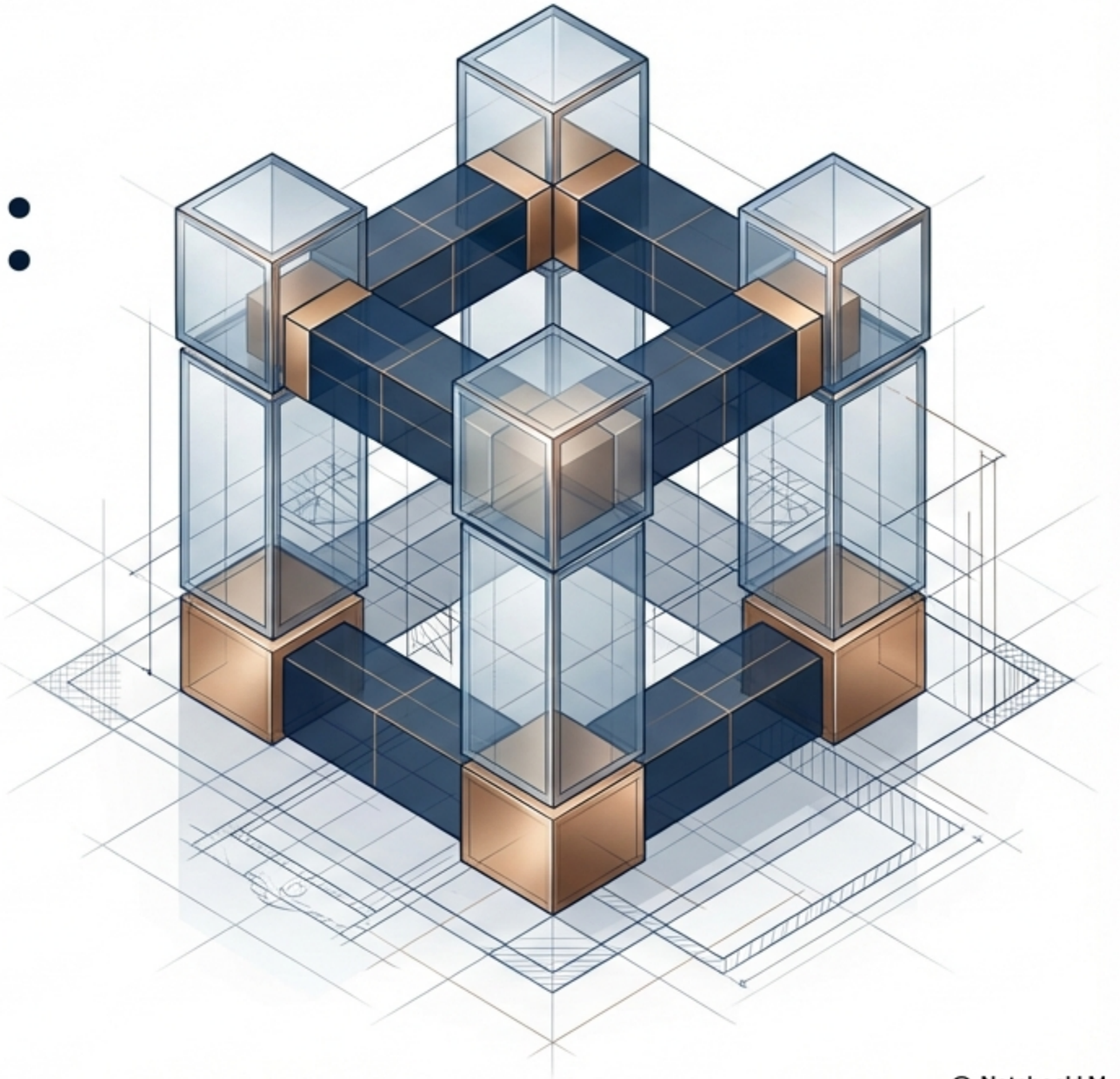
信頼を資産に変える：ISMS（ISO 27001）構築と戦略的活用

組織の持続可能性を高める情報セキュリティマネジメントの全貌



本資料は、ISO 27001およびNIST SP 800-30のガイドラインに基づき構成されています。

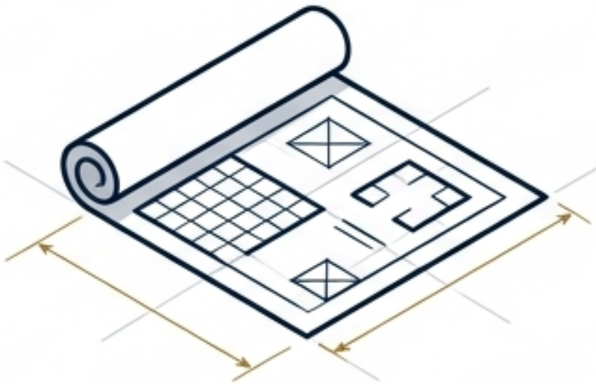
エグゼクティブ・サマリー：経営戦略としてのセキュリティ投資

The Context

背景: サイバー攻撃の高度化と、SaaS普及によるサプライチェーンリスクの増大。

データ: 経営者の**66.5%**が**「認証未取得のSaaSツール導入に消極的」**と回答（ISOプロ調査）。

The Solution



解決策: ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）の構築。

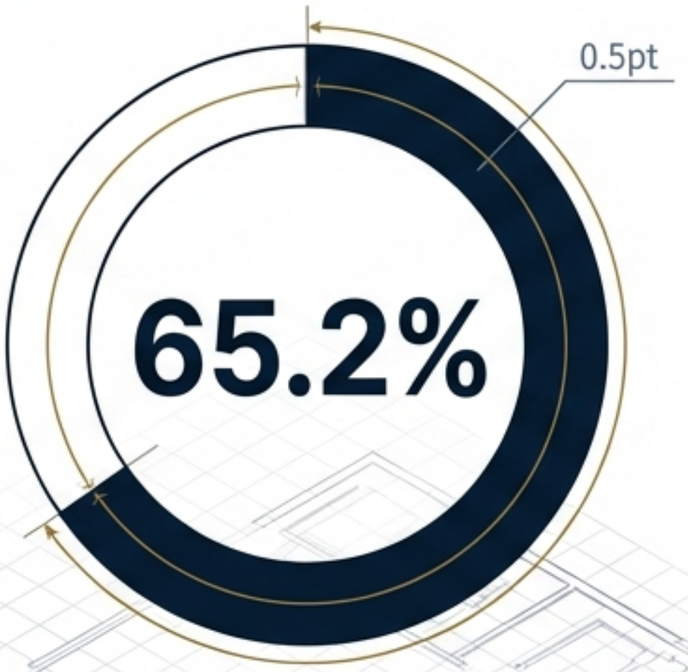
特徴: 単なる「ルールの順守」ではなく、NIST基準などの科学的アプローチを用いた「リスクアセスメント」のプロセス化。

The Impact

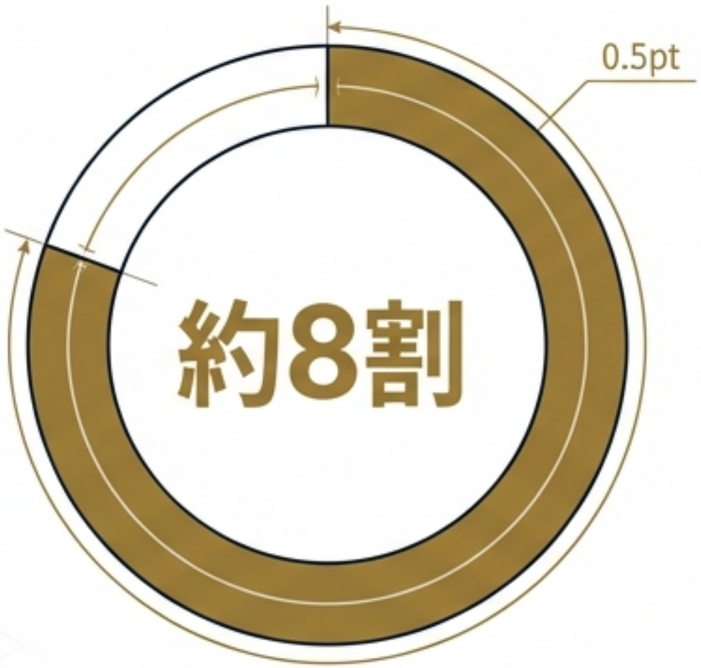
結論: 初期投資と運用コストは発生するが、対外的な「信頼の証明」と「入札・取引要件のクリア」により、中長期的な事業機会を拡大させる。

なぜ今、ISMSが必要なのか？：取引参加への必須チケット

セキュリティ認証の有無が、BtoB取引や入札の成否に直結する時代。



ISO 27001未取得を理由に
取引に失敗した経験がある経営者



SaaSツール導入時に
「高いセキュリティレベル」を
重視するIT企業経営層

Market Drivers

- **官公庁・大企業**：入札参加条件や取引基準として認証取得を要求するケースが増加。
- **DX・リモートワーク**：クラウド利用拡大により、従来の境界防御が通用せず、統一的な管理基準が必要不可欠に。

ISMSの定義と「情報の3要素（CIA）」

ISMSとは、組織の情報資産をリスクから保護し、運用するための体系的な仕組み（Information Security Management System）。

機密性 (Confidentiality)

アクセス権限を持つ者だけが情報に触れられる状態（漏洩防止）。
重視される資産: 顧客個人情報、技術機密、従業員データ。

完全性 (Integrity)

情報が最新かつ正確で、改ざんされていない状態。
重視される資産: 金融データ、Webサイトコンテンツ、会計情報。

可用性 (Availability)

必要な時にいつでも情報やシステムが使える状態（停止防止）。
重視される資産: サービス提供サーバー、業務システム。

戦略的選択：ISMS（ISO 27001）vs Pマーク

	ISMS（ISO 27001）	Pマーク
保護対象	全種別の情報資産（技術情報、顧客リスト、ノウハウ等）	個人情報に特化
規格の性質	国際規格（ISO/IEC）。海外取引や外資系企業へのアピールに有効。	日本国内規格（JIS Q 15001）。国内BtoC事業に強み。
取得範囲	部門単位、事業所単位での取得が可能（スモールスタート向き）。	法人全体での取得が必須。

Strategic Advice:
海外展開、**SaaS提供**、**技術情報の保護**を重視する場合は、
国際的信頼性の高いISMSが推奨される。

メリットとデメリットの投資対効果分析

メリット (Pros)

- **対外的信頼:** 国際基準の第三者認証により、顧客・パートナーからの信頼獲得。

- **機会損失の回避:** 入札参加資格や大手企業との取引要件をクリア。

- **組織強化:** 社員のセキュリティ意識向上と、リスクの可視化。

デメリット (Cons)

- **コスト:** 審査費用、コンサルティング費、設備投資などの初期・維持費用。

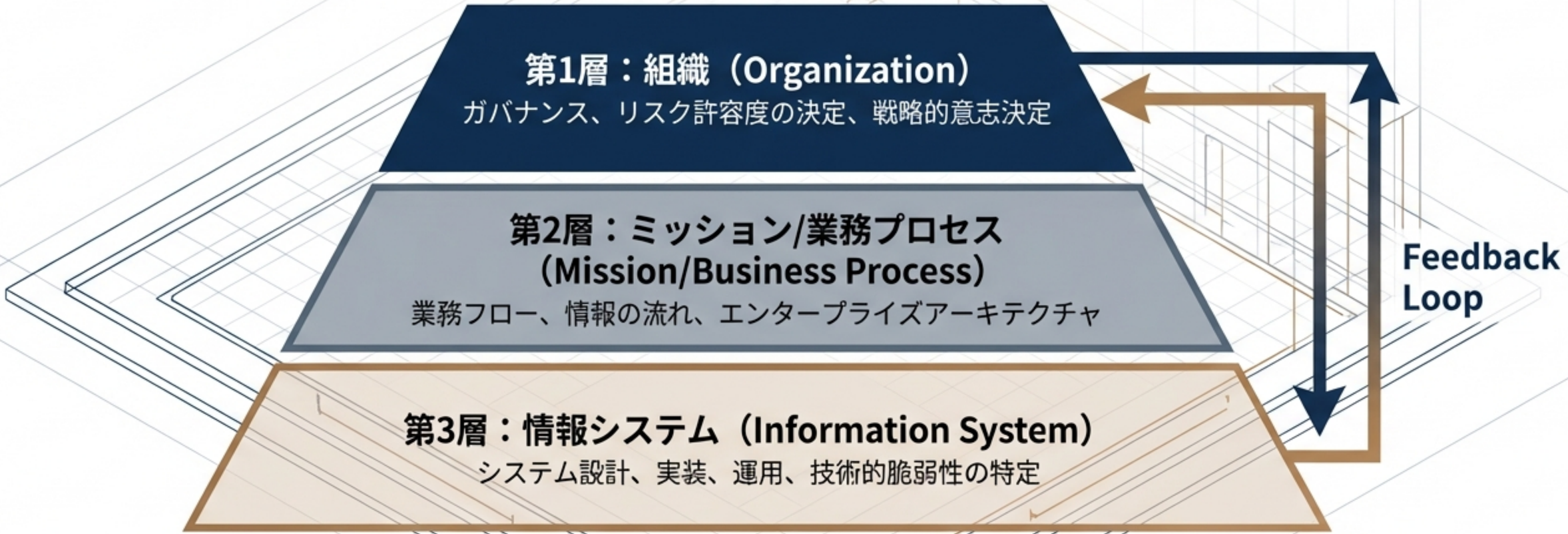
- **業務負荷:** 文書化（規定・手順書）や教育、内部監査による工数発生。

Bottom Line: コストはかかるが、事業継続性（BCP）と売上機会の拡大を考慮すれば、BtoB/SaaS企業にとって投資対効果は明白である。

リスクマネジメントの3層構造（NIST SP 800-39に基づく）

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

リスクアセスメントは現場（システム）だけでなく、組織全体で連携して行う必要がある。



上層部（第1層）がリスク許容度を示し、現場（第3層）が具体的な脆弱性に対処するフィードバックループが重要。

リスクアセスメントの実行プロセス（NIST SP 800-30）

1. 準備 (Prepare)
目的・範囲・前提条件・情報源の特定

2. 実施 (Conduct)
脅威・脆弱性の特定
リスクレベルの判定

3. 伝達 (Communicate)
意思決定者への報告・共有

4. 保守 (Maintain)
継続的なモニタリング・更新

変化し続ける脅威に対し、プロセスを回し続けることがセキュリティの本質である。

リスクの構成要素と計算モデル

リスク（Risk）＝ 脅威 × 脆弱性 × 影響度 × 発生確率

脅威（Threat）

組織に損害を与える潜在的原因（サイバー攻撃、人的ミス、災害）。

脆弱性（Vulnerability）

脅威に付け込まれる弱点（パッチ未適用のOS、不十分な管理体制）。

素因的条件（Predisposing Condition）

脆弱性の利用可能性を高める環境要因。

影響（Impact）

機密性・完全性・可用性が損なわれた際の被害の大きさ。

脅威の識別と発生可能性の分析

脅威 (Threats)

0.5pt

敵対的脅威 (Adversarial)

攻撃者の「能力」「意図」「標的」から発生確率を分析。

0.5pt

非敵対的脅威 (Non-adversarial)

人的過失、構造的欠陥、自然災害など。統計や環境から発生確率を予測。

考慮すべき要素: 脅威のシフト (Threat Shifting) - 攻撃者が戦術を変える可能性。
不確実性 (Uncertainty) - 完全な予測は不可能であることを前提とする。

4つのリスク対応策（Risk Treatment）

低減 (Modify)

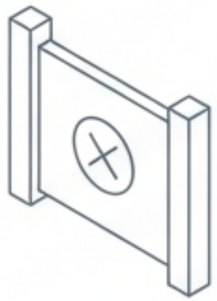
セキュリティ対策を導入して
リスクを下げる（基本）。

保有 (Retain)

受容範囲内として認め、
監視する（経営判断）。

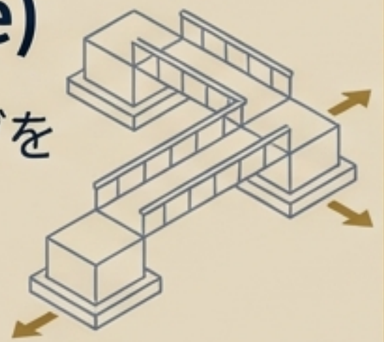
回避 (Avoid)

リスクの原因となる事業や
プロセスそのものをやめる。



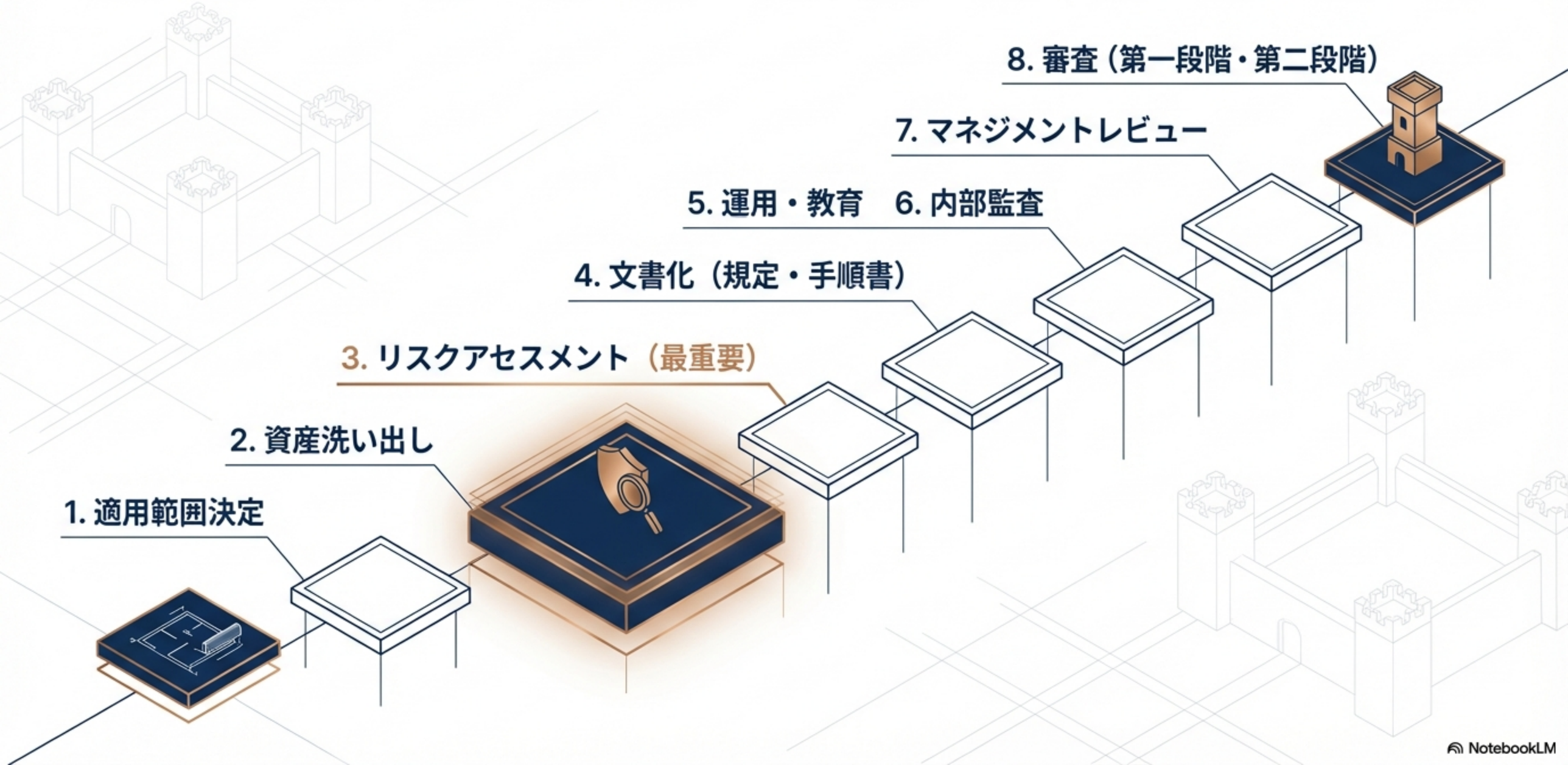
共有/移転 (Share)

保険やアウトソーシングを
利用して分散する。



重要: 全てのリスクをゼロにする必要はない。組織の「リスク許容度」に基づき選択する。

認証取得までの実装ロードマップ（全8ステップ）



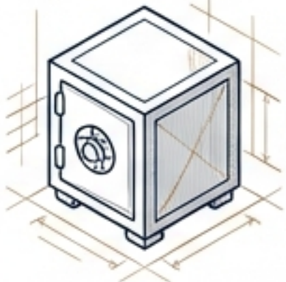
必要となるリソース：期間と費用

期間（Timeline）

自社取得：
1年以上（ノウハウ不足による試行錯誤）

コンサルタント利用：
半年程度
（効率的な文書作成）

費用（Cost Structure）



審査費用：
目安 **50〜100万円程度**
（+維持審査費）

構築・運用費用：
コンサルティング料 + 人件費 + 設備投資

必須体制: 情報セキュリティ委員会、運用事務局、内部監査員

形骸化を防ぐ運用の成功要因

よくある課題：
「文書を作って終わり」になり、現場の負担増でルールが守られない。

プロセスアプローチ

旧来の厳格なPDCAに
にこだわらず、
実態に合わせた
柔軟な改善。

スコープの最適化

「部門認証」で
スモールスタート
トし、
ノウハウを蓄積。

クラウド活用

SaaS利用による
物理セキュリティ
負担の軽減。

結論：攻めのセキュリティとしてのISMS

顧客の信頼を勝ち取り、ビジネスを加速させる戦略的投資。

NIST基準のリスク管理で、組織の「復元力（Resilience）」を高める。

Next Action: まずは「適用範囲（スコープ）の決定」から始めよう。