【モデルプラン】

IT統制整備 標準ロードマップ

IPO準備（N-2期）・従業員50〜200名規模のモデルケース

本資料は、SecuROI創業者が事業会社のIPO準備・IT統制実務で用いてきた計画フレームを、**匿名化・一般化した標準例（モデルプラン）**です。**特定企業の導入事例ではありません。**実際の期間・投資・体制は各社の状況により異なります。

0. このモデルの出発点（よくある現在地）

- 従業員の私物PC（BYOD）比率が高く、会社が端末を把握・制御できていない
- ID・アカウントが各SaaSで個別管理され、退職者アカウントの削除が手作業と記憶に依存している
- 監査法人のショートレビューで、IT統制（ITGC）について初回の指摘・コメントを受けた

この3つが揃っている状態は、IPO準備期の企業として珍しくありません。重要なのは「どこから始まったか」を記録し、そこからの推移を示せるようにすることです。診断（20問・15分）は、この出発点を数値として確定させる作業にあたります。

1. 3つの水準 —— 「どこまでやるか」を先に決める

	水準A：現状維持	水準B：IPO実務標準	水準C：先行投資
位置づけ	リスク残存（監査実務で指摘対象になりやすい状態）	IPO実務で一般に求められる水準	自動化・高度化による将来の運用負荷削減
主な内容	何もしない	ID一元管理（SSO）・会社支給端末＋MDM・ログの改ざん耐性ある保持・EDR	水準Bに加え、入退職の自動同期（SCIM）・SIEM・CASB等
費用感	追加投資ゼロ。ただし後述の「現状維持のコスト」が掛かり続ける	1人あたり月額 **約1万〜1.5万円**（下記出典）	水準Bの1.5〜2倍程度
体制	—	兼任1名で運用可能な設計にできる	専任0.5〜1名相当を想定

水準の選び方：経営会議は「やる/やらない」の二択では紛糾しますが、**「どの水準か」の三択なら判断が進みます。**IPO準備企業の実務では水準Bが標準的な着地です。現状維持（水準A）が無料ではないことに注意してください——手作業のID管理・端末不備の対応時間・監査指摘への後追い対応は、見えない人件費として掛かり続け、組織拡大とともに増えます。

> **費用感の出典**：IPO標準相当のツール群（SSO：1ユーザー月額300〜500円程度、端末管理・セキュリティ統合スイート：同2,000〜4,000円程度、ビジネスチャット上位プラン差額・パスワード管理等：同数百円〜、端末のリース/レンタル：機種により同2,000〜10,000円程度）の公表価格の積算によるレンジです。個々の製品選定・構成により変動します。

2. フェーズド・ロードマップ（審査から逆算した目安）

アンカーは自社が動かせない外部日程です：**監査法人のショートレビュー** → **N-2期末** → **N-1期** → **上場審査**。以下はN-2期に着手した場合の標準的な流れです。

Phase 1｜土台（1〜3ヶ月目）：鍵をひとつにする

- **実施**：SSO導入・全SaaSのアカウント棚卸し・退職者ID即時削除フローの確立
- **到達点**：「退職者のアクセスを、1操作で全サービスから遮断できる」状態
- **監査への説明**：「IDはSSOで一元管理しており、退職時は当日中に全アクセスを停止します」
- **稟議イベント**：Phase 1着手前に、水準の選択と年間予算枠を経営会議で確定（ここを飛ばすとPhase 2の端末調達で稟議が二度手間になります）
- ⚠ よくあるつまずき：SSO対象のSaaS棚卸し漏れ。部門が個別契約したツールが後から見つかり手戻りになります。着手時に経費精算データからSaaS利用を洗い出すのが定石です
- 📊 測定点：ここで再診断すると、ID・アクセス管理領域のスコアが動いているはずです

Phase 2｜資産（3〜6ヶ月目）：端末を会社の管理下に置く

- **実施**：会社支給端末への切り替え（購入でなくリース/レンタルで初期費用を平準化）・MDM登録・BYODの段階的解消
- **到達点**：「業務データに触れる端末を、会社がすべて特定・制御している」状態
- **監査への説明**：「全端末をMDMで管理し、紛失時は遠隔消去できます。資産台帳は自動生成です」
- **稟議イベント**：端末調達の契約（リース/レンタルは月額費用なので、初期一括購入より稟議が通りやすい構造にできます）
- ⚠ よくあるつまずき：BYOD回収の現場反発。移行期間と代替手段（私物スマホはアプリ管理＝MAMで会社領域のみ制御等）を先に示さないと停滞します
- 📊 測定点：資産・物理管理領域のスコア

Phase 3｜証跡（6〜9ヶ月目）：運用していることを証明できるようにする

- **実施**：ログの改ざん耐性ある保持設定・定期的な権限棚卸しの運用開始・インシデント対応手順の文書化
- **到達点**：「言われた時に、記録を出せる」状態
- **監査への説明**：「操作ログは利用者側で消去できない形式で保持し、権限は四半期ごとに棚卸ししています」
- ⚠ よくあるつまずき：ログ保持設定の遡及不能。**ログは設定した日からしか貯まりません。**「監査前に慌てて有効化しても過去分は存在しない」——早期着手が効く代表例です
- 📊 測定点：システム運用・証跡領域のスコア

Phase 4｜定着（9〜12ヶ月目・N-1期へ）：仕組みを回し続ける

- **実施**：四半期ごとの定点測定・監査法人への整備状況の定期報告・新入社員/新規SaaSを仕組みに乗せる運用
- **到達点**：「整備した」でなく**「運用実績が推移として残っている」**状態——審査で問われるのは後者です
- 📊 測定点：全領域。ここまでの四半期ごとの測定が「推移の線」として揃い、そのまま監査法人・審査への提出資料になります

3. このモデルプランの使い方

診断結果（現在地）と本モデルを重ねると、「自社はどのPhaseから始めるべきか」「次の四半期に取り組む3つは何か」が具体化します。単発診断スタンダードの読み合わせでは、この重ね合わせを一緒に行います。なお、**本モデルの各Phaseの到達を当社が判定・保証するものではありません。**順序と目安を示すのが本資料の役割です。

作成：小山幸輝（こやま よしき）｜合同会社SecuROI 代表。情報システム・セキュリティの現場に20年以上。警察庁関連を経て、世界4大監査法人グループのセキュリティコンサルティングファームで監査対応に従事。その後、事業会社で統制の内製化とIPO準備の実務を担う。

ご相談：https://www.securoi.com/contact
お問い合わせ後、担当よりご返信します。

合同会社SecuROI
https://www.securoi.com
最終更新：2026年7月