IT資格道場

CRISC 学習用テキスト

予備知識ゼロから合格ラインへ ―― 読んで理解する1冊目

無料サンプル(第1章まで)

CRISC 試験範囲(ISACA 公式 CRISC Exam Content Outline・2025年11月発効)準拠
2026年11月版

SAMPLE

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

SAMPLE

目次

第1章 Governance [1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5]

- 戦略・ゴール・目標 [1.1.1]
- 組織の構造・役割・責任 [1.1.2]
- 組織の文化と倫理 [1.1.3]
- ポリシーと標準 [1.1.4]
- 業務プロセスとレジリエンス [1.1.5]
- 組織の資産管理 [1.1.6]
- エンタープライズリスクマネジメント（ERM） [1.2.1]
- 防衛線（ラインズ・オブ・ディフェンス） [1.2.2]
- リスクプロファイル [1.2.3]
- リスク選好とリスク許容度 [1.2.4]
- リスクフレームワーク、法律、規制、契約上の要件 [1.2.5]

サンプルはここまでです

SAMPLE

このテキストの骨組みは、ISACA 公開の **CRISC Exam Content Outline（2025 年 11 月 3 日から適用。以下 ECO）** です[1]。ECO は試験の範囲を 4 つの分野と 44 の細目で決めており、章と節の並びも ECO のままにしました。節見出しの末尾の `[1.1.1]` は細目の番号で、公式の番号「1A1」の A を 1、B を 2 に置き換えた形。

分野の比率は、1 ガバナンス 26%、2 リスクアセスメント 22%、3 リスクへの対応と報告 32%、4 テクノロジーとセキュリティ 20% です[2]。試験は 150 問・240 分で、4 択から最も適切な答えを 1 つ選びます。合格は、200〜800 の換算点で 450 点以上です[2]。

CRISC の問題の中心は、用語の暗記ではありません。「リスク実務者はこの場面で最初に何をするか」「最も適切な対応はどれか」を問います。章見出しの末尾には、その章が扱う細目の番号を並べています。

SAMPLE

第1章 Governance [1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5]

ECO の比率は 26%、細目は 11 件。

この章は、IT リスクを事業の言葉で扱うための土台です。出題の多くは「誰が決め、誰が実行し、誰が確かめるか」を場面から判断させます。前半は組織のガバナンス（戦略・役割・文化・ポリシー・継続性・資産）、後半はリスクのガバナンス（ERM・防衛線・プロファイル・選好と許容度・枠組みと法令）を扱います。

戦略・ゴール・目標 [1.1.1]

ガバナンスは、利害関係者の必要・状況・選択肢を評価して企業の目標を決め、優先順位づけ、意思決定、達成状況の監視で方向を示すやり方です[3]。**コーポレートガバナンス**は企業を指揮し統制する仕組みで、取締役会が自社のガバナンスに責任を負います。ガバナンスは「何を目指すかを決めて監督すること」、マネジメントは「決まった方向で実行すること」と覚えます。

IT リスク管理の目的は、リスクをゼロにすることではありません。事業の戦略と目標の達成を支えることです。リスクを取ること自体が事業の価値を生むので、リスク実務者の仕事は「取るリスクを見えるようにして、取りすぎを防ぐこと」になります。ガバナンスの主な目的は価値創造で、便益実現・リスク最適化・資源最適化の3つの目的の釣り合いが取れた時に達成されます。便益実現は、新しい便益を生み、既存の便益を維持・拡張し、十分な価値を生まない取組みと資産をなくすことです[3]。

SAMPLE

アラインメントは、ガバナンスとITマネジメントの仕組みが企業の目標・戦略を支えている状態を指します。リスクの評価は、このアラインメントを前提にします。ITのリスクの大きさは、そのITが支える事業目標の大きさ次第で、技術の深刻さだけでは決まりません。

目標のカスケード

事業の目標からITの目標を導き、さらにリスクの目標（どのリスクをどこまで抑えるか）を導く流れを、目標のカスケードと呼びます。たとえば事業目標が「オンライン販売の売上を伸ばす」なら、ITの目標は「受注システムの可用性を保つ」です。リスクの目標は「受注システムの停止リスクを許容度内に収める」となります。

上の階層ほど経営の言葉、下の階層ほど現場の言葉です。カスケードがつながっていないと、現場の統制が事業目標と無関係なものになりかねません。測定の道具も階層ごとに違います。

用語	意味	使いどころ
バランスト・スコアカード	財務・顧客・社内業務プロセス・学習と成長の4つの視点で業績指標をまとめた枠組み	戦略を指標に落とす
重要成功要因（CSF）	ITプロセスを統制するために経営陣が達成すべき最も重要な課題または行動	目標達成の条件を絞る
KGI	事後に、ITプロセスが事業要件を達成したかを経営陣に伝える指標	結果の確認
KRI	先行して、リスクが現実になる兆しを示す指標	早めの警告

SAMPLE

用語	意味	使いどころ
ビジネスケース	投資に進むか判断する根拠となる文書。投資を経済的ライフサイクル全体で管理する道具にもなる	投資の判断

KGI は結果、KRI は兆しと対にして覚えます[3]。**エンタープライズアーキテクチャ（EA）**は、事業システムの基本設計と構成要素間の関係、それらが企業の目標をどう支えるかの記述です。価値は、ライフサイクル全体の便益から費用を引き、リスクで調整した値として見ます。

戦略計画は、企業の目標と、その変更、目標達成に要る資源の取得・使用を律する方針を決めるプロセスです。COSO ERM では、ERM・戦略・目標設定が戦略計画の中で一緒に働きます。リスク選好を戦略と整合させて決め、目標が戦略を実行に移すとともにリスク特定の土台になります[4]。取締役会は、提案された戦略とリスク選好、および戦略が使命・ビジョン・中核的価値と整合しているかを、経営陣と確認し、異議も述べる立場にあります。NIST SP 800-39 の第1層（組織の視点）では、組織全体のリスクを扱い、リスクフレーミングを実施して、第2層・第3層の活動の文脈を与えます[5]。CSF 2.0 の GV.OC は、サイバーリスクの意思決定を取り巻く状況（使命、利害関係者の期待、依存関係、法令・規制・契約上の要件）を理解することを、GOVERN の出発点とします[6]。

戦略が変わった時のリスクプロファイル

新規事業・合併・デジタル化は、事業の戦略を変えます。戦略が変わると、守る資産、頼る委託先、受ける規制が変わるので、リスクプロファイルの前提が古くなります。場面で考えます。小売企業がクラウド上の会員アプリで新規事業を始める決定をした場合、リスク実務者は、決定済みの戦略に反対することから始めません。新しい事業が加える資産・データ・委託先・規制を洗い出し、既存

SAMPLE

のリスク登録簿に照らして差分を評価し、リスクプロファイルを更新します。評価は、事業の目標への影響で語ります。「新しいアプリは個人情報を扱うため、漏えいが起きると会員獲得の目標そのものが損なわれます」のような形です。

リスク実務者が戦略に関わる時の役割

戦略を決めるのは取締役会と経営層で、リスク実務者ではありません。リスク実務者の役割は、助言とリスク情報の提供です。戦略の案に対して、そのリスクの大きさ、選好に収まるかどうか、必要な統制の費用を示します。決めるのは経営層で、リスク実務者は決めた内容に責任を負う立場ではありません。

場面です。経営会議で、リスクの高い提携案が提案されました。リスク実務者が「このリスクは受け入れられません」と案を差し止める行動は役割を超えます。正しい行動は、リスクの大きさと選好・許容度との距離を数字と根拠つきで提示し、選択肢（条件つきで進める・統制を足す・見送る）と各選択肢の残存リスクを示すことです。決定は経営層が行い、決定の記録を残します。決定の後は、記録した残存リスクの状況を、決定に沿って監視し続けます。

組織の構造・役割・責任 [1.1.2]

組織構造は、ガバナンスの仕組みの構成要素の一つで、企業とその構造・階層・依存関係を含みます[3]。リスクに関する役割は、次のように分担されます。

役割	内容
取締役会（統治機関）	リスク選好を決め、リスク管理を監督し、独立した内部監査を設置する
経営層（上級管理者）	方針と全体の指針を示す。日々の監視・統制は通常しない。資源配分を指示する権限を持ち、CEO を含む

SAMPLE

役割	内容
リスク委員会	経営陣レベルでリスク管理の方向付けと承認、報告の受け皿になる
CRO	企業の資産に対するリスクの評価と対応を任された役員
CIO	IT 擁護、IT と事業戦略の整合、IT サービス提供の計画・資源配分・運営に説明責任を負う最上級の役員
CISO	企業の情報セキュリティを担当する個人
IT ステアリングコミッティ	経営陣レベルの委員会。IT 戦略の実現を支え、IT サービス提供と IT プロジェクトの日常運営を監督し、実装面に注力する

NIST SP 800-39 は、組織全体の包括的なリスク管理の視点を与える個人またはグループを**リスクエグゼクティブ（機能）**と呼びます。上級幹部や業務責任者に共通のリスク管理の拠り所を与える役割です[5]。取締役会は「監督と承認」、経営層は「方向付け」、実務者は「実行と報告」です。この分担を崩す選択肢は誤りになりやすい。

RACI と説明責任

RACI チャートは、組織の枠組みの中で、誰が何の役を担うかを示す表です[3]。役は4つで、実行責任者（R: Responsible）、説明責任者（A: Accountable）、相談先（C: Consulted）、報告先（I: Informed）です。相談先は、事前に意見を求められる相手で、やり取りは双方向です。報告先は、進み具合を知らされるだけの相手で、やり取りは一方向です[3]。1つの活動に Accountable は1人だけです。説明責任が複数人にあると、誰も最終的に責任を取らない状態になります。Responsible は複数いてもかまいません。

SAMPLE

アカウンタビリティは、ある活動や出来事を責任者に結びつけて辿れることです。共有のアカウントでは操作した人を辿れないので、利用者ごとに別の識別子を割り当て、ログから実施者を特定できるようにします。**リスクオーナー**は、リスクに基づく判断を行う権限と説明責任を組織から与えられ、リスクが現実化した時の損失を負う人です。リスクオーナーは通常、事業部門の管理者で、IT 部門やリスク管理部門の担当者ではありません。**プロセスオーナー**はプロセスの開発・更新・遵守に責任を持つ人またはチームです。

NIST の枠組みでも同じ考え方です。サイバーリスク管理に関する役割・責任・権限は、確立し、周知し、理解させ、徹底します（CSF 2.0 GV.RR-02）。サイバーリスク戦略・役割・責任・方針に見合う十分な資源も割り当てます（GV.RR-03）[6]。NIST SP 800-37 では、システムの運用によるリスクを受け入れられるのは**認可責任者（AO）**だけです。AO は評価報告書と是正計画を見て、認可前にリスクを下げる必要があるか判断します[7]。

職務分掌（SoD）は、取引の開始・記録と資産の保管を別の人に割り当て、誤りや不正を防止・発見する基本的な内部統制です[3]。たとえば、支払の申請者と承認者、システム開発者と本番の変更承認者は別の人にします。小さな組織で人が足りない時は、分離の代わりに事後の監視やレビューを置かなければなりません。

リスク機能の独立性と報告の経路

リスク管理機能が IT 部門の下にあると、IT 部門の成果に不利な報告をしにくくなります。評価される側の部門の指揮下で、その部門のリスクを評価する形になるからです。報告の経路は、IT 部門の長ではなく、経営層やリスク委員会、取締役会に直接つなげる形が望ましくなります。3 ラインモデルでも、組織または規制当局は、CRO などの第2線の責任者に統治機関への直接の報告ラ

SAMPLE

インを持たせることを望みまたは求めうるとされます。これはモデルと矛盾しません[8]。

場面です。リスク管理担当が CIO の直属で、CIO が進める移行計画のリスクを高く評価したところ、CIO から報告書の表現を弱めるよう求められました。正しい対応は、評価の根拠を保ったまま、リスク委員会や CRO など独立した経路にも報告することです。表現を弱める、評価を取り下げる、黙って受け入れる選択肢は、独立性を損ないます。

事業部門の管理者・プロセスオーナー・データオーナー

リスクへの対応を決めて責任を負うのは、事業部門の管理者・プロセスオーナー・データオーナーです。データオーナーは組織内のデータの完全性、正確性、利用に責任を持つ者です。データカストディアンは、コンピュータ化されたデータの保管と保護に責任を持つ個人や部署です[3]。アクセスを許可する・分類を決めるのはデータオーナー、設定を実施するのはカストディアンと区別します。IT 部門がカストディアンであることは、リスクの責任が IT 部門に移ったことを意味しません。リスクオーナーは、事業を持つ側にとどまります。

組織の文化と倫理 [1.1.3]

文化は、行動、信念、前提、態度、物事の進め方のパターンです。**リスク文化**は、リスクを取ること、注意、誠実さへの姿勢を決める共有された価値観と信念で、リスクや損失がどれだけ率直に報告・議論されるかも決めます[3]。

文化は戦略と合っていなければ機能しません。表明されたリスク管理戦略が組織文化と合わなければ、戦略の実装は難しい、あるいは不可能になりやすいと NIST SP 800-39 は述べます。リスク許容度にも唯一の正解はなく、組織文化を反映し、損失の種類で変わり、上級幹部個人の主観にも強く左右され

SAMPLE

ます。文化の影響は、組織・業務プロセス・情報システムの全3層で感じられます[5]。

リスクを意識する文化の作り方

文化を作るのは経営層の姿勢と行動です。COSO ERM では、ガバナンスは組織の基調（トーン）を設定し ERM の監督責任を定めます。文化は倫理的価値観、望ましい行動、リスクの理解に関わります[4]。CSF 2.0 の GV.RR-01 は、組織の指導層がサイバーリスクに責任と説明責任を負い、リスクを意識し倫理的で継続的に改善する文化を育てることを求めます。GV.RR-04 は、サイバーセキュリティを人事の慣行（採用・教育・評価など）に含めることを求めます[6]。統治機関の役割にも、倫理的行動と説明責任を促す文化を育てることが含まれます[8]。

作り方の手は4つです。1つ目は、経営層が報告を歓迎する姿勢を行動で示すこと。2つ目は、役割と責任を周知すること。3つ目は、教育と認識向上を継続することです。セキュリティ意識とは、特定の主題を知り、心にとめ、理解して、それに従って行動することを指します。4つ目は、評価や報酬にリスクへの対応を含めることです。取締役会は、経営陣にリスクのプロセスだけでなく文化についても語らせることができ、文化がリスクの議論をどう後押しするかを確かめられます[4]。その場では、文化が責任あるリスクの取り方を後押ししているか妨げているか、経営陣がリスク文化をどう監視しているかも確かめます[4]。

倫理規程と違反への対応

倫理規程は、組織の価値観と、特定の状況で適用する規則を定めて、従業員個人と組織の行動に影響を与える文書です[3]。行動規範とも呼ばれます。違反の報告窓口を設けること、報告者を不利益から守ること、違反には一貫した対応を取ることが、規程を機能させます。例外が経営層に対してだけ許されると、規程は信頼されません。

SAMPLE

関連する用語を区別します。**相当の注意（due care）**は、同程度の能力を持つ合理的な人が同様の状況で払うと期待される注意の水準です。**デューデリジェンス**は、徹底的で客観的な調査・レビュー・分析を行うために、慎重で責任ある必要な行動を取ることです。**コンプライアンス**は、法令・規制が定める義務と、契約上の義務や社内方針による任意の要件を守り、守っていることを示せることです[3]。

ISACA の職業倫理規定

CRISC 保持者は、ISACA の職業倫理規定に従います。規定は7つの約束から成ります[9]。

1. 組織のガバナンスと管理に関する適切な標準・手順の実装と遵守を支援する。
2. 客観性、デューデリジェンス、専門職としての注意を持って、職業上の標準に沿って職務を行う。
3. 利害関係者のために、合法的に、高い行動基準と人格を保って行動し、専門職や協会の評判を損なわない。
4. 活動で得た情報のプライバシーと機密を守る。法的権限による開示が必要な場合を除く。個人的な利益のために使わない。
5. 専門分野の能力を保ち、必要な技能・知識・能力を合理的に期待できる活動だけを引き受ける。
6. 作業結果を適切な関係者に伝え、報告を歪めるおそれのある重要な事実はすべて開示する。
7. 利害関係者の教育を支援し、ガバナンスと管理への理解を高める。

場面で試されるのは、第4と第6の組合せです。顧客のデータで見つけた重大な欠陥を、個人的な利益のために使うことはできません。一方で、報告を歪め

SAMPLE

る事実の隠蔽もできません。経営層に結果を伝えるときは、不都合な事実を省かない、が基本です。

リスクを隠す文化の兆しと是正

兆しは5つあります。悪い知らせが上がらないこと。例外の承認が増えて常態化すること。リスクの指摘をした人が不利な扱いを受けること。指標が目標値に合わせて調整されること。報告が常に「問題なし」であることです。是正は、まず経営層の姿勢を変えることから始めます。報告者を保護し、リスクの報告を評価する仕組みを作り、例外の承認の件数と理由を定期的に取締役会やリスク委員会に報告します。是正の効果は、例外の承認の件数と理由、指標の定義の変更件数、報告者への不利益の有無の推移で確かめます。担当者への処分は、文化の問題を個人に押し付けるだけで、解決になりません。

場面です。四半期のリスク報告で、重要なシステムの指標が3期続けて「緑」でした。ところが現場の聞き取りで、赤になりそうな指標は報告の前に定義を変えて緑にしていたと分かりました。背景には、赤を報告した部署が経営会議で責められてきた経緯があります。正しい対応は、担当者の処分から入らず、指標の定義の変更履歴を調べ、元の定義で再計算した結果を経営層に報告することです。同時に、悪い知らせを報告した人を責めない方針を経営層から明示し、指標の定義を変える時の承認者と記録の手続も整えます。

文化がリスク対応とコントロールの受け入れに与える影響

リスク対応の選び方は文化に左右されます。リスクを取ることに積極的な組織は受容を選びやすく、慎重な組織は回避や軽減を選びやすい。統制の受け入れも同じで、自由度を重んじる組織に厳格な統制を押し付けると、迂回や形骸化が起きます。したがって、リスク実務者は統制を設計するときに、組織の文化に合う運用の形（承認の経路、教育の方法、監視の強さ）を選びます。文化に合わせるのは、統制の水準を下げるためではなく、実際に守られる形に

SAMPLE

するためです。水準が下がっていないかを測る物差しは、運用の形ではありません。変えた後も統制目標が満たされているかで確かめます。

ポリシーと標準 [1.1.4]

文書は階層になります。上位ほど変わりにくく、下位ほど具体的で変わりやすい。評価の尺度やスコア表などの細目は、段階の数も含めてポリシーに書かず、ポリシーから導く手順や標準に置きます。

文書	内容	拘束力
ポリシー	求められる行動と禁止される行動を伝える文書	必須
標準（standard）	ISO など認知された外部の標準化団体が承認した必須の要件・実施基準・仕様（組織内の標準も同じ位置で使う）	必須
手順（procedure）	標準に沿って特定の作業を行うための具体的な段階を詳しく記した文書	必須
ガイドライン	何かを達成する特定の方法の説明。手順より拘束力が弱い	推奨

ISACA の用語集は、標準を外部の標準化団体が承認したものとして定義します[3]。組織が内部で決める必須の技術要件を「標準」と呼ぶ運用も多いので、問題文の文脈から読み分けます。**セキュリティポリシー**は、企業の情報セキュリティに対する考え方と取組みの約束を示す上位の文書です。**許容される使用ポリシー（AUP）**は、ネットワークやインターネットを使う前に、利用者と企業の間で承認される利用範囲を定める取り決めです。**ベースライン**は、正式にレ

SAMPLE

ビューされ合意された仕様や成果物で、以後の開発の基礎になり、正式な変更管理の手続でしか変えられません。**規制（regulation）**は、当局が定め、行為を規制するために強制する規則や法律で、ポリシーとは別物です。

統制（control）は、リスクを管理する手段の総称です。方針・手順・ガイドライン・慣行・組織構造を含み、管理的・技術的・マネジメント上・法的な性質のものがあります。**統制目標**は、特定のプロセスで統制手続を実施して達成したい結果や目的を述べたもので、統制の手段そのものではありません。

NIST SP 800-53 によると、手順は、方針や統制をどう実施するかを示します。手順は個人や役割を対象に書け、システムのセキュリティ・プライバシー計画の中に置くことも別文書にすることもできます。方針も、全般的な方針の一部にしても、組織の複雑さを反映して複数に分けてもかまいません[10]。事業継続・復旧の計画づくりの最初の段階も、正式な方針を作ることです。方針が、有効な計画を作る権限と指針を与えます[11]。

リスク管理ポリシーの要素と承認者

リスク管理ポリシーには、目的、適用範囲、役割と責任、リスク選好（許容度）、リスク管理のプロセス、報告の頻度と経路、例外の扱いを入れます。選好（許容度）が欠けると、受け入れてよいリスクの線が無くなり、部門ごとに対応の判断がばらつきます。CSF 2.0 の GV.PO-01 は、サイバーリスクを管理する方針を、組織の状況・戦略・優先事項に基づいて作り、周知し、徹底させることを求めます[6]。承認するのは取締役会または経営層の最上位です。担当部門が自分で承認するポリシーは、組織全体を拘束する力を持ちません。場面です。部門ごとにバラバラに作られたリスクの基準を統一するには、経営層が承認した全社のポリシーを定め、部門の手順はそこから導きます。

SAMPLE

見直しと更新の契機

GV.PO-02 は、方針を、要件・脅威・技術・組織の使命の変化に合わせて、見直し、更新し、周知し、徹底させることを求めます[6]。契機は、規制の改正、事業の変化（新規事業・合併）、大きなインシデント、新しい技術の採用、リスク評価で見つかった乖離です。定期的な見直し（たとえば年1回）に加えて、契機が起きた時点でも見直します。

遵守の監視と逸脱の扱い

遵守は、監視（自己評価・指標・レビュー）と監査で確かめます。逸脱は、無視も、一律の拒否もしません。例外の申請を受け、リスクを評価し、権限のある者が期限と補完の統制つきで承認し、記録して期限に再評価します。恒久的な例外が増えたら、ポリシーの方が現実に合っていない印なので、ポリシー自体を見直します。

場面です。セキュリティポリシーが「パスワードは 12 文字以上」と定め、ガイドラインが「パスフレーズの利用を推奨」と書いています。ある部門が 10 文字のパスワードで運用したいと申し出ました。ポリシーは必須の要件なので、申し出は例外の申請として扱います。リスクを評価し、補完の統制（多要素認証など）を条件に、権限のある者が期限つきで承認します。ガイドラインは推奨なので、従わなくても違反にはなりません。承認を得ないまま 10 文字で運用を始めるのは逸脱です。

業務プロセスとレジリエンス [1.1.5]

業務プロセスのリスクは、プロセスの中身と、それが頼る資源（システム・人・施設・委託先）の依存関係から特定します。プロセスオーナーがプロセスの流れと依存関係を最もよく知っているので、聞き取りの相手を IT 部門だけにし

SAMPLE

てはなりません。IT のリスクを事業に結びつけるには、「どの業務プロセスがこのシステムに頼っているか」を先に押さえます。

BCP と DRP の違いと関係

事業継続（business continuity）は、中断を防ぎ、軽減し、そこから復旧することを指す言葉です。**BCP（事業継続計画）**は、重要な業務プロセスの中断に対応するために企業が使う計画で、重要システムの復旧は不測事態対応計画に依存します[3]。**DRP（災害復旧計画）**は、緊急事態や災害で中断した活動を、定めた時間と費用の範囲内で復旧するための人・物・技術・手続の資源の集合です。**不測事態対応計画（contingency plan）**は、特定のシステム障害や中断に対応するために企業または事業部門が使う計画です。

焦点が違います。NIST SP 800-34 によれば、BCP は中断中も後も使命・業務プロセスを維持することに焦点を置きます。DRP は情報システム中心で、主要設備を使えない大きな中断の後に、代替拠点などでシステムを復旧します[11]。BCP が事業全体、DRP がその中の IT の復旧です。DRP は BCP の一部として働きます。

比較	BCP	DRP
守る対象	使命・業務プロセス	情報システム
範囲	人・施設・手作業の代替を含む	技術の復旧が中心
例	代替の事務所で受注を手作業で続ける	代替拠点でサーバーを再構築する

BIA と RTO・RPO・MTD

BIA（事業影響度分析）は、情報資産の重要度と機微性を、資源を失う影響から評価するプロセスです。時間とともに損失が拡大する様子を示し、復旧に要

SAMPLE

る最小資源を特定し、復旧の優先順位を決めます[3]。NIST SP 800-34 は BIA を3つの段階で行うとします。(1)業務プロセスと復旧の重要度を決める、(2)資源要件を洗い出す、(3)システム資源の復旧優先順位を決める、の順です[11]。

復旧の時間の指標は4つあります。

指標	定義	決め方
MTD（最大許容停止時間）	業務プロセスやシステムが使えなくても、損害が組織にとって許容できなくなる前までに耐えられる最長期間	事業への影響から事業が決める
RTO（目標復旧時間）	災害後に業務機能や資源を復旧するために許される時間	MTD を超えない範囲で決める
RPO（目標復旧時点）	許容できるデータ損失から決まる、データを復旧してよい最も早い時点。許容されるデータ損失量を定量化する	失ってよいデータ量から決める
中断許容時間（interruption window）	障害点から最低限の重要なサービスを復旧するまで、企業が待てる時間	超えると累積の損失が過大になる

ISACA 用語集は、MTD と同じ趣旨の MTO（最大許容停止時間）も定義します[3]。**SDO（サービス提供目標）**は、通常状態に戻るまでの代替処理モードの間に、事業の必要から達成すべきサービス水準です。

大小関係は次のとおりです。RTO は MTD を超えないようにする値なので、通常は MTD より短くなります。復旧後にデータの再処理などの作業が加わる場合、その時間も足して MTD に収めます。RPO は、RTO と違い、MTD には含ま

SAMPLE

れません。復旧の過程で、その業務がどれだけのデータ損失に耐えられるかで決まります[11]。

計算で確かめます。MTD が 8 時間の受注システムで、再構築による復旧に 6 時間かかり、復旧後に滞留した受注の再処理に 2 時間かかるとします。6 + 2 = 8 時間で、MTD ちょうどです。余裕がありません。RTO を 6 時間と定めると、再処理を含めて MTD を使い切ります。再処理を含めた合計が MTD に収まるよう、RTO は 6 時間より短くするか、再処理を速める手段を足します。RPO は別の軸です。バックアップが 4 時間おきなら、最悪 4 時間分のデータが失われるので、RPO を 1 時間と定めた業務には足りません。RPO を縮めるには、バックアップの間隔を短くするか、複製（レプリケーション）を使います。

決めるのは事業です。RTO と RPO を IT 部門が技術の都合で決めるのは誤りです。事業側（プロセスオーナー）が BIA に基づく許容を示し、IT 部門はそれを満たす復旧の方法を選びます。IT 部門が示せるのは、要求を満たすための費用と、満たせない場合の差だけで、要求そのものを決める権限はありません。

場面です。受注システムの MTD は 24 時間、RTO は 8 時間、RPO は 1 時間と BIA で決まりました。現在のバックアップは 1 日 1 回で、復旧先は電源と空間だけを備えた施設です。この構成は2点で要件を満たしません。バックアップが 1 日 1 回では、最悪 24 時間分のデータを失うので、RPO の 1 時間に届きません。コールドサイトは機器の調達と構築から始めるため、8 時間以内の復旧は難しくなります。対応は、バックアップの間隔を 1 時間以内にするか複製を使うこと、復旧先をウォームサイトかホットサイトへ上げることです。ミラーサイトまでは要りません。MTD が 24 時間の業務に、ほぼ 100% の可用性までは求められていないからです。

SAMPLE

代替拠点

NIST SP 800-34 は、代替拠点の主な型をコールドサイト・ウォームサイト・ホットサイトの3つとし、変形の例としてミラーサイトとモバイルサイトを挙げます。型ごとに、費用と立ち上がりの時間が違います[11]。

種類	内容	費用
コールドサイト	電力・通信・環境制御などの基盤と十分な空間だけを備えた施設で、システム復旧作業を支える	維持費が最も安い。機器の調達と設置に長い時間がかかりうる
ウォームサイト	システムのハードウェア・ソフトウェア・通信・電源の一部または全部を備えた、一部設備つきの事務スペース	中間
ホットサイト	システム要件に見合う規模で、必要なハードウェア・支援基盤・支援要員まで構成済みの施設	高い
ミラーサイト	自動のリアルタイム複製を行う完全冗長な施設で、主拠点と技術的に同一。ほぼ 100% の可用性を確保する	最も高い

選び方は、RTO と RPO から逆算します。RTO が数日のシステムにミラーサイトを置くのは過剰で、RTO が数分のシステムにコールドサイトを選ぶと要求を満たせません。

計画づくりの7段階とレジリエンス

不測事態対応計画は、方針策定、BIA、予防統制の特定、不測事態対応戦略の作成、システム計画の策定、試験・訓練・演習、計画の維持、の7段階で進めま

SAMPLE

す[11]。計画は作って終わりにせず、試験と訓練で実際に動くか確かめ、事業やシステムが変わるたびに維持します。

レジリエンスは、システムやネットワークが障害に耐え、または中断から素早く回復し、通常は目立った影響を最小にする能力です[3]。リスク管理との関係は、許容できる中断の程度（MTD・RTO・RPO）を決め、重要な業務を特定し、その範囲で耐えられるように設計することです。リスクを下げる予防の統制だけでなく、起きた後に立て直す力も含めて評価します。

組織の資産管理 [1.1.6]

資産は、保護する価値のある有形・無形の価値あるもので、人・情報・インフラ・資金・評判を含みます。**資産台帳**は、関連する資産をすべて記録する台帳です[3]。CSF 2.0 の ID.AM は、データ、ハードウェア、ソフトウェア、システム、施設、サービス、人などの資産を識別することを求めます。管理は、組織目標への相対的な重要度とリスク戦略に沿って行います[6]。

台帳と最新の保ち方

台帳は、作るより最新に保つほうが難しい。**構成品目（CI）**は、構成管理の下にある（または置く予定の）インフラの構成要素や変更要求などの項目です。**構成管理**は、システムのライフサイクルを通じて、構成品目の集合に対する変更を管理することです[3]。変更管理と台帳を連動させ、購入・変更・廃棄のたびに台帳を更新します。

NIST SP 800-53 の CM-8 では、システム構成要素とは、ハードウェア・ソフトウェア・ファームウェアを含む識別可能な IT 資産です。台帳は、システムを正確に映し、全構成要素を含み、重複計上しません。台帳には、その構成要素の管理に責任と説明責任を持つ個人（氏名・職位・役割）の情報を含められます

SAMPLE

[10]。CSF 2.0 の ID.AM-07 はデータとそのメタデータの台帳、ID.AM-08 はライフサイクル全体にわたる管理を求めます[6]。

資産のオーナーと価値の評価

資産には、オーナーを割り当てます。データならデータオーナーです。データオーナーは、組織内のデータの完全性、正確性、利用に責任を持ち、データカストディアンは保管と保護を担います[3]。オーナーのいない資産は、誰もリスクを引き受けないので、評価も対応も止まります。台帳にオーナーを入れることは、リスクオーナーを決める第一歩です。

価値の評価では、2つの用語を分けます。**重要度（criticality）**は、ある資産や機能の企業にとっての重要性と、それが使えなくなった時の影響です。**機微性（sensitivity）**は、情報が不適切に開示された時に企業に与える影響の大きさの尺度です[3]。重要度は「止まったらどうなるか」、機微性は「漏れたらどうなるか」です。優先順位は、止まった時の影響（重要度）と漏れた時の影響（機微性）を別々に評価し、分類や使命への影響と合わせて決めます[6]。受注システムは重要度が高く、機微性が低い場合があり、社員の評価資料は機微性が高く、重要度が低い場合があります。

資産の分類とリスク評価への使い方

データ分類は、データに機微性の水準を割り当て、水準ごとの統制を定めることです。分類水準は、データの企業にとっての価値や重要性を示します[3]。CSF 2.0 の ID.AM-05 は、資産を、分類、重要度、資源、使命への影響に基づいて優先順位づけることを求めます[6]。

分類は、リスク評価の入力です。資産の分類が高いほど、損失の大きさの見積もりが大きくなり、優先順位が上がり、必要な統制の水準も上がります。分類が付いていない資産は、評価の対象から漏れやすい。分類が無いと、損失の大

SAMPLE

きさの見積もりも、優先順位も、統制の水準も決められません。場面です。全社で同じ強さの統制を一律にかけていて、費用が膨らんでいる場合、分類に応じて統制を段階づけると、重要な資産に厚く、そうでない資産に薄く配分できます。分類を始める時は、まず分類の水準と水準ごとの統制を決め、主要な資産から分類を付けます[3]。

管理されていない資産のリスク

台帳に載っていない資産は、評価も、パッチも、監視も受けません。代表は、部門が独自に契約したクラウドサービスや、承認なしに導入した端末とアプリ（シャドー IT）です。台帳にないということは、リスク登録簿にもなく、残存リスクが誰にも見えない状態を意味します。見つけるには、ネットワークの検出、費用の支払記録、クラウドの利用状況の確認を使い、見つけた資産を台帳へ入れてオーナーを決めます。禁止して終わりにする対応では、隠れた利用が減りません。利用の目的を聞き、承認の経路を用意して、台帳の中に取り込みます。

エンタープライズリスクマネジメント（ERM） [1.2.1]

ERM は、あらゆる業種の企業が、あらゆる源泉のリスクを評価・統制・活用・資金手当て・監視し、利害関係者にとっての短期・長期の価値を高める営みです。**リスクマネジメント**は、リスクについて企業を指揮し統制するための、調整された活動です[3]。**リスクユニバース**は、組織の機能を損なうおそれのある、あらゆる階層のあらゆるリスクを含む全体です。

ERM は部門ではありません。COSO は、ERM を機能や部署ではなく、戦略設定と一体にして実行時に適用する文化・能力・実践と説明します[4]。NIST IR 8286r1 は、ERM でリスクを縦割りで個別に扱わないと述べます。相互に関連するポートフォリオとして合わせた影響を理解し、組織全体で重大なリスクに取り組む方法です[12]。

SAMPLE

IT リスクを ERM に統合する

ERM のガバナンスが、IT のリスク管理などの各分野の戦略と方法を指示します。各分野はリスク登録簿に記録し、それを集約・正規化・分析して企業リスクプロファイルを作ります[12]。CSF 2.0 の GV.RM-03 も、サイバーセキュリティのリスク管理の活動と成果を、企業のリスク管理プロセスに含めることを求めます[6]。統合の効果は、共通の言葉（リスクの定義・用語）と共通の尺度（影響・可能性の段階）で、IT のリスクを他の事業リスクと並べて比べられることです。共通のリスクの分類を定め、各分野の登録簿を同じ分類で記録すると、種類ごとに全社で集約できます。ERM のプログラムは、下位の階層から集まるリスク情報の用語・書式・基準などの指針を定め、各分野はその指針に沿って登録簿に記録します。他のリスクと揃った形のサイバーセキュリティの報告は、リスク選好とリスク許容度の判断と表明を支えます。使命や事業目標に対する不確実性の影響は企業のリスクで、IT のリスクも同じ形で管理します[12]。IT 部門だけが独自の尺度で「高」と評価しても、全社の優先順位づけには使えません。

IT リスクを事業のリスクとして表す

IT リスクは、技術の言葉ではなく事業への影響で語ります。「脆弱性が 12 件ある」は技術の言葉で、「受注システムの停止が 8 時間を超えると売上の損失が許容度を超える」が事業の言葉です。経営層が判断できる形に直すのは、リスク実務者の仕事です。

ERM の枠組み

COSO ERM（2017）は、相互に関連する5つの構成要素から成ります。20 の原則が、これらの構成要素に割り当てられています[4]。

SAMPLE

構成要素	内容
ガバナンスと文化	組織の基調を設定し、ERM の監督責任を定める。文化は倫理的価値観、望ましい行動、リスクの理解に関わる
戦略と目標設定	ERM・戦略・目標設定は戦略計画の中で一緒に働く。リスク選好を戦略と整合させる
パフォーマンス	戦略・目標に影響しうるリスクを特定・評価し、重大度をリスク選好に照らして優先順位づけ、リスク対応を選び、引き受けたリスク量をポートフォリオとして見る
レビューと修正	企業の業績を見直すことで、ERM の構成要素が時間とともに、また大きな変化の中でどれだけ機能しているかを考え、必要な修正を判断する
情報・コミュニケーション・報告	内外の必要な情報を継続して得て共有する。情報は組織の上・下・横に流れる

ISO 31000:2018 は、原則・枠組み・プロセスで構成されます。プロセスは6つの要素から成ります。コミュニケーションと協議、適用範囲・状況・基準の設定、リスクアセスメント（特定・分析・評価）、リスク対応、モニタリングとレビュー、記録と報告です[13]。ISO/IEC 27005 は、情報セキュリティのリスク管理に絞った指針です[14]。

リスク管理のプロセスの一巡

どの枠組みも、核は同じ一巡で、特定、評価、対応、監視、報告が回り続けます。ISACA 用語集は、リスクの対応を、回避・軽減・移転・受容の4つに分けます。**リスク回避**は、リスクを体系的に避けるプロセスです。**リスク軽減**は、対策と統制を使ってリスクを管理することで、リスクを消す手段ではありません。**リスク**

SAMPLE

移転は、リスクを別の企業に割り当てるプロセスで、通常は保険の購入や業務の外部委託によります。**リスク受容**は、上級管理者が定めたリスク選好と許容度に従い、企業がリスクを引き受け損失を吸収できる場合に行う判断です[3]。

NIST SP 800-39 は、対応の選び方の条件を示します。リスク回避は、特定したリスクが組織のリスク許容度を超える時に適切な対応となりうるもので、許容できないリスクを生む活動や技術の利用を取りやめるなどの行動を取ります。リスク軽減（低減）は、受容も回避も共有・移転もできない部分のリスクに対する適切な対応です。リスク受容は、特定したリスクが組織のリスク許容度の範囲内にある時の適切な対応で、場合に応じて低・中・高のリスクを受容しうるとされます[5]。ここで大事なのは、受容の可否は「リスクの大きさ」ではなく「許容度に収まるか」で決まる点です。高いリスクでも許容度に収まれば受容できます。低いリスクでも許容度を超えるなら受容できません。

防衛線（ラインズ・オブ・ディフェンス） [1.2.2]

3ラインモデルの役割

IIA の3ラインモデル（2020）は、目標達成を助け、強いガバナンスとリスク管理を促す体制と手続を、組織が見極めるのを助けます[8]。6つの原則から成り、役割は次のとおりです。

役割	内容
統治機関	責任を委任して経営陣に資源を与え、法令・規制・倫理の期待が満たされることを確保し、リスク選好を決め、リスク管理を監督し、独立した内部監査を設置・監督する

SAMPLE

役割	内容
第1線	目標達成のための行動（リスク管理を含む）と資源の運用を主導し、統治機関に計画・実績・見込みとリスクを報告し、法令・規制・倫理の遵守を確保する
第2線	リスク管理に関する補完的な専門知識、支援、監視、牽制を提供し、リスク管理（統制を含む）の十分性と有効性の分析・報告を行う
第3線（内部監査）	ガバナンスとリスク管理の妥当性・有効性について独立・客観的な保証と助言を提供し、結果を経営陣と統治機関に報告して継続的な改善を促す
外部の保証提供者	法令・規制上の期待を満たす保証と、内部の保証を補う保証を追加で提供する

「線」は組織構造ではなく役割の区別で、番号は順番を意味しません。すべての役割が同時に働きます。また、モデルは防御だけでなく、リスク管理が目標達成と価値創出に果たす貢献にも注目すると最も効果的になります[8]。

第2線と第1線の責任の分け方

第1線の役割は、顧客への製品・サービス提供に最も直結する役割（支援機能を含む）です。第2線はリスク管理を支援する役割です。リスクを管理する責任は、第2線をリスクの専門家に任せても、第1線の役割と経営陣の範囲に残ります。第2線の役割は、牽制や支援を行っても経営陣の判断・行動と一体で、経営陣の報告ラインにかかわらず経営陣から完全に独立することはありません[8]。

場面です。リスク管理部門（第2線）が、事業部門のシステムのリスク対応を「代わりに」決めて実施している場合、第1線が自分のリスクを管理する責任を失

SAMPLE

います。正しい形は、第1線のリスクオーナーがリスクを特定し対応を決め、第2線が方法論・助言・監視・報告で支えることです。第2線の責任者（CRO など）が統治機関に直接報告する経路を持つことは、モデルと矛盾しません。

内部監査（第3線）の独立性

内部監査の独立性は、統治機関への説明責任、必要な人・資源・データへの制約のないアクセス、監査の計画と実施での偏りや干渉からの自由によって確立されます。内部監査は統治機関に対して主たる説明責任を持ち、経営陣の責任から独立しています。経営陣から独立しているので、内部監査の保証は、第 1 線と第 2 線が統治機関に示せる保証を超える客観性と確信を持ちます。独立性と客観性への障害があれば、内部監査はそれを統治機関に報告し、必要な保護策を取ります[8]。監査責任者（CAE）の主たる報告先は統治機関です[8]。

リスク実務者との関係は、役割が違うことを理解した協力です。独立性は隔離を意味しません。内部監査の仕事を組織の戦略と業務の必要に合わせるため、内部監査と経営陣の間には定期的な対話が要ります[8]。内部監査は、リスク実務者が運用した統制を独立の立場で評価するので、リスク実務者が内部監査の判断を左右してはいけません。一方、監査の指摘をリスク登録簿に反映しない運用は認められません。監査が見つけた欠陥は、リスク評価の新しい入力になります。場面です。内部監査部門の長が、リスク管理部門の長を兼ねている場合は、自分の運用を自分で評価する形になり、独立性が損なわれます。内部監査は、経営陣の責任に当たる決定や行動（リスク管理を含む）を引き受けず、現在または最近責任を持った活動への保証を控えることで独立性を守ります。内部監査部門の長がそうした責任を引き受けた活動について、統治機関が独立した保証を求める時は、資格のある第三者が保証を提供します[8]。

SAMPLE

線の間の連携と重複・抜けの防止

すべての役割は、互いに、また利害関係者の優先する利益に沿っている時に、価値の創出と保護に貢献します。整合は、コミュニケーション、協力、協働で達成します[8]。重複を防ぐには、リスクの用語と評価の尺度を共通にし、リスク登録簿・監査の指摘・コンプライアンスの結果を共有します。抜けを防ぐには、各線の担当範囲を図にして、どの統制を誰が運用し、誰が監視し、誰が保証するかを RACI で明らかにします。複数の線が同じ統制を別々に何度も検査し、事業部門が疲弊する状態が重複の典型です。誰も評価していない領域が残る状態が抜けです。

リスクプロファイル [1.2.3]

定義と内容

リスクプロファイルは、特定したリスクの完全な一覧ではなく、リスク評価で特定・評価された最も重大なリスクを優先順位づけた一覧です（OMB A-123 の定義）[15]。組織が抱えるリスクの全体像です。企業レベルの意思決定者は、これを使って、どの企業リスクに対処するか、資源をどう割り当てるか、どのリスクオーナーに責任を委ねるかを決めます[12]。

用語	定義
リスクシナリオ	リスクを具体的に評価できる形にした表現
リスク登録簿（ISACA）	特定され、分析され、優先順位づけされたリスクシナリオの一覧
リスク分析	IT のリスクシナリオの頻度と大きさを見積もるプロセス
リスク評価（risk assessment）	リスクとその潜在的影響を特定し評価するプロセス

SAMPLE

用語	定義
リスク要因	IT に関連するリスクシナリオの頻度・大きさ・最終的な事業影響に影響を与える条件
固有リスク	経営陣が取った（または取りうる）対策、たとえば統制の実装を考慮しない水準のリスク
残存リスク	経営陣がリスク対応を実施した後に残るリスク
リスク指標	企業がリスクを現実のものとしうることを示せる指標
KRI	リスク指標のうち、重要なリスクを予測または示す確率が高い、関連性の高い部分集合

これらの定義は ISACA 用語集のものです[3]。NIST SP 800-30 は、リスクを、主体が潜在的な状況や事象で脅かされる程度の尺度と定義します。通常は、(1) それが起きた時の悪影響と(2)発生の可能性の関数です[16]。OMB A-11 によるリスク登録簿は、時間とともに把握したリスクのデータを含む、リスク情報の保管庫です[12]。リスク登録簿は個別のリスクを記録する台帳で、リスクプロファイルは重大なものを選んだ全体像です。この違いは問われやすい。

CSF 2.0 の組織プロファイルは別の語です。現在の成果を示す現状プロファイルと、望む成果を選んで優先順位づけた目標プロファイルのいずれか、または両方を含みます[6]。リスク管理のプロファイルと、CSF の成果のプロファイルを取り違えないようにします。

リスクの大きさの計算

リスクエクスポージャーは、リスクが起きた場合の総損失に、そのリスクが起きる確率を掛けて求めます。損失は従来の BIA で算出します[12]。たとえば、総

SAMPLE

損失 1,200 万円、年間の発生確率 25% のリスクのエクスポージャーは、12,000,000 × 0.25 = 3,000,000 円です。

同じ考え方の古典の式が ALE です。1 回の損失額（SLE）は、資産 4,000,000 円の 30% を失う事象なら、4,000,000 × 0.3 = 1,200,000 円です。年間の発生頻度（ARO）が 0.5 なら、ALE（年間予想損失額）は 1,200,000 × 0.5 = 600,000 円であって、1 回の損失額ではありません。統制が発生確率を 60% 下げるなら、残存リスクは 3,000,000 × (1 − 0.6) = 1,200,000 円で、固有リスクの 40% です。統制の費用が年 500,000 円で、下がる期待損失が年 1,800,000 円なら、費用対効果は見合うので、導入を見送る理由はありません。計算式は定量的な見積もりの道具で、数字が出ない場合は定性的な段階づけ（高・中・低）を使います。

IT のリスク登録簿を全社のリスクプロファイルに組み込む

各分野のリスク登録簿を相関させ、集約し、正規化して重要なリスクを選び、企業リスクプロファイルにまとめます[12]。IT のリスク登録簿の尺度が全社の尺度とずれていると、集約できません。たとえば IT 部門が影響を 5 段階、事業部門が 3 段階で付けていると、そのまま並べても比べられません。尺度の変換か統一が先に必要です。

更新の契機と集約

プロファイルは、事業の変化（新規事業・合併）、新しい脅威、インシデント、規制の改正、リスク対応の完了、KRI の閾値の超過で更新します。年次の定期更新だけでは足りません。

集約では、個別のリスクを全体で見ます。個々のリスクは許容度内でも、同じ原因を共有する複数のリスクが同時に起きると、合計が許容度を超えることがあります。クラウドの1つのサービスに複数の業務が依存している場合が典

SAMPLE

型で、これを相関と集中のリスクと呼びます。相関のあるリスクを個別に低と評価して合算を見落とすのは、よくある誤りで、避けなければなりません。

場面です。主要なクラウドの委託先でインシデントが起き、自社のデータへの影響の有無が確認中です。これはリスクプロファイルの更新の契機で、確認の完了を待つ理由はありません。リスク実務者は、まず台帳から、その委託先に依存する業務と資産を洗い出し、影響の範囲を評価します。次に、該当するリスクシナリオを登録簿で更新し、同じ委託先に依存する複数の業務のリスクを合算して、企業のリスクプロファイルでの順位と許容度との距離を見直します。結果はリスクオーナーとリスク委員会に報告しなければなりません。原因調査の完了を待ってから登録簿を更新する対応は、遅すぎます。

リスク選好とリスク許容度 [1.2.4]

3つの定義の違い

用語	定義	性格
リスク選好（risk appetite）	使命を追求する上で、事業体が広いレベルで受け入れる意思のあるリスクの量	広い・方針の水準
リスク許容度（risk tolerance）	企業が目標を追う中で、経営陣が特定のリスクについて許容する変動の許容水準	狭い・具体的
リスクキャパシティ	企業が存続を危うくせずに耐えられる損失の客観的な大きさ	上限・客観

キャパシティは、組織が存続を危うくせずに耐えられる損失の客観的な大きさで、一番外側の上限です[3]。選好はその内側に経営が広いレベルで決める意

SAMPLE

思、許容度は個別のリスクについて認める変動の水準で、選好より狭く具体的な線です。選好をキャパシティの外に置くと、存続を危うくします。

NIST IR 8286r1 の例で見ます。選好の例は「メールは24時間の大部分で使えること」、それに対応する許容度は「営業時間帯に5分を超えて中断しないこと」です。許容度のほうが狭く具体的です[12]。リスク許容度は、リスクへの対応後に残るリスクを負う組織・利害関係者の備えで、法令や規制の要件に左右されえます。許容度は企業レベルで定義されることが多いものの、プログラム・目標・構成要素のレベルで定めることもでき、実際は担当部門が解釈して適用します[12]。

NIST SP 800-39 は、リスク許容度を、組織が受け入れるリスクの水準または不確実さの程度で、組織のリスクフレームの重要要素と述べます。リスク管理の判断に直接の影響と制約を与えます。決まる時点は、リスクフレーミングの構成要素の中で、リスク管理戦略の中で定義されます[5]。

選好を決めるのは誰か

リスク選好は企業の最上級の指導層が定め、戦略の設定や目標の選択などの判断の指針になります[12]。統治機関は通常、ビジョン、使命、価値観、組織のリスク選好を定めて組織の方向を決め、責任を経営陣に委任します[8]。リスク実務者は決める人ではなく、支援する人です。経営層が議論できるように、現状のリスクの水準、同業の状況、選好案の影響、過去の損失の実績を材料として示します。CRISC の補助タスクにも、主要な利害関係者によるリスク選好と許容度の閾値の選択を支援することが含まれます[17]。

場面です。リスク実務者が、自分の判断で選好を「低」と定め、それに従って全社の統制を厳しくした場合、役割の逸脱で、認められません。選好の設定は取締役会・経営層の権限なので、案を作って提案し、承認を得て記録しなければなりません。

SAMPLE

許容度の閾値を指標に落とす

許容度は、測れる指標にして初めて運用できます。上のメールの例なら、「営業時間帯の中断時間」が指標です。KRI は、許容度に近づいていることを早めに知らせる指標なので、閾値を二段にします。たとえば、パッチ適用が期限を過ぎている重要システムの割合を KRI とし、許容度が 10% だとします。120 台のうち 18 台が期限超過なら、18 ÷ 120 = 15% で許容度を超えており、放置できません。警告の閾値を 7%、許容度を 10% に置くと、7% を超えた時点で早めに動けます。受容と記録したリスクも、許容度の範囲内に収まっているかを KRI などで測り続け、選好の範囲内で運営できていることを確かめます[12]。

超えた時の対応も先に決めておきます。閾値を超えた時の連絡先（リスクオーナー、リスク委員会）、期限、選択肢（統制を足す、受容を経営層に求める、事業を見直す）を、ポリシーに書いておきます。超えたリスクを黙って受容することはできません。受容は、上級管理者が定めた選好と許容度に従って行う判断です[3]。NIST SP 800-39 でも、リスク受容は、特定したリスクが許容度の範囲内にある時の適切な対応です[5]。

リスク登録簿には、残存リスクを記録します。リスク選好と許容度に基づく望ましい状態としての目標残存リスクも記録しうるので、現在の残存リスクと目標のずれが、追加の対応の要否を決める材料になります[12]。選好を変えたら、その変更を管理者へ伝え直し、許容度の閾値、KRI の閾値、目標残存リスクを新しい選好に合わせて見直します[12]。CSF 2.0 の GV.RM-02 は、リスク選好とリスク許容度の記述を確立し、周知し、維持することを求めます[6]。

選好の見直し

事業の目標が変わると、選好も変わります。新規事業を攻めの姿勢で始める時期は選好を広げ、財務が悪化した時期は狭めます。見直しは定期的に、また

SAMPLE

大きな変化（合併・戦略の転換・重大なインシデント）のたびに行います。選好が古いまま、事業は変わっている状態は、許容度の閾値と事業の実態のずれを生むことになりかねません。戦略案が今の選好を超える時は、リスク実務者は案を自分で書き換えず、ずれを根拠とともに示して、選好の見直しを経営層と取締役会に提起します。COSO も、取締役会のリスク監督の役割に、提案された戦略とリスク選好を経営陣と共に検討し、異議を述べ、同意することを挙げます[4]。

場面です。受注システムの停止の許容度は「営業時間帯に累計 5 分」です。今月は2分の障害が3回あり、合計 6 分で許容度を超えました。リスクオーナーは、選好の範囲内だからと黙って受容できません。許容度の超過をリスク委員会に報告し、3つの道から選びます。1つ目は、統制を足して再発を減らすこと。2つ目は、期限と理由をつけて、超過の受容を経営層に承認してもらうこと。3つ目は、事業の変化に合わせて許容度そのものを見直すことです。

リスクフレームワーク、法律、規制、契約上の要件 [1.2.5]

主な枠組み

枠組み	位置づけ
ISACA Risk IT Framework 第 2 版（2020）	IT リスクに特化した ISACA の枠組み。COBIT を補完する。リスクのガバナンス、リスクマネジメント、リスク評価、リスクの認識・報告・伝達、リスク対応を含む
COBIT 2019	IT のガバナンスとマネジメントの枠組み。40 の目的を5つの領域に分ける。EDM（評価・指示・監視）が統治、APO・BAI・DSS・MEA がマネジメント
NIST SP 800-37 RMF	システムの認可までの 7 段階のリスク管理の枠組み

SAMPLE

枠組み	位置づけ
NIST SP 800-30	リスク評価の手引き
ISO/IEC 27005	情報セキュリティのリスク管理の指針
COSO ERM、ISO 31000	組織全体の ERM の枠組み

Risk IT は、COBIT が扱う統制の細部を持たず、COBIT と組み合わせて使う位置づけです[18][19]。COBIT 2019 では、EDM 領域は統治機関が戦略の選択肢を評価し、経営陣に指示し、戦略の達成を監視する領域です[20]。

NIST の枠組みは、役割が違います。SP 800-39 は、リスク管理を組織全体の活動として、戦略レベルから戦術レベルまでリスクを扱い、リスクに基づく意思決定をあらゆる面に組み込むとします。第1層は組織、第2層は使命・業務プロセス、第3層は情報システムの視点です。第2層は第1層の文脈・判断・活動を踏まえ、第3層は第1層・第2層に導かれます[5]。**リスクフレーミング**は、組織のリスク管理の進め方を形づくる前提、制約、リスク許容度、優先順位・トレードオフの集合です。ガバナンス構造・財務・法規制・文化などの影響を受けます。

SP 800-30 のリスク管理は、フレーミング、評価、対応、継続的な監視の4つから成り、効果的な組織内の連絡とフィードバックによる継続的改善で進めます。リスク評価プロセス自体は、評価の準備、評価の実施、結果の伝達、評価の維持の4段階です。評価は3つの層のどこでも実施でき、層を限りません。手法は定量的・定性的・半定量的で、組織の文化、特に不確実さとリスクの伝達に対する姿勢に基づいて選べます[16]。SP 800-37 の RMF は、準備（Prepare）と6つの主要段階（分類、選択、実装、評価、認可、監視）の計7段階で、すべてが成功に不可欠です[7]。

SAMPLE

CSF 2.0 のコアは、GOVERN、IDENTIFY、PROTECT、DETECT、RESPOND、RECOVER の6機能です。GOVERN は、サイバーリスク管理の戦略・期待・方針が確立され、周知され、監視されることで、他の5機能の成果を決める文脈を与えます。ティアは、リスク管理の実践を、部分的（Tier 1）、リスク情報に基づく（Tier 2）、反復可能（Tier 3）、適応的（Tier 4）の4段階で表します[6]。NIST SP 800-39 の「層（Tier）」と CSF の「ティア」は別物です。前者は組織・業務・システムの視点、後者は実践の成熟度です。

フレームワークは、複雑な問題に取り組むための基本的な概念構造で、ガバナンスのイネーブラーの一つです[3]。

枠組みの選び方

枠組みは手段です。組織は、事業の特性、規制、すでにある枠組みの採用状況、成熟度を見て選び、組織に合わせて調整します。CSF は、規模や業種を問わず、どの組織も調整して使えるように作られています[6]。複数を組み合わせるのが普通で、たとえば ERM は COSO ERM、IT のガバナンスは COBIT、システムの評価は NIST という組合せがあります。枠組みを導入すること自体が目的になり、事業の目標と切り離されている状態は、誤りの典型で、避けなければなりません。場面です。経営層が「業界の標準だから」と別の枠組みへの全面移行を決めた場合、リスク実務者は、移行が事業の目標とリスク管理に何をもたらすかを示します。さらに、既存の評価結果を新しい枠組みの用語へ対応づける計画を、移行前に立てなければなりません。

求めることごとに、使う枠組みの目安は次のとおりです。

求めること	枠組み
組織全体のリスクを戦略と一体で扱う	COSO ERM、ISO 31000

SAMPLE

求めること	枠組み
IT のガバナンスとマネジメントの統制を整える	COBIT 2019
IT リスクのガバナンスと評価・対応を体系化する	Risk IT
情報システムのリスク評価の手順を決める	NIST SP 800-30
システムの分類・選択・認可を段階で進める	NIST SP 800-37 RMF
サイバーセキュリティの成果を整理し、現状と目標を比べる	NIST CSF 2.0
情報セキュリティのリスク管理の指針を得る	ISO/IEC 27005

法令・規制・契約上の要件

法令・規制・契約上の要件は、リスクフレームの制約です。NIST SP 800-39 は、リスクフレーミングの入力に、法律・方針・指令・規制・契約関係・財務上の制限が含まれ、リスク対応などの選択肢に制約を課すとします[5]。CSF 2.0 の GV.OC-03 は、サイバーセキュリティに関する法令・規制・契約上の要件を理解し、管理することを求めます。要件にはプライバシーと市民的自由の義務を含みます[6]。

要件の特定は、事業の所在地・扱うデータ・顧客・業界から、適用されるものを洗い出す作業です。洗い出す対象は3種類です。法令（個人情報の保護に関する法令、財務報告の内部統制に関する法令）、業界の基準（クレジットカード業界の PCI DSS など）、契約の条項です。特定した要件は統制に結びつけ、遵守の状況を確かめなければなりません。コンプライアンスのリスクは、違反した時の罰金・処分・訴訟・信用の低下です。ISACA 用語集は、コンプライアンスのリスクを、企業が適用される法令・規制・倫理基準・行動規範を守れない確率

SAMPLE

とその結果と定義します[3]。法令の要件は選好や許容度で割り引けません。法令を守るかどうかは、リスク受容の対象ではなく、守る前提です。

規制は変わるので、規制の変化の監視は、法務・コンプライアンス部門と連携し、改正の予定を把握して、影響を評価します。影響する統制、データ、プロセスを洗い出し、期限までの対応計画を立て、リスク登録簿に反映します。同時に複数の改正に対応しきれない時は、違反した時の影響と施行までの期間でリスクの大きさを比べて順番を決め、計画を経営層に承認してもらいます。期限に間に合わない見込みが分かったら、施行の直前まで報告を先送りしません。その時点で影響と合わせて経営層に報告し、施行までの当面の対策と是正の期限を含む計画の承認を求めます。

契約上の要件には、顧客との契約、SLA、委託先の契約の条項があります。**SLA** は、サービス提供者と利用者の間で、サービスの最低限の性能目標とその測定方法を定める合意で、文書化が望ましいものです[3]。SLA には、性能の目標と測り方に加えて、目標に届かなかった時の対応も定めます[10]。顧客との契約でセキュリティ対策や復旧時間を約束していれば、約束を守れないことが契約違反のリスクになります。委託先のサイバーリスクは、要件を定め、優先順位をつけ、供給者や関係する第三者との契約等の合意に組み込みます（CSF 2.0 GV.SC-05）[6]。委託先に任せても、リスクの責任は委託元に残ります。契約に、監査の権利、インシデントの通知期限、再委託の制限、データの返却・削除を入れておく理由はここにあります。

用語を一つ、取り違えないようにします。ISO Guide 73 のリスク評価（risk evaluation）は、推定したリスクを定めた基準と比べ、リスクの重大さを判断するプロセスです[3]。リスクの特定・分析・評価をまとめる risk assessment とは、範囲が違います。

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、CRISC 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

Footnotes

1. ISACA「CRISC Exam Content Outline」https://www.isaca.org/credentialing/crisc/crisc-exam-content-outline ↩

2. ISACA「認定試験 受験者ガイド」（CRISC の項）https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/exam-candidate-guides/2026/exam-candidate-guide.pdf ↩ ↩2

3. ISACA Glossary. https://www.isaca.org/resources/glossary ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16 ↩17 ↩18 ↩19 ↩20 ↩21 ↩22 ↩23 ↩24 ↩25 ↩26 ↩27 ↩28 ↩29 ↩30 ↩31

4. COSO, Enterprise Risk Management: Integrating with Strategy and Performance（2017）, Executive Summary / Components and Principles. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7

5. NIST SP 800-39, Managing Information Security Risk, Chapter 2（Tier 1/2/3・リスクフレーミング・リスク許容度・リスク対応）.

SAMPLE

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8

6. NIST CSWP 29, The NIST Cybersecurity Framework (CSF) 2.0（GV・ID.AM・ティア）. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16

7. NIST SP 800-37 Rev.2, Risk Management Framework for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf ↩ ↩2

8. The IIA, The IIA's Three Lines Model（2020）, Principles 1 から 6. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11

9. ISACA, Code of Professional Ethics. https://www.isaca.org/code-of-professional-ethics ↩

10. NIST SP 800-53 Rev.5, Security and Privacy Controls（CM-8 システム構成要素の台帳・ポリシーと手順）. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2 ↩3

11. NIST SP 800-34 Rev.1, Contingency Planning Guide for Federal Information Systems, 2.2 と 3（BIA・RTO/RPO/MTD・代替拠点・7段階）.

SAMPLE

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6

12. NIST IR 8286r1, Prioritizing Cybersecurity Risk for Enterprise Risk Management. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8286r1.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13

13. NC State ERM Initiative, ISO's Risk Management Framework（ISO 31000:2018 の原則とプロセスの要約）. https://erm.ncsu.edu/resource-center/isos-risk-management-framework ↩

14. Wikipedia, ISO/IEC 27005. https://en.wikipedia.org/wiki/ISO/IEC_27005 ↩

15. NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management（リスクプロファイルの定義）. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf ↩

16. NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf ↩ ↩2

17. ISACA, CRISC Exam Content Outline（Domain 1 の補助タスク）. https://www.isaca.org/credentialing/crisc/crisc-exam-content-outline ↩

18. ISACA, ISACA's Risk IT Framework Offers a Structured Methodology（2020-06-25）. https://www.isaca.org/why-isaca/about-

SAMPLE

us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology ↩

19. ISACA, Risk IT Revitalized（2020-06-25）. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/risk-it-revitalized ↩

20. ISACA, Employing COBIT 2019 for Enterprise Governance Strategy. https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy ↩

SAMPLE

CRISC 学習用テキスト(無料サンプル)

版

2026年11月版(CRISC 試験範囲(ISACA 公式 CRISC Exam Content Outline・2025年11月発効)準拠)

発行

IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com

ISACA および CRISC は、ISACA の登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は ISACA が公開している試験内容の概要（Exam Content Outline・受験者ガイド）などを基に作成したもので、ISACA との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。

SAMPLE