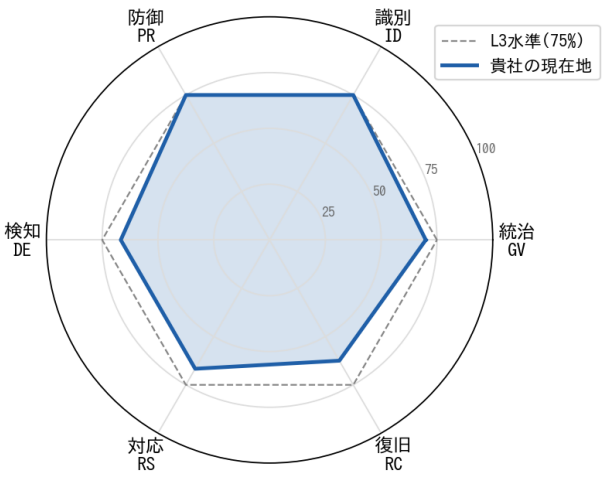
セキュリティ投資判断レポート ＜経営サマリー＞

株式会社セイカ・ヘルステック | 2026Q3 | 診断基準：NIST CSF 2.0・ITGC観点

株式会社セイカ・ヘルステックの2026Q3時点における総合セキュリティスコアは69.31%、自走度は83.33%です。自走度が高く、社内での継続的な取り組み姿勢は評価できる一方、検知・対応・復旧の各機能が相対的に低く、IPO審査およびJ-SOX対応に向けた優先的な強化が求められる段階にあります。

セキュリティ成熟度（NIST CSF 2.0）



投資の正当化:2つの時間軸
【IPO準備（短期）】 J-SOX/ITGC整備に向けた明確な締切と優先度があります。
【中長期：事業成長】 セキュリティ成熟度の継続的な向上が、将来の取引先・顧客要件への対応力を高め、受注競争力に育ちます。
J-SOX/ITGC整備には明確な審査スケジュールが伴うため、最優先（L2）ドメインの対処を先行させ、引き上げ対象（L3）ドメインは並行して計画的に整備を進めることが、IPOタイムラインとの整合性を保つうえで重要です。各施策の完了証跡を早期に蓄積することで、監査法人への説明資料としても活用できます。

ITGC観点（IPO準備度）— 統制の土台となる主要領域

※ セキュリティ成熟度スコアと審査の合否は直結しません。下記は準備の目安です（最終的な要求水準は監査法人の判断によります）。

ITGC領域	現在地	準備度の目安
アクセス管理	L3 — 整備済み	引き上げ対象
資産管理	L3 — 整備済み	引き上げ対象
変更管理	L3 — 整備済み	引き上げ対象
運用管理	L2 — 部分対応	最優先
統制環境	L2 — 部分対応	最優先

これらの現状を踏まえた具体的な改善施策は、後述の「経営の意思決定事項」に整理しています。

セキュリティ投資判断ROIサマリー ※すべて想定値・前提依存レンジ推定

対策なし時の想定最大損失：8.7億円

JCICサイバーリスク数値化モデルに基づく想定（事業停止損失・法的制裁金・インシデント対応費用＋保有個人データ件数に応じた想定損害賠償額）。幅は保有個人データ件数の業界平均レンジ（下限～上限）の違いによるもので、他の算定要素は下限・上限で同一です。

ROI区分	想定インパクト(年間)
攻めROI（受注機会拡大）	2700万円～6300万円/年
守りROI（損失削減・改善分）	443万円/年
効率ROI（工数削減）	145万円/年
合計	3288万円～6888万円/年

※ 守りROIは「改善により実際に削減できる損失額」のみ計上（最大損失・現状リスクは上行参照）

SecuROI投資額：年22万円（税込）で、四半期ごとの診断・ROI可視化・IPO準備の進捗管理ができます。
参考：守りROI（業界平均ベースの想定値）は投資額を上回る水準ですが、実際の効果は貴社の状況（保有データ量・事業規模等）により大きく異なります。日本企業の約半数は年1千万〜5千万円を投資（経産省/IPA調査）しており、SecuROIはその中で診断・ROI可視化を年22万円（税込）で担います。

※ 本レポートのROIは2026-09-07生成時点（2026Q3・診断スコア69.31%）の診断・施策状況に基づく試算です。すべて前提依存のレンジ推定。最新の施策状況はダッシュボードでご確認いただけます。
出典（算定モデル）：JCICサイバーリスク数値化モデル2022 / JNSA JOモデル / 経産省・IPA「企業のCISOやCSIRTに関する実態調査2017」（従業員300人以上・N=755）。業界平均の初期値は、公開統計を参考に当社が設定した想定値です（ご入力いただいた項目は、その値のみを用います）。なお、診断スコアから事故発生確率への変換は、当社の想定モデルによるものです。

今四半期の優先タスク

※ 今回の回答から機械的に選んだ、着手の優先順です。四半期ごとに入れ替わります。

1. 外部送信監視（DLP）の導入［関連設問：Q7］
2. インシデント対応手順の制定と年次訓練の実施［関連設問：Q8］
3. 重要委託先の選定基準整備と定期評価（SOC報告書等の入手）［関連設問：Q12・Q14］

経営の意思決定事項(改善施策ロードマップ･初回確定)

※ 初回診断時に確定し、以降の四半期を通じて継続管理する改善計画です（ステータスはダッシュボードで随時更新）。上の「今四半期の優先タスク」（今回の回答から機械的に選定した着手順）とは別の一覧です。

1. アクセス管理の基盤整備：退職者アカウント停止・MFA全社適用・権限棚卸しの実施［関連設問：Q1・Q2・Q5］
2. 変更管理プロセスの確立：承認・テスト・記録手順と職務分掌の文書化［関連設問：Q3・IPO-Q1・IPO-Q2］
3. 統制環境の整備：セキュリティ方針文書化とリスク評価・経営報告の仕組み構築［関連設問：Q11・Q12・Q13・Q14］
4. 資産・データ管理の可視化：IT資産一覧・データ重要度分類・個人データ所在の把握［関連設問：Q10・Q15・Q16・Q4］
5. 運用管理体制の構築：ログ集約・インシデント対応手順・バックアップ復旧テストの整備［関連設問：Q6・Q7・Q8・Q19・Q20］

※最終的な要求水準・適用範囲は監査法人の判断によります。 各施策の社内での進め方は、ダッシュボードの施策ToDoに設問ごとに掲載しています。外部活用の要否は体制・リソースにより異なります。 本スコアは較正中の相対指標であり、価値は単発の絶対値でなく四半期ごとの推移にあります。