ITAM/SAM ポリシー管理の体系化と大手企業向け統合テンプレート

エグゼクティブサマリ

本成果物は、大手企業（かつグローバル対応を想定）において、IT 資産管理（ITAM）とソフトウェア資産管理（SAM）を「社内規定（規程）／基準（標準）／運用プロセス（手順）／記録様式（証跡）」として統合し、監査・コンプライアンスとコスト最適化、セキュリティ／プライバシー要件を同時に満たすための実務テンプレートである。設計の背骨は、IT 資産管理システム（ITAMS）の要求事項を定める ISO/IEC 19770-1（組織の状況における IT 資産管理システム要求事項、全ての IT 資産タイプ・全ての組織規模に適用可能）であり、導入ガイダンスを提供する ISO/IEC TS 19770-10（管理システム／機能管理／ライフサイクルの各プロセス群の整理）をあわせて「文書体系」と「運用体系」に落とし込む。[1]

運用実装の観点では、ITIL 4 の「IT 資産管理」実践が示す“ライフサイクル全体を計画・管理し、価値最大化／コスト統制／リスク管理を行う”という目的と、同じく「サービス構成管理」が示す“必要なときに必要な場所へ、サービスや構成項目に関する正確で信頼できる情報を提供する”という目的を、ITSM・CMDB・SAM ツール連携要件として組み込む。[2]

セキュリティ統制は、資産インベントリの最新化・自動化・集中リポジトリ化や、不正コンポーネント検知などを求める NIST の管理策（例：CM-8 系）を、ITAM/SAM 統制の最低要件・監査チェック観点に反映する。[3] さらに、経営責任・体制整備・重要指示事項を明確化する日本の「サイバーセキュリティ経営ガイドライン」（大企業も対象）を、規程レベルの統治要件（トップマネジメント、CISO 等）に接続する。[4]

プライバシーは、個人情報保護委員会のガイドライン（通則編、外国第三者提供編）に基づき、境界を跨ぐデータ処理（委託・クラウド・海外拠点）に伴う情報提供・同意・継続的確保措置などを“IT 資産・SaaS・委託先”の管理条文に落とし込む。[5] ベンダー監査対応は、監査・検証機能を明示する各社公式情報（例：Oracle License Management Services、IBM のサブキャパシティ要件・ILMT 必須性、Microsoft の SAM ベストプラクティスガイド）を、監査フローと証跡要件に取り込む。[6]

前提条件と未指定事項

本テンプレートは、以下の前提で設計する。

- 対象組織規模：**大手企業**（複数事業部・複数拠点・外部委託を含む可能性が高い）
- グローバル展開：**未指定（ただし“グローバル対応を想定”として扱う）**
- 基盤：**クラウド／オンプレ混在**（IaaS/PaaS/SaaS、仮想化を含む）
- 資産カテゴリ：**ハードウェア、ソフトウェア、SaaS、仮想資産、モバイル**（ユーザー端末・サーバ・ネットワーク・クラウドリソースを含む想定）
- ライセンス形態：**プロプライエタリ、OSS、サブスクリプション**
- 統制要求：**セキュリティ・プライバシー、ライセンス監査対応、コスト管理、ライフサイクル管理、ツール連携（ITSM、CMDB、SAM ツール）**
- 文書階層：日本企業の一般的運用に合わせ、**規程（Must）→基準/標準（Must）→手順（How）→様式/記録（Evidence）**を採用（ISO/IEC 19770-1 の「マネジメントシステムとしての要求事項」を、社内規程に展開する狙い）。[1]

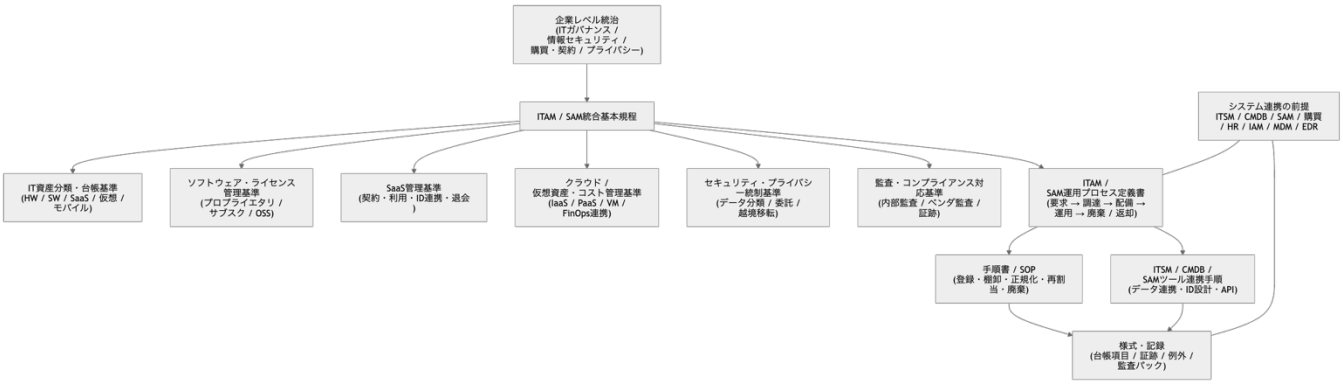
未指定であり、テンプレート内では明示的に「未指定」として扱う事項（例）：

- 対象業種・規制要件（例：金融、医療、重要インフラ等）：**未指定**
- 適用国・地域（データ越境・輸出管理・労働法制等の影響）：**未指定**
- 現行ポリシーの有無・成熟度（ITIL/ISMS 導入状況、資産台帳精度、監査履歴）：**未指定**
- 管理対象規模（端末台数、サーバ台数、SaaS 契約数、アプリ数）：**未指定**
- 採用ツール（ITSM 製品名、CMDB 製品名、SAM ツール製品名、EDR/MDM 等）：**未指定**
- 調達・契約形態（集中購買、分散購買、販売代理店、海外契約主体など）：**未指定**

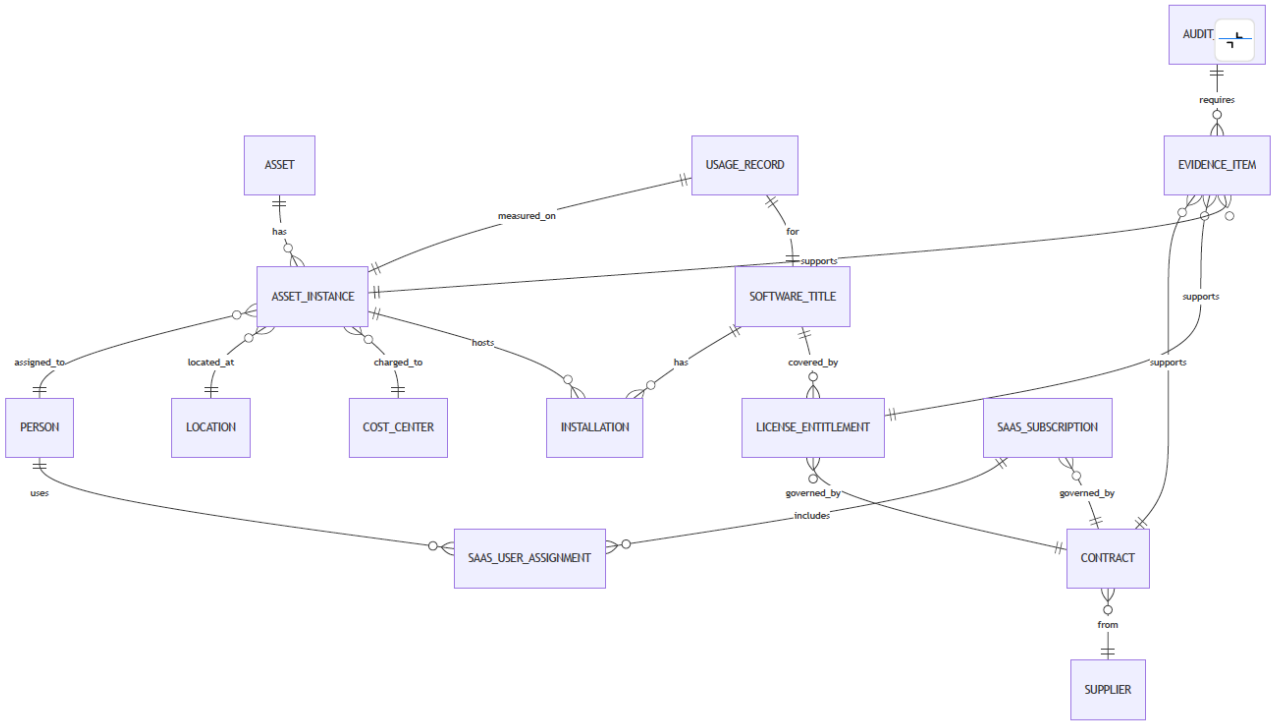
統合ポリシー体系とデータモデル

ISO/IEC 19770-5 は、ISO/IEC 19770 ファミリーの概観、ITAM/SAM の導入、基礎原則、用語を提供する（無償提供の版も存在）。そのため、本テンプレートでは 19770-5 を「用語・概念の共通辞書」として位置づけ、規程・基準・手順の用語ブレを抑制する。[7]
また、ISO/IEC 19770-2（SWID タグ）、19770-3（エンタイトルメント）、19770-4（利用量測定）、19770-6（HWID タグ）など“識別・権利・利用・ハード識別”の情報構造標準を、ツール連携・データ品質要件に反映する。[8]

統合ポリシー体系図（文書体系：フローチャート）



統合データモデル（ER 図：最低限の“台帳・権利・利用・証跡”）



（補足：上図は“最低限”であり、CMDB の CI 関係、クラウドリソース（アカウント/RG/プロジェクト、タグ、課金、リージョン）や、SWID/HWID/エンタイトルメントタグ等の標準化データは、採用ツール・契約要件に応じて拡張する想定。ISO/IEC 19770-2/3/4/6 は情報構造の標準であり、これらの標準を採用すると識別・権利・利用量の整合性を取りやすい。[8]）

文書テンプレート一式

ISO/IEC 19770-1 は「IT 資産管理システム（ITAMS）」の要求事項を定め、内部・外部が組織の IT 資産管理要求を満たす能力を評価できるとしている。[9]

したがって大手企業では、監査可能性（説明責任）を担保するために「規程（統治）」と「運用プロセス（実装）」と「記録（証跡）」を分け、かつ整合させた“文書体系”が必要になる。ISO/IEC TS 19770-10 は、管理システム、機能管理（データ管理・ライセンス管理・セキュリティ管理・関係/契約・財務・変更管理等）、ライフサイクル（仕様→取得→展開→運用→廃棄等）の各プロセス群を明確化しているため、文書の章立てと RACI 整理に直結させる。[10] また ITIL 4 の Practice Guide は、目的・用語・スコープ、プロセス、役割、情報と技術、サプライヤ等の共通構造を持つため、各文書のテンプレート骨格として利用しやすい。[11]

文書カタログ（大手企業向け“最小完結セット”）

文書名（テンプレート）	目的（要旨）	適用範囲（例）	A（説明責任）/R（実行責任）/C/I（例）
ITAM/SAM 統合基本規程	統治・適用範囲・原則・遵守義務・監査/例外を定義（全社規程）	全社（国内外拠点含む想定）、対象資産：HW/SW/SaaS/仮想/モバイル	A: CIO（未指定） / R: ITAM 統括（未指定） / C: CISO・法務・購買・財務 / I: 全従業員
IT 資産管理基準（台帳・CMDB）	台帳項目、識別子、棚卸頻度、CMDB 連携、品質 KPI を標準化	IT 部門＋子会社/委託先、資産登録・移動・廃棄	A: IT 運用責任者（未指定） / R: ITAM 運用 / C: ITSM・インフラ / I: 監査
ソフトウェア資産管理基準（ライセンス/OSS 含む）	ソフトウェア識別・正規化、権利（契約）管理、利用量、OSS 遵守を統合	インストール媒体、端末/サーバ、仮想化、VDI、コンテナ等	A: ITAM/SAM 責任者 / R: SAM 運用 / C: 法務・購買・セキュリティ / I: 事業部
SaaS 管理基準（サブスク）	契約・利用状況・ID 連携・退会・データ返却/削除・費用配賦を統一	全 SaaS（シャドーIT 含む検知対象）	A: IT ガバナンス / R: SaaS 管理担当 / C: 情報セキュリティ・プライバシー / I: 監査
クラウド/仮想資産・コスト管理基準	アカウント/サブスク/タグ/課金、未使用検知、FinOps 連携を標準化	IaaS/PaaS、仮想マシン、ストレージ、ID、リージョン	A: CCoE（未指定） / R: クラウド運用 / C: 財務・セキュリティ / I: 事業部
ITAM/SAM 運用プロセス定義書（統合）	取得→配備→運用→回収→廃棄と、SAM 適正化（ELP）を標準化	ITSM 要求/変更/構成/購買/HR と連携	A: ITSM 責任者 / R: ITAM/SAM プロセスオーナー / C: 各運用チーム / I: 全社
監査・コンプライアンス対応手順書	内部監査・外部監査・ベンダ監査の受付/証跡/是正を定義	監査イベント、証跡保管、対外コミュニケーション	A: コンプライアンス責任者（未指定） / R: ITAM/SAM 監査対応 / C: 法務 / I: 経営層
ツール連携要件定義（ITSM/CMDB/SAM）	SoR 設計、データ連携、ID 体系、API、責任境界を定義	ITSM、CMDB、SAM、購買、HR、IAM/SSO、MDM 等	A: アーキ/運用統括 / R: ツール管理者 / C: 全関係部門 / I: 監査

（補足：ISO/IEC 19770-1 は「金融・会計・技術要件そのもの」は規定しないため、企業内“基準”として具体条文を補完する必要がある。[9]）

共通メタ情報テンプレート（全文書）

- 文書 ID：{DOC-ID}
- 文書名：{文書名}
- 版数：{vX.Y}／施行日：{YYYY-MM-DD}／改定日：{YYYY-MM-DD}
- 所管：{部門名}／承認：{承認者（役職）}／文書オーナー：{役職}
- 適用開始：{YYYY-MM-DD}／適用終了：{該当時}
- 関連文書：{上位規程/下位基準/手順/様式}
- 例外管理：{例外手順書 ID}
- 記録保管：{保管年限・保管場所・閲覧権限}
- 監査：{内部監査頻度}（未指定）／{外部監査}（未指定）

ITAM/SAM 統合基本規程（条文テンプレート）

（目的）
第 1 条　本規程は、当社グループにおける IT 資産管理（ITAM）およびソフトウェア資産管理（SAM）を統合し、
(1) 法令・契約・ライセンス条件の遵守、(2) セキュリティおよびプライバシー確保、
(3) コスト最適化、(4) IT サービスの品質確保、(5) 監査対応可能性の確保
を目的として、必要な統治・責任・遵守事項を定める。

（適用範囲）
第 2 条　本規程は、当社および子会社・関連会社（適用範囲：未指定）ならびに当社 IT 資産を取り扱う委託先に適用する。
2　本規程でいう IT 資産は、ハードウェア、ソフトウェア、SaaS、仮想資産、モバイル端末、クラウド上の利用権・サブスクリプション・サービスを含むものとする。

（定義）
第 3 条　本規程の用語は別紙「用語集（ISO/IEC 19770-5 準拠の用語統一）」に従う。
2　ライセンス、エンタイトルメント、利用量、台帳、CMDB、SoR（System of Record）等の定義を付す。

（基本原則）
第 4 条　当社は、IT 資産管理システム（ITAMS）を確立し、維持し、継続的に改善する。
2　当社は、IT 資産のライフサイクル（仕様→取得→展開→運用→廃棄/返却）を通じて統制を適用する。
3　当社は、SaaS およびクラウドに関する IT 資産も含め、全社横断で可視化・統制する（グローバル対応想定）。

（役割と責任）
第 5 条　CIO（未指定）は本規程の説明責任（Accountable）を負う。
2　ITAM/SAM 統括責任者（未指定）は本規程の運用責任（Responsible）を負い、必要な基準・手順を整備する。
3　情報セキュリティ責任者（CISO 等・未指定）、法務、購買、財務、内部監査は所掌範囲で協議・助言を行う（Consulted）。

（遵守義務）
第 6 条　従業員および委託先は、認可された手順により IT 資産を取得・利用・変更・廃棄しなければならない。
2　認可されていないソフトウェアの導入、未登録 SaaS の業務利用（シャドーIT）は禁止する。

（記録と権限）

第 7 条　IT 資産台帳、ソフトウェア台帳、SaaS 台帳、契約・権利記録、利用量記録、監査証跡を維持する。
2　台帳の正は、別紙「SoR 定義」に従い一意に定める。SoR 以外の複製台帳の利用は制限する。

（例外）
第 8 条　本規程からの例外は、別紙「例外管理手順」に従い、期限付きで承認されなければならない。

（監査・是正）
第 9 条　当社は、内部監査（頻度：未指定）および必要な外部監査に協力し、監査指摘に対し是正処置を実施する。

（懲戒・契約上の措置）
第 10 条　本規程違反が重大な場合、就業規則等（未指定）または委託契約に基づく措置を行う。

根拠設計：ISO/IEC 19770-1（ITAMS 要求事項、適用範囲・対象資産タイプ、ISO 55001 との関係）、ISO/IEC 19770-5（用語・概観）、ISO/IEC TS 19770-10（管理システム／機能管理／ライフサイクル整理）。[12]

IT 資産管理基準（台帳・CMDB）テンプレート

（目的）
第 1 条　本基準は、IT 資産台帳および CMDB の登録要件、識別子、更新、棚卸、品質 KPI、連携要件を定める。

（SoR とデータ責任）
第 2 条　SoR は以下のとおり定める（未指定の箇所は導入時に決定する）。
- 物理資産台帳 SoR：{CMDB/ITAM ツール/ERP 等：未指定}
- ソフトウェア検知 SoR：{SAM ツール/EDR/MDM 等：未指定}
- 契約・購買 SoR：{購買システム：未指定}
- 人・組織 SoR：{HR：未指定}
- 認証・ID SoR：{IAM/SSO：未指定}

2　SoR データ項目の定義・品質・アクセス権はデータオーナーが責任を負う。

（必須登録項目：資産）
第 3 条　資産カテゴリごとに必須項目を定める（例）。
- HW：資産 ID、型番、シリアル、HWID（取得可能な場合）、保有/リース区分、所在、利用者、状態、取得日、保証、廃棄日
- 仮想：リソース ID、サブスクリプション/アカウント、リージョン、タグ、所有者、課金先、稼働状態
- モバイル：MDM 管理 ID、端末 ID、回線契約、暗号化状態、紛失対応、利用者

（更新タイミング）
第 4 条　資産登録は、取得・配備・移動・返却・廃棄の各イベントで更新しなければならない。
2　自動取得（エージェント/API）を基本とし、人手更新がある場合は根拠を記録する。

（棚卸）
第 5 条　棚卸は、{四半期/半期/年次：未指定}に実施し、差分の原因分析・是正・再発防止を行う。

（品質 KPI）
第 6 条　最低 KPI を以下とする（目標値は未指定）。
- カバレッジ：管理対象に対する検知率
- 正規化率：型番/ソフトウェア名の正規化率
- 更新遅延：イベント発生から台帳反映までの時間
- 重複率：同一資産の重複登録率

セキュリティ統制整合：資産・構成要素インベントリの更新（インストール/削除時更新、集中リポジトリ）、不正コンポーネント検知などの管理策思想（CM-8 系）を満たすよう、更新イベントと集中台帳を明記する。[13]

ITIL 整合：構成情報は「必要なときに必要な場所へ正確に提供」する目的を明示し、CMDB/構成情報の品質 KPI を置く。[14]

ソフトウェア資産管理基準（ライセンス/OSS 含む）テンプレート

（目的）
第 1 条　本基準は、ソフトウェア識別、インストール統制、ライセンス遵守、OSS 遵守、利用量測定、再割当を定める。

（ソフトウェア識別と正規化）
第 2 条　検知したソフトウェアは、Publisher/Product/Edition/Version 等の正規化辞書により一意化する。
2　SWID タグ等の識別情報が利用可能な場合は、識別の優先順位および信頼度（Authoritative）を定める。

（エンタイトルメント管理）
第 3 条　権利（契約・利用許諾）は、契約書・注文書・ライセンス証書等の原本記録を“法的優先”とし、
台帳上の権利データは原本の参照可能性を担保する（証跡リンク必須）。
2　ライセンスメトリクス（ユーザー数/デバイス数/コア/仮想化/同時接続等）は製品ごとに定義し、計算式を文書化する。

（インストール統制）
第 4 条　認可ソフトウェア（ホワイトリスト）を定義し、未承認ソフトの導入を禁止する。
2　例外は例外管理手順により期限付きで処理する。

（利用量測定と最適化）
第 5 条　利用実績（起動回数/利用時間/ピーク等）の取得方式を定義し、再割当（リハーベスト）基準を定める。

（OSS コンプライアンス）
第 6 条　OSS 利用は、ライセンス種別・義務（表示、原文提供、ソース公開等）を把握し、
配布物/社内利用/クラウド提供の区分に応じて遵守する。
2　OSS 台帳（部品表/依存関係/ライセンス）と承認フローを定める。

標準根拠：SWID タグ標準（ISO/IEC 19770-2）と、権利スキーマ（ISO/IEC 19770-3）、利用量測定（ISO/IEC 19770-4）、および軽量表現 CoSWID（IETF RFC 9393）を、識別・権利・利用量の整合性確保に使える。[15]
OSS は、オープンソースライセンス遵守プログラムの要求事項を示す ISO/IEC 5230（OpenChain）を参照し、プロセスとして定着させる。[16]
セキュリティ統制整合：NIST の「不正コンポーネント検知」や「集中インベントリ」等の思想に沿って、未承認ソフト検知と是正をプロセス化する。[17]

SaaS 管理基準テンプレート（サブスク・ID・退会）

（目的）
第 1 条　本基準は、SaaS の調達・利用・ID 連携・権限・退会・データ処理/返却・費用配賦を定める。

（SaaS の定義と対象）
第 2 条　業務に利用されるクラウドアプリケーションおよびサブスクリプションを SaaS として管理対象に含める。

（導入前審査）
第 3 条　SaaS 導入は、(1)セキュリティ評価、(2)プライバシー/データ処理評価、(3)契約条項評価、
(4)費用・配賦、(5)退出（Exit）計画、を満たした場合に承認する。

（ID 連携とアカウント統制）
第 4 条　SaaS は、原則として SSO/IAM 連携（未指定）を必須とし、入退社・異動（HR イベント）と連動して
アカウントの付与/停止/削除を実施する。

（シャドーIT 対策）
第 5 条　未承認 SaaS の業務利用を禁止し、検知（CASB 等：未指定）と是正フローを定める。

（退会・データ返却/削除・ログ保全）
第 6 条　契約終了時は、データ返却/削除、ログ保全（保管年限：未指定）を実施し証跡を記録する。

プライバシー整合：越境移転・外国第三者提供等のリスク変化に対応し、本人同意や情報提供、相当措置の継続確保、定期確認等を企業特性に応じて組み込む（PPC ガイドラインの“しなければならない/してはならない”の区分を踏まえて規程・手順に落とす）。[18]
クラウドの役割分担・統制は、クラウドサービス向け管理策ガイダンス（ISO/IEC 27017）や、クラウド PII 処理者としての保護ガイダンス（ISO/IEC 27018）と整合させやすい。[19]

クラウド/仮想資産・コスト管理基準テンプレート（FinOps 連携含む）

（目的）
第 1 条　本基準は、クラウド/仮想資産の台帳化、タグ、課金、利用最適化、コスト統制を定める。

（アカウント・責任境界）
第 2 条　クラウドアカウント/サブスクリプション/プロジェクトの責任者（Owner）と財務責任（Cost Owner）を定める。

（タグ標準）
第 3 条　リソースには必須タグ（例：Owner、CostCenter、System、Env、DataClass、Region）を付与しなければならない。

（利用最適化）
第 4 条　未使用/過剰リソース、停止忘れ、重複契約を検知し、是正期限を定める。

（FinOps 運用）
第 5 条　FinOps の Inform/Optimize/Operate サイクルにより、可視化→最適化→運用統制を反復する。

根拠：FinOps は、技術価値の測定に財務アカウンタビリティを持ち込み、クラウドや SaaS 等の領域で、スピード/コスト/品質のトレードオフを支援する実務枠組みとして定義される。[20]

監査・コンプライアンス対応手順書テンプレート（監査パック）

（目的）
第 1 条　本手順書は、内部監査・外部監査・ベンダ監査に対し、受付、範囲確定、証跡収集、レビュー、提出、是正を標準化する。

（監査イベントの分類）
第 2 条　監査イベントを以下に分類する。
- 内部監査（定期/随時：未指定）
- 外部監査（規制/顧客要求：未指定）
- ベンダ監査（ライセンス条項に基づく）

（受付と体制）
第 3 条　窓口は{法務/コンプライアンス/ITAM：未指定}とし、監査対応責任者を任命する。

（範囲確定）
第 4 条　対象製品、対象期間、対象環境（オンプレ/クラウド/仮想化）、対象法人（国内外）を確定し、監査計画書を作成する。

（証跡収集）
第 5 条　標準“監査パック”を作成する（例）。
- 契約・権利（注文書、契約書、数量、メトリクス定義）
- 検知・インベントリ（台帳スナップショット、収集方式、除外理由）
- 利用量・割当（利用データ、再割当記録）
- 是正（過不足分析、是正計画、実施結果）

（提出前レビュー）
第 6 条　法務レビュー（対外提出の適法性・契約整合）と、セキュリティレビュー（秘匿情報）を実施する。

（是正と再発防止）
第 7 条　監査指摘は是正チケット化し、原因分類（データ品質/プロセス逸脱/契約解釈/例外）と再発防止策を記録する。

参照：監査・認証の枠組み（ISO/IEC 19770-11 は、ISO/IEC 19770-1 に基づく ITAMS の監査・認証を行う機関の要求事項とガイダンスを示す）。[21]
ベンダ監査の実務観点は、各社公式の監査・検証・要件（例：Oracle LMS、IBM サブキャパシティ）に合わせて“証跡パックの中身”を調整する。[22]

実装手順と運用プロセス

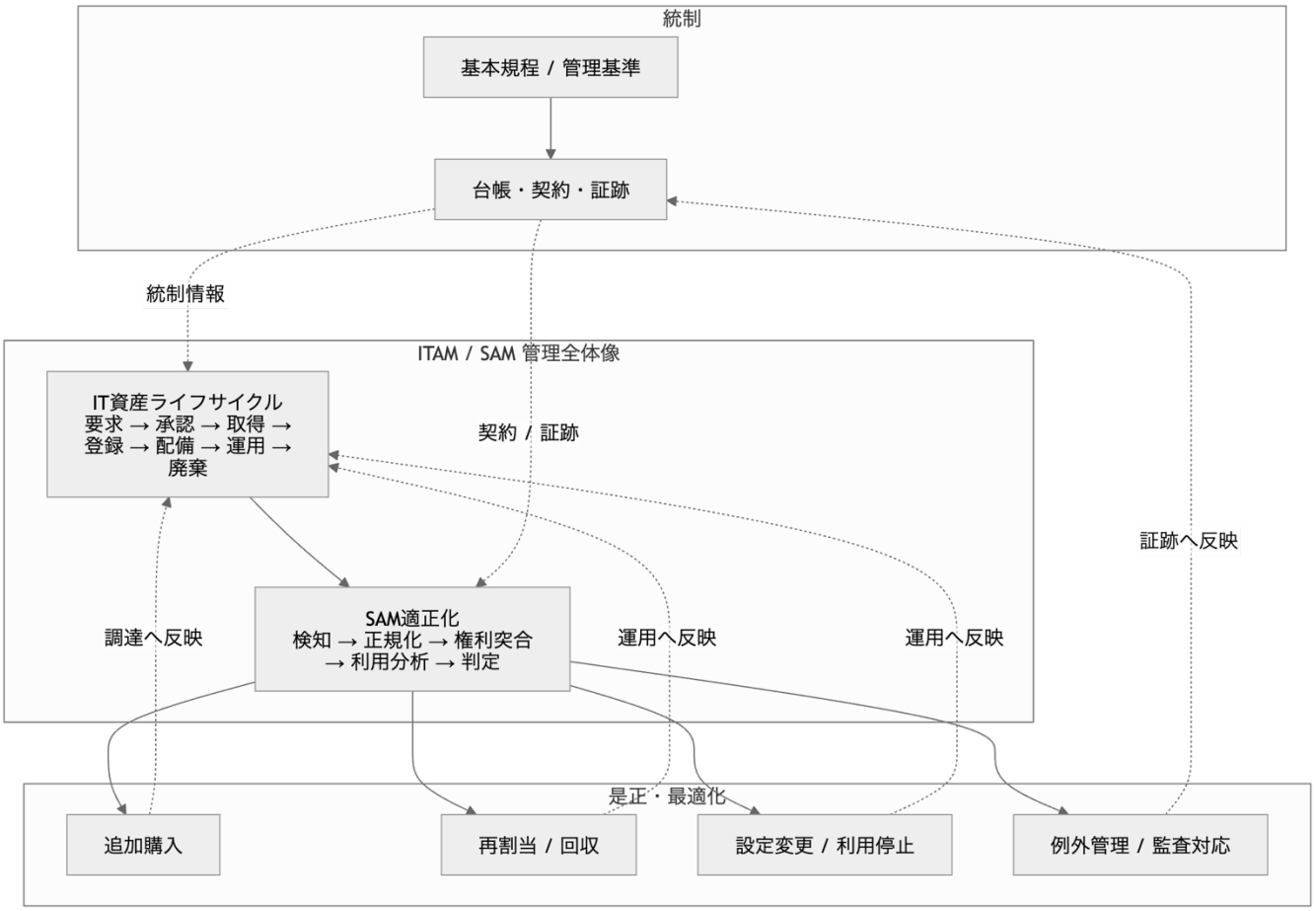
ISO/IEC TS 19770-10 は、ITAM 実装を「管理システムプロセス」「機能管理プロセス（データ/ライセンス/セキュリティ/契約・関係/財務/変更等）」「ライフサイクルプロセス（仕様→取得→展開→運用→廃棄）」として整理している。[10] 本章は、この整理を“導入手順”と“運用ワークフロー”に変換する。

実装手順（大手企業向け・統合実装）

1. **スコープ確定**：法人範囲、資産カテゴリ（HW/SW/SaaS/仮想/モバイル）、対象環境（クラウド/オンプレ）を決め、除外は理由と期限を明記。ISO/IEC 19770-1 は、スコープ定義を前提に要求事項を適用する。[23]
2. **統治体制（RACI）確定**：CIO/CISO/購買/法務/財務/監査/ITAM/SAM/ITSM の役割とエスカレーションを定義。経営層の責務と重要指示事項を明確化する日本のガイドラインとも整合させる。[4]
3. **SoR 設計**：台帳・契約・検知・ID・費用の“正”を定義し、二重管理を抑止（SoR 不明確は不整合の主要因）。NIST は集中インベントリや自動更新の重要性を示す。[13]
4. **資産分類・識別子標準化**：資産 ID、命名規則、タグ（クラウド）、SW 正規化辞書、SaaS カタログを設定。ISO/IEC 19770-2/6 のタグ概念（SWID/HWID）を取り込み、識別精度を上げる。[24]
5. **検知基盤確立**：端末/サーバ検知（エージェント等）、SaaS 検知（SSO ログ等）、クラウド API 収集を整備。
6. **契約・権利台帳の整備**：注文・契約・メトリクス・権利（エンタイトルメント）を構造化し、監査に耐える証跡リンクを付与（ISO/IEC 19770-3 は権利の原本優先性を明記）。[25]
7. **コアプロセス（取得→配備→運用→廃棄）を ITSM に埋め込む**：要求/変更/構成管理に ITAM ゲートを設定。ITIL の「IT 資産管理」「サービス構成管理」の狙いと整合。[2]
8. **トップベンダ優先の SAM 適正化（ELP）**：監査リスク・費用影響の大きいベンダ順に、検知→正規化→権利突合→是正を回す（下記の監査要件を前提に）。[26]
9. **例外・既知逸脱の棚卸**：BYOL、DR、検証環境、M&A 移管、OEM、地域差等を例外プロセスで管理。
10. **プライバシー・越境移転統制の実装**：SaaS・委託・海外拠点での個人データ取扱いと越境移転の要件（情報提供、同意、継続的確保措置等）を、審査・契約条項・運用手順に落とす。[27]
11. **監査パック自動化**：証跡（契約・インベントリ・利用量・是正履歴）を“いつでも切り出せる”形で保管。ISO/IEC 19770-11 の監査・認証思想とも整合。[21]

12. **KPI/継続改善（PDCA）**：棚卸差分、台帳品質、監査指摘、コスト削減、未使用回収、SaaS 最適化等を定例会で回す（19770-10 が示す「評価と改善」も包含）。[28]

運用プロセス（統合ワークフロー図）



（補足：ISO/IEC 19770-4 は利用量測定（RUM）の情報構造標準を定め、利用量データを“統一形式で扱う”方向性を示す。[29]）

監査・コンプライアンスチェックリスト

本チェックリストは、(1)標準準拠（ISO/IEC 19770-1/10）、(2)セキュリティ統制（NIST/ISO2700x）、(3)プライバシー（PPC ガイドライン等）、(4)ベンダ監査要件、の観点で“監査で見られる証跡”を中心に構成する。ISO/IEC 19770-1 が「内部・外部が能力評価に用い得る」とする前提から、証拠（記録）を必須に置く。[30]

統制領域別チェック（代表例）

統制領域	監査質問（チェック）	典型証跡（Evidence）	関連根拠（例）
ガバナンス	スコープは文書化され、対象資産カテゴリ（HW/SW/SaaS/仮想/モバイル）と法人範囲が明確か	スコープ定義書、規程、例外一覧	ISO/IEC 19770-1（スコープ・要求事項）[9]
体制（RACI）	CIO/CISO/購買/法務/財務/ITAM/SAM/ITSM の責任分界が明確か	RACI、会議体議事録、承認履歴	サイバーセキュリティ経営ガイドライン（経営者・CISO 等の指示）[4]
インベントリ	インベントリはインストール/削除/更新時に更新されるか、集中リポジトリを持つか	CMDB/台帳、収集設定、棚卸結果	NIST SP 800-53（CM-8 更新/集中/検知）[13]
不正資産/不正ソフト	未承認ソフト/機器を自動検知し、遮断/隔離等の対応が定義されているか	検知ルール、是正チケット、隔離ログ	NIST SP 800-53（CM-8(3) 等）[17]
契約・権利	契約原本（注文/契約/証書）に紐づく権利台帳があり、契約が優先であることが明記されているか	契約リポジトリ、権利台帳、メトリクス定義	ISO/IEC 19770-3（原本優先性）[25]
利用量	利用量（起動/利用時間等）取得・再割当基準が定義され、継続的に見直されているか	利用量レポート、再割当記録	ISO/IEC 19770-4（RUM）[31]
SaaS 統制	承認前審査、SSO/IAM 連携、退会・データ削除、シャドーIT 対策があるか	SaaS 審査票、SSO 連携証跡、退会ログ	ISO/IEC 27017/27018（クラウド統制補助）[19]
越境移転/委託	外国第三者提供に関する本人同意・情報提供、継続確保措置・定期確認が運用されているか	情報提供文面、同意取得記録、委託先評価	PPC ガイドライン（外国第三者提供編）[18]
ベンダ監査対応	監査受付～範囲確定～証跡提出～是正の手順が標準化されているか	監査対応手順、監査パック、レビュー記録	ISO/IEC 19770-11（監査・認証機関要件）[21]
特定ベンダ要件	監査・検証要件（例：Oracle LMS、IBM サブキャパシティ）を満たすデータ・ツール要件があるか	LMS/ILMT 関連証跡、計測レポート	Oracle LMS/パンフ、IBM ILMT FAQ [32]
OSS	OSS のライセンス遵守プロセス（台帳、承認、配布/提供時の義務）が定義されているか	OSS 台帳、レビュー記録、配布物の NOTICE 等	ISO/IEC 5230（OpenChain）[16]
セキュリティ/プライバシーMS	ISMS/PIMS（未指定）の枠組みに ITAM/SAM 統制が結合しているか	ISMS/PIMS 方針、リスク評価、適用宣言	ISO/IEC 27001（ISMS 要求事項）、ISO/IEC 27701（PIMS）[33]

（補足：国内法令は、国家サイバー統括室がサイバーセキュリティ関連法令として、個人情報保護法、著作権法、不正アクセス禁止法等を例示している。ITAM/SAM は“資産統制”であり、これら法令・契約遵守の実装レイヤとして機能する。[34]）

導入ロードマップと優先度・工数見積り

以下は、**管理対象規模が未指定**であるため、一般的な大手企業の複雑性（複数拠点・複数システム・クラウド混在）を前提にした“レンジ見積り”である。実数（端末/サーバ/SaaS/契約数、成熟度、外部委託範囲、M&A 頻度等）により大きく変動する（未指定）。ISO/IEC TS 19770-10 が示すように、ライフサイクルだけでなく、データ/ライセンス/セキュリティ/契約/財務/変更など横断プロセスを同時に整備する必要があるため、大手企業では段階導入（スモールスタート＋拡張）が現実的である。[35]

フェーズ	期間目安	主要成果物（抜粋）	優先度	工数目安（人日レンジ）	依存・前提（未指定は未指定）
企画・現状評価	0–2か月	スコープ定義、現状成熟度診断、文書体系ドラフト、SoR 方針	高	40–120	経営スポンサー確定（未指定）、現行台帳抽出可否（未指定）
統治確立・基盤整備	2–5か月	統合基本規程・基準の制定、RACI 確定、台帳項目・ID 体系、棚卸設計	最優先	120–300	稟議・承認期間（未指定）、法務/購買連携（未指定）
ツール連携・データ品質向上	4–9か月	ITSM/CMDB/SAM 連携、検知基盤整備、正規化辞書、品質 KPI 運用	高	250–600	採用ツール（未指定）、API 可否（未指定）
トップリスク領域の SAM 適正化	6–12か月	主要ベンダの ELP、監査パック雛形、是正運用（再割当等）	高	200–500	契約原本の集約状況（未指定）、仮想化条件（未指定）
SaaS/クラウド統制拡張	9–15か月	SaaS 審査・SSO 連携・退会、クラウドタグ標準、コスト配賦	中–高	200–550	SSO/IAM/MDM 導入状況（未指定）
継続改善・監査自動化	12–18か月	定期棚卸の安定運用、監査対応の半自動化、KPI 改善サイクル	中	120–350/年	内部監査頻度（未指定）、改善会議体（未指定）

コスト管理の成熟化（クラウド/サブスク領域）は、FinOps の Inform→Optimize→Operate の反復を“ITAM/SAM の利用量・費用配賦”に接続すると、運用として回しやすい。[36]

参考出典一覧

以下は、本テンプレートの設計・条文観点・監査観点を支える原典（公式優先、日本語優先を含む）である。

- ISO/IEC 19770-1:2017（ITAMS 要求事項、適用範囲、ISO 55001 との関係）[9]
- ISO/IEC TS 19770-10:2025（ITAM 実装ガイダンス：管理システム／機能管理／ライフサイクルのプロセス整理）[10]
- ISO/IEC 19770-5:2015（ISO/IEC19770 ファミリー概観、ITAM/SAM 導入、用語・定義）[37]
- ISO/IEC 19770-2:2015（SWID タグ：ソフトウェア識別タグ仕様）[38]
- ISO/IEC 19770-3:2016（エンタイトルメントスキーマ：契約原本優先性の前提を含む）[25]
- ISO/IEC 19770-4:2017（RUM：利用量測定情報構造）[31]
- ISO/IEC 19770-6:2024（HWID タグ：ハード識別タグ、SWID との対比）[39]
- ISO/IEC 19770-11:2021（ITAMS 監査・認証機関の要求事項）[21]
- ISO/IEC TS 19770-13（ITAMS へサステナビリティ観点を組み込むガイダンス：※将来拡張領域）[40]
- SAMAC 公開資料：JIS 化状況・ITAM 標準（日本の標準化・実装の文脈）[41]
- ITIL 4（Practice Guide の共通構造、IT 資産管理/サービス構成管理の目的）[42]
- NIST SP 800-53 Rev.5（資産・構成要素インベントリ、集中リポジトリ、不正検知等の管理策）[3]
- NIST Cybersecurity Framework 2.0（CSF 2.0：リスク理解・評価・優先付け・コミュニケーションの枠組み）[43]
- NIST SP 800-137（継続的モニタリング：資産可視性・脅威/脆弱性認知・統制有効性の可視化）[44]
- NIST SP 800-161（サプライチェーン C-SCRM：方針・計画・リスク評価の統合）[45]
- NIST SP 800-218（SSDF：ソフトウェアの安全な開発・調達の基礎）[46]
- 個人情報保護委員会：個人情報保護法ガイドライン（通則編、外国第三者提供編：越境移転の情報提供・同意・継続確保措置等）[5]
- 経産省：サイバーセキュリティ経営ガイドライン Ver3.0（大企業も対象、3 原則・重要 10 項目）[47]

- 国家サイバー統括室：サイバーセキュリティ関連法令リンク（個人情報保護法、著作権法、不正アクセス禁止法等の位置づけ）[48]
- 警察庁：不正アクセス対策（不正アクセスの定義・対策、関連法令リンク）[49]
- Microsoft：SAM ベストプラクティス資料（Download Center 掲載）および SAM ソリューション概要（Partner 向け）[50]
- Oracle：Oracle License Management Services（公式ライセンス機関としての位置づけ、監査サービス等）[51]
- IBM：サブキャパシティと ILMT 要件（必須性、期限、代替ツール等）[52]
- OSS 遵守：ISO/IEC 5230（OpenChain：OSS ライセンス遵守プログラムの要求事項）[16]
- CoSWID：IETF RFC 9393（SWID の簡潔表現：ISO/IEC 19770-2 との関係）[53]
- クラウド統制：ISO/IEC 27017（クラウド向け統制ガイダンス）、ISO/IEC 27018（クラウド PII 処理者向けガイダンス）、ISO/IEC 27001（ISMS 要求事項）、ISO/IEC 27701（PIMS 要求事項）[54]
- コスト最適化：FinOps Foundation（FinOps 定義、Inform/Optimize/Operate）[20]

---

[1] [9] [12] [23] [30] ISO/IEC 19770-1:2017 - Information technology — IT asset management — Part 1: IT asset management systems — Requirements

https://www.iso.org/standard/68531.html

[2] ITIL 4 Practitioner: IT Asset Management |

https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1/itil-4-practitioner-it-asset-management-3792

[3] [13] [17] Security and Privacy Controls for Information Systems and Organizations

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[4] [47] meti.go.jp

https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

[5] 個人情報の保護に関する法律についてのガイドライン（通則編） ｜個人情報保護委員会

https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

[6] [26] [32] [51] License Management Services | オラクル | Oracle 日本

https://www.oracle.com/jp/corporate/license-management-services/

[7] [37] ISO/IEC 19770-5:2015 - Information technology — IT asset management — Part 5: Overview and vocabulary

https://www.iso.org/standard/68291.html

[8] [15] [24] [38] ISO/IEC 19770-2:2015 - Information technology — IT asset management — Part 2: Software identification tag

https://www.iso.org/standard/65666.html

[10] [28] [35] ISO/IEC TS 19770-10:2025 - Information technology — IT asset management — Part 10: Guidance for implementing ITAM

https://www.iso.org/standard/86588.html

[11] [42] Reader's manual: ITIL 4 Practice Guide | Axelos

https://uat2.axelos.com/resource-hub/practice/readers-manual-itil-4-practice-guide

[14] ITIL 4 Practitioner: Service Configuration Management |

https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1/itil-4-practitioner-service-configuration-management-3800

[16] ISO/IEC 5230:2020(en), Information technology

https://www.iso.org/obp/ui?utm_source=chatgpt.com

[18] [27] 個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）｜個人情報保護委員会

https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore

[19] [54] ISO/IEC 27017:2015 - Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

https://www.iso.org/standard/43757.html

[20] What is FinOps?

https://www.finops.org/introduction/what-is-finops/?utm_source=chatgpt.com

[21] ISO/IEC 19770-11:2021 - Information technology — IT asset management — Part 11: Requirements for bodies providing audit and certification of IT asset management systems

https://www.iso.org/standard/77741.html

[22] License Management Services: Advice, Support and Expert Guidance for Making the Most of Your Oracle Investments

https://www.oracle.com/assets/license-mgmt-services-interactive-070709.pdf

[25] ISO/IEC 19770-3:2016 - Information technology — IT asset management — Part 3: Entitlement schema

https://www.iso.org/standard/52293.html

[29] [31] ISO/IEC 19770-4:2017 - Information technology — IT asset management — Part 4: Resource utilization measurement

https://www.iso.org/standard/68431.html

[33] ISO/IEC 27001:2022 - Information security management systems

https://www.iso.org/standard/27001

[34] [48] 法令 - 国家サイバー統括室

https://www.cyber.go.jp/law/lawlink.html

[36] FinOps Phases

https://www.finops.org/framework/phases/?utm_source=chatgpt.com

[39] ISO/IEC 19770-6:2024 - Information technology — IT asset management — Part 6: Hardware identification tag

https://www.iso.org/standard/77642.html

[40] ISO/IEC TS 19770-13 - Information technology — IT asset management — Part 13: Guidance on the incorporation of sustainability aspects in an IT asset management system

https://www.iso.org/standard/88836.html

[41] samac.or.jp

https://www.samac.or.jp/manage/wp-content/uploads/2022/04/ITAM-Standard-Ver.1.0.pdf

[43] The NIST CSF 2.0 is Here! - CSRC

https://csrc.nist.gov/news/2024/the-nist-csf-20-is-here?utm_source=chatgpt.com

[44] Information Security Continuous Monitoring (ISCM) for ...

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf?utm_source=chatgpt.com

[45] NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk ...

https://csrc.nist.gov/pubs/sp/800/161/r1/final?utm_source=chatgpt.com

[46] SP 800-218, Secure Software Development Framework ...

https://csrc.nist.gov/pubs/sp/800/218/final?utm_source=chatgpt.com

[49] 不正アクセス対策｜警察庁 Web サイト

https://www.npa.go.jp/bureau/cyber/countermeasures/unauthorized-access.html

[50] Download Software Asset Management (SAM) from Official Microsoft Download Center

https://www.microsoft.com/en-us/download/details.aspx?id=31382

[52] サブ・キャパシティーに関する FAQ IBM License Metric Tool（ILMT）

https://www.ibm.com/jp-ja/software/passportadvantage/subcapfaqilmt

[53] RFC 9393 - Concise Software Identification Tags

https://datatracker.ietf.org/doc/rfc9393/