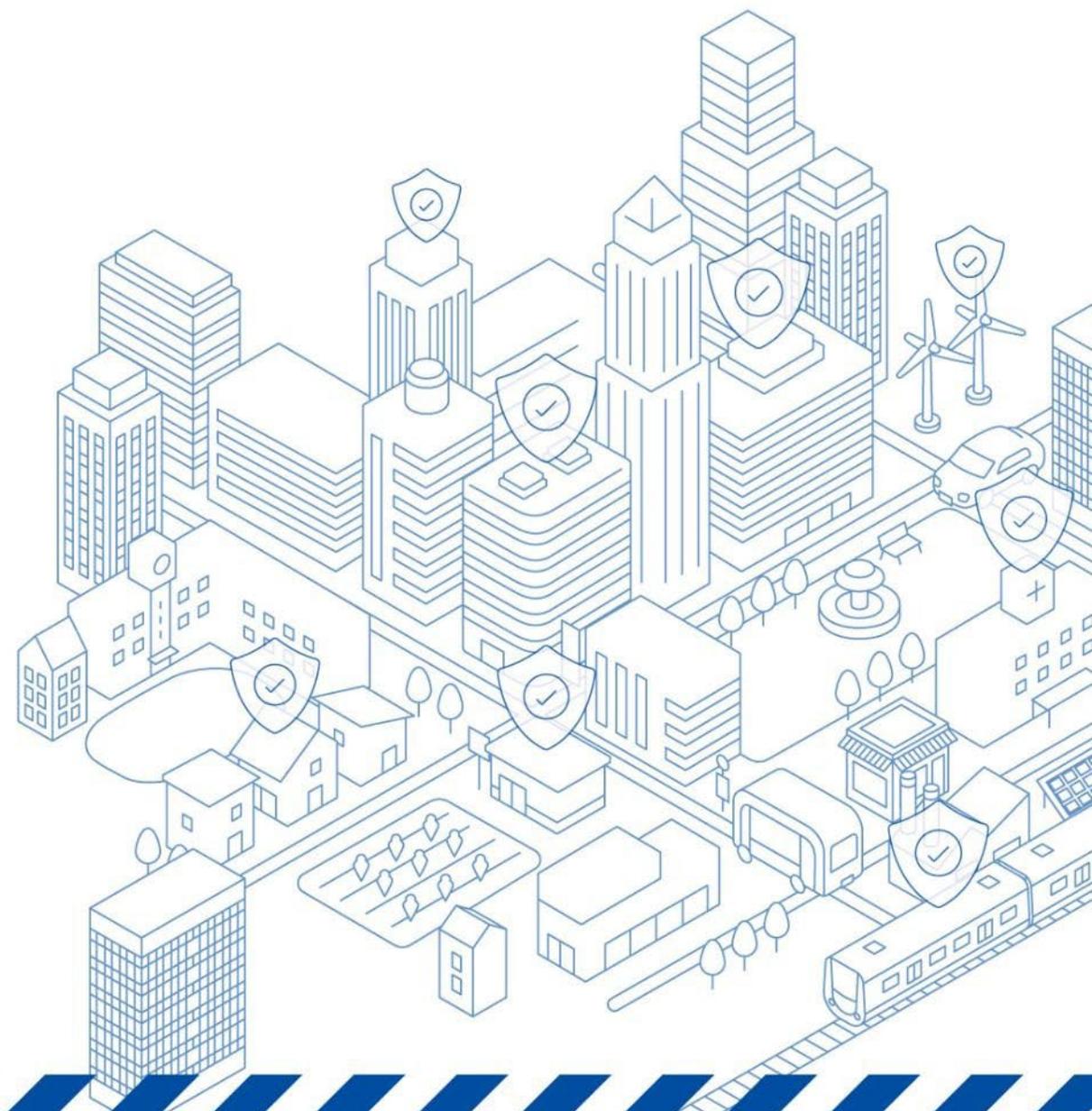


リスクアセスメント実践
ラーニングキット
解説・研修展開マニュアル
～自己学習、研修教材～

内閣官房 国家サイバー統括室



Agenda

Agenda

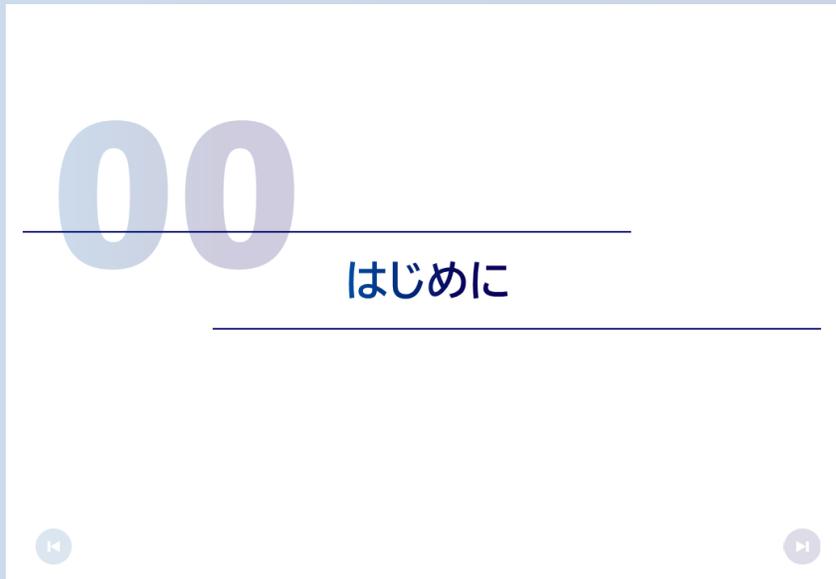
- 00 はじめに
- 01 事前準備
- 02 リスクアセスメントの対象の特定
- 03 リスク評価方針の策定
- 04 リスクアセスメント
- 05 リスクアセスメントの妥当性確認・評価
- 06 リスクアセスメントの継続的な見直し
- 99 おわりに

1

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。

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。

はじめに①

はじめに ①

近年、情報通信技術の活用場面が広がる一方、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

3

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となっています。

はじめに②

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

4

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。

はじめに③

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

人員の割当

追加対策の実施

予算の割当

5

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ふおそれもあります。

その結果、ルールが守られなくなったり、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、といっ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。

はじめに④

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。



6

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。

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

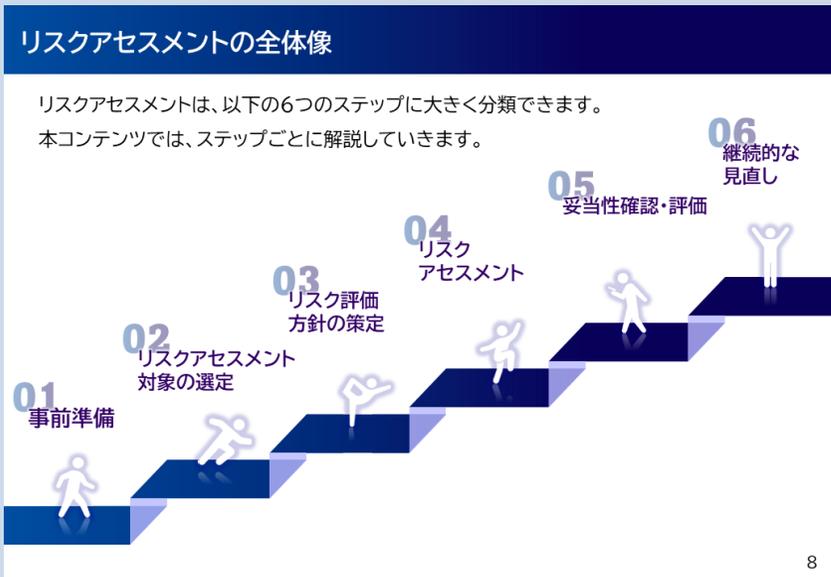
本コンテンツでは、「機能保証のためのリスクアセスメント・ガイドライン[※]」の考え方に基づいて、「社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために必要なサービスの提供を維持・継続する」という「機能保証」の観点から、リスクアセスメントの手順を紹介します。



[※] <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。

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

事前準備

01

事前準備

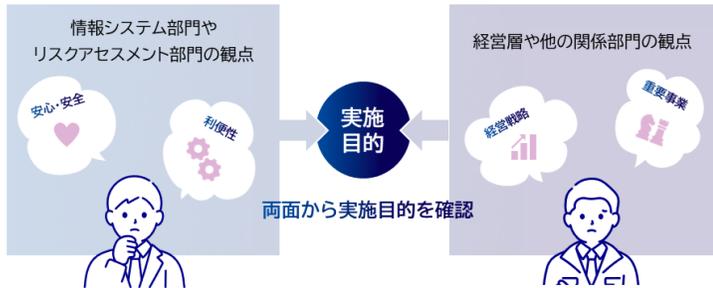
まず、最初の工程です。

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。

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。



10

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。

リスクアセスメントの実施目的の確認の必要性: Question

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。



11

なぜ、目的の確認が必要なのでしょう。

リスクアセスメントの実施目的の確認の必要性:
Answer

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。



12

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。

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。

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。

スケジュールの策定と実施体制の構築

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。



16

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。

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。

重要サービスの特定

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。



18

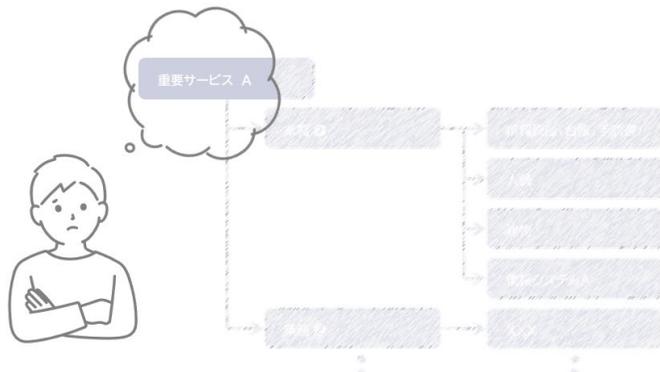
リスクアセスメントの実施には時間も人員も必要となります。

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。

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

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…



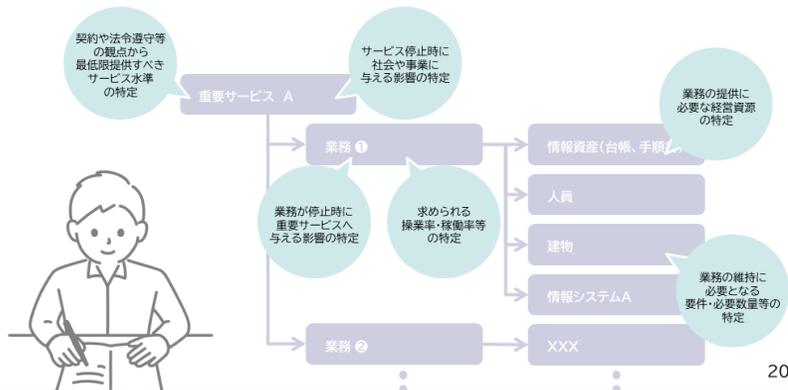
19

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、

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

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な業務や経営資源まで詳細化して、リスク評価を行きましょう。



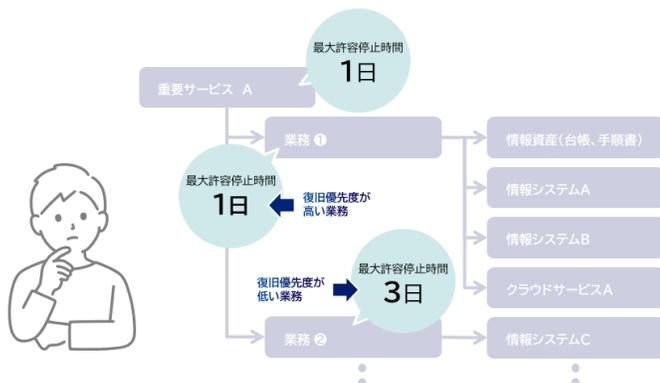
そのサービスに求められているサービス水準や、その提供のために必要となる業務、経営資源まで詳細化を行って、リスク評価を行っていきましょう。

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、

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

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。



21

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②の最大許容停止時間は3日となっていますので、業務①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。

様式3 重要サービスの影響分析

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、サービスの提供が停止した場合の影響程度に依り影響分析し、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) 最低限許容されるサービスの範囲・水準を明らかにし、サービスの提供が停止した場合の影響程度に依り影響分析し、最大許容停止時間を決定する。 | | (4) サービスの提供が停止した場合の影響程度に依り影響分析し、最大許容停止時間を決定する。 | | | | | | | (5) サービスの提供が停止した場合の影響程度に依り影響分析し、最大許容停止時間を決定する。 | | |
|-------|---------|---|-------------|--|------|------|----|-----|-----|----|--|------|--|
| | | 契約責任、法令遵守 | 社会的責任 (CSR) | 影響度 | 影響範囲 | 影響期間 | 1日 | 1週間 | 1か月 | 1年 | MTPO | 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

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
 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。

ワンポイントアドバイス ①

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。

STEP3 最終版評価表の例(1)～(2)

| リスク | 対応策 | 評価 |
|-----|-----|----|
| | | |
| | | |
| | | |
| | | |

自組織における
重要サービス

評判や信用

人命や環境



24

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。

様式4 業務の洗い出し・業務が停止した場合の影響

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可能な最低水準（必要な機能等）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伴う最大許容停止時間を特定する。 (様式4)

| (1) 編 | (2) 業務サービス | (3) 重要サービス提供のために必要な業務（業務サービス提供に不可欠な業務） | (4) 重要サービス提供のために必要な最低水準（必要な機能等） | (5) 業務停止に伴う影響度合いの評価 | | | | | | | MTPD | JAGD |
|-------|------------|--|---------------------------------|---------------------|------|------|------|------|-------|-------|------|------|
| | | | | 影響度 | 影響範囲 | 影響時間 | 影響頻度 | 影響回復 | 影響コスト | 影響リスク | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

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

「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。

ワンポイントアドバイス ②

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



26

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」に着目してみよう。

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。

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

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



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。

様式5 業務を支える経営資源の要件・必要数量

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。

| STEP1 重要サービス(リスク)の特定 | | STEP2 重要サービス(リスク)の発生原因(脅威)の特定 | | STEP3 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の特定 | | STEP4 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の特定 | | STEP5 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク)の特定 | |
|----------------------|----------------------|--------------------------------|--|--|--|--|--|---|--|
| 重要サービス(リスク) | 重要サービス(リスク)の発生原因(脅威) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) | 重要サービス(リスク)の発生原因(脅威)の発生原因(リスク)の発生原因(リスク)の発生原因(リスク) |
| | | | | | | | | | |

| STEP5 業務を支える経営資源の要件・必要数量 | | | | | | | |
|--------------------------|--------|-----------------------|-----------|------------------------------|-------------------------|----|--------------------|
| 人 | 情報、データ | 設備、特許権、商標、著作権、特許権、特許権 | 設備、機器、消耗品 | 情報通信設備(IC)システム、ソフトウェア、ハードウェア | 交通機関、ライオネット(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

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。

Question 2

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

29

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。

Answer 2



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。

30

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。

リスク評価方針の策定

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。

リスク分析手法の検討

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

32

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で、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。

リスク分析手法の検討

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。

33

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。

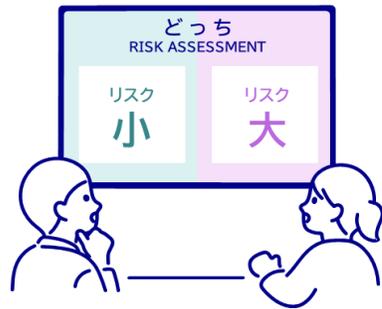
リスクアセスメントの分析手法や評価の軸は、リスクアセスメントの目的や組織の状況等を踏まえ、最適なものを検討してみてください。

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。

リスク基準の決定

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——



34

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——

リスク基準の決定

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——

どっち
RISK ASSESSMENT

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



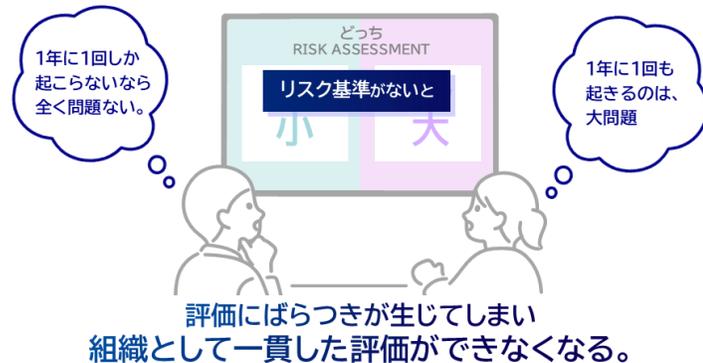
35

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ましょう。

リスク基準の決定

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。



36

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。

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 | | | | 事象の発生頻度 | |
|--------------------------|----------------|---------------------------------|----------------------------|---------|---|
| Example | 影響度 | 影響度合い | | Example | 発生頻度 |
| | 事象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 | | 事象の予想発生頻度 |
| 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。 | 5 | 非常に多い 頻発 ほぼ確実に発生する |
| 4 | 大きな影響 | 当該業務が阻害され、業務の最低水準が維持が困難である。 | 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。 | 4 | 多い 1年に1回程度発生 超過する確率が高い |
| 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。 | 3 | 中程度の頻度 数年に1回程度発生 超過する確率と止められる確率が拮抗 |
| 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。 | 2 | 少ない 10年に1回程度発生 止められる確率が高い |
| 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。 | 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 |

「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。

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。

| | | | | | | | | | | |
|---|--------|------------------------|--------|--|---|---|----|----|----|----|
| <small>事例の結果による 重要サービス・業務 への影響度合い</small> | | <small>事例の発生頻度</small> | | <small>事例の結果による 重要サービス・業務への影響度合い</small> | | | | | | |
| example | 影響度 | example | 発生頻度 | example | 5 | 5 | 10 | 15 | 20 | 25 |
| 5 | 重大な影響 | 5 | 非常に多い | <small>事例の発生頻度</small> | 4 | 4 | 8 | 12 | 16 | 20 |
| 4 | 大きな影響 | 4 | 多い | | 3 | 3 | 6 | 9 | 12 | 15 |
| 3 | 中程度の影響 | 3 | 中程度の頻度 | | 2 | 2 | 4 | 6 | 8 | 10 |
| 2 | 小さな影響 | 2 | 少ない | | 1 | 1 | 2 | 3 | 4 | 5 |
| 1 | 軽微な影響 | 1 | 非常に少ない | | 1 | 2 | 3 | 4 | 5 | |
| | | | | | | | | | | |
| | | | | | | | | | | |

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。

Question 3

リスク基準を利用して、
リスク評価をしてみましょう。

Question

 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 - |

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。

Answer 3

- 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の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広がるおそれがある。
- 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

実際に

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・サービスだけでなく、業務や人員等を総合的に評価することが重要です。

40

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。

機能保証の観点からのリスクの特定

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、サービスを停止 |

42

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。

様式6-2 リスクアセスメント(リスクシナリオ)

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。

The diagram illustrates the structure of the risk assessment template. It is divided into several vertical sections:

- Left Section:** Labeled '今までの様式で洗い出した事業・サービス・業務' (Business/Service/Business Process identified in the current format). It contains columns for '経営資源' (Management Resources), '業務の阻害につながる結果' (Results leading to business disruption), and '結果を生じ得る事象' (Incidents that can result in results).
- Middle Section:** Labeled 'リスクシナリオ' (Risk Scenario). It features a large grid with a diagonal shaded area, representing the identification of risks based on scenarios.
- Right Section:** Labeled '事象の影響度合い、発生頻度の評価' (Evaluation of the degree of impact and frequency of occurrence). It includes columns for '影響度' (Degree of Impact) and '発生頻度' (Frequency of Occurrence).
- Far Right Section:** Labeled 'リスク評価結果' (Risk Assessment Result). It contains columns for 'リスクレベル' (Risk Level) and 'リスク評価結果' (Risk Assessment Result).

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。

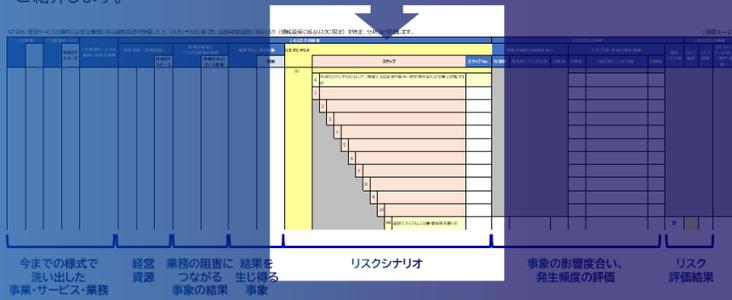
ここからは、リスクアセスメントの進め方について説明を行っていきます。

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。

Case Study: リスクシナリオの作成 1

まずは、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。
この図式は、リスクアセスメントの手法を
 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。

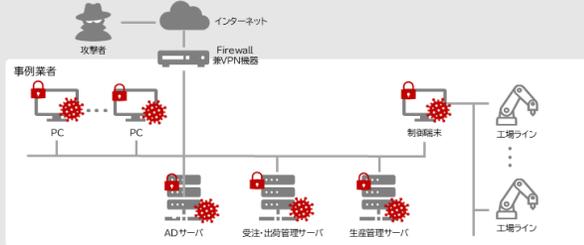
では、実際にリスクシナリオの作り方を体験していきましょう。
 様式6-2の真ん中の部分を埋めていく作業となります。

Case Study: リスクシナリオの作成 2



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。



45

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。

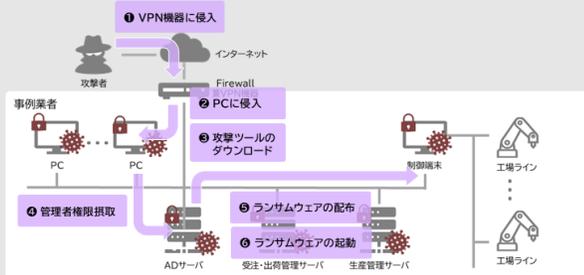
ランサムウェアにより、サーバに保存されていたファイルが暗号化され、業務の継続が困難になったという事例です。

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

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。



46

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

Case Study: リスクシナリオの作成 4

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 |

47

「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。

インシデントを踏まえたリスクシナリオの考察

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 | カスタマイズ例 |
|---|--|
| <p>原因 VPN機器が初期パスワードのまま運用されている。</p> <p>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。</p> | <p>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。</p> <p>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。</p> |

自組織では、初期パスワードは利用していないから、実際に発生し得る攻撃を考えてみよう

自組織の環境を踏まえて攻撃ステップをカスタマイズ

確かに、この内容なら、自組織でも起こり得るリスクシナリオになっている。

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けます。

48

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。

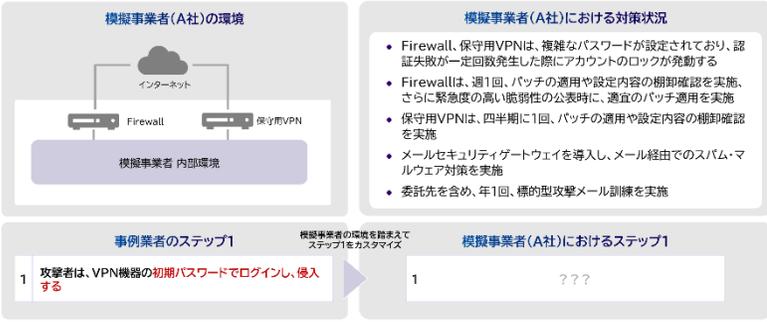
攻撃ステップのカスタマイズを簡易に体験いただくために、本コンテンツでは、模擬事業者(A社)を用意しました。

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。

Question 4-1

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)を考えてみましょう。



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――

Question 4-2

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

50

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を考えていきましょう。

Answer 4

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。

51

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。

模擬事業者(A社)におけるリスクシナリオ | ステップ2

Case Study 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(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

52

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。

模擬事業者(A社)におけるリスクシナリオ | ステップ3

Case Study
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(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**

模擬事業者の環境を踏まえてステップ3はそのまま適用

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

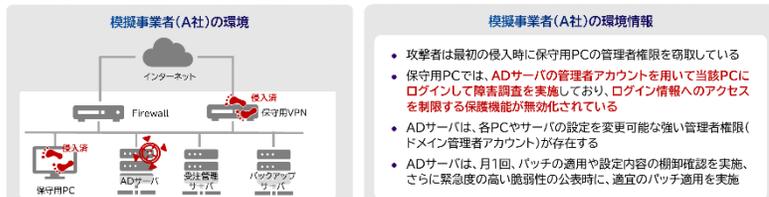
- 攻撃者は、侵入したPC(保守用PC)に攻撃ツールをダウンロードするとなります。

模擬事業者(A社)におけるリスクシナリオ | ステップ4



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(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

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。

Question 5-1

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(A社)におけるステップ5

5 ???

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

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。

Question 5-2

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

56

こちらにも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。

Answer 5

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

57

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なので、△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。

Case Study: リスクシナリオの作成 5

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 |

58

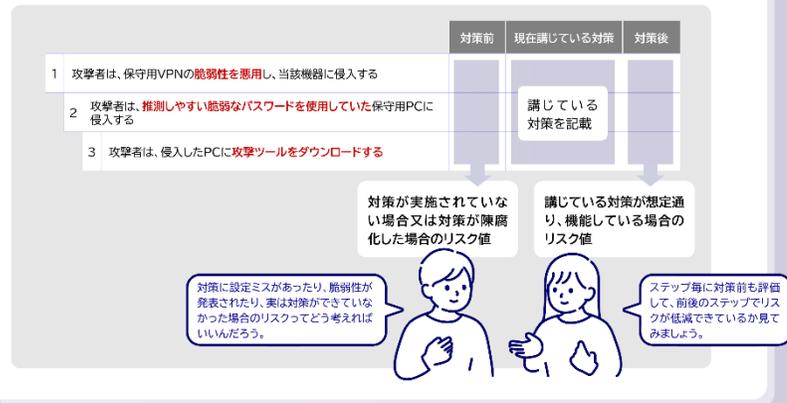
これまで考えてきた模擬事業者(A社)における攻撃ステップを、様式6-2の「リスクシナリオ」に記載できるように書き直したものが本スライドの内容となります。

「リスクシナリオ」が完成したら、次は――

ステップ毎・事象の発生頻度の評価

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。



60

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。

Question 6-1

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

| 攻撃ステップ | 回答箇所 | | |
|---------------------------------|------|-----------|-----|
| | 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 | | | |

61

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。

Question 6-2

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

62

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。

Answer 6

| | |
|--|---|
| 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

63

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。

Question 7-1

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

| 攻撃ステップ | 対策前 | 現在講じている対策 | 回答箇所 |
|---------------------------------|-----|------------------------------------|------|
| 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転記確認を実施 | 対策後 |

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(遭遇する確率が高い) |
| 3 中程度の頻度 | 数年に1回程度発生(遭遇する/止められる確率が特防) |
| 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、偶発的な状態で発生(ほとんどの場合止められる) |

64

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。

Question 7-2

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、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

65

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。

Answer 7

| | |
|---|--|
| <p>A 発生頻度：5 頻発(ほぼ確実に発生する)</p> <p>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。</p> | <p>B 発生頻度：4 1年に1回程度発生</p> <p>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。</p> |
| <p>C 発生頻度：3 数年に1回程度発生。</p> <p>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・メーカー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。</p> | <p>D 発生頻度：1 ごくまれに、例外的な状況で発生</p> <p>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・メーカー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。</p> |

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

Answer

66

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・メーカー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。

Case Study: リスク評価 2



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制御確認を実施 | 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 |

67

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。

Case Study: リスク評価 3



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検証確認を実施 | 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に攻撃ツールをインストールする | 5 | 侵入したPCに攻撃ツールをインストールする | 5 |
| 4 攻撃者は、攻撃ツールを用いて保守用PCの管理者アカウントの情報を窃取する | 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。 | 5 |
| 5 攻撃者は、ネットワーク上のサーバー（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 | 5 |
| 6 攻撃者は、ネットワーク上のサーバー（バックアップソフトウェア）や端末でランサムウェアを起動し、保存されているデータを暗号化する | 5 | バックアップソフトウェアをインストールし、EDRを導入 | 5 |

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

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。

Case Study: リスク評価 4



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検証確認を実施 | 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サーバに不正アクセスを行う | 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。 | 5 |
| 5 攻撃者は、ネットワーク上のサーバと端末に対して一括配布する機能(グループポリシーオブジェクトの無効化命令とランサムウェアを配布する) | 5 | 全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入 | 5 |
| 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 |

69

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確認確認を実施 | 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 |

70

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」とともに「5:頻発」と評価しています。

Case Study: リスク評価 5



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検証確認を実施 | 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 | 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。 | 5 |
| 4 攻撃者は、攻撃ツールを用いて保守用PCに保存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 | 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 |
| 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 | 全てのサーバ・端末に、ウイルス対策ソフト・EDRを導入 | 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 | | 5 |

71

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 | 現在している対策 | 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検証確認を実施 | 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 | | 5 |
| 4 攻撃者は、攻撃ツールを用いて保守用PCに保存された管理者アカウントの情報を窃取し、ADサーバに | | | |
| 5 攻撃者は、ネットワーク上のサーバと端末に特定を一括配布する機能(グループポリシー)で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。

72

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」を行っているのですが、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。

重要サービス・業務への影響度合いの評価

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。 | |

73

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。

Case Study:
重要サービス・業務への影響度合いの評価

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か月を要した。 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 業務の被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 業務の被害が生じない時間内での復旧が可能である。 |

74

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。

模擬事業者(A社)の残留リスク値の算出

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、リスクオーナーを選出し、残留リスクの低減等の取組に繋げてください。



リスクオーナーの役割

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「リスクオーナー」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

75

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で、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。

リスクアセスメント

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。



76

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な手法のひとつで、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。

リスクアセスメントの妥当性確認・評価

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。

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を解消」や「フィードバック・改善」に繋がっていきます。

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。



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。

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(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。



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。



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。

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(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を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。

80

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。

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。

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。



82

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。

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。



83

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

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

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。



85

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。