ISMS & ISO 27001: 認証取得とリスクアセスメント完全ガイド

Complete Guide to Certification and Risk Assessment

組織の信頼と競争力を高める情報セキュリティマネジメント

Based on NIST SP 800-30 & ISO 27001 Standards

セキュリティ認証の欠如は、直接的な「機会損失」につながる

65.2%

ISO 27001がないことで、取引に失敗した経験がある

66.5%

ISO 27001を取得していないSaaSツールの導入には消極的

Source: ISOプロ「約1,000人の経営者に聞いたISMS認証に関する実態調査」

Cyber Threats

ランサムウェアや不正アクセスの脅威が増加。

DX & Remote Work

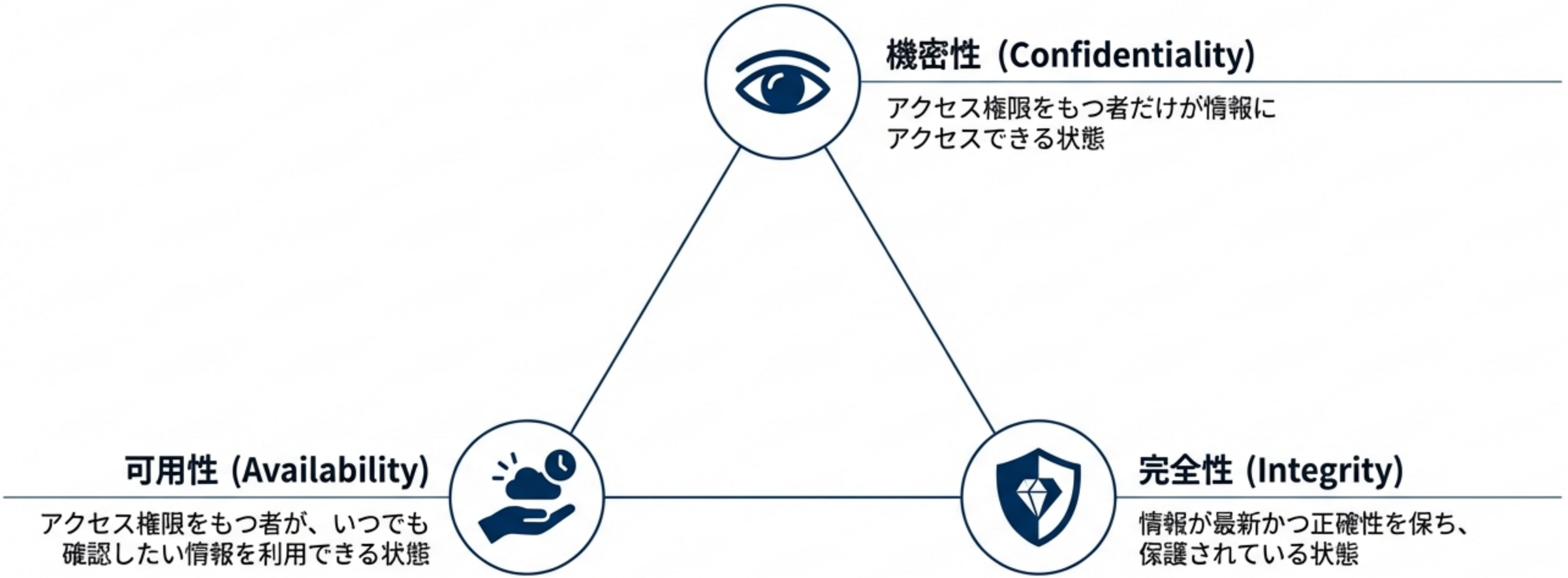
クラウドサービス拡大により、セキュリティ統一管理が複雑化。

Business Impact

システムの問題ではなく、入札条件や大企業の取引要件としての必須化。

ISMS（情報セキュリティマネジメントシステム）の定義と3要素

組織が保有する情報資産を情報セキュリティリスクから保護する仕組み



機密性 (Confidentiality)

アクセス権限をもつ者だけが情報にアクセスできる状態

可用性 (Availability)

アクセス権限をもつ者が、いつでも確認したい情報を利用できる状態

完全性 (Integrity)

情報が最新かつ正確性を保ち、保護されている状態

セキュリティとは「隠すこと」だけではなく、「使えること」「正しいこと」を維持する活動である。

戦略的選択：ISO 27001（ISMS）vs プライバシーマーク

ISMS（ISO 27001）		プライバシーマーク（Pマーク）	
保護対象	全情報資産 （技術・ノウハウ含む）	保護対象	個人情報に特化
規格	国際規格（ISO/IEC 27001）	規格	国内規格（JIS Q 15001）
適用範囲	適用範囲を任意に設定可能 （部門・拠点単位）	適用範囲	企業全体（全社取得が必須）
メリット	国際的な信頼・官公庁入札・ B2B向け	メリット	国内消費者向け（B2C）の信頼

Decision Guide → **技術情報や海外取引、官公庁案件を目指すならISO 27001を選択**

導入のメリットとデメリット

メリット（投資対効果）

- **対外的な信頼向上**
  （海外・国内取引先）
- **競争優位性の確保**
  （入札・契約条件のクリア）
- **リスク低減**
  （情報漏洩・内部不正の防止）
- **組織文化の醸成**
  （社員の意識向上）

デメリット（投資コスト）

- **コスト**
  （審査費用・コンサル費用・維持費）
- **業務負荷**
  （文書作成・教育・運用工数）

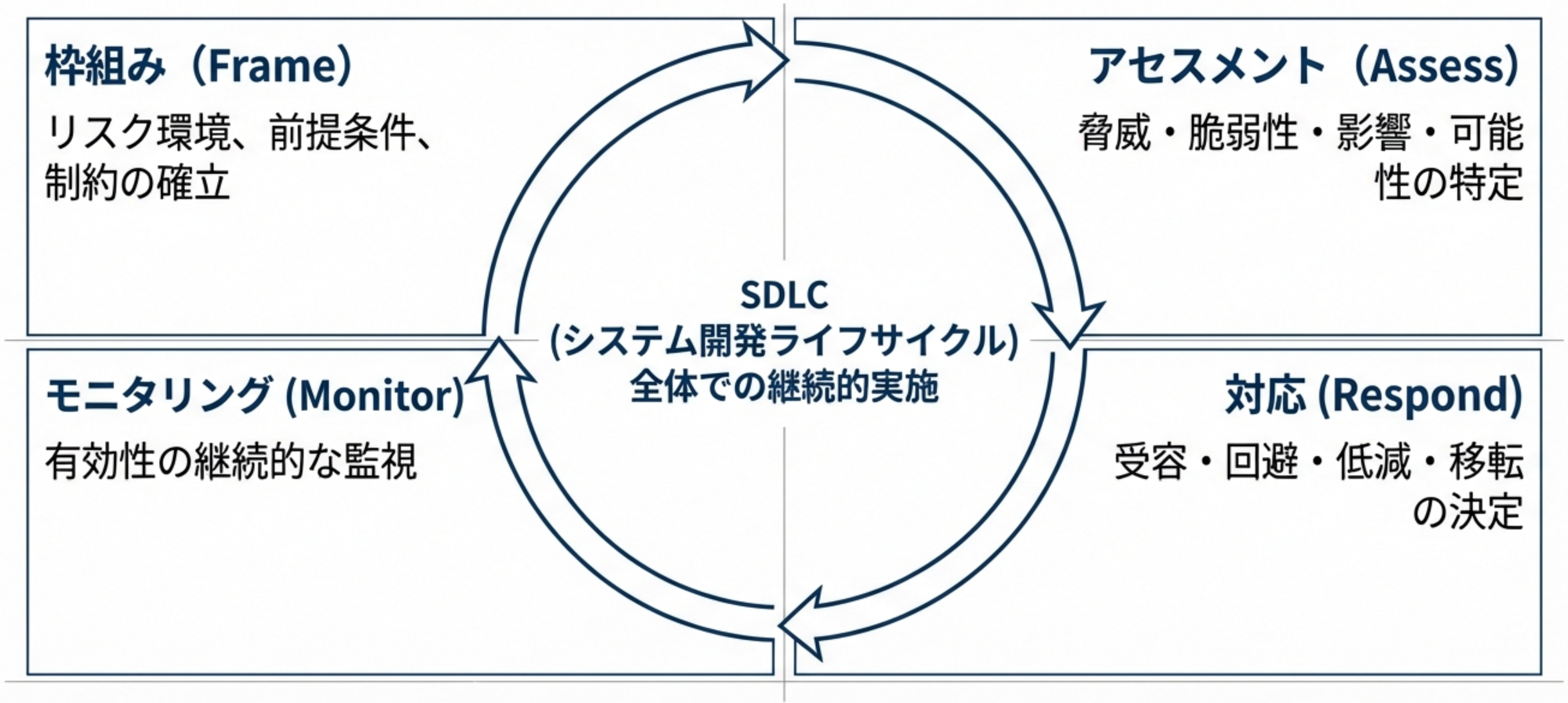
初期負荷は高いが、機会損失（Lost Opportunity）を防ぐための必須投資となる。

認証取得までの8ステップ

リスクマネジメントの枠組み

NIST SP 800-30に基づくプロセス

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



Noto Sans JP

リスクの構成要素とモデル

Risk =

Threat (脅威)

組織に悪影響を与える事象の潜在的原因。
（敵対的：攻撃者 / 非敵対的：エラー・災害）

Vulnerability (脆弱性)

脅威によって利用される弱点。
（システム欠陥・組織的不備・素因的条件）

→

Likelihood (発生の可能性)

脅威が顕在化し、影響が生じる確率。

Impact (影響)

情報の漏洩・改ざん・停止による組織への損害。

リスクアセスメントの実施手順

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

Step 1: 特定 (Identify)

- 資産の特定
- 脅威源の特定 (敵対的/非敵対的)
- 脆弱性の特定 (パッチ未適用など)

Step 2: 分析 (Analyze)

- 発生可能性の算定 (攻撃者の能力/意図)
- 影響度の算定 (機密性・完全性・可用性へのダメージ)

Step 3: 評価 (Evaluate)

- リスク値の算出
- リスク受容基準との比較
- 対応優先度の決定

リスク対応の4つの選択肢

リスク低減 (Mitigate)

セキュリティ対策を導入し、発生確率や影響を下げる。（最も一般的）

リスク回避 (Avoid)

リスクの原因となる活動そのものを停止する。

リスク移転 (Transfer)

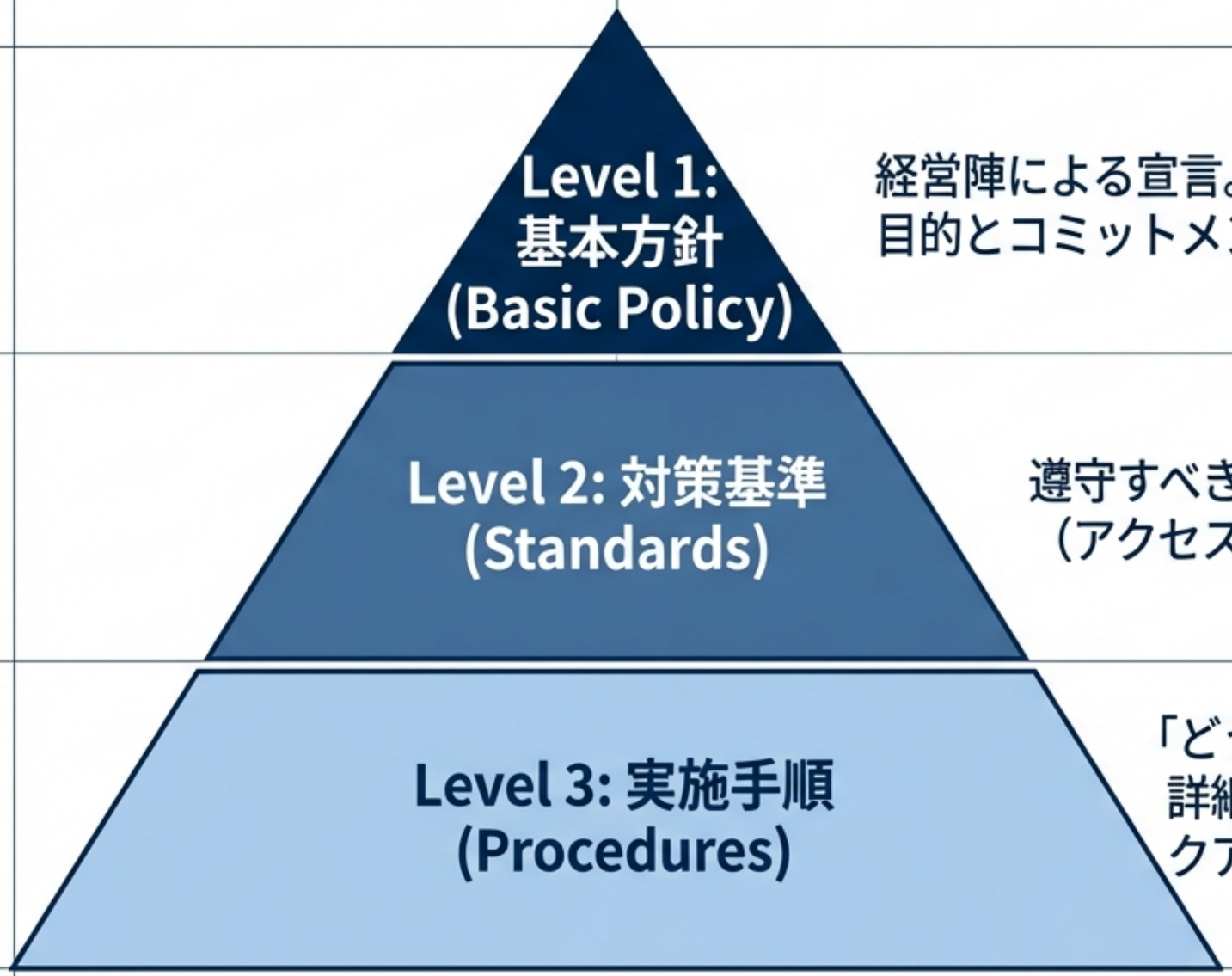
保険への加入やアウトソーシングでリスクを他社へ移す。

リスク受容（Accept)

リスクが許容範囲内であることを認め、そのまま保有する。

情報セキュリティ文書の階層構造

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



経営陣による宣言。
目的とコミットメント。

遵守すべき具体的なルール
（アクセス制御規定など）。

「どうやるか」を記した
詳細マニュアル（バッ
クアップ手順書など）。

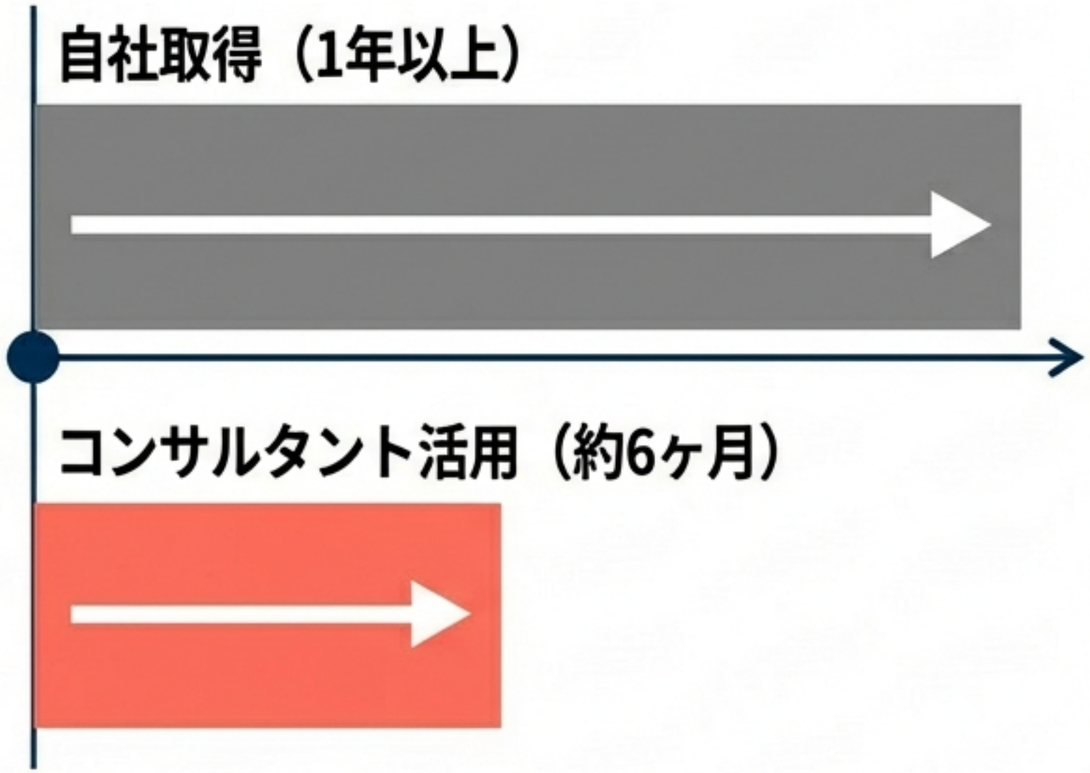
適用宣言書
(Statement of
Applicability)
によりリスクと
紐付け

認証審査のプロセス：2段階審査

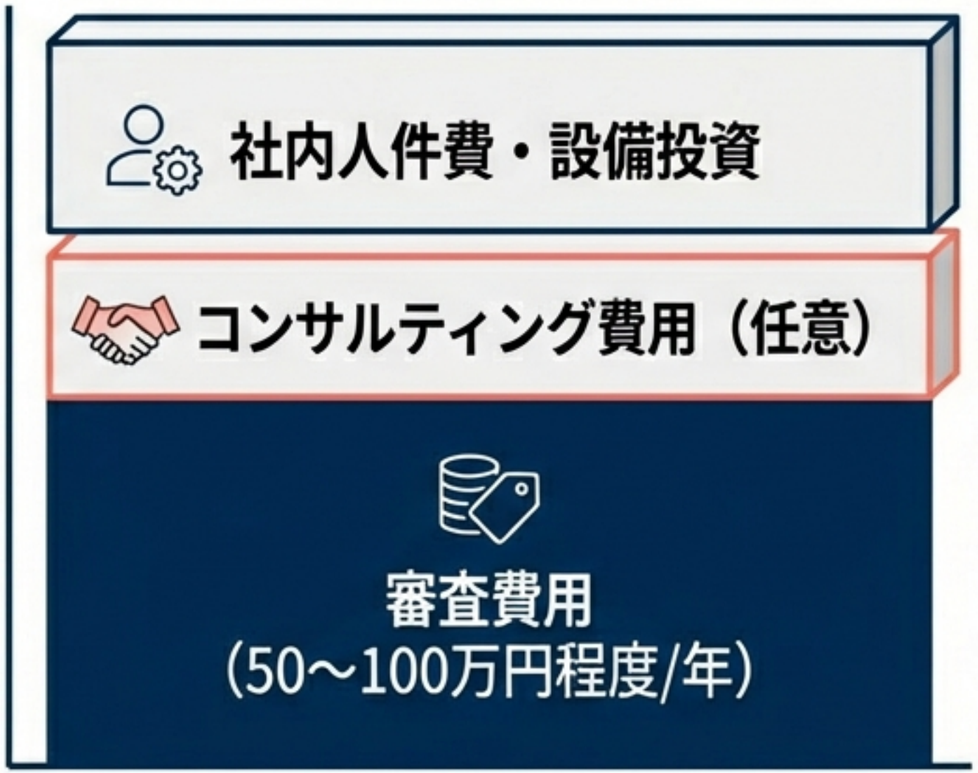
取得にかかる期間と費用

National Institute of Standards and Technology
U.S. Deporiment of Commerce

取得にかかる期間（Time）



取得にかかる費用（Money）



※維持審査（年1回）と更新審査（3年毎）のランニングコストも考慮が必要。

ISO 27001取得が推奨される企業

☐ 官公庁・大企業との取引がある

入札参加資格や取引基本契約で必須となるケース多数。

☐ 機密情報・個人情報を大量に扱っている

B2Bの技術データや顧客リストの保護。

☐ SaaS・クラウドサービス事業者

サービス導入時のセキュリティチェックシート対応と信頼性確保。

結論：ISMSは「コスト」ではなく「投資」である

Business Continuity: サイバー脅威と内部不正から事業を守る。

Market Trust: 取引の「パスポート」として機会損失を防ぐ。

Risk Mastery: 文書作成だけでなく、NISTに基づく実効的なリスク評価が鍵。

Next Action: 適用範囲の決定と情報セキュリティ委員会の立ち上げ