令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

セキュリティリスク評価及び対策基準に記載されるべき管理策
【対策基準レベル②】

サイバーセキュリティ
人材育成
社内体制整備支援

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	組織として策定すべき対策基準及び情報セキュリティの 三大要素【対策基準レベル①】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	組織的対策と人的対策【実施手順・実施者マニュアルレベル②】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

1．リスクマネジメント

リスクマネジメント：概要

リスクマネジメント：リスクアセスメント

リスクマネジメント：リスク対応

リスクマネジメント：概要

【参照：セミナーテキスト11-1-1.】
第11章 - 02

リスクマネジメントプロセス（ISO31000）

リスクマネジメントとは

存在するリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のこと

ISO31000では

原則

枠組み

プロセス

リスクマネジメント：概要

【参照：セミナーテキスト11-1-1.】
第11章 - 02

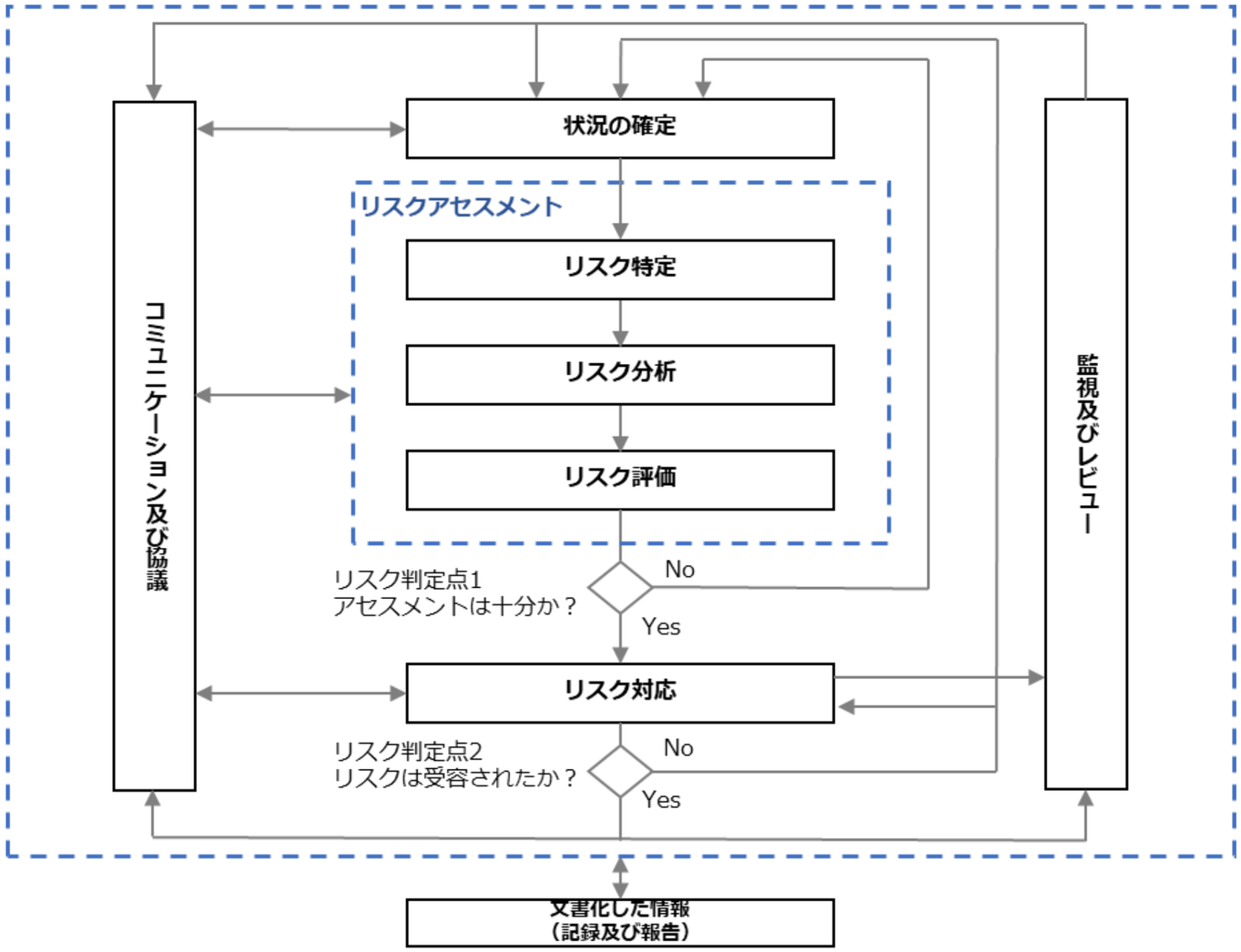
リスクマネジメントの3要素

要素	概要
原則	リスクマネジメントを実施する際に、組織が取り組むべき事項。 「価値の創出および保護」を中心に、次の８つの要素で構成されている。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」 「利用可能な最善の情報」「人的及び文化的要因」「継続的改善」
枠組み	リスクマネジメントを組織全体に定着させるための仕組み。 「リーダーシップおよびコミットメント」を中心に、次の５つの要素で構成されている。 「統合」「設計」「実施」「評価」「改善」
プロセス	リスクマネジメントに取り組む上で実施すべき一連の活動。 次の６つの要素で構成されている。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」 「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」 「記録作成及び報告」

リスクマネジメント：概要

【参照：セミナーテキスト11-1-2.】
第11章 - 03

情報セキュリティリスクマネジメント（ISO/IEC27005）

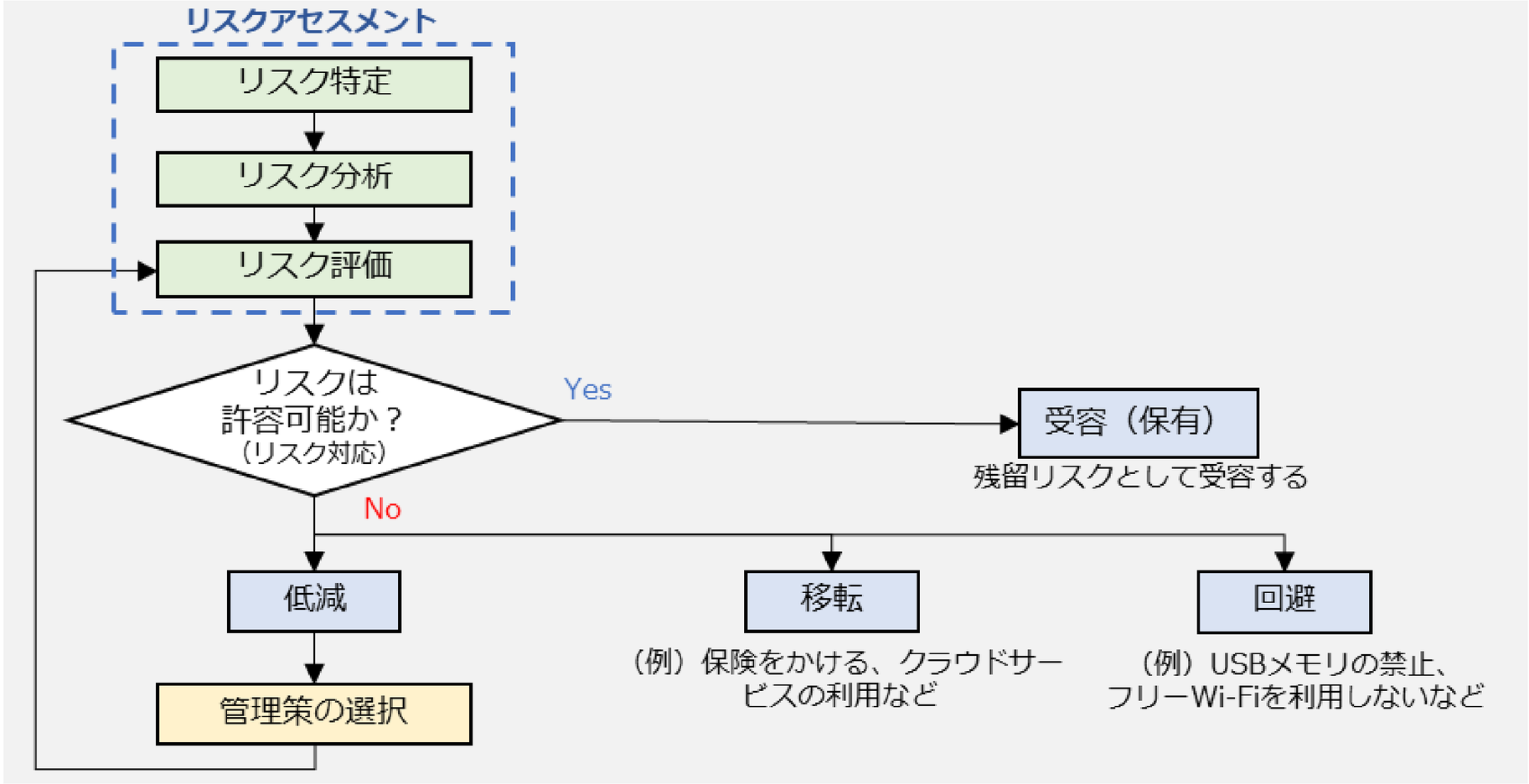


情報セキュリティマネジメントプロセスの概要
（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスクマネジメント：概要

【参照：セミナーテキスト11-1-2.】
第11章 - 04

情報セキュリティリスクマネジメント（ISO/IEC27005）

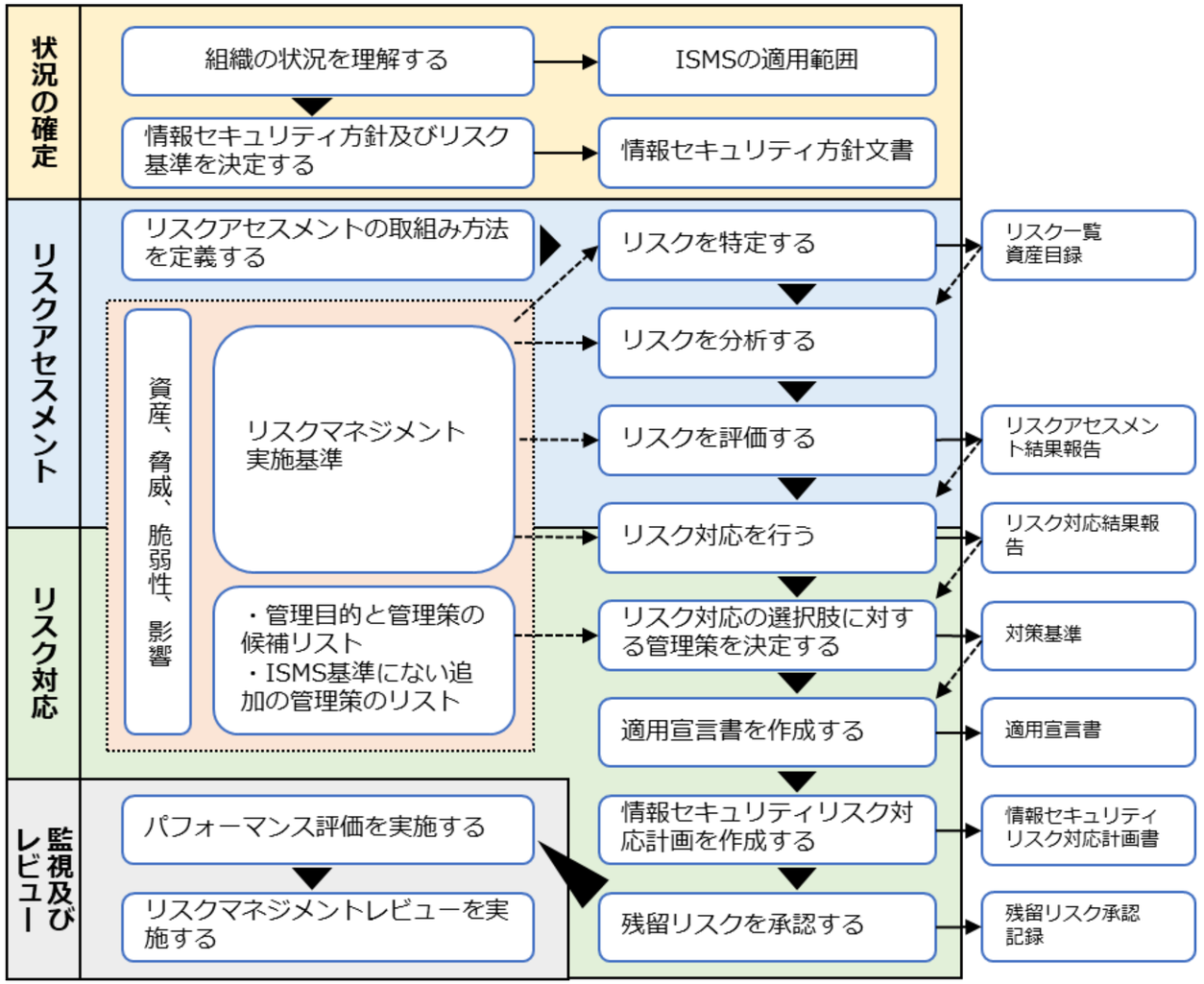


リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクマネジメント：概要

【参照：セミナーテキスト11-1-3.】
第11章 - 05

ISO/IEC 27001におけるリスクマネジメント手順



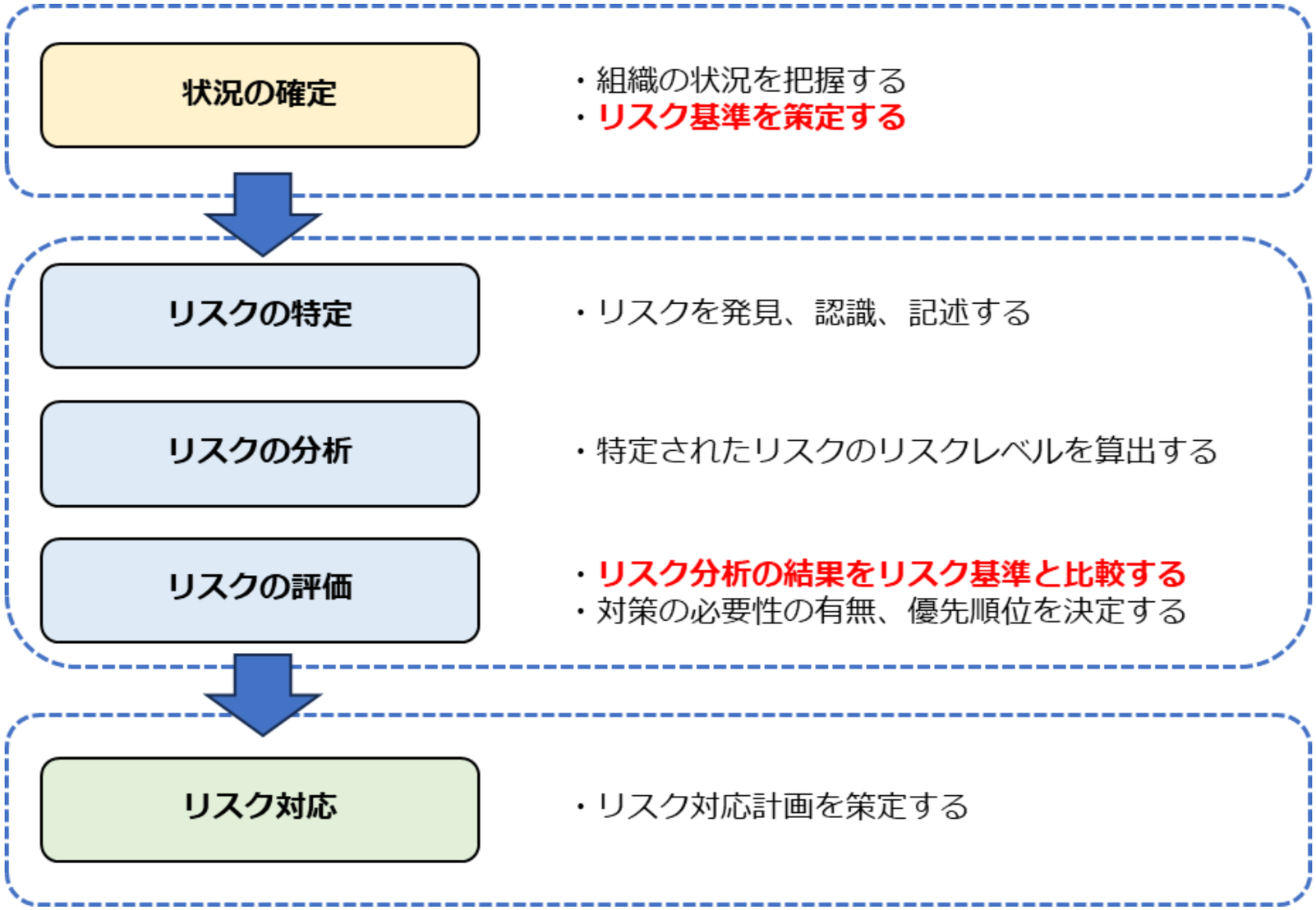
ISMSにおけるリスクアセスメントおよびリスク対応に関する作業の概要

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-1.】
第11章 - 06

リスク基準の確立

必要なリスク基準



リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 07

リスク特定

アプローチ手法と特徴

アプローチ手法	概要
資産ベースのアプローチ	• 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 • 資産は、その種類及び優先度に従って主要資産及び支援資産として特定できる。 • 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 • 資産のリストを作成することが望ましい。
事象ベースのアプローチ	• 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。 • 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び組織の状況を決定する際に特定された要求事項によって発見できる。

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 07

リスク特定

アプローチ手法のメリット・デメリット

アプローチ手法	メリット	デメリット
資産ベースのアプローチ	• 資産、脅威及び脆弱性のすべての有効な組合せをISMSの適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	• 情報資産が増えたときに、資産のリストの行数が多くなる。 • 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	• 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルまたは戦略的なシナリオを確立することができる。	• 網羅性において、資産ベースのアプローチに劣る。

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 07

リスク特定

リスク所有者の特定

- 特定されたリスクに対し、リスク所有者を関連付ける。
- リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする（通常、組織内で一定の権限を持つ人が選ばれる）。

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 08

リスク特定（資産ベースのアプローチ）

アプローチ手法

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 08

リスク特定（資産ベースのアプローチ）

情報資産の洗い出し（例）

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部長	人事部	書類
経理	給与システムデータ	税務署提出用 源泉徴収票	給与計算担当	経理部長	人事部	事務所PC
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	経理部長	総務部	書類
経理	発行済請求書控え	当社発行の請求書の控え（過去3年分）	総務部	経理部長	総務部	書類
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部長	営業部	可搬電子媒体
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部長	営業部	社内サーバ
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部長	営業部	書類

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 09

リスク特定（資産ベースのアプローチ）

資産目録作成の効率化

- 情報資産を、「主要／事業資産」と「支援資産」のカテゴリに分類する

資産種別	概要
主要／事業資産	「主要/事業資産」とは、「組織にとって価値のある情報又はプロセス」のことです。主要資産は、「事業プロセス及び事業活動」と「情報」の2つに分けられます。
支援資産	「支援資産」とは、「1つ以上の事業資産の基礎となる情報システムの構成要素」のことです。

（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	• 取引先から秘密として提供された情報 • 取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	• 自社の独自技術・ノウハウ • 取引先リスト • 特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	• 見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	• 自社製品カタログ • ホームページ掲載情報

（情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
完全性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	• 取引先から処理を委託された会計情報 • 取引先の口座情報 • 顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	• 自社の会計情報 • 受発注・決済・契約情報 • ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	• 廃版製品カタログデータ

（情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	• 顧客に提供しているECサイト • 顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	• 製品の設計図 • 商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	• 廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 11

リスク特定（資産ベースのアプローチ）

影響度の評価をもとに重要度を算定

重要度	情報資産の価値・事故の影響の大きさ
3	事故が起きると、 「 法的責任を問われる」 「 取引先、顧客、個人に大きな影響がある」 「 事業に深刻な影響を及ぼす」 など、企業の存続を左右しかねない
2	事故が企業の事業に重大な影響を及ぼす
1	事故が発生しても事業にほとんど影響はない

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 11

リスク特定（資産ベースのアプローチ）

重要度の判断例

要素	情報資産の価値・事故の影響の大きさ	評価値
機密性	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	1
完全性	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	3
可用性	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	3

完全性と可用性の評価値3が最大値なので、重要度は評価値：3

重要度の判断例
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 12

リスク特定（事象ベースのアプローチ）

アプローチ手法

① リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」
② リスク所有者の特定	①で特定されたリスクの所有者を記載します。

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-2.】
第11章 - 12

リスク特定（事象ベースのアプローチ）

リスク特定の例

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	○○○○
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響をおよぼす事象である	3		

事象ベースのアプローチによるリスク特定の例
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-3.】
第11章 - 13

リスクの分析

リスク分析の例

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性とは

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する （いつ発生してもおかしくない）
2	特定の状況で脅威が発生する （年に数回程度）
1	通常の状況で脅威が発生することはない （通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない （ほぼ無防備）
2	部分的に対策を実施している （一部対策を実施）
1	必要な対策をすべて実施している （対策を実施）

「起こりやすさ」と「つけ込みやすさ」の換算表で算出する

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性の換算表

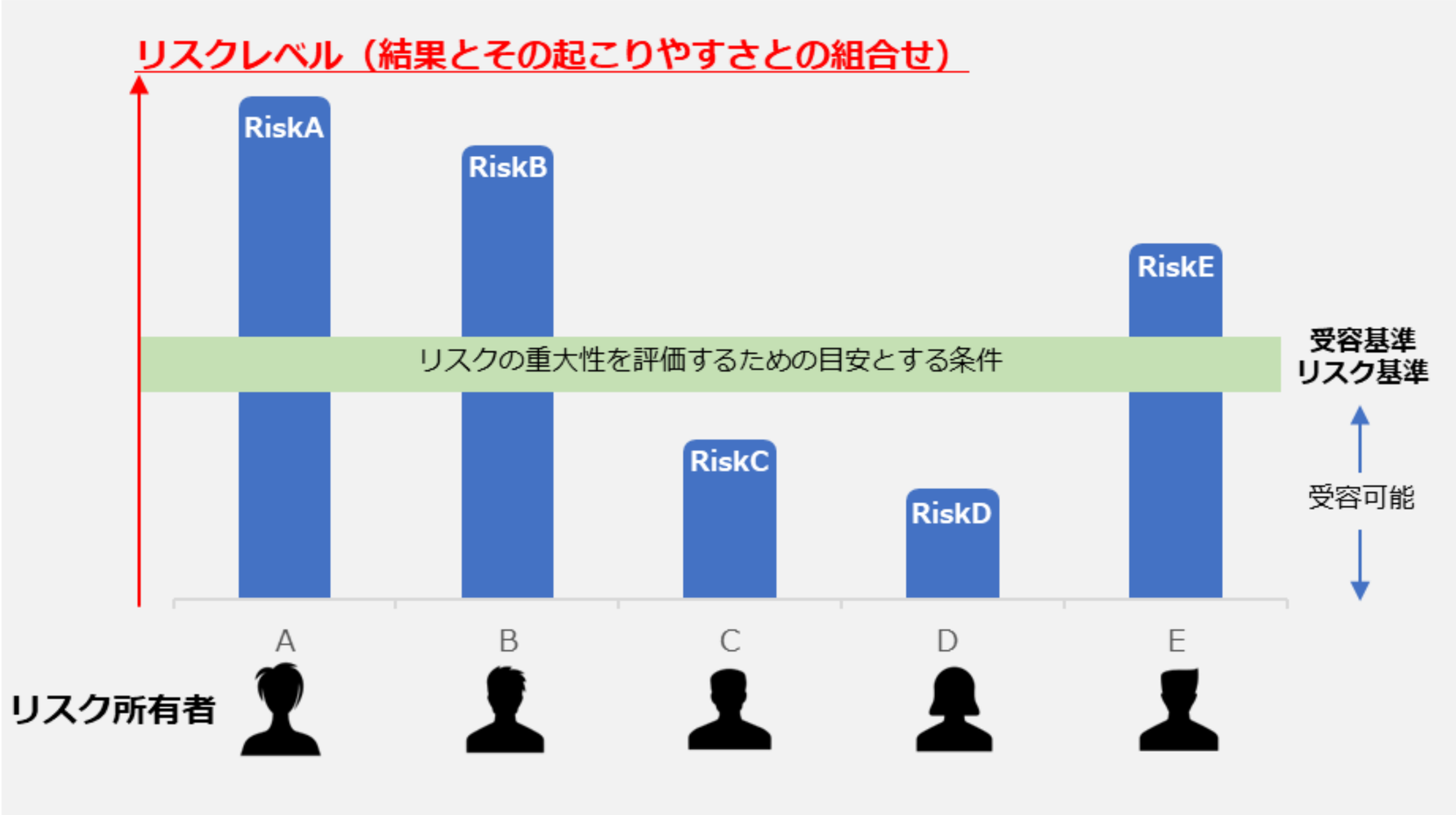
被害発生可能性の換算表		付け込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-4.】
第11章 - 14

リスクの評価

リスク評価



リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：セミナーテキスト11-2-4.】
第11章 - 15

リスクの評価

リスク評価（例）

リスクレベル評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 16

対応策の検討

リスク対応プロセス

1. 適切な情報セキュリティリスク対応の選択肢の選定
2. 情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定
3. 決定した管理策とISO/IEC27001:2022附属書Aの管理策との比較
4. 適用宣言書の作成
5. 情報セキュリティリスク対応計画
6. リスク所有者による承認
7. 残留している情報セキュリティリスクの受容

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 16

対応策の検討

１．適切な情報セキュリティリスク対応の選択肢の選定

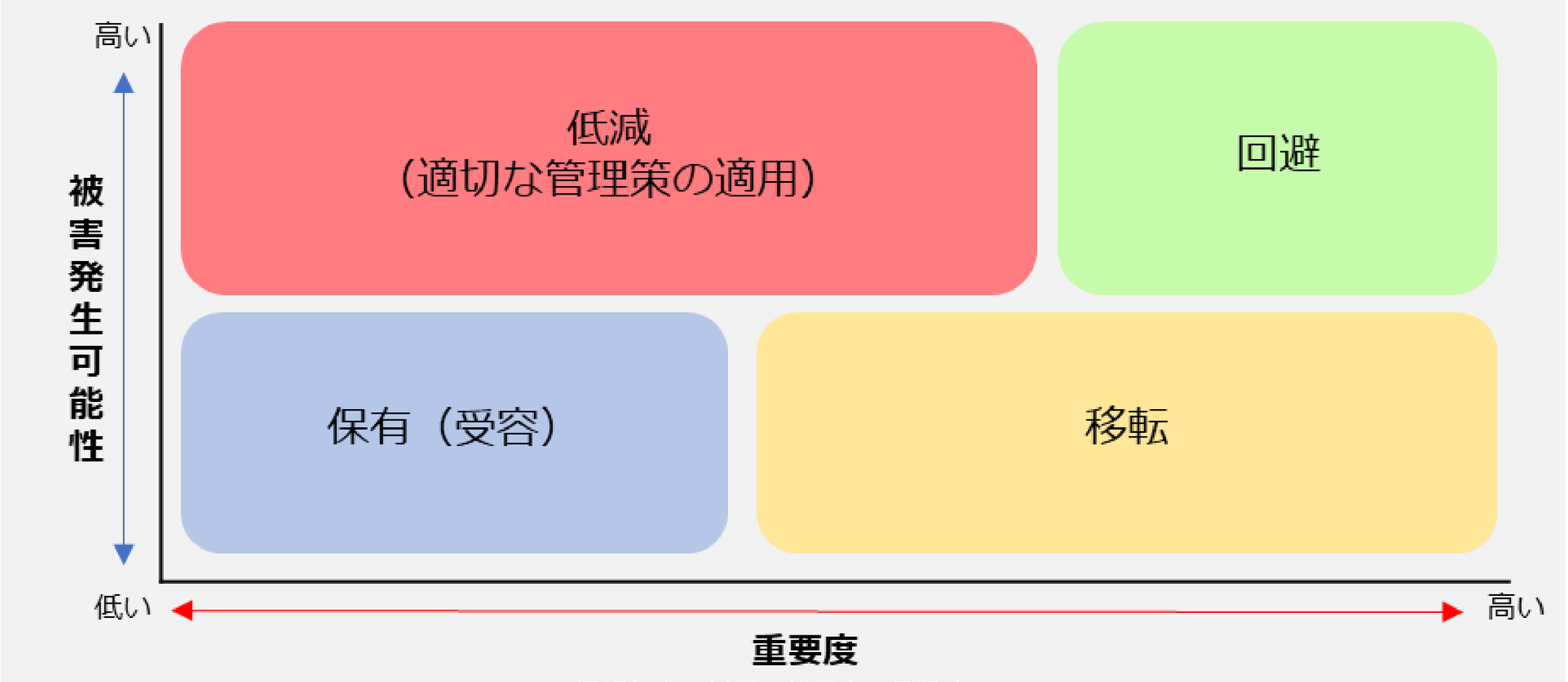
選択肢	対応内容
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-2-4.】
第11章 - 15

対応策の検討

リスク対応の選択肢の選定方法



情報セキュリティリスクの考え方
（出典）JNSA.”2-4 リスクアセスメントとリスク対応”. https://www.jnsa.org/ikusei/01/02-04.html,（参照 2023-09-21）

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-2-4.】
第11章 - 15

対応策の検討

リスク受容基準（例）

リスクレベル	リスク評価	記述
低	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい。そうでない場合、活動の全部又は一部を拒否することが望ましい

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 16

対応策の検討

２．情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定

　ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な全ての管理策を決定します。

３．決定した管理策とISO/IEC27001:2022附属書Aの管理策との比較

　必要な全ての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 16

対応策の検討

４．適用宣言書の作成
　必要な全ての管理策と、その理由及び実施状況を文書化します。

５．情報セキュリティリスク対応計画
　組織がリスクに対応する必要性を含んだリスク対応計画を作成します。

6．リスク所有者による承認
　リスク所有者は、リスク対応計画を承認します。

7．残留している情報セキュリティリスクの受容
　リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 17

対応策の検討

リスク対応プロセス（例）

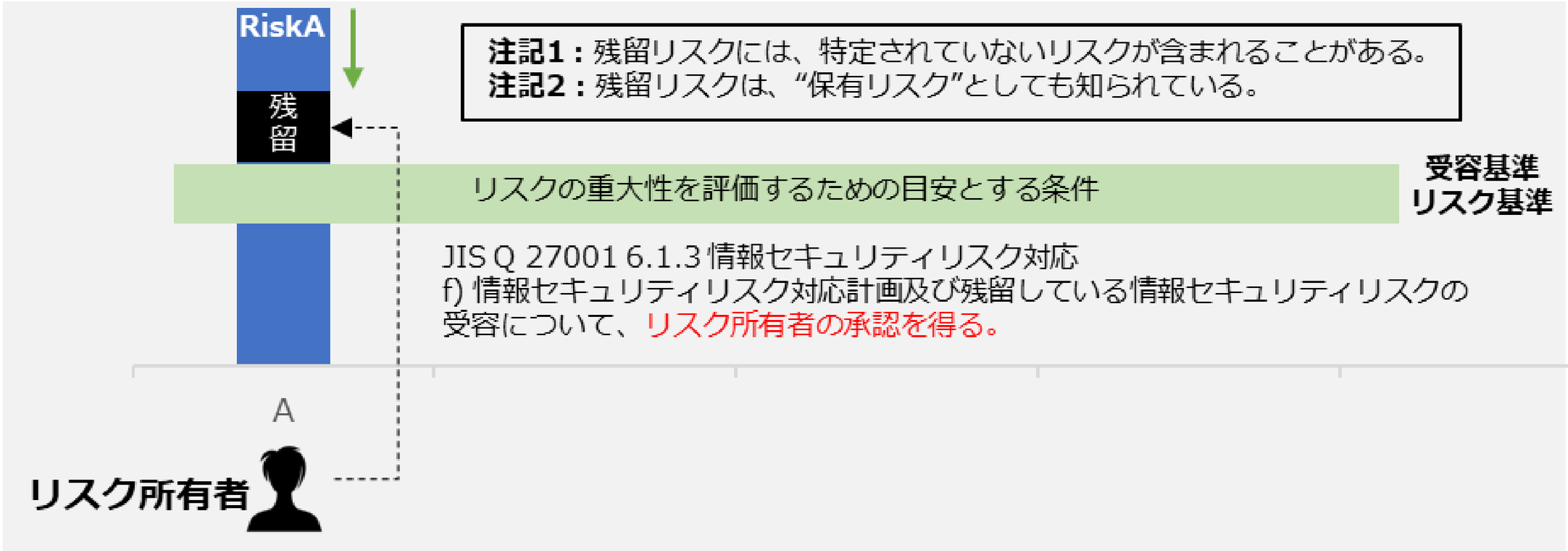
項目	内容
リスクの内容	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う
リスク対応	リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）
対策例	対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する 対応する管理策：5.15アクセス制御
対策基準の策定	技術的対策 • 公開サーバへの不正アクセス対策 • 公開サーバへのアクセス権の最小化と管理の強化 • 多要素認証の設定の有効化 • WAFの導入

リスクマネジメント：リスクの対応

【参照：セミナーテキスト11-3-1.】
第11章 - 17

対応策の検討

残留リスク



残留リスクの概要
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業