程度割り当てるのか、新たな対策をどこまで実施するのか、どれくらいの予算を割り当てるのか、こうした判断は現場だけではなく、経営戦略の一部として考える必要があります。

SLIDE 05

はじめに③



しかし、どんな組織であっても、使える人員や予算には限りがあります。

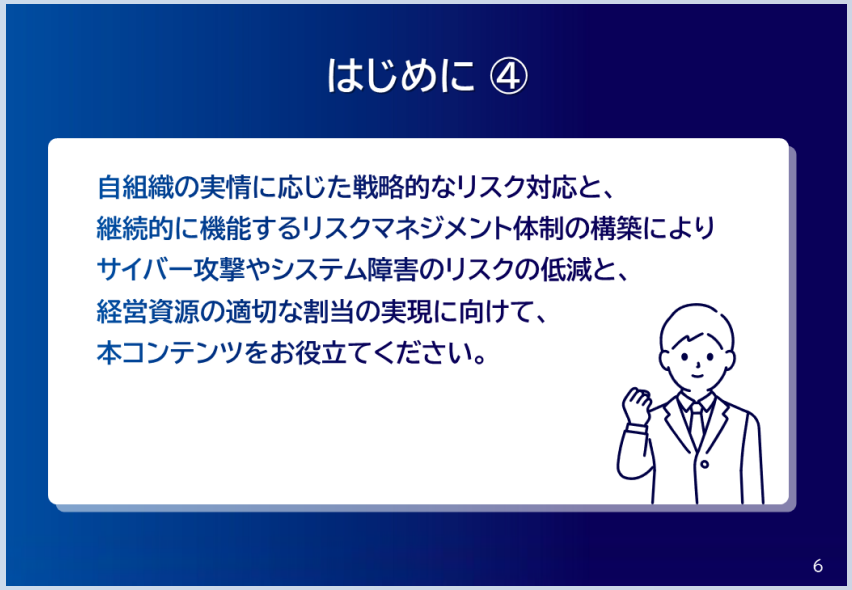
また、すべてのリスクに対して完璧な対策を行おうとすると、手続きが複雑になったり、業務に時間がかかるようになったりと、かえって業務効率を損なってしまうおそれもあります。

その結果、ルールが守られなくなってしまったり、本来注力すべき重要な業務や重大なリスクへの対応が後回しになってしまったり、といた事態も起こりうります。

情報セキュリティリスクへの対策の実施にあたって、重要となるのは「すべてを守ること」ではなく、「どのリスクに、どこまで対応するのかの評価、判断を適切に行うこと」になります。

SLIDE 06

はじめに④



　サイバー攻撃やシステム障害へのリスク低減と、限られた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いただければ幸いです。

SLIDE 07

機能保証に向けたリスクアセスメント

機能保証に向けたリスクアセスメント

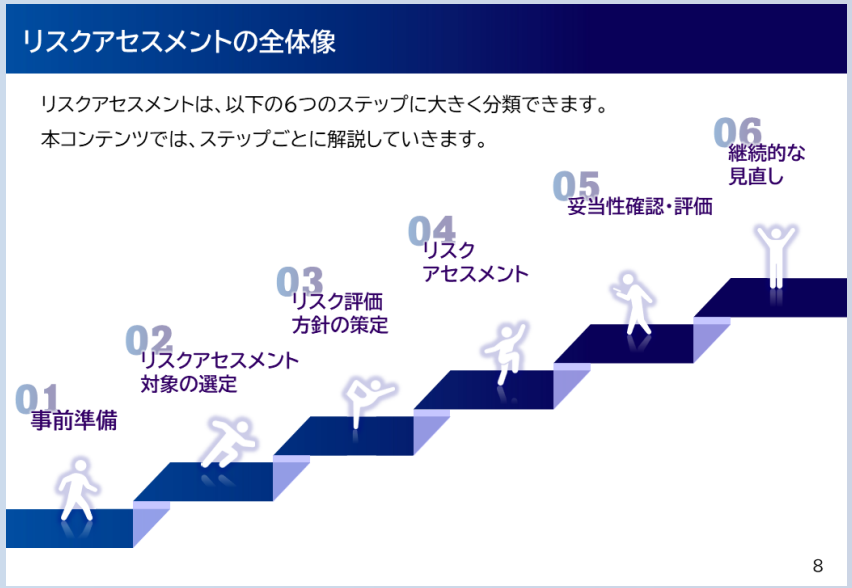
本コンテンツでは、「機能保証のためのリスクアセスメント・ガイドライン※」の考え方に基づいて、**「社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために必要なサービスの提供を維持・継続する」**という「機能保証」の観点から、リスクアセスメントの手順を紹介します。

※https://www.cyber.go.jp/policy/group/cyber/policy.html 7

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」の考え方に基づき、「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ています。

SLIDE 08

リスクアセスメントの全体像



「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、リスクアセスメントを大きく6つのステップに分けており、本コンテンツの章も同じ構成をとっています。

- 01：事前準備
- 02：リスクアセスメントの対象の特定
- 03：リスク評価方針の策定
- 04：リスクアセスメント
- 05：リスクアセスメントの妥当性確認・評価
- 06：リスクアセスメントの継続的な見直し

SLIDE 09

事前準備

01

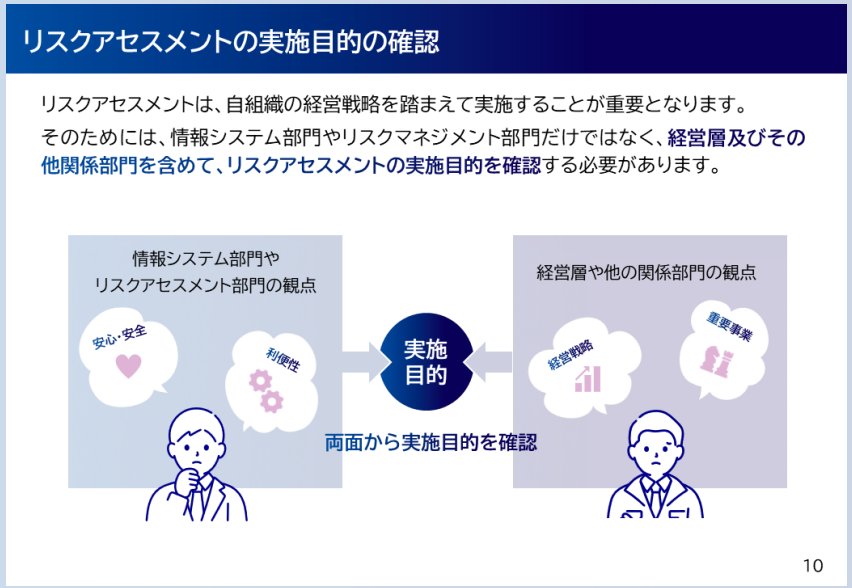
事前準備

まず、最初の工程です。

リスクアセスメントを行うにあたって必要となる事前準備について説明します。

SLIDE 10

リスクアセスメントの実施目的の確認



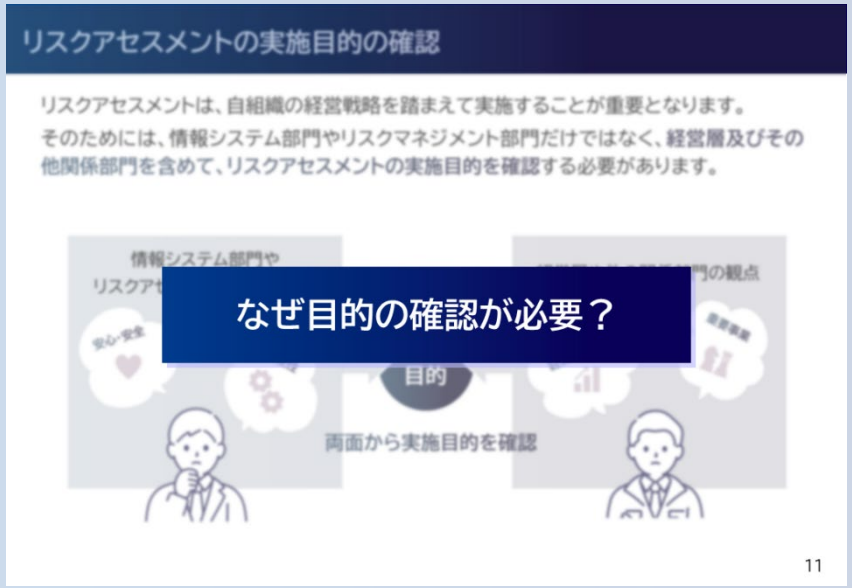
まず最初に、リスクアセスメントの実施目的を確認することが重要です。

リスクアセスメントは、自組織の経営戦略や事業の方向性を踏まえた上で実施することが重要となります。

情報システム部門やリスクマネジメント部門だけで進めるのではなく、経営層や関係部門も含めて、何のためにリスクアセスメントを行うのか、実施目的を確認・共有しましょう。

SLIDE 11

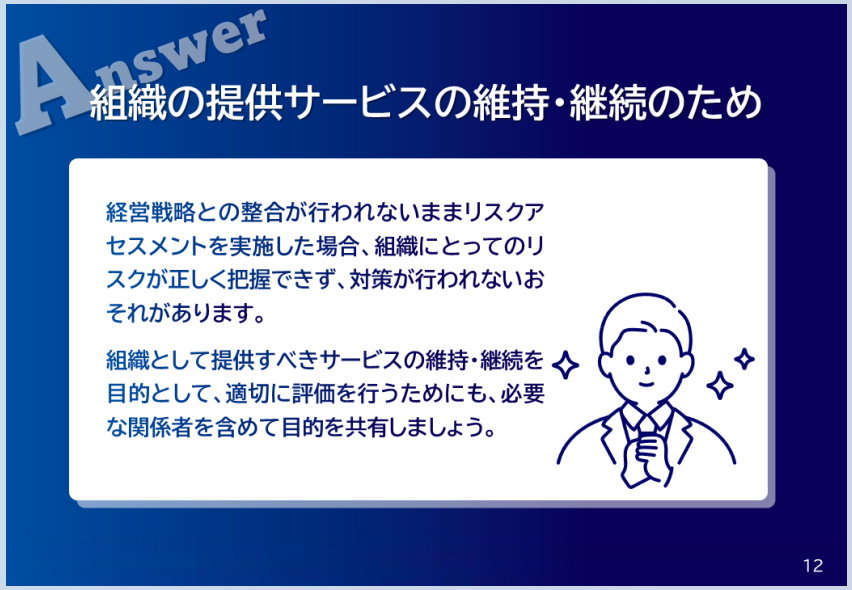
リスクアセスメントの実施目的の確認の必要性：Question



なぜ、目的の確認が必要なのでしょうか。

SLIDE 12

リスクアセスメントの実施目的の確認の必要性：Answer



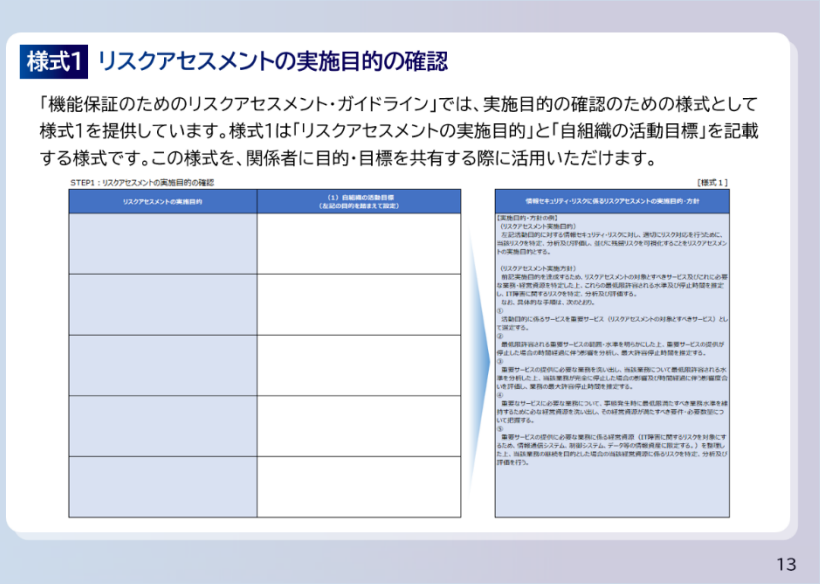
もし、経営戦略との整合が取れないままリスクアセスメントを実施してしまうと、組織にとって本当に重要なリスクが正しく把握できないおそれがあります。

重要なリスク＝優先的に対応すべきリスクに、適切に対策を講じるためにも、リスクの正しい把握を行うことが大切になります。

「機能保証のためのリスクアセスメント・ガイドライン」では、組織として提供すべきサービスの維持・継続を目的としています。経営層や関係部門を含めた必要な関係者で、「何を守るためのリスクアセスメントなのか」という目的を共有し、同じ認識を持った上で評価を進めていくことが重要です。

SLIDE 13

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、事前準備の工程を実施するための様式として、様式1を用意しています。

「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、「なぜリスクアセスメントを行うのか」、「何を守るためにリスクアセスメントを行うのか」を整理することができます。

また、経営層や関係部門など、関係者に対して目的や目標を共有する際の共通資料としても活用できます。

SLIDE 14

Question 1

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。

14

もし、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たとしたら、リスクアセスメントの結果には、どのような影響がありそうでしょうか。

少し時間をとって、考えてみてください。

SLIDE 15

Answer 1

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

15

想定される状況を「回答例」としてお示しします。

情報システム部門を中心にリスクアセスメントが実施されると、「情報システム」を中心とした視点で評価が行われやすくなります。その結果、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ります。

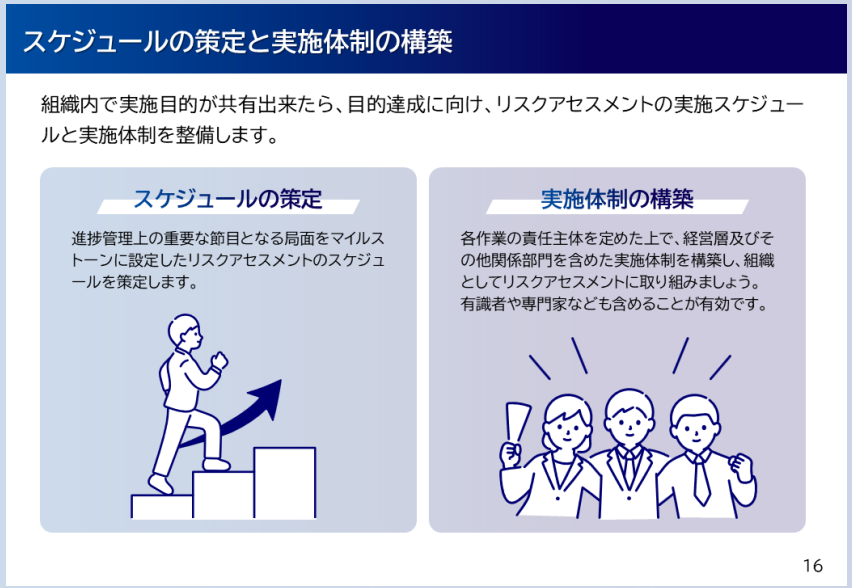
また、リスクへの対策が、「情報システム」で実装できる技術的対策に偏ってしまい、業務継続の視点や、人的・組織的な対策といった観点での検討が不足するおそれがあります。

さらに、経営上それほど重要ではないサービスや業務に対して、過剰な対策が実施されてしまうおそれもあります。

このように、特定の部門の視点だけでは、組織全体のリスクを適切に把握することは難しいです。だからこそ、リスクアセスメントの実施目的は、経営層や関係部門を含めた複数の視点で確認・共有することが重要なのです。

SLIDE 16

スケジュールの策定と実施体制の構築



組織内でリスクアセスメントの実施目的が共有できたら、「実施スケジュールの策定」と「実施体制の構築」を行っていきます。

リスクアセスメントを、いつ、何を、どこまで行うのかを明確にしたうえで、進捗管理の上で重要となる節目を、マイルストーンとして設定したスケジュールを策定しましょう。これにより、作業の遅れや抜け漏れを防ぎ、関係者間で進捗状況を共有しやすくなります。

次に、リスクアセスメントの各作業について、誰が責任を持つのか、責任主体を明確にした実施体制を構築します。リスクアセスメントは、特定の部門だけで完結するものではありません。組織全体として取り組むためにも、経営層をはじめ、業務部門、管理部門など、必要な関係者を巻き込むことが重要です。

SLIDE 17

リスクアセスメントの対象の特定

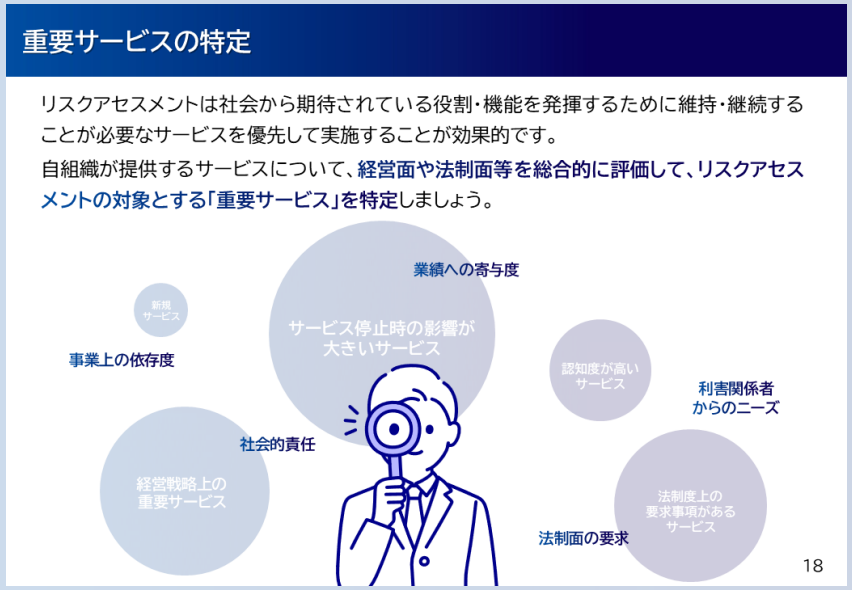
02

リスクアセスメントの対象の特定

続いて、リスクアセスメントの対象を選定します。

SLIDE 18

重要サービスの特定

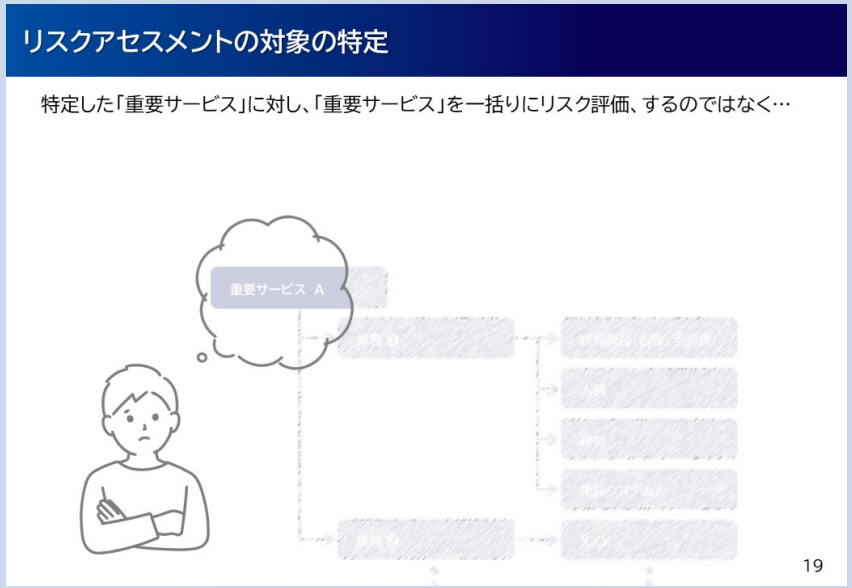


リスクアセスメントの実施には時間も人員も必要となります。

自組織が提供している様々なサービスの中から、事業上の依存度、業績への寄与度や社会的責任、法制面の要求、利害関係者からのニーズ等を総合的に評価し、自組織における「重要サービス」を特定していきましょう。

SLIDE 19

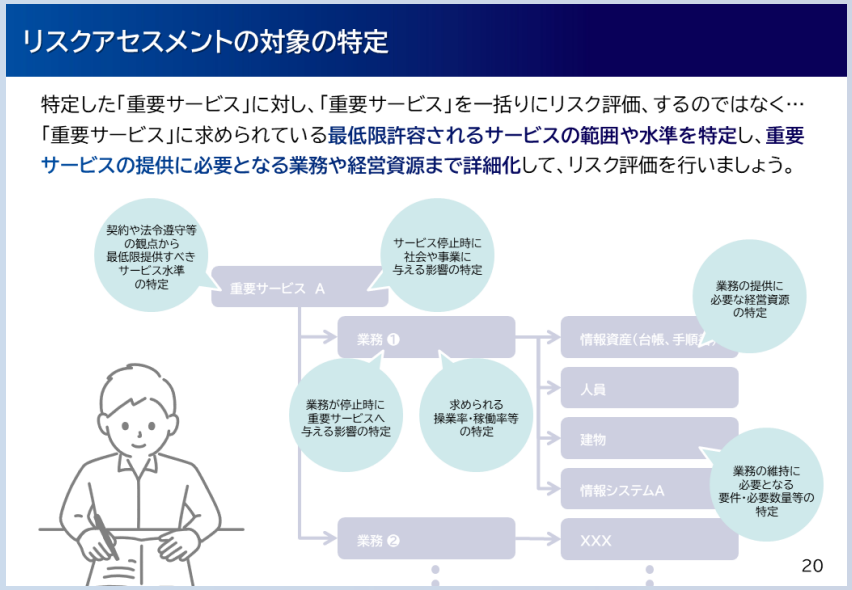
リスクアセスメントの対象の特定



　特定した重要なサービスに対して、リスク評価を行っていくのですが、評価の際には、「重要サービス」として一括りに評価するのではなく、

SLIDE 20

リスクアセスメントの対象の特定

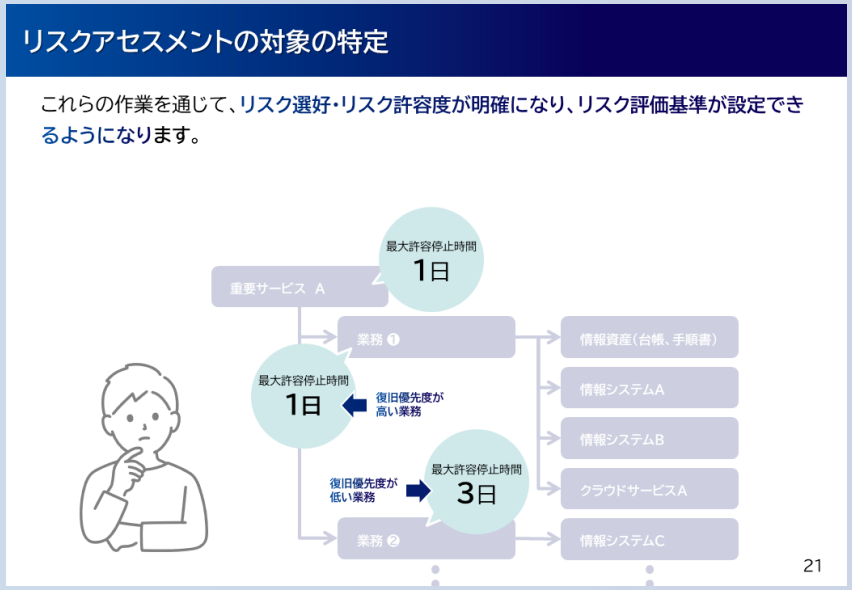


そのサービスに求められているサービス水準や、その提供のために必要となる業務、経営資源まで詳細化を行って、リスク評価を行っていきましょう。

サービスそのものが停止したときの社会や事業に与える影響の評価はもちろんサービスの提供を支えている業務の停止や業務の実施に必要な人や設備等の経営資源が欠けてしまったときに、サービスへどのような影響が生じ得るか評価することで、

SLIDE 21

リスクアセスメントの対象の特定



重要サービスを支える業務や経営資源のうち、どの業務/経営資源がリスクが高いのか、どの程度のリスクなら許容できるのかを整理することができます。

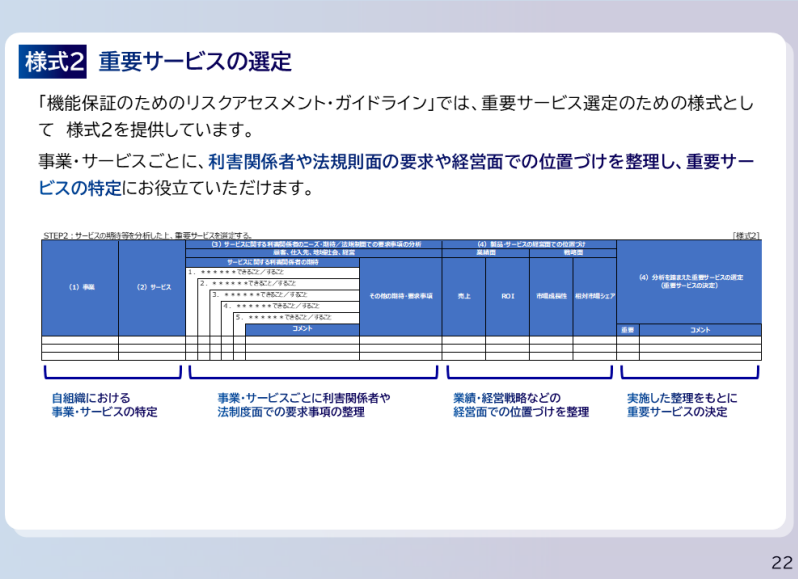
この作業を通じて、リスクの重大さを評価するための目安となるリスク評価基準が設定することができるようになります。

例えば、このスライドにある重要サービスAの場合、最大許容停止時間は1日となっています。ただ業務❷の最大許容停止時間は3日となっていますので、業務❶に比べると優先度が低い、逆に言えばリスクの許容度が高い業務、と言えます。

冒頭にもお伝えした通り、どんな組織であっても、使える人員や予算には限りがあります。許容できるリスクは許容しながら、停止してはならない重要な業務への対策・対応を優先させる等の判断がしやすくなります。

SLIDE 22

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、重要サービスを選定を支援するための様式として、様式2を用意しています。

自組織内で重要と考えらえる事業・サービスごとに、利害関係者からのニーズ・期待や法制面で要求されている事項、業績・経営戦略などの経営面での位置づけを整理することができます。

SLIDE 23

様式3 重要サービスの影響分析

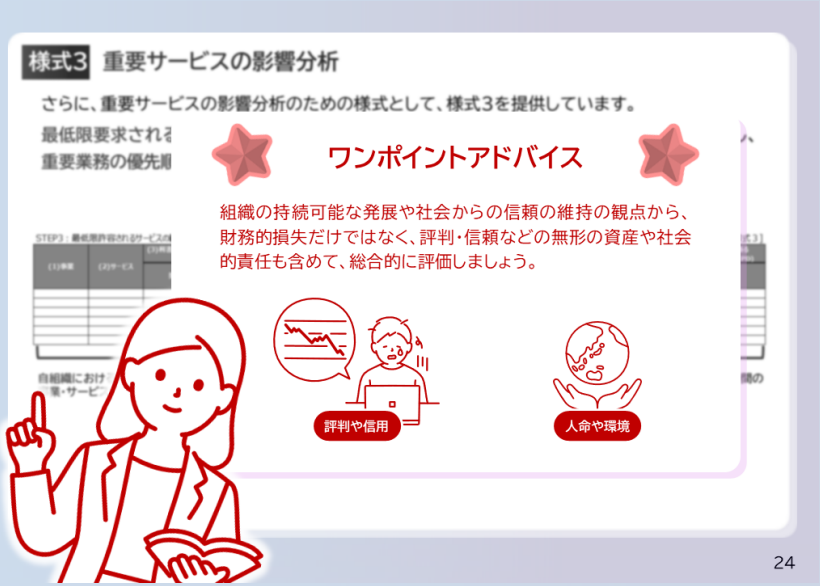
また、重要サービスの影響分析のための様式として様式3を用意しています。

様式2を用いて選定した重要サービスに対し、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を評価し、最大許容停止時間の特定を整理するための様式となっています。

重要サービスの中でも優先順位が高い重要サービスがどれか判断するためのひとつの指標として活用いただけます。

SLIDE 24

ワンポイントアドバイス ❶



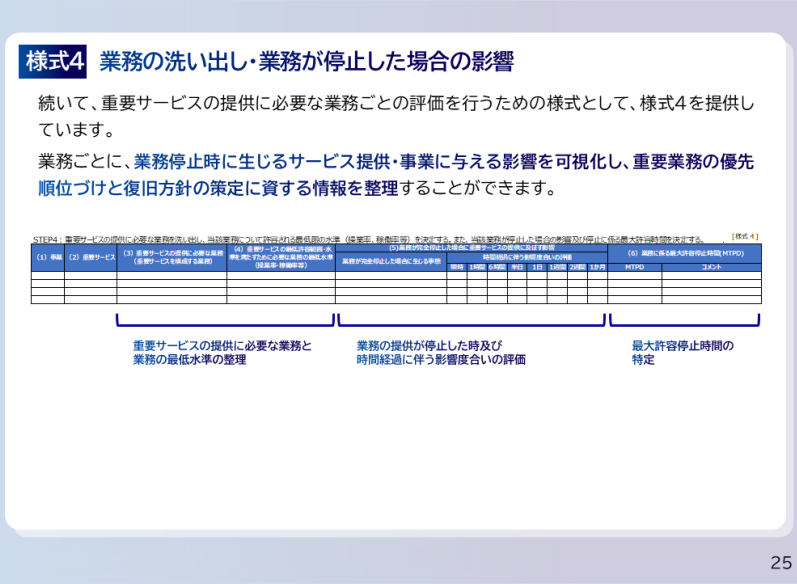
重要サービスの影響分析を実施する際のワンポイントアドバイスです。

実施にあたっては、選定した重要サービスが停止等した際の、売り上げの損失といった財務的な損失の観点だけでなく、サービスの評判や信用面・人命・環境への配慮といった重要サービスの社会的責任を含めて総合的な影響度の評価となるようにしましょう。

サービスや業務の特性によっては短時間の停止であっても、信用面や企業イメージに大きな毀損が生じ、長期的な損失に波及することもあります。

SLIDE 25

様式4 業務の洗い出し・業務が停止した場合の影響

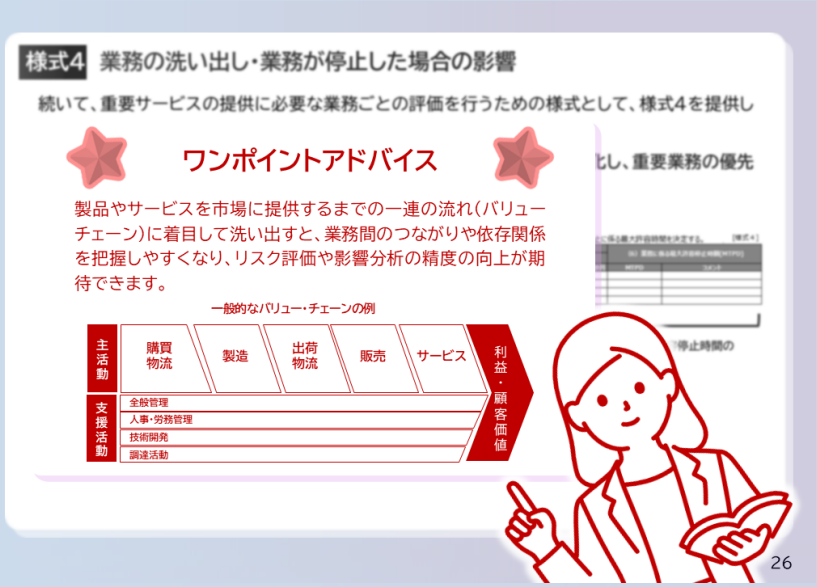


「機能保証のためのリスクアセスメント・ガイドライン」の様式4は、重要サービスの提供に必要な業務ごとの評価を行うための様式です。

先ほどの様式3の評価対象は「重要サービス」ごとでしたが、ここでは「重要サービス」の提供に必要な業務」ごとに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を評価し、最大許容停止時間の整理を行うことができます。

SLIDE 26

ワンポイントアドバイス ❷



本作業におけるワンポイントアドバイスです。

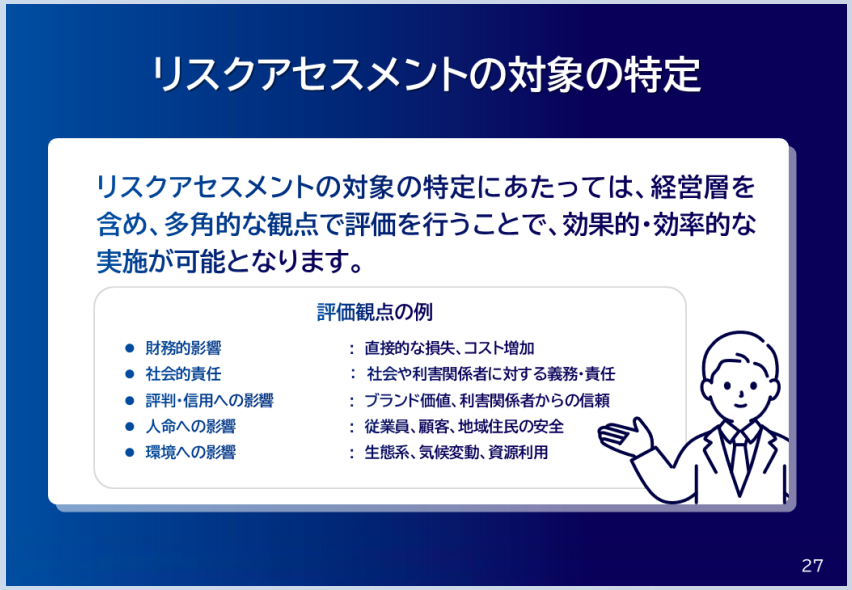
業務の洗い出しにあたっては、製品やサービスを市場に提供するまでの一連の流れ、いわゆる「バリューチェーン」に着目してみしょう。

業務のつながりや依存関係が把握しやすくなるため、「この業務が何時間止まると、次の工程にもどの程度影響する」といった見立てもしやすくなりますし、業務の洗い出しに抜け漏れが所持にくくなります。

また本スライドの下部に記載している「支援活動」も重要サービスを支えている業務です。是非、評価の対象に加えていただければと思います。

SLIDE 27

リスクアセスメントの対象の特定



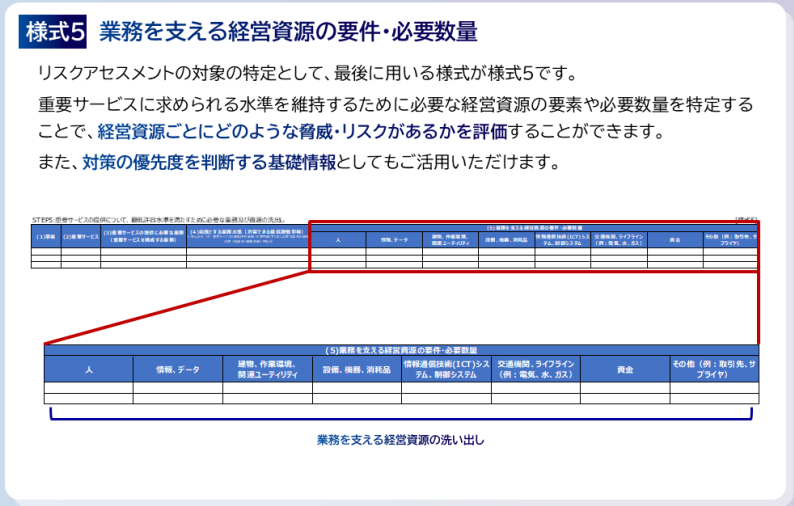
リスクアセスメントの対象の特定にあたっては、財務的影響の観点に限らず、社会的責任や評価・信用、人命や環境の観点を含めることで、リスクアセスメントがより効果的・効率的に機能します。

評価の観点の例をお示しします。

重要サービスや業務の特性等に応じて、必要に応じて評価の観点に追加してみてください。

SLIDE 28

様式5 業務を支える経営資源の要件・必要数量



28

リスクアセスメントの対象を特定するための最後の様式として、様式2から様式4までの作業を通じて洗い出された業務ごとに必要となる経営資源を整理するための様式5をご用意しています。

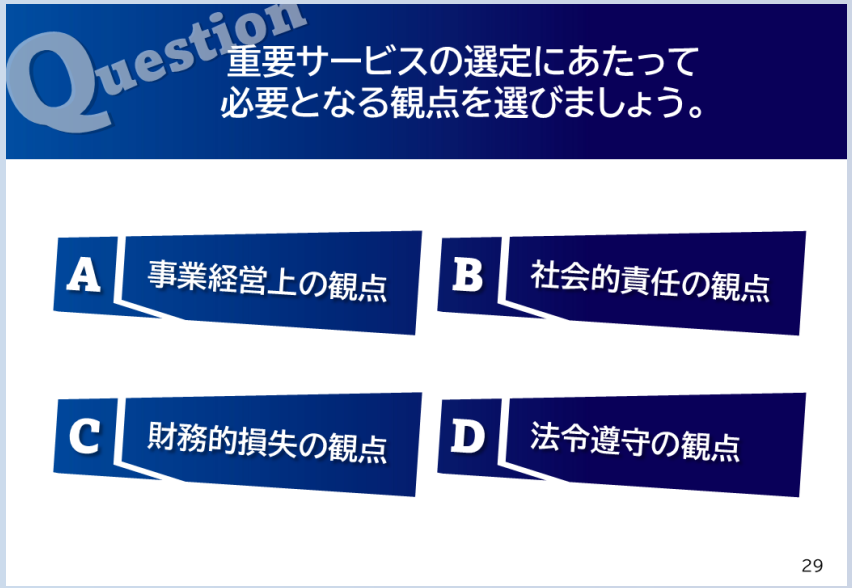
業務に必要な経営資源の要素や数量を特定することで、経営資源ごとにどのような脅威やリスクが存在するか評価できます。また、対策する重要サービスの優先度を判断する基礎情報として活用が可能となります。

「機能保証のためのリスクアセスメント・ガイドライン」においては、様式2から様式5までを活用いただくことで、自組織における重要サービスを特定、重要サービスを支える業務、業務に必要なる経営資源を整理することを支援しています。

この一連の作業を通じて、重要サービスがどのような業務や経営資源に支えられていて、それらが停止、欠けてしまった場合に社会経済や経営にどのような影響が生じるのか、どの程度までリスクが許容できるのか、どの業務/経営資源から復旧を行うべきなのか、といった判断を行うための情報の整理ができます。

SLIDE 29

Question 2

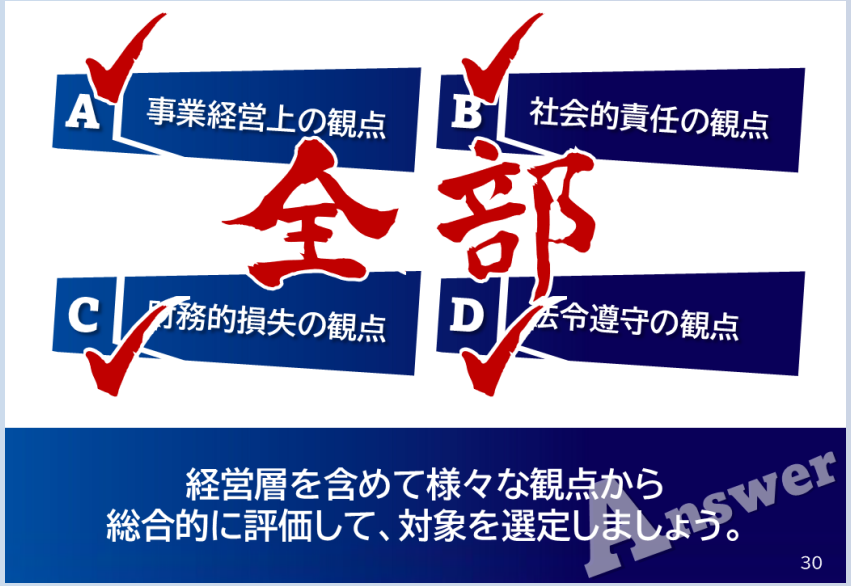


では、ここで問題です。

お示しする4つの観点の中から、重要サービスの選定にあたって必要な観点を選んでみてください。

SLIDE 30

Answer 2



４つとも「全部」必要な観点となります。

重要サービスの選定にあたっては、サービス停止による「財務的損失の観点」はもちろんのこと、経営層の視点を含む「事業経営上の観点」、重要サービスや事業への信用・評判に関わる「法令遵守の観点」、従業員、顧客、地域住民の安全・環境への影響への配慮といった「社会的責任の観点」を含めて、総合的に評価を行いましょう。

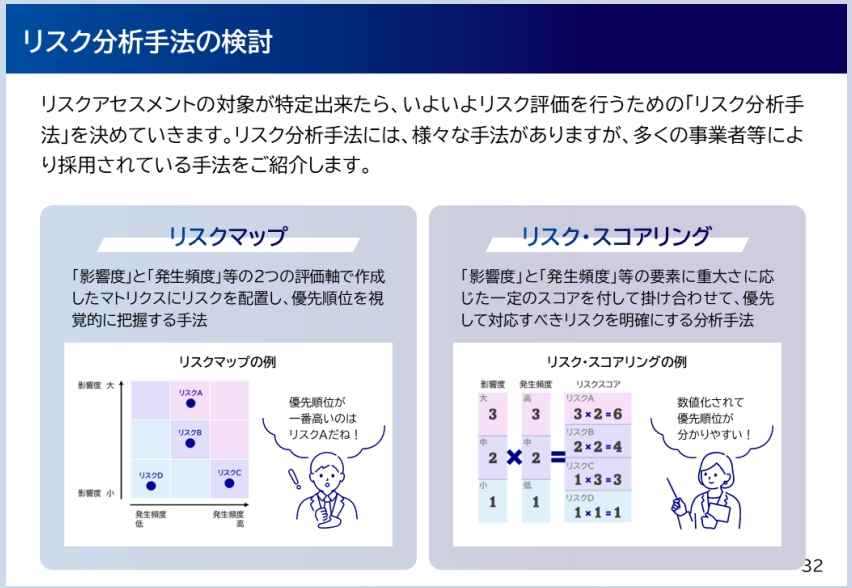
03

リスク評価方針の策定

続いて、リスク評価方針の策定を行っていきます。

SLIDE 32

リスク分析手法の検討



まず、リスク分析手法を検討していきましょう。

リスク分析手法には、様々な手法があり、これが正解・最適、と言える手法はなく、自組織の特性等に合った方式を採用いただくのが良いです。

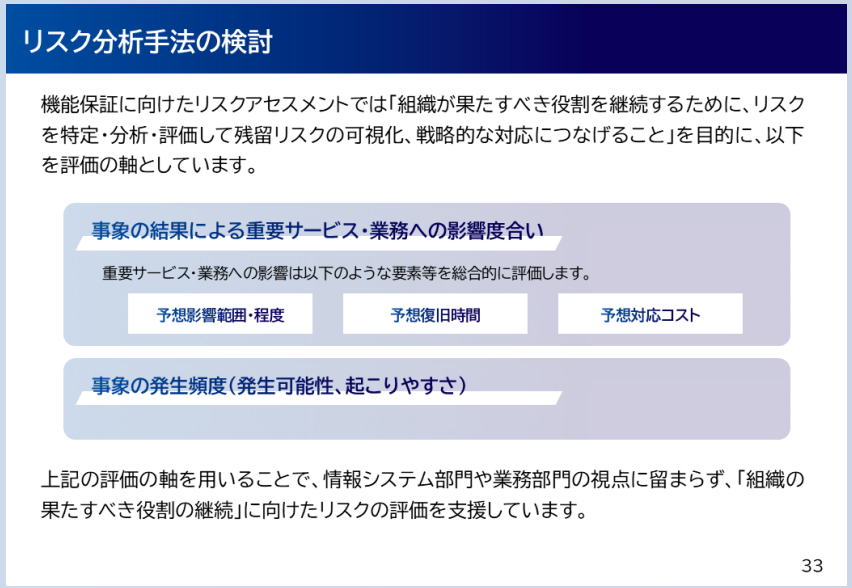
本コンテンツでは、多くの組織で採用されているリスクマップ方式とリスク・スコアリング方式を紹介します。

リスクマップ方式とは、「影響度」と発生の可能性や起こりやすさを示す「発生頻度」を評価軸として作成したマトリクスにリスクを配置し、相対比較で優先度を視覚的に把握できる手法です。

リスク・スコアリング方式は、「影響度」と発生の可能性や起こりやすさを示す「発生頻度」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数値で明確にする分析手法です。

SLIDE 33

リスク分析手法の検討



リスク分析を行う「評価の軸」についても、様々な指標が用いられます。

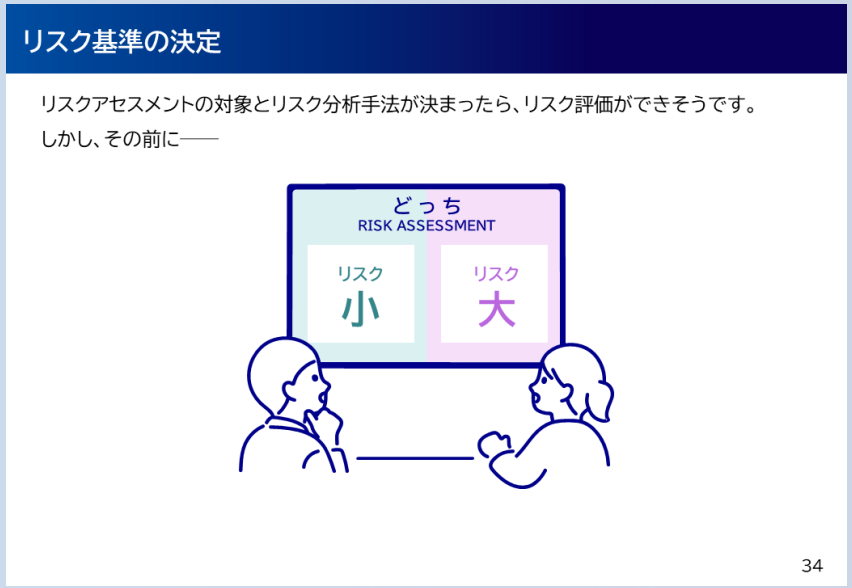
「機能保証のためのリスクアセスメント・ガイドライン」では、組織が果たすべき役割を継続するためのリスクを特定・分析・評価できるように、機能保証の観点から評価の軸を「事象の結果重要サービス・業務への影響度」×「事象の発生頻度」としています。

リスクアセスメントの分析手法や評価の軸は、リスクアセスメントの目的や組織の状況等を踏まえ、最適なものを検討してみてください。

その際に機能保証の保証の観点も含めていただけると、より有効なリスクアセスメントの実施に繋がると考えています。

SLIDE 34

リスク基準の決定

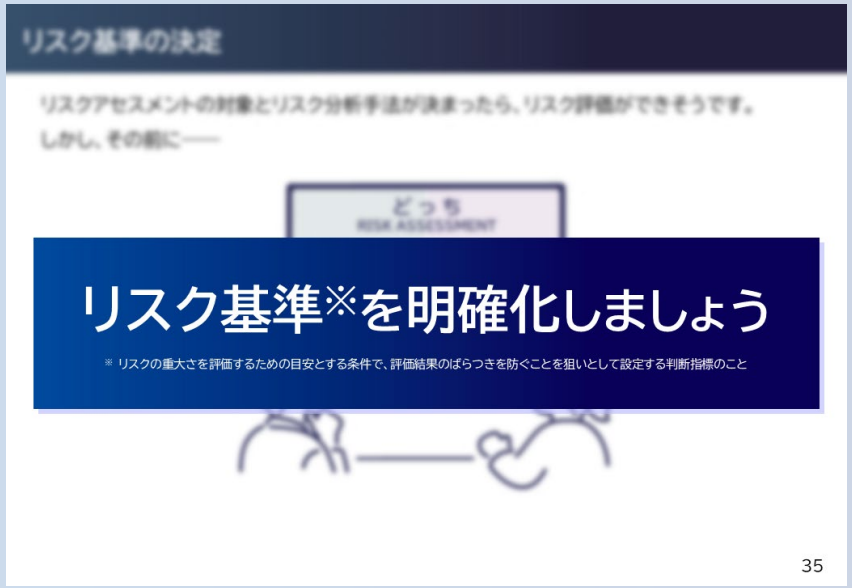


さて、リスクアセスメントの対象もリスク分析手法も決まりましたので、
いよいよ、リスク評価ができそうです。

しかし、その前に――

SLIDE 35

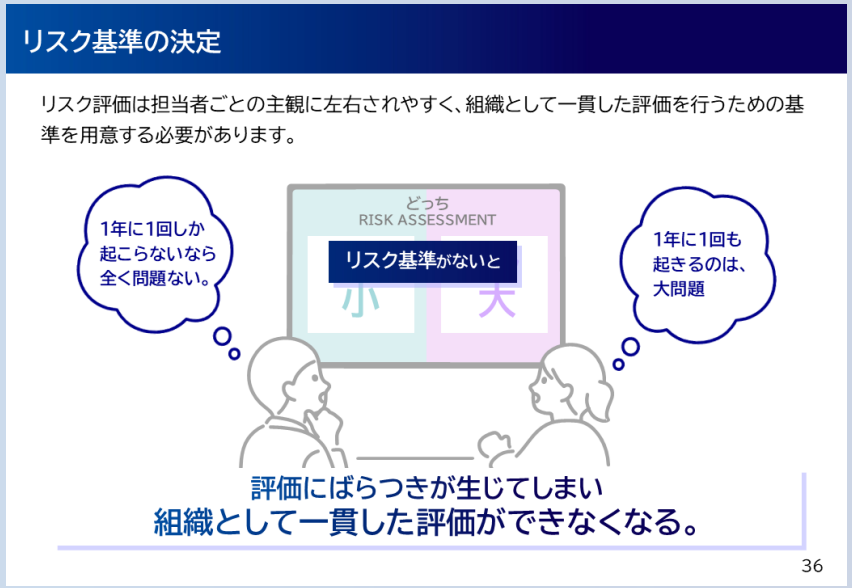
リスク基準の決定



　リスク評価結果のばらつきを防ぐための判断指標となる、リスク基準を設定してましょう。

SLIDE 36

リスク基準の決定



リスク基準がないままリスク評価を行うと、担当者ごとの主観による判断が生じやすく、リスク評価結果にばらつきが発生しやすくなります。

リスク評価結果のばらつきを防ぐ又はばらつきを低減し、組織として一貫した評価を行えるように「リスク基準」を設定していきます。

SLIDE 37

評価基準の例 1/2

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

	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

	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

37

「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、「組織が果たすべき役割の継続」という目的を踏まえて、「業務への影響度合い」と「事象の発生頻度」という2つの評価の軸を採用しています。

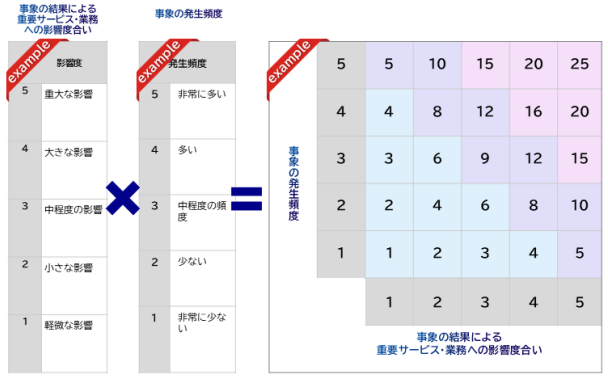
この2つの評価の軸を用いた場合の判断指標の例を紹介します。

「最低限水準を保てるのか」、「許容停止時間内に復旧できるか」、「復旧に要するコストはどの程度か」という客観的に測定しやすい目安を用意し、評価を行う担当者が評価できるように設定しています。

SLIDE 38

評価基準の例 2/2

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。



38

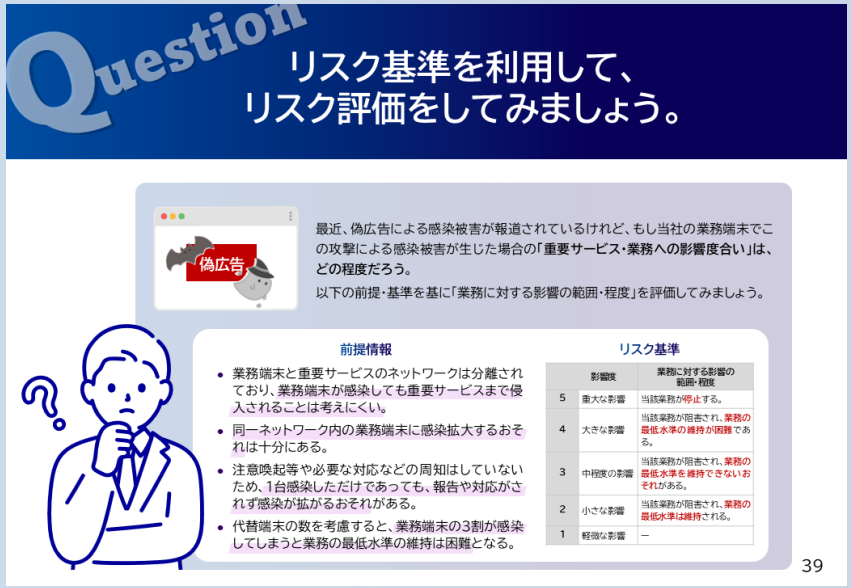
判断指標をもとにリスクを数値化することで、リスク対応の対象となるリスク値を超えているか定量的な評価が行えるようになります。

リスク対応の対象となるリスク値は、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。

また一度設定したリスク基準値は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。

SLIDE 39

Question 3



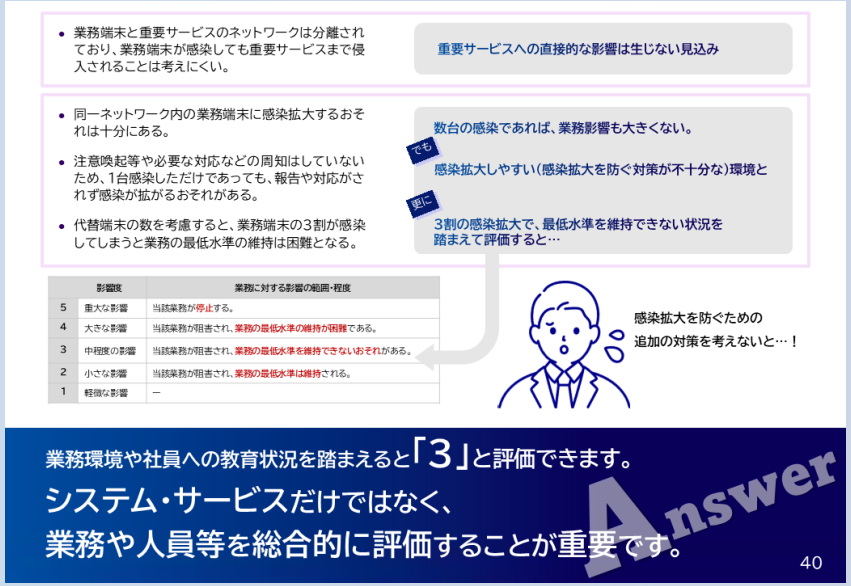
では、リスク基準を利用してリスク評価をしてみましょう。

「最近、偽広告による感染被害が報道されているけれど、もし自社の業務端末でこの攻撃による感染被害が生じた場合、重要サービス・業務への影響度合い」は、どの程度になるのだろうかと考えているリスクアセスメントの実施担当者がいます。

スライド下部に記載されている前提情報とリスク基準を基に、この事業者において、偽広告によるウイルス感染が発生した際の「重要サービス・業務への影響度合い」を評価してみてください。

SLIDE 40

Answer 3



答えは、3：中程度の影響　となります。

業務端末において偽広告による感染被害が生じた場合であっても、業務端末と重要サービスは分離されているため、直接的に重要サービスが被害に遭うことはなさそうです。

また、数台の感染が生じても業務継続は問題なくできますが、従業員への注意喚起や必要な対応に関する周知等が行われていないので、感染拡大してしまうおそれはある、と考えられます。

代替端末の数等を考慮しながら、業務の最低水準の維持が可能か、という観点で判断指標に則り評価してみると――「3」となりました。

リスクを評価する際は、システムやサービスだけで評価せずに業務や人員の状況を踏まえて総合的に評価することが大切です。

リスクアセスメント

04

リスクアセスメント

いよいよ、リスクアセスメントを実施していきます。

SLIDE 42

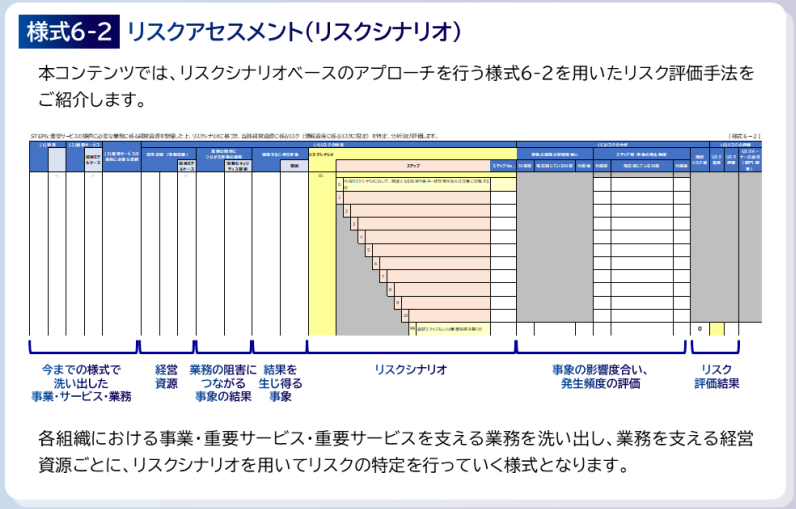
機能保証の観点からのリスクの特定

東日本大震災発生当時、多くの企業や組織では、過去に経験していない、あるいは発生確率が低いと考えられていた事象がリスクとして想定されていなかったことにより、大きな混乱を招いてしまいました。

「機能保証のためのリスクアセスメント・ガイドライン」においては、この教訓を踏まえて、事象の結果からリスク源やリスクシナリオへと遡って考える「演繹的なアプローチ」を採用しています。

SLIDE 43

様式6-2 リスクアセスメント(リスクシナリオ)

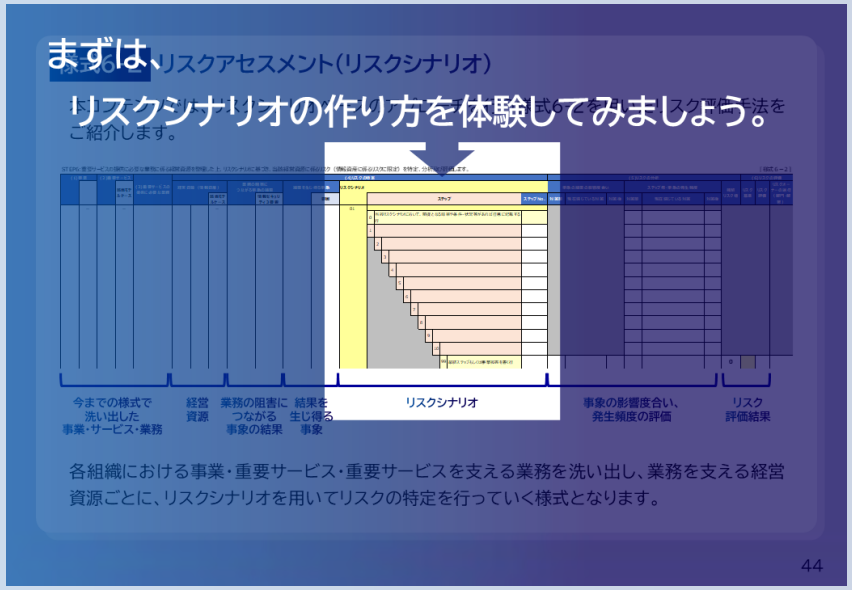


ここからは、リスクアセスメントの進め方について説明を行っていきます。

前の章でお伝えしている通り、リスクアセスメントの実施方法には様々な方法がありますが、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」における様式6-2を用いたリスクシナリオベースでのリスク評価手法を紹介していきます。

SLIDE 44

Case Study:リスクシナリオの作成 1

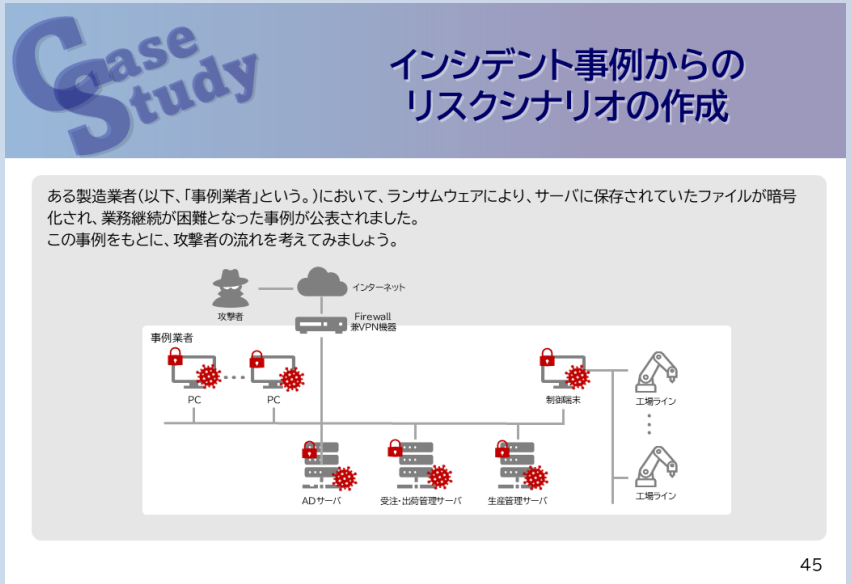


では、実際にリスクシナリオの作り方を体験していきましょう。

様式6-2の真ん中の部分を埋めていく作業となります。

SLIDE 45

Case Study:リスクシナリオの作成 2



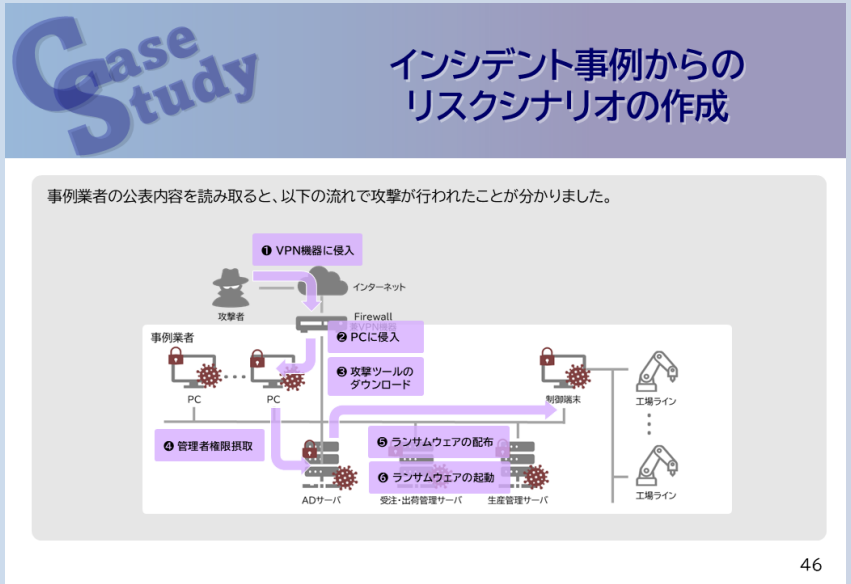
リスクシナリオベースのリスクアセスメントを実施される際には、実際に報道・公表されたインシデント事例を活用していただくと効果的です。

本コンテンツでも「仮」の事例としてある製造業者――事例業者のインシデント事例を用意しています。

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、業務の継続が困難になったという事例です。

この事例をもとに、攻撃者がどのような流れで侵入し、ランサムウェアを実行するに至ったのか――リスクシナリオを一緒に考えていきます。

Case Study:リスクシナリオの作成 3



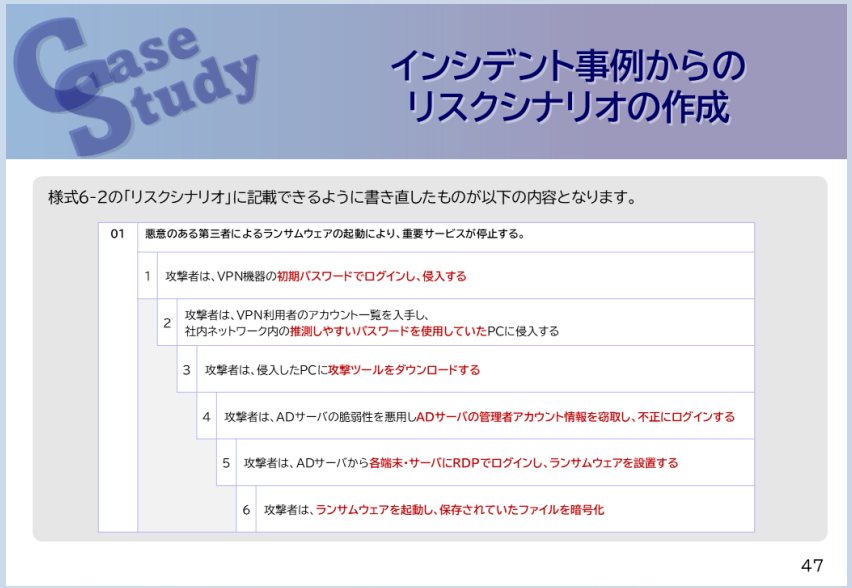
まず、事例業者が公表した事故報告などから、事例業者における攻撃がどのような流れで攻撃されたか、を整理していきます。

事例業者においては、VPN機器を起点に、社内のPCへと侵入され、攻撃ツールのダウンロードを行った上でADサーバへ攻撃を行い、管理者権限の窃取されています。その後、ランサムウェアの配布と実行が行われたようです。

この一連の攻撃の流れ――攻撃ステップを

SLIDE 47

Case Study:リスクシナリオの作成 4

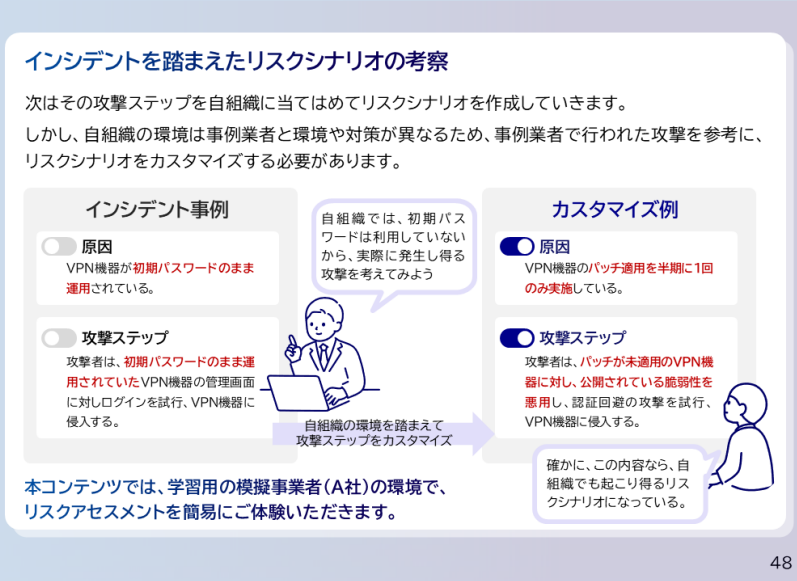


「様式6-2」のリスクシナリオ部分に記載する場合、このような記載になります。

事例業者でリスクシナリオを作成する場合は、この攻撃ステップに対し、リスクアセスメントを実施いただくこととなります。

SLIDE 48

インシデントを踏まえたリスクシナリオの考察



ただ皆さまの組織は事例業者――報道・公表された業者とは異なる環境になっています。事例業者と全く同じリスクシナリオを使ってリスクアセスメントを行っても、環境や対策が異なれば攻撃ステップそのものが成立しない場合もあります。

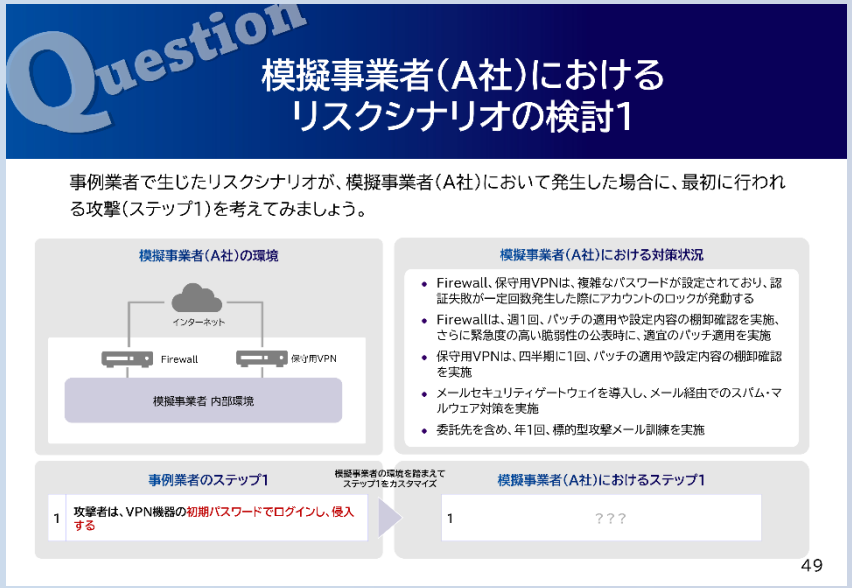
そのため、事例の攻撃内容をそのまま使用するのではなく、自組織の現実に合わせて、実際に発生し得る攻撃にはどのような攻撃があるかを考え、攻撃ステップをカスタマイズすることが大切です。

攻撃ステップのカスタマイズを簡易に体験いただくために、本コンテンツでは、模擬事業者（A社）を用意しました。

模擬事業者（A社）の環境を踏まえて、事例業者のリスクシナリオを用いたリスクアセスメントを実施していきましょう。

SLIDE 49

Question 4-1



　では、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の最初の攻撃(ステップ1)を考えてみましょう。

　模擬事業者(A社)における対策状況を右側に、事例業者のステップ1を左下に記載しています。最初に、事例業者のステップ1が模擬事業者(A社)でも発生し得るか考えてみましょう。

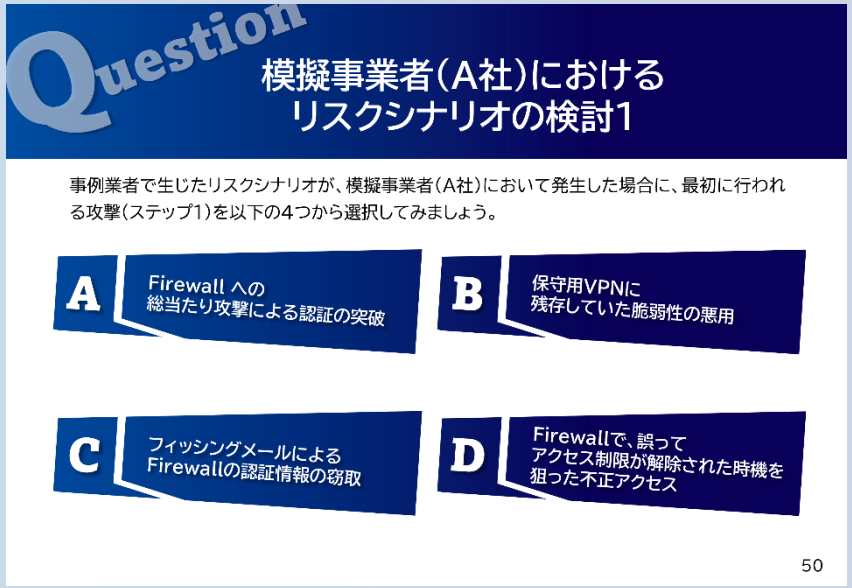
　もし発生し得ると考えられる場合は、模擬事業者(A社)におけるステップ1にも同じ記載が入ります。

　しかし、「複雑なパスワードが設定されており」との記載があることから、初期パスワードは使われていないと考えた方がよさそうです。

　では、どのような攻撃ステップが考えられるか――

SLIDE 50

Question 4-2

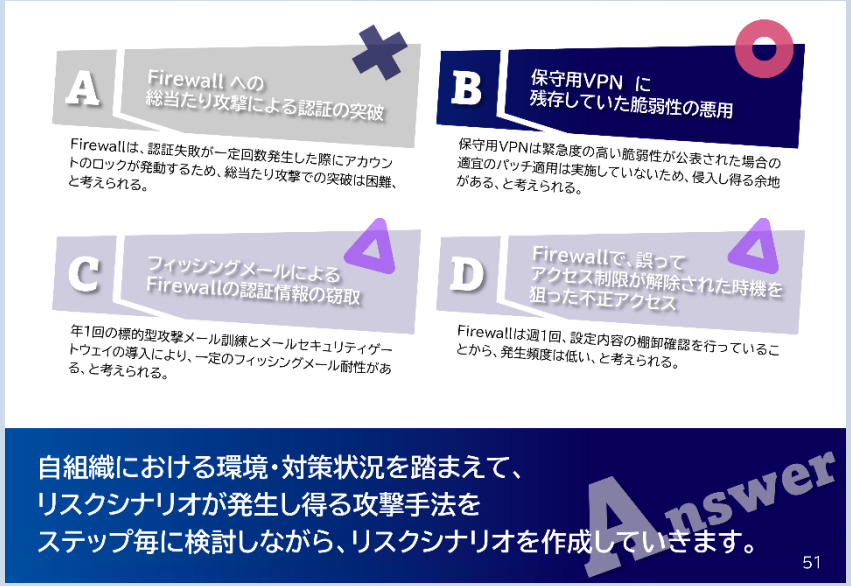


4つの選択肢をご用意しました。

前ページに記載されている「模擬事業者(A社)における対策状況」と選択肢を見比べていただきながら、模擬事業者(A社)におけるステップ1を考えていましょう。

SLIDE 51

Answer 4



正解は、B　保守用VPNの脆弱性を悪用する攻撃です。

「模擬事業者における対策状況」を読むと、Firewallは週1回パッチを適用していますが、保守用VPNは四半期に1回棚卸確認を実施しているのみとなっており、パッチが適用されずに悪用可能な脆弱性が残っているおそれがあります。

その他の選択肢は以下のように考えることができます。

- A｜Firewallへの総当たり攻撃

  Firewallには、アカウントロックが設定がされており、ログイン失敗が連続して生じ得る総当たり攻撃が成立する可能性は低いと考えられます。

- C｜フィッシングメールによる認証情報窃取

  メールセキュリティゲートウェイを導入し、年1回の標的型攻撃メール訓練を実施しており、フィッシングメールへの対策は一定に図られています。

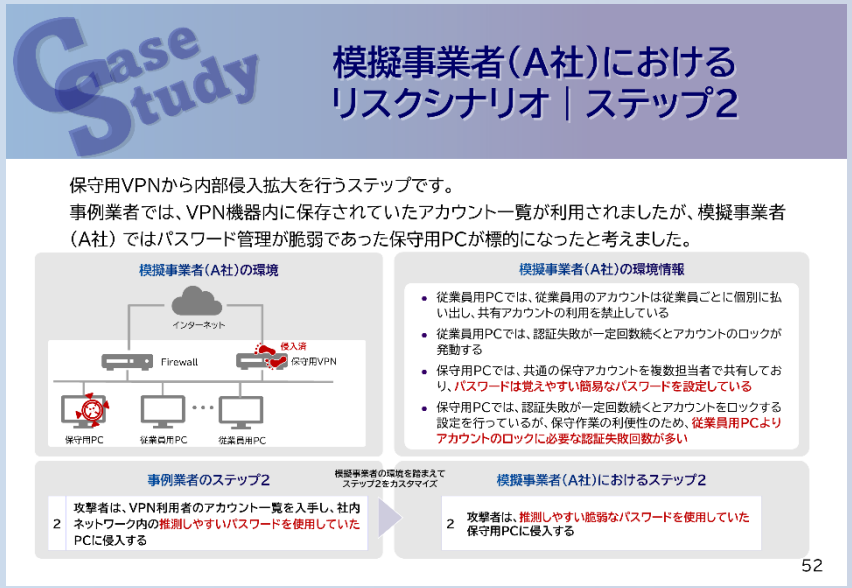
- D　Firewallの設定ミスを狙う攻撃

  Firewallは週1回、設定内容の棚卸確認が行われているため、攻撃が可能な設定ミスが残置されている期間は限定的であると考えられます。

このように、インシデント事例を自組織に置き換え、環境と対策状況を踏まえて「どの攻撃手法が成立するか」を攻撃ステップごとに検討し、リスクシナリオを作成します。

SLIDE 52

模擬事業者（A社）におけるリスクシナリオ｜ステップ2



攻撃者は先ほどのステップで保守用VPNに侵入しました。

事例業者では内部侵入拡大のために、「VPN利用者のアカウント一覧」から、その後の攻撃先を選定していましたが、模擬事業者（A社）の環境では攻撃先をどのように選定されるでしょうか。

模擬事業者（A社）の環境情報から考えてみましょう。

環境情報を読むと、保守用PCでは、アカウントを複数担当者で共有を行い、簡易なパスワードが利用されており、アカウントロックは設定しているものの、認証失敗回数の閾値が高くなっていることが分かります。このことから、保守用PCに対し、総当たり攻撃での侵入が可能なのではないか、と考えられます。

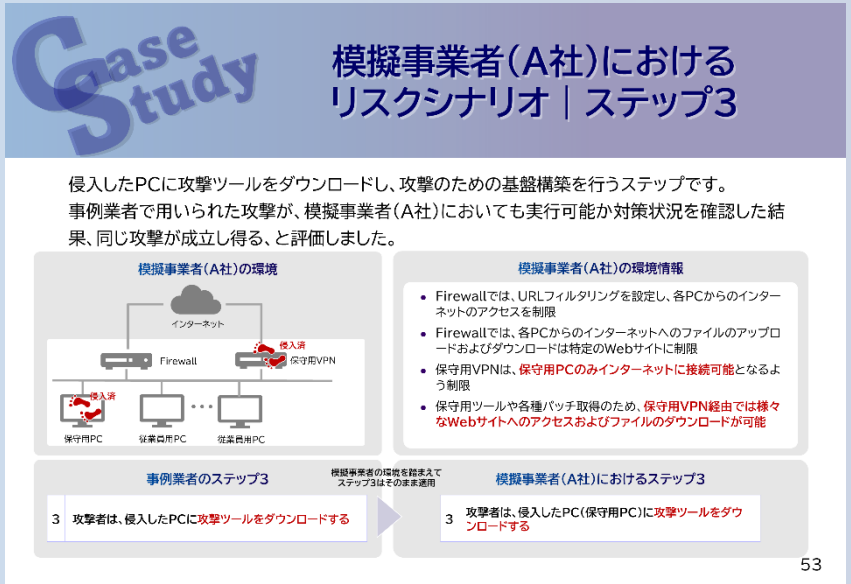
ステップ2は

- 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

となりました。

SLIDE 53

模擬事業者（A社）におけるリスクシナリオ｜ステップ3



足場となる機器となる保守用PCに侵入できましたので、攻撃のための基盤構築を行っていきます。事例業者では「攻撃者は、侵入したPCに攻撃ツールをダウンロードする」という攻撃ステップでした。

模擬事業者（A社）でも同じ攻撃ができるのか、環境情報を見てみましょう。

保守用VPNの設定を見ると、保守用PCはインターネットに接続可能であり、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を許可されているとあります。侵入した機器は保守用PCですので、保守用VPN経由であれば、攻撃ツールのダウンロードができそうです。

このように、インシデント事例と同様の攻撃が成立し得る場合は、事例業者のステップをそのまま利用いただいて問題ありません。

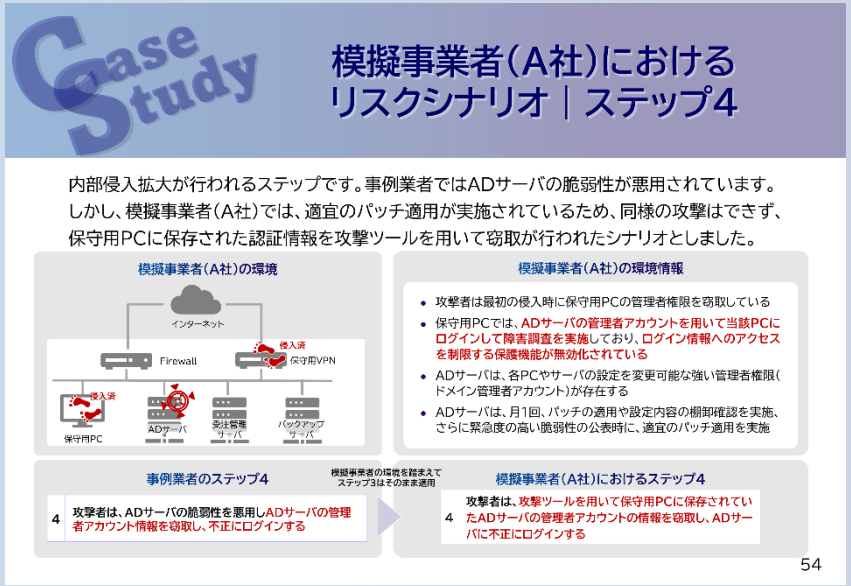
ステップ3は

- 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

となります。

SLIDE 54

模擬事業者（A社）におけるリスクシナリオ｜ステップ4



攻撃者は、更なる侵入拡大を狙っていきます。

事例業者では、ADサーバの脆弱性を悪用され、管理者アカウント情報が窃取されています。模擬事業者（A社）でも同じ攻撃が可能か環境情報を見てみましょう。

環境情報を読むと、模擬事業者（A社）では月1回定期的にパッチ運用を行っており、さらに緊急度の高い脆弱性の公表時に、適宜のパッチ適用する等、脆弱性を悪用する攻撃には一定の対策が講じられており、事例業者と同じ攻撃は困難であることが想定されます。

しかし、一方で保守用PCでは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、との記載もあります。保守用PCでは障害調査の際にADサーバの管理者アカウントでログインを行っていることから、その際のログイン情報が端末内に保存されており、攻撃ツールを用いることで窃取ができる可能性がある、と考えられます。

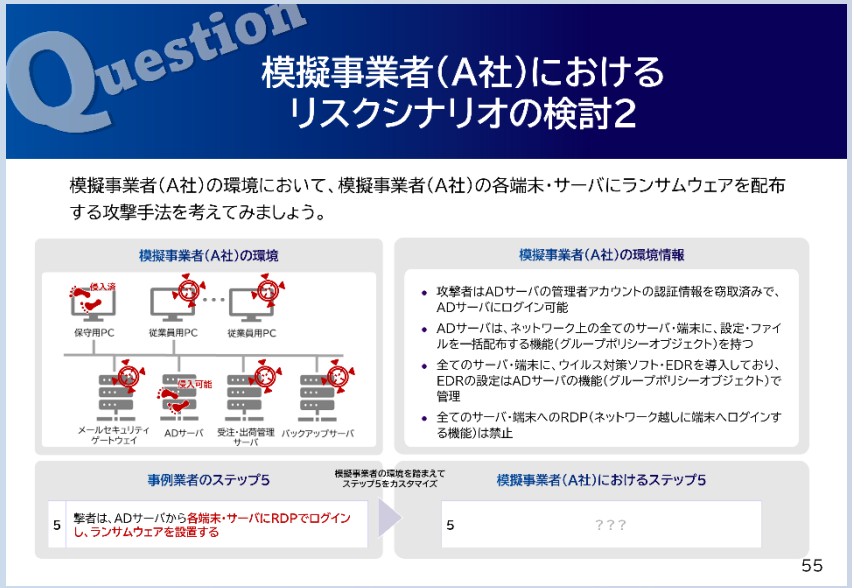
ステップ4は

- 攻撃ツールを用いて保守ベンダー用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

となります。

SLIDE 55

Question 5-1

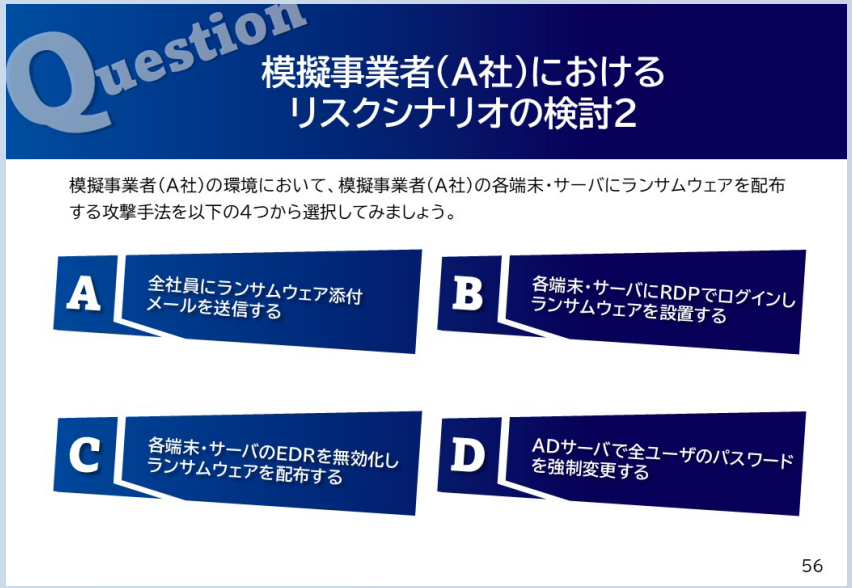


ステップ5は問題になっています。

今までのステップと同様に、事例業者のステップを参考に、模擬事業者(A社)の環境情報を踏まえて、模擬事業者(A社)においてランサムウェアを設置する方法を考えていきます。

SLIDE 56

Question 5-2

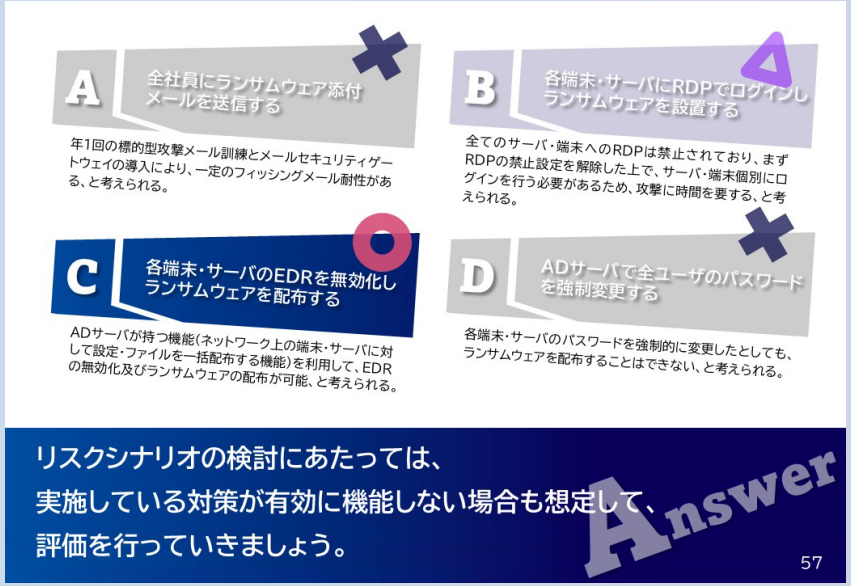


こちらも4つの選択肢をご用意しています。

それぞれの攻撃が模擬事業者(A社)の環境で実施可能か考えてみてください。

SLIDE 57

Answer 5



答えは、C(EDRを無効化しランサムウェアを配布する攻撃)となります。

ADサーバには、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)があり、この機能を利用することで全てのサーバ・端末に導入されているEDRの無効化を行い、マルウェアを配布することが可能です。

RDPを制限したり、EDRを導入していても、攻撃者により無効化されてしまうことも想定する必要があることに留意してください。

その他の選択肢は以下のように考えることができます。

- A｜ランサムウェア添付メールを送信する攻撃

  メールセキュリティゲートウェイを導入し、年1回の標的型攻撃メール訓練を実施しており、フィッシングメールへの対策は一定に図られています。

- 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攻撃

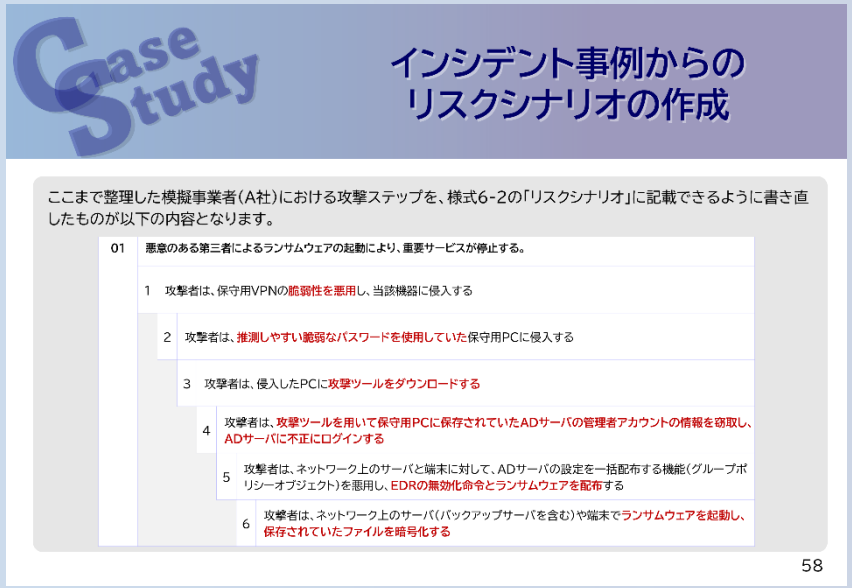
  RDPが禁止されているため、そのままでは攻撃が成立しません。解除した場合でも端末・サーバごとにログインをするため時間がかかってしまいます。ただ、時間をかければ攻撃は可能でので、△としています。

- D｜全ユーザのパスワードを強制変更する攻撃

  パスワードの変更によるユーザ影響は大きいものの、ランサムウェアの展開には直結しません。

SLIDE 58

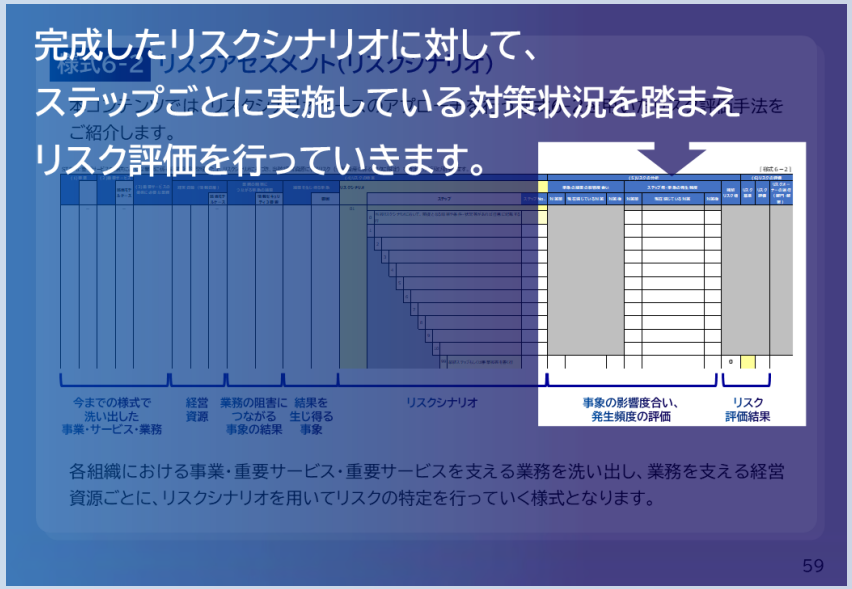
Case Study:リスクシナリオの作成 5



これまで考えてきた模擬事業者(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本スライドの内容となります。

「リスクシナリオ」が完成したら、次は――

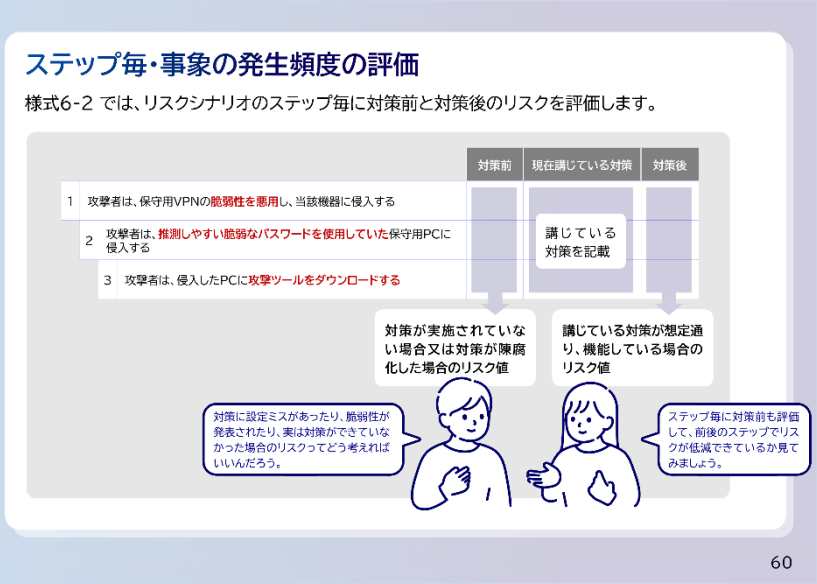
Case Study:リスク評価 1



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洗い出し、対策状況を踏まえたリスク評価を行っていきます。

SLIDE 60

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」のリスクと、「現在講じている対策」を踏まえた「対策後」のリスクを評価する様式となっています。

「対策前」の列では、ステップで行われる攻撃への対策が、何も実施されていない又は対策が陳腐化していることを前提に、ステップごとに発生頻度を評価します。

続いて、「現在講じている対策」の列に、ステップで行われる攻撃を防ぐために現在実施している対策を記載します。

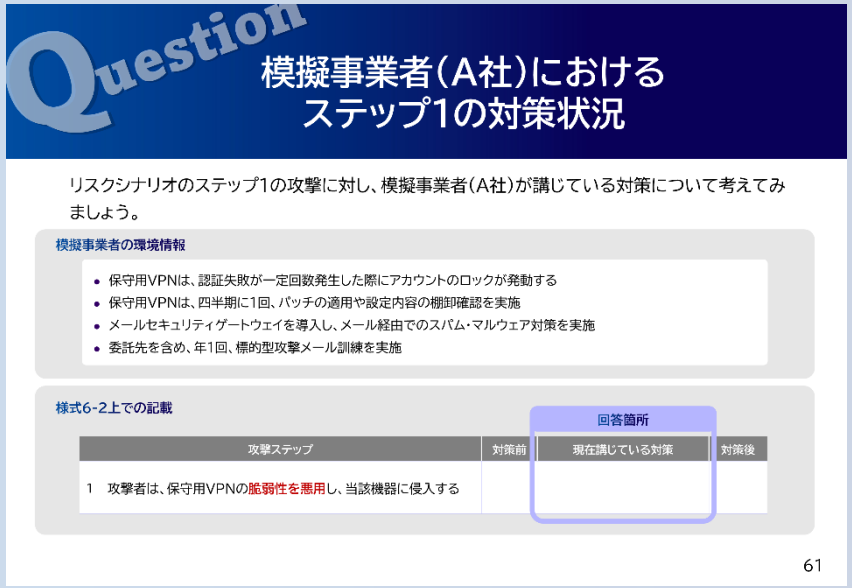
例えば、ステップ2はパスワードの推測による攻撃ですので、防ぐための対策として、複雑なパスワードを使用するよう制限していたり、多要素認証を導入していたりする場合、本列に記載できます。

最後に「対策後」の列に、「現在講じている対策」の列に記載した対策が想定通り機能している場合を想定して、ステップごとに発生頻度を評価します。

なお、「対策前」と「対策後」の評価は、本コンテンツ 03 リスク評価方針の決定で決定した自組織のリスク基準を使用して、評価します。

SLIDE 61

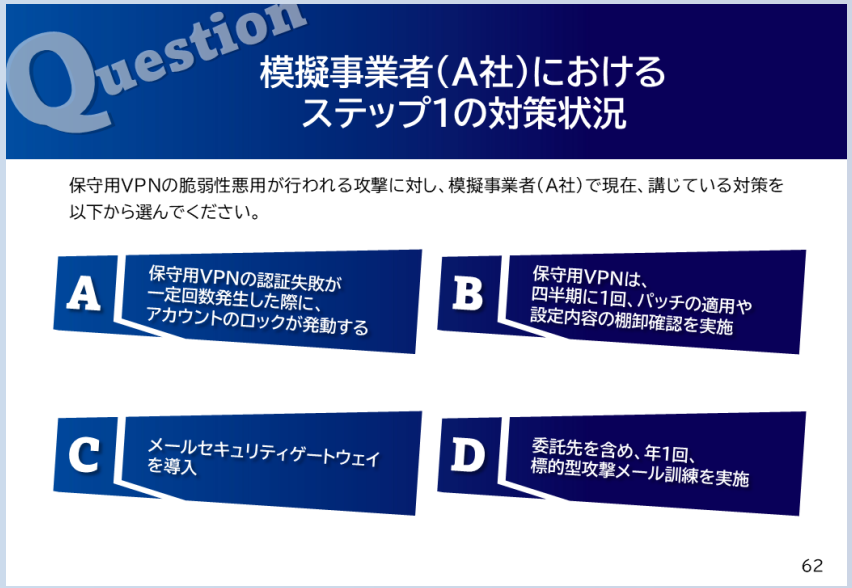
Question 6-1



それでは、練習として、リスクシナリオのステップ1において、模擬事業者(A社)が「現在講じている対策」を、模擬事業者の環境情報の情報をもとに考えてみましょう。

SLIDE 62

Question 6-2

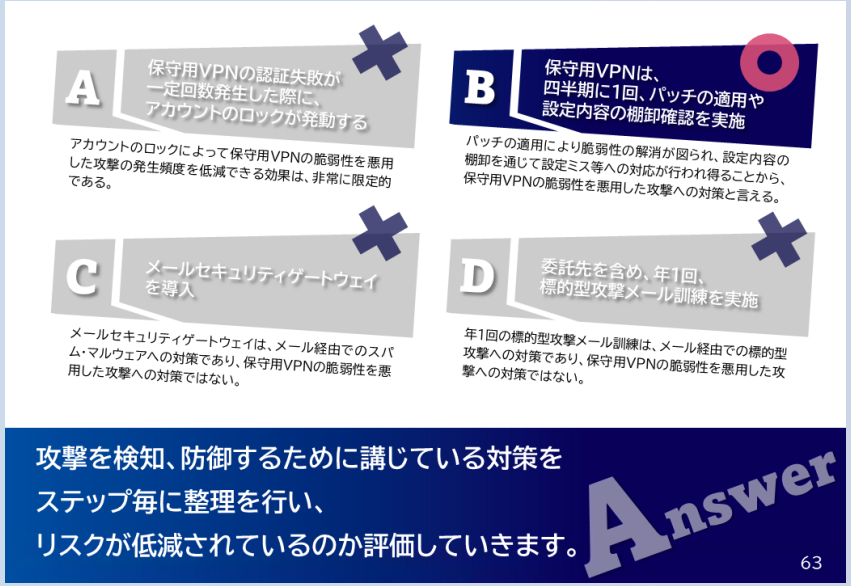


４つの選択肢をご用意しています。

ステップ1の攻撃を防ぐために、模擬事業者(A社)で実施している対策を選んでみてください。

SLIDE 63

Answer 6



答えは B になります。

ステップ1は、保守用VPNの脆弱性が原因で侵入されています。模擬事業者（A社）において、保守用VPNの脆弱性への対応のために実施している対策内容を記載する必要があるため、「四半期に1回のパッチ適用や設定内容の棚卸確認」が記載すべき内容となります。

攻撃を防ぐために追加で実施すべき対策を記載するのではなく、現状で実施できている対策を書く必要があることにご留意ください。

その他の選択肢は以下のように考えることができます。

- A｜保守用VPNにおけるアカウントロックの実施

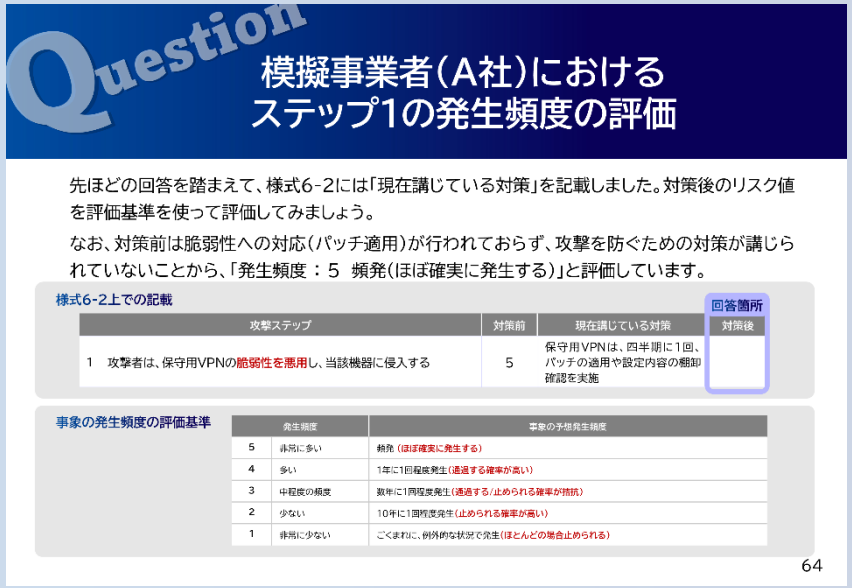
  アカウントロックは総当たり攻撃等の認証を突破する攻撃には有効ですが、脆弱性を悪用した攻撃の発生頻度を低減する効果は限定的です。
- C｜メールセキュリティゲートウェイの導入

  メール経由でのスパム・マルウェアや標的型攻撃への対策であり、脆弱性を悪用した攻撃への対策にはなりません。
- D｜標的型攻撃メール訓練の実施

  メール経由でのスパム・マルウェアや標的型攻撃への対策であり、脆弱性を悪用した攻撃への対策にはなりません。

SLIDE 64

Question 7-1



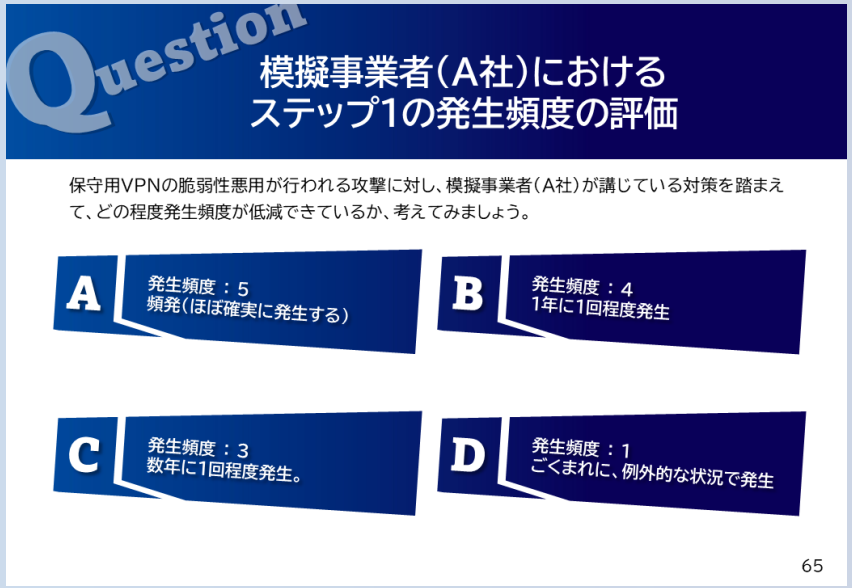
続いて「対策後」のリスク値を考えてみましょう。

先ほどの問題で考えていただいた「現在講じている対策」を考慮しながら、対策後のリスク値を「事象の発生頻度の評価基準」を用いて、評価してみてください。

なお、「対策前」のリスク値は、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状態となりますので、「発生頻度 ： 5 頻発（ほぼ確実に発生する）」と評価しています。

SLIDE 65

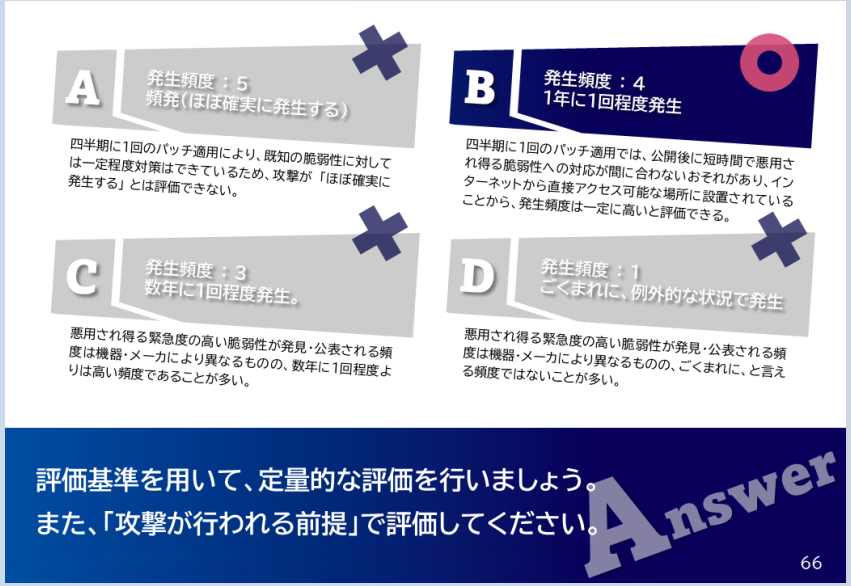
Question 7-2



選択肢の中から、どの程度発生頻度が低減できているか選んでみてください。

SLIDE 66

Answer 7



答えは B（1年に1回程度）です。評価の方法について解説していきます。

模擬事業者（A社）では、保守用VPNに対し四半期に1回、パッチ適用や設定内容の棚卸をしています。

そのため、一定の対策はとられており「ほぼ確実に発生する」という評価である「A：頻発」は、選択肢から外すことができます。

一方で、脆弱性は日々発見・公表されています。

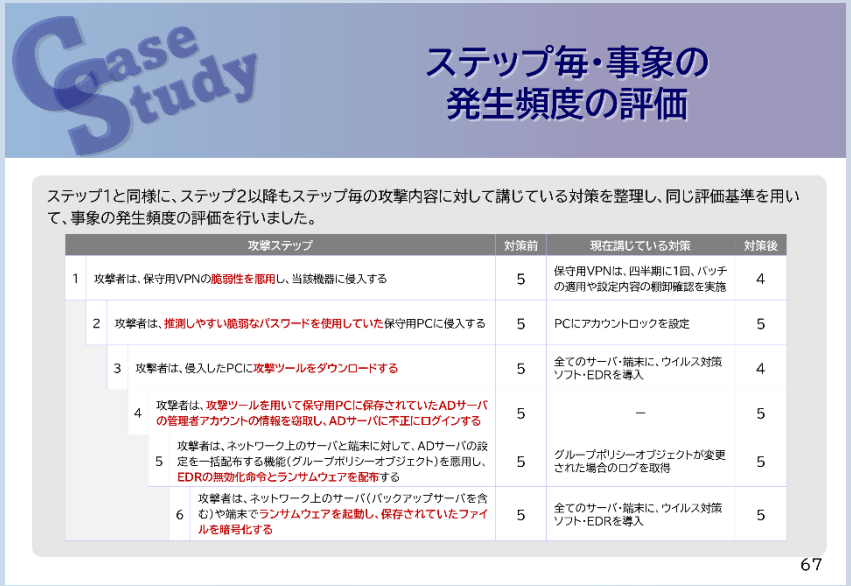
緊急度の高い脆弱性が発見・公表される頻度は、機器・メーカにより異なりますが、四半期に1回のパッチ適用という頻度を踏まえると、「C：数年に1回程度」や「D：ごくまれに/例外的な状況で発生」というほどの発生頻度の低減はできていないと考え、「B：1年に1回程度発生」と評価しています。

評価基準を用いることで、定量的な評価が行え、属人的な判断を防ぐことができます。

なお、評価にあたっては、攻撃が行われないかもしれないといった希望的観測を排し、「攻撃が行われる前提」で評価してください。

SLIDE 67

Case Study:リスク評価 2

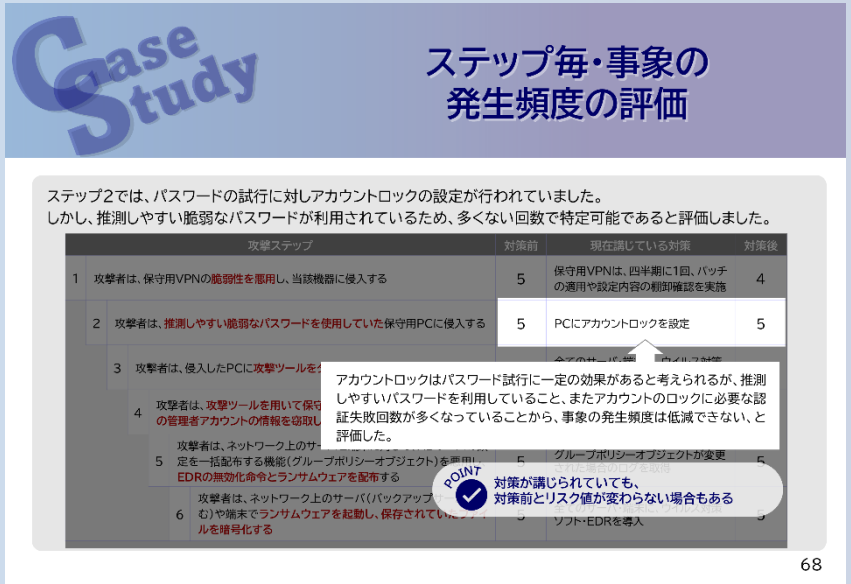


ステップ1で実施いただいた内容を踏まえて、ステップ2以降もステップ毎の攻撃内容に対して講じられている対策を整理し、「対策前」「現在講じている対策」「対策後」を記載した結果をこちらに記載しています。

ステップ2以降を簡単に解説していきます。

SLIDE 68

Case Study:リスク評価 3



ステップ2の「対策前」のリスク値は「5:頻発」と評価しています。

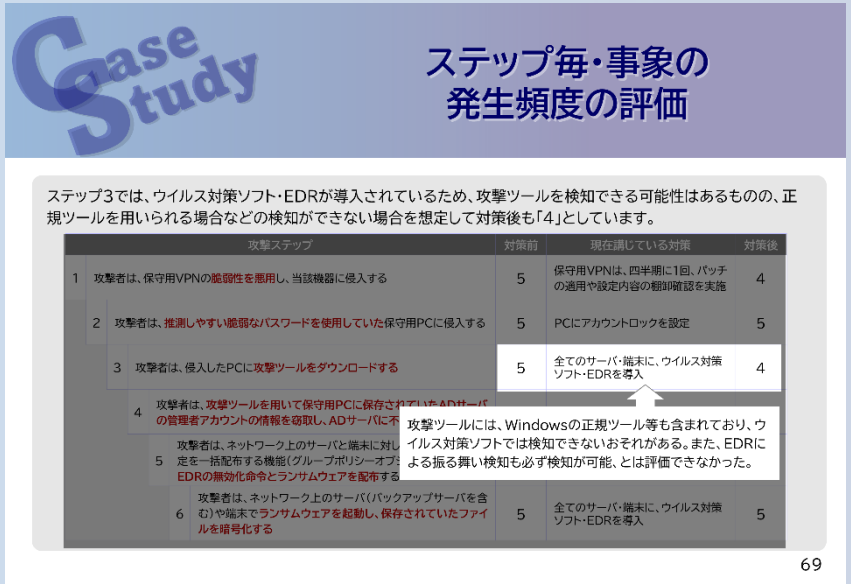
本ステップは、保守用PCで利用されていたパスワードを推測されて侵入が行われています。パスワードの推測を防ぐための対策として「現在講じている対策」には、「アカウントロックの設定」が入ります。

しかし、保守用PCでは推測しやすい脆弱なパスワードが使用されており、またアカウントロックに必要な回数もいることから、十分にリスクが低減できないと評価し、「対策後」のリスク値も変わらず「5:頻発」と評価しています。

対策が講じられていても、必ずしもリスク値が下がらない場合があることにご注意ください。

SLIDE 69

Case Study:リスク評価 4



ステップ3の「対策前」のリスク値は「5:頻発」と評価しています。

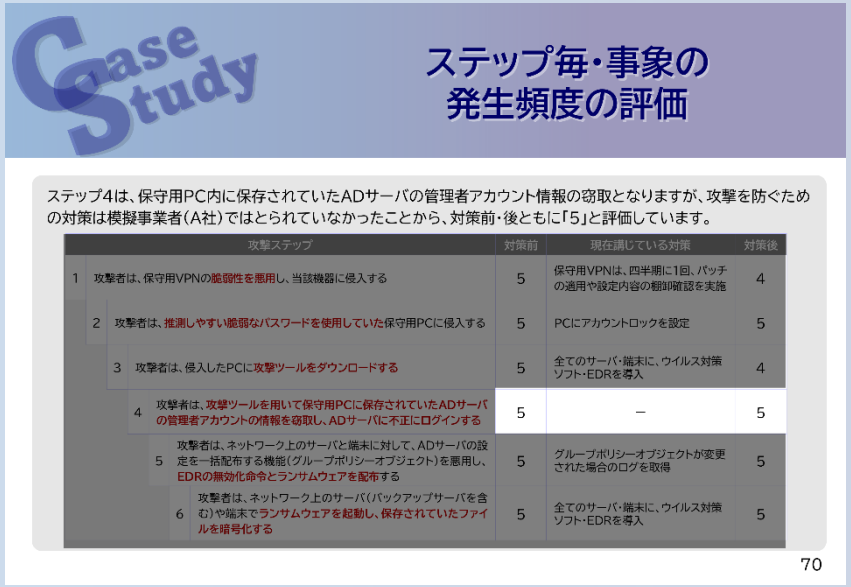
侵入したPCへの攻撃ツールのダウンロードが行われたステップです。

攻撃ツールへの対策として、模擬事業者(A社)は「ウイルス対策ソフト・EDRの導入」を実施しています。ウイルス対策ソフト・EDRの機能を用いることで攻撃ツールの検知は一定に可能と考えられます。

しかし攻撃ツールには、Windowsの正規ツール等も含まれており、ウイルス対策ソフト・EDRで検知できないおそれもあります。

そのため、ウイルス対策ソフト・EDRにより一定発生頻度が低減したとしても、数年に1回程度、まで発生頻度は低減できないと評価し、「4:1年に1回程度」と評価しています。

Case Study:リスク評価 5



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。

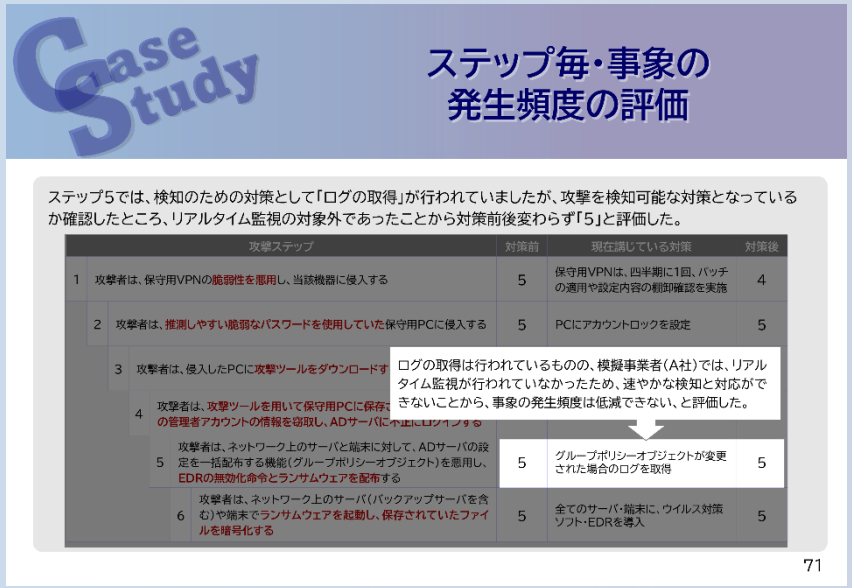
この攻撃を防ぐためには、ログイン情報へのアクセスを制限する保護機能を有効化する、管理者アカウントでログインする環境を制限する等の対策が考えられますが、模擬事業者(A社)では実施されていませんでした。

そのため、「現在講じている対策」は無し。

リスク値も「対策前」「対策後」ともに「5:頻発」と評価しています。

SLIDE 71

Case Study:リスク評価 5



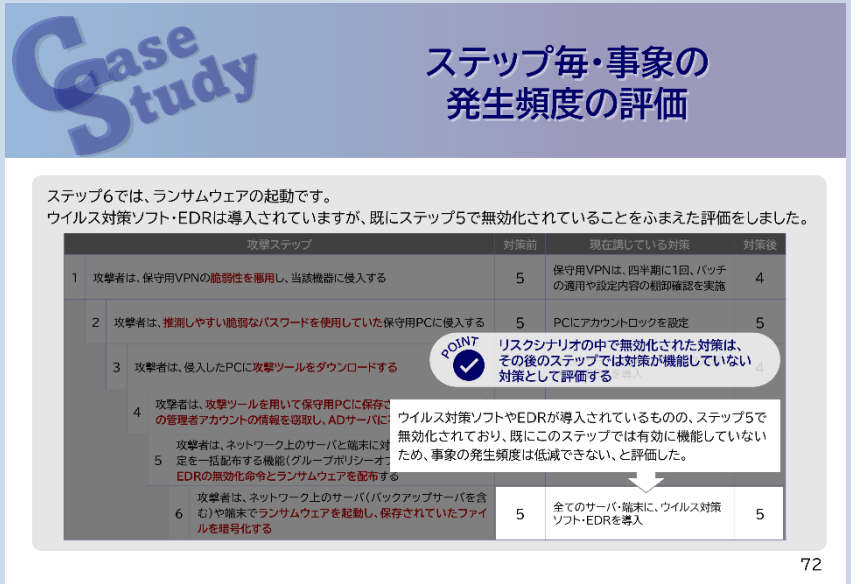
ステップ5の「対策前」のリスク値は「5:頻発」と評価しています。

本ステップではADサーバの機能を利用してEDRの無効化とランサムウェアの配布が行われています。設定変更が行われた際のログを取得し、点検・監視を行うことで検知することができる可能性はあります。

模擬事業者(A社)もログの取得は行っていますので、「現在講じている対策」には、ログの取得が記載されています。しかし、攻撃の検知が可能であったか確認したところ、リアルタイム監視の対象外であったことから、速やかな検知は難しい状況であったことが確認できています。

そのため、事象の発生頻度の低減ができないとの評価により、対策後の評価も「5」としています。

Case Study:リスク評価 6



ステップ6の「対策前」のリスク値は「5：頻発」と評価しています。

本ステップではランサムウェアの起動が行われています。

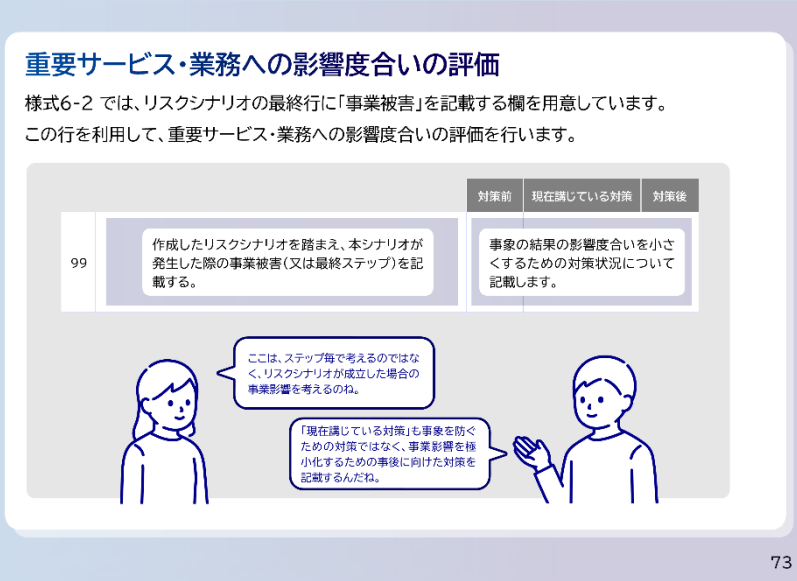
模擬事業者（A社）は「ウイルス対策ソフト・EDRの導入」を行っているので、発生頻度の低減を期待したいのですが、当該対策はステップ5で既に無効化されてしまっています。

そのためこのステップの段階では有効に機能しておらず、事象の発生頻度の低減ができないとの評価により、対策後も「5：頻発」と評価しています。

今までのステップで無効化されてしまった対策は、その後のステップでは対策が機能していない、講じられていないものとして評価してください。

SLIDE 73

重要サービス・業務への影響度合いの評価



最後に、様式6-2 では「事業被害」に関する評価を行います。

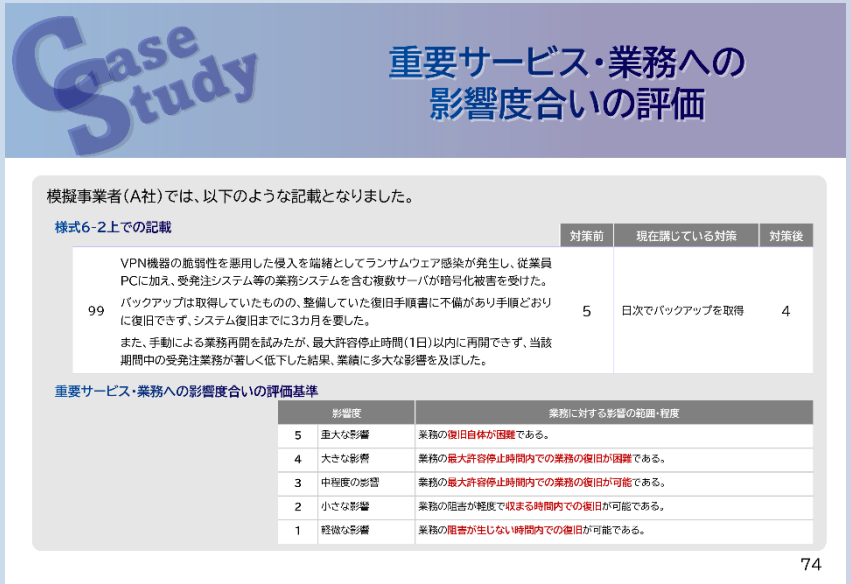
リスクシナリオの最終行（ステップ99）に、リスクシナリオが発生した場合の事業被害（又は最終ステップ）を記載します。

そして、リスクシナリオが発生した場合の事業被害（又は最終ステップ） に対し、事業影響の評価を行っていきます。

「現在講じている対策」の欄には、リスクシナリオが成立し、実際に被害が生じた場合に事業影響を極小化するために実施されている対策を記載します。

SLIDE 74

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、本スライドのような記載になりました。

ステップ99には、発生した被害の内容、復旧に要する期間と業務に生じた影響を記載しています。

ステップ99に記載した内容を踏まえて影響度の評価を行います。

「対策前」は、影響を極小化するための対策は一切講じられていない状態となりますので、業務の復旧ができなかった、と評価し「5：重大な影響」としています。

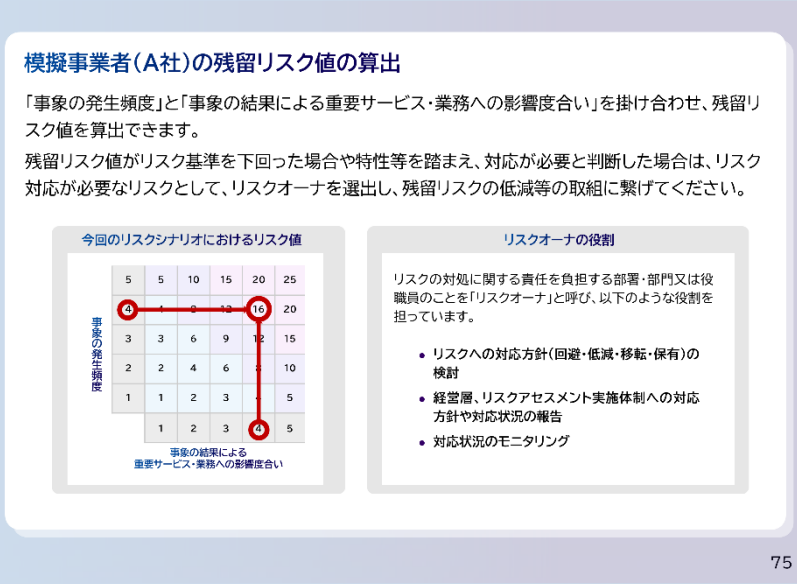
模擬事業者（A社）において影響の極小化や早期復旧のために講じている対策としては「日次でのバックアップ取得」があったため、「現在講じている対策」にその旨を記載しています。

しかし、復旧訓練等は実施されていないことから復旧手順書の有効性は確認されておらず、最大許容停止時間内での復旧は困難と評価しています。

そのため、「対策後」のリスク値は「4：大きな影響」との評価になりました。

SLIDE 75

模擬事業者（A社）の残留リスク値の算出



ここまで算出したリスク値に基づいて、残留リスク値を算出します。

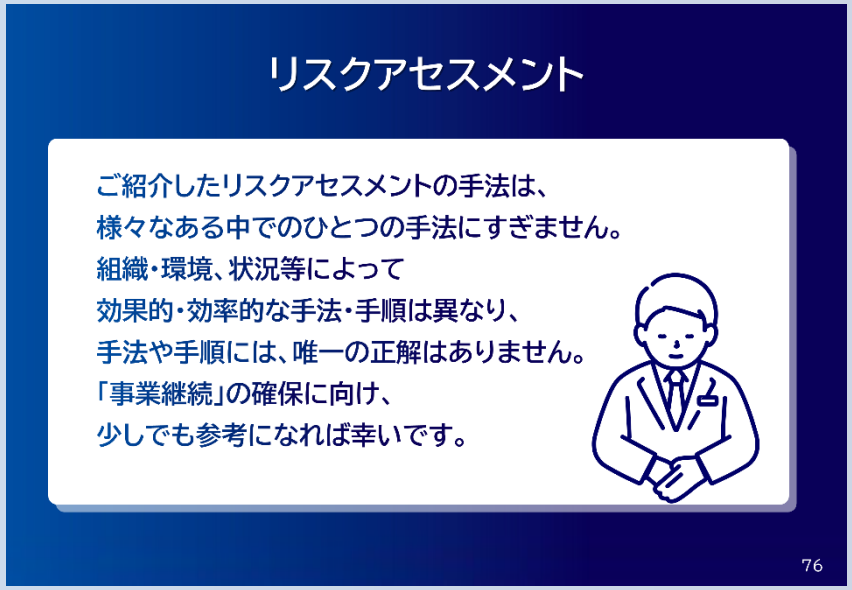
模擬事業者（A社）では、「事象の発生頻度」の「対策後」の最小値と「事象の結果による重要サービス・事業への影響度合い」の「対策後」の数値を掛け合わせることにより、残留リスク値を算出しています。

結果、残留リスク値は16となりました。

算出された残留リスク値とリスク基準を比較し、リスク対策が必要であると判断した場合は、リスクオーナーを選出し、残留リスクの低減等の取組を通じて、サイバー攻撃への対策強化に繋げることとなります。

SLIDE 76

リスクアセスメント



ここまでで、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についてみてきました。

紹介した手順は様々ある手法のひとつで、唯一の正解ではありませんが、事業継続の確保に向けて、少しでも参考となれば幸いです。

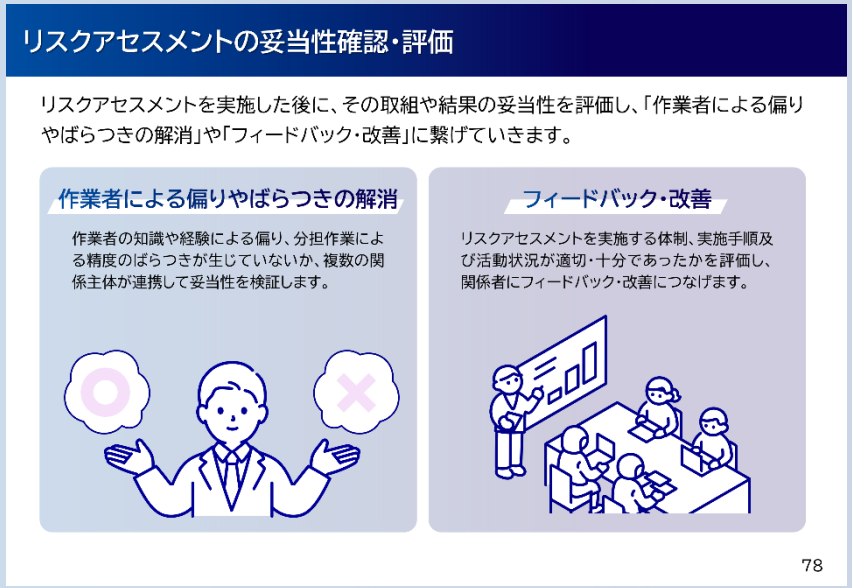
05

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実施が終わった後、実施したリスクアセスメントの妥当性の確認や評価を行っていきます。

SLIDE 78

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取組や結果の妥当性を評価することで、作業者による偏りやばらつきを解消するとともに、フィードバックや改善に繋げることができ、リスクアセスメントの質を継続的に高めていくことができます。

SLIDE 79

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内容の妥当性を確認する具体的な方法として、「ウォークスルー」という手法を紹介します。

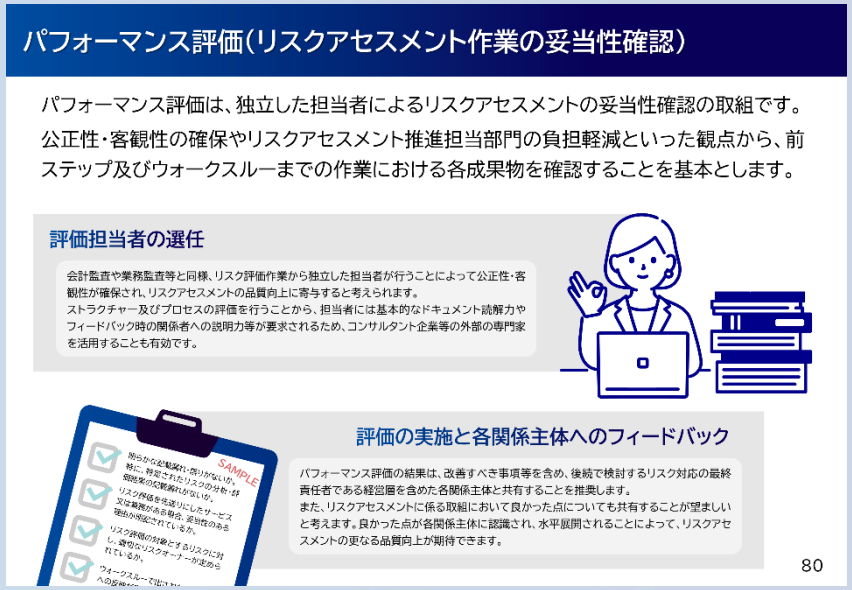
リスクアセスメントの実施目的の確認から、リスクの洗い出し、リスク評価に至るまでの一連の取組を対象として、関係者で内容を確認します。

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・管理部門にも参画し、評価結果の粒度や精度のばらつきを抑えるための意見交換をすることができます。必要に応じて、経営企画部門や法務部門などの間接部門をレビュー役として加えることも有効です。

指摘事項を出し合い、修正内容をリスクアセスメントの成果物に反映することで、組織として妥当性の高いリスクアセスメントを行うことができます。

SLIDE 80

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）



もうひとつの手法として、リスクアセスメント作業全体の妥当性を確認する「パフォーマンス評価」という手法をご紹介します。

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・客観性の確保やリスクアセスメント推進担当部門の負担軽減が期待できます。

パフォーマンス評価の結果は、経営層を含む各関係主体と共有することが推奨されています。評価結果を各関係主体が認識し、水平展開されることによって、リスクアセスメントの品質向上につなげることができます。

SLIDE 81

リスクアセスメントの継続的な見直し

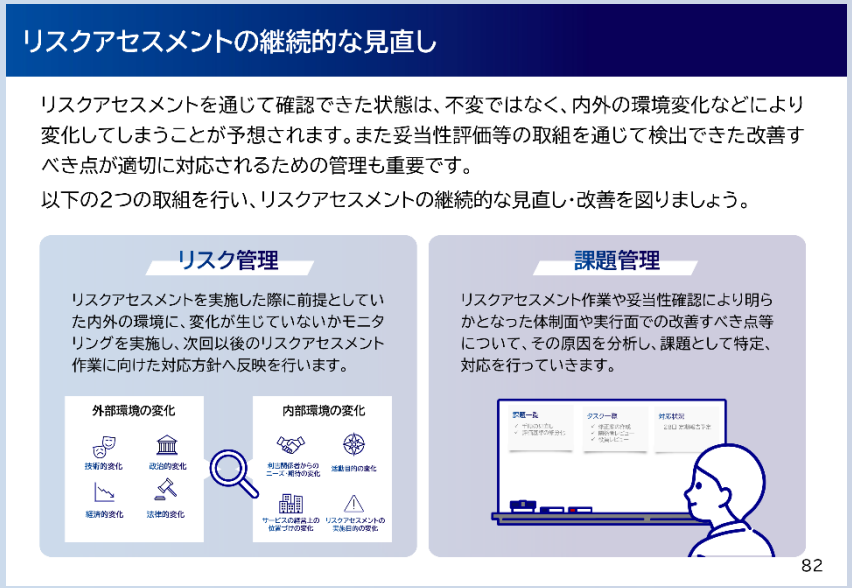
06

リスクアセスメントの継続的な見直し

最後に、リスクアセスメントの継続的な見直しを行っていきます。

SLIDE 82

リスクアセスメントの継続的な見直し



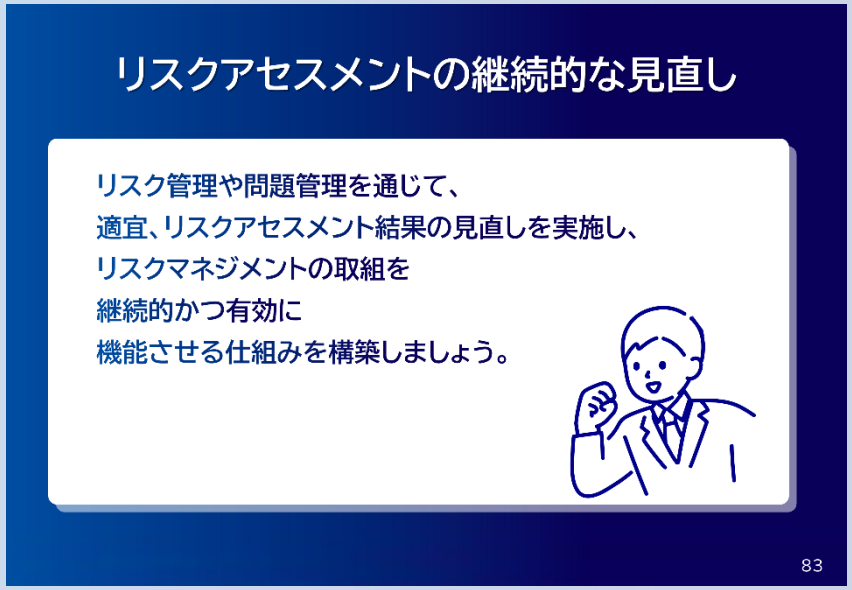
リスクアセスメントを通じて確認できたリスクの状態や評価結果は、組織の内外の環境変化により、時間の経過とともに変化していきます。また、妥当性評価などの取組を通じて明らかになった改善点について、適切に対応されているかを管理していくことも重要です。

そのため、リスクアセスメントは一度実施して終わりではなく、継続的な見直しと改善を前提とした取組とする必要があります。

リスクアセスメント実施後の内外の環境に変化をモニタリングし次回以降のリスクアセスメントに向けた対応方針へ反映したり、リスクアセスメント作業や妥当性確認を通じて明らかになった体制面や実行面での課題管理への対策を通じて、リスクアセスメントの品質を維持させることができます。

SLIDE 83

リスクアセスメントの継続的な見直し



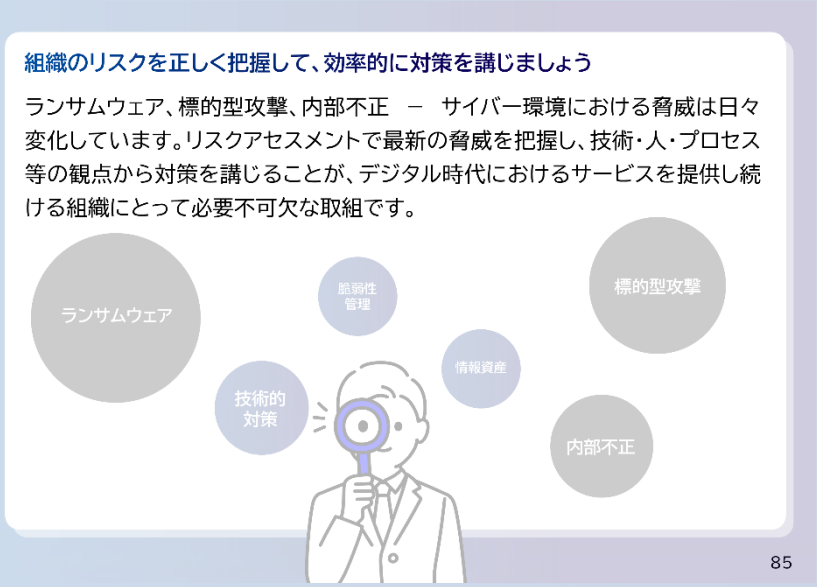
　このように、リスクアセスメントは一度実施して終わりではなく、リスク管理や課題管理の取組を通じて、適宜見直しを行うことが重要です。

　こうした見直しを継続的に行う仕組みを構築することで、リスクマネジメントが組織の活動に定着し、有効に機能し続ける仕組みを構築しましょう。

おわりに

SLIDE 85

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



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。

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。