

内部監査報告書

サンプル SaaS 株式会社 内部監査室

情報セキュリティ・IT 全般統制の内部監査

AI 生成ドラフト・会計士レビュー前提。会社・人物・数値はすべて架空

対象期間	2028 年 3 月期（申請期）。母集団期間 2026 年 7 月 1 日～2027 年 6 月 30 日・アクセス権の基準日 2027 年 6 月 30 日・本調査 2027 年 7 月 7 日～7 月 30 日	文書番号	内監報第 2027-01 号
報告日	2027 年 8 月 27 日（金）	機密区分	社外秘（会計監査人および主幹事証券への提供を除き、社外への開示を禁ずる）
宛先	代表取締役社長 殿 監査役会 御中		
発信	内部監査室長		
配布先	開発責任者 運用（SRE）責任者 情報システム責任者 セキュリティ管理責任者 コンプライアンス責任者 会計監査人（写し）		

1. 総合意見

結論区分: 一部要改善

【総合意見：一部要改善】サンプル SaaS 株式会社の情報セキュリティ及び IT 全般統制について、2026 年 7 月 1 日～2027 年 6 月 30 日を母集団期間として 14 手続を実施した。収益計上を支える ITGC（契約～課金～会計の整合、手作業仕訳、SLA とサービスクレジット）、バックアップと復旧、個人データの取扱い、研修・内部通報・利益相反管理については、統制が有効に機能していると認められた。一方で、(1)開発者がマルチテナント本番環境に恒常的な書込/デプロイ権限を保持し開発と運用が分離されていないこと（F-01・整備不備・重要度高）、(2)クラウド root を含む特権 ID が共有され操作者を個人まで特定できないこと（F-02・運用不備・重要度高）に、財務報告の信頼性と顧客データの保全の双方へ影響し得る残余リスクが残る。加えて、退職・異動時の失効遅延（F-03）、承認ゲートを通さない本番デプロイ（F-04）、個人情報漏えいを想定したインシデント通知手順の不足（F-05）、重要委託先の契約条項と SOC 報告書評価の不足（F-06）を重要度中として指摘する。上場申請期であることに鑑み、F-01・F-02 は内部管理体制の有効性に関する説明の前提となるため、暫定策を 2027 年 9 月末までに、恒久策を 2027 年 12 月末までに完了することを求める。なお、当年度に監査対象としなかった決算・財務報告プロセス、BCP、労務、ガバナンスの各領域は、第二線の自己点検と本監査の一部手続（P-08・P-11）で部分的にカバーしたにとどまり、翌期に独立的評価を行う予定である。本監査はグローバル内部監査基準（2025 年 1 月 9 日発効）に準拠して実施した。

2. 監査の概要

目的	サンプル SaaS 株式会社(従業員 150 名(2027 年 3 月末。2025 年 6 月の 120 名から採用計画どおり増加)、クラウド型 SaaS を単一プロダクトで多数テナントに提供)の情報セキュリティ及び IT 全般統制(ITGC)の整備・運用状況を、グローバル内部監査基準(GIAS、2025 年 1 月 9 日発効)に基づきリスクベースで独立的・客観的に評価する。少人数開発体制で DevOps/CI-CD により開発～本番デプロイが高頻度に行われる同社特性を踏まえ、(a)マルチテナント本番環境へのアクセス統制(開発と運用の分離)、(b)クラウド IAM/root 等の特権 ID 管理、(c)変更管理・脆弱性/パッチ対応、(d)セキュリティインシデント対応(顧客テナント越境影響を含む)、(e)顧客個人情報の取扱いの適切性を確かめ、財務報告の信頼性(サブスクリプション課金=MRR/ARR の計上を支える ITGC)・業務の有効性/効率性・コンプライアンス(個人情報保護法等)・資産の保全(顧客データ)の 4 目的への影響を検証する。
範囲	対象組織: サンプル SaaS 株式会社(従業員 150 名)の開発・運用(SRE)・情報システム・セキュリティ管理の各機能、及び関連するコンプライアンス・委託先管理・販売/課金機能。少人数ゆえ開発者と運用者の兼務が生じやすい点を重点。対象システム: 多数テナントが同居する本番 SaaS 基盤(パブリッククラウド上、IaC/CI-CD で運用)、サブスクリプション課金・請求システム、SSO/IdP(ID 管理基盤)、変更管理/チケットツール、監査ログ・SIEM 基盤、バックアップ基盤。対象勘定への影響: 売上高(月額サブスク=一定期間にわたる収益)・売掛金・返金負債(SLA 未達クレジット等の変動対価)の網羅性/正確性を支える ITGC。対象期間: 2026 年 7 月 1 日～2027 年 6 月 30 日の 12 か月をログ・変更・インシデントの母集団期間とし、収益/仕訳系は 2027 年 1 月～6 月の半期を重点とした。アクセス権の基準日は 2027 年 6 月 30 日。四半期報告書は 2024 年に廃止済みのため、半期・年次の決算関連統制期間と整合させている。
基準	社内規程(情報セキュリティ規程・アクセス管理規程・変更管理手順・インシデント対応手順・個人情報取扱規程・委託先管理規程・研修/内部通報/利益相反管理規程)、個人情報保護法及びガイドライン(漏えい等報告・本人通知の要件、委託先監督義務)、J-SOX(財務報告に係る内部統制の評価・監査の基準)の 3 点セット(業務記述書・フローチャート・RCM)、COSO 内部統制フレームワーク及び ITGC 評価の枠組み(COBIT 等。フレームワークの帰属は要照合)。※GIAS は内部監査部門自身を律する基準であり、被監査部門の統制を測る判断基準(criteria)としては用いない。
アプローチ	リスクベース・アプローチ。監査ユニバース→リスク評価(固有・残余)→キーコントロール連携(icfrLink)→監査プログラム→指摘の一気通貫で設計。ITGC は(1)アクセス管理(付与承認/失効の適時性=特権に限らず一般ユーザーも人事データと突合/定期棚卸)(2)変更管理・パッチ/脆弱性(3)運用(バックアップ/復旧・インシデント)の 3 領域で評価。DevOps 特性を踏まえ CI-CD パイプラインの承認ゲートとチケットの整合を重点検証。証跡突合・ログレビュー・再実施・分析は内部監査の権限(社内データ・ログ・台帳への直接アクセス)の範囲で実施し、クラウド/データ処理委託先へのデータ徴求・実査は取引基本契約の監査/立入検査条項・報告徴収権を権限根拠に行う(外部会計監査固有の残高確認等の転

	写ではない)。年度監査計画は監査資源(人員・工数・実施時期・監査種別)の配分を明示する(GIAS ドメイン IV/基準 9.4 内部監査計画の趣旨)。監査結果は経過報告を経て、最終報告を経営者及び監査役等・取締役会へ伝達する(GIAS の伝達要求=ドメイン V)。整備不備(統制のデザイン)と運用不備(統制の運用実態)を区分して評価する。
体制	監査責任者(内部監査室長・専任・CIA)1 名、外部専門家(IT 監査・CISA)の支援 1 名、担当 1 名 (N-2 期末に社長直轄で新設し、N-1 期に初回監査を実施した体制を拡充)。少人数組織のため被監査部門との独立性に留意し、第二線(情報セキュリティ管理部門・人事部門)からは独立性を保った説明協力のみを受ける。クラウド IAM/SIEM ログ解析は専門性補完のため上記外部専門家(CISA)が担当する(独立性・客観性の確保を前提)。
日程	予備調査 (2027 年 6 月 8 日～19 日。規程・体制・前回結果・クラウド構成/テナント分離設計・課金～会計のデータフローのウォークスルー、母集団範囲/抽出条件の確定) →リスク評価の確定・監査プログラムの承認 (6 月 18 日) →本調査 (2027 年 7 月 7 日～7 月 30 日。IAM 権限一覧/CI-CD デプロイログ/変更チケット/SIEM ログ/委託先 SOC 報告書を入手し、証跡突合・ログレビュー・再実施・分析を実施) →講評会 (8 月 6 日・被監査部門との事実確認) →報告書ドラフト (8 月中旬) →内部監査報告書の提出 (8 月 27 日) →追加手続 (9 月上旬・講評会で合意した事実確認事項の再検証) →フォローアップ (3 か月後・6 か月後)。

3. 発見事項の要約

- ・ 重要度の定義 (内部監査規程第 17 条・内部監査マニュアル) : 高=本番環境・顧客データ・収益データに直接関わる ITGC/情報セキュリティ統制の整備不備・運用不備で、補完統制によっても検出・是正が担保されないもの。中=統制の欠陥はあるが補完統制・自動制御により影響が限定され、期限内の是正で足りるもの。低=文書・記録・体制の整備上の不備で、顧客データ・財務報告への直接の影響が無いもの
- ・ 総合意見への集約: 「高」が 1 件以上あれば「一部要改善」以上とし、「高」が顧客データの漏えい又は財務報告の虚偽の事実を伴う場合は「不十分」。「高」が無く「中」以下のみであれば「有効 (改善余地あり)」

重要度別件数: 高 2 件／中 4 件／低 0 件 (計 6 件)

ID	件名	重要度	改善責任者	期限	状況
F-01	開発者がマルチテナント本番環境に恒常的アクセス権を保持 (職務分掌の整備不備)	高	情報システム責任者 (IAM 再設計の主管) / 運用 (SRE) 責任者 (break-glass 手順の主管)	2027-09-30	未着手
F-02	特権 ID (クラウド root・管理者) の共有と利用ログの個人紐付けの不足 (運用不備)	高	情報システム責任者	2027-09-30	未着手

ID	件名	重要度	改善責任者	期限	状況
F-03	退職・異動時のアクセス失効に遅延（一般ユーザーを含む・運用不備）	中	情報システム責任者／人事責任者	2027-10-31	未着手
F-04	承認ゲートを通過しない本番デプロイと緊急変更の事後承認の未了（運用不備）	中	開発責任者／運用（SRE）責任者	2027-11-30	未着手
F-05	個人情報漏えいを想定したインシデント通知手順の実効性が不十分（整備の不備）	中	セキュリティ管理責任者／コンプライアンス責任者	2027-11-30	未着手
F-06	重要委託先契約の個人情報・監査権条項とSOC報告書評価が不十分（整備の不備）	中	コンプライアンス責任者／情報システム責任者	2027-12-31	未着手

4. 発見事項の詳細

F-01 開発者がマルチテナント本番環境に恒常的アクセス権を保持（職務分掌の整備不備） [重要度高]

事実: 【欠陥種別:整備の不備】2027年6月30日時点のIAM権限一覧47件を職務マスタと全数突合したところ、開発担当9名が本番クラウド環境への恒常的な書込/デプロイ権限を保持し、うち3名はテナント横断の管理者ロール（AdministratorAccess相当）を有していた（P-01）。IAMポリシー上、開発ロールと運用ロールの境界が定義されておらず、恒常権限と緊急権限（break-glass）の区分ルールも存在しない。緊急アクセス発動6件のうち4件は、恒常権限を保持する開発者が自らの常用権限で対応しており、発動記録・事後承認が残っていなかった。

基準: 社内アクセス管理規程(最小権限・開発と運用の分離)、J-SOXのITGC(アクセス管理)における職務分掌の要求、個人情報保護法(不要アクセスの排除)。

原因: (1)【整備】従業員150名の少人数DevOps体制で開発と運用を兼務する前提のまま、IAMロールが職務単位に分割されずに設計されている。(2)【整備】恒常権限と緊急権限の区分ルールが規程・IAMポリシーのいずれにも定められていない。(3)【運用】緊急対応の便宜が優先され、break-glass手順が実質的に使われていない。

影響: 本番データ/プログラムの不正・誤変更により課金・収益データの正確性/網羅性が毀損し、他テナントの顧客データ漏洩を含む資産保全と財務報告の信頼性に影響するリスク。

改善提案: 開発者の恒常的な本番書込/デプロイ権限を撤廃し、緊急時のみの承認付き一時権限（break-glass）へ移行する。テナント横断の管理者ロールは付与対象を情報システム責任者に限定す

る。CI-CD の承認ゲートを必ず介在させ、付与・返却・操作ログのレビューを月次で定例化する。整備不備（統制デザイン）であり、権限設計の修正を優先する。

被監査部門の回答: 指摘に同意する。上場申請期であり内部管理体制の根幹に関わるため最優先で対応する。暫定策として、テナント横断の管理者ロールの付与を 2027 年 9 月末までに 1 名へ縮減し、恒常的なデプロイ権限保持者の月次レビューを開始する。恒久策の IAM ロール再設計と break-glass 手順の整備は 2027 年 12 月末までに本番反映する。

改善責任者・期限: 情報システム責任者（IAM 再設計の主管）／運用（SRE）責任者（break-glass 手順の主管）／2027-09-30

F-02 特権 ID（クラウド root・管理者）の共有と利用ログの個人紐付けの不足（運用不備） [重要度高]

事実: 【欠陥種別:運用の不備】特権 ID 全 14 件を検証した結果、クラウド root および DBA 権限の計 4 件が複数名で共有され、払出台帳と特権操作ログ（CloudTrail 相当）を突合しても操作者を個人まで特定できなかった（P-02）。root のうち 1 件は MFA が未設定であった。払出イベント 118 件から抽出した 30 件のうち、返却記録が残っていないものが 7 件あった。統制のデザイン（払出台帳による管理）は存在するため、運用不備に区分する。

基準: 社内アクセス管理規程(特権 ID 個別管理・操作記録の保持)、J-SOX の ITGC(アクセス管理)。

原因: (1) 【運用】共有 ID の廃止方針が定められておらず、緊急時に使い回す運用が定着している。(2) 【運用】払出後の返却確認が担当者の自主性に委ねられ、未返却を検出する仕組みがない。(3) 【整備】root の MFA 必須化がアカウント作成手順に組み込まれていない。

影響: 権限濫用・操作の否認可能性が高まり、不正アクセス・データ改ざんの検知と追跡が困難となる(資産保全・コンプライアンスへの影響)。

改善提案: 特権操作は個人 ID からの権限昇格（sudo／PAM）方式へ移行し、共有 ID を廃止する。root の MFA を必須化し、未設定を検出する定期チェックを設ける。特権操作ログの月次レビューと未返却の自動検出を制度化する。

被監査部門の回答: 指摘に同意する。root の MFA 未設定は 2027 年 8 月中に是正済みとする。共有 ID の廃止と権限昇格方式への移行は、PAM 製品の選定を含め 2027 年 12 月末までに完了させる。特権操作ログの月次レビューは 2027 年 9 月から開始する。

改善責任者・期限: 情報システム責任者／2027-09-30

F-03 退職・異動時のアクセス失効に遅延（一般ユーザーを含む・運用不備） [重要度中]

事実: 【欠陥種別:運用の不備】退職者 18 名・権限変更を伴う異動者 23 名の全アカウントを突合したところ、退職者 5 名で失効が人事イベント日から遅延しており（最長 23 日）、うち 2 名は連携 SaaS（チケットツール・SIEM）のアカウントが基準日時点で有効のまま残存していた（P-03）。異動者

では、旧部署の権限が削除されないまま新権限が追加された事例が6件あった。特権IDに限らず一般ユーザーでも生じている。

基準: 社内アクセス管理規程(退職・異動時の速やかな失効)、個人情報保護法(不要アクセスの排除)。

原因: (1)【整備】人事システムとID管理基盤(IdP)が連携しておらず、失効が情報システムへの個別依頼に依存している。(2)【整備】失効のSLA(期限)が定められていない。(3)【運用】連携SaaSはIdP経由でない個別アカウントが残り、棚卸の対象から漏れている。

影響: 退職者IDの残存により不正アクセス・顧客データ漏洩のリスク(資産保全・コンプライアンス)。

改善提案: 人事システムとIdPを連携して失効を自動化し、失効SLA(退職当日、遅くとも翌営業日)を定めて例外をモニタリングする。異動時は旧権限の削除を付与とセットの手順にする。IdP未連携のSaaSを洗い出し、棚卸の対象に加える。

被監査部門の回答: 指摘に同意する。残存アカウント2件は指摘当日に失効させた。失効SLAの規程化と異動時の旧権限削除の手順化を2027年10月末までに行い、人事とIdPの連携は2028年3月末までに実装する。

改善責任者・期限: 情報システム責任者/人事責任者/2027-10-31

F-04 承認ゲートを通過しない本番デプロイと緊急変更の事後承認の未了(運用不備) [重要度中]

事実: 【欠陥種別:運用の不備】本番変更1,284件のうち緊急変更33件を全件検証した結果、事後承認が完了していないものが11件あった(P-05)。通常変更から抽出した25件では、テスト結果の証跡が保存されていないものが3件あった。CI-CDデプロイログと変更チケットを全件突合した分析では、チケット番号を伴わない本番デプロイが期間中に9件検出された(うち7件は緊急変更、2件は設定変更)。パイプラインには承認ゲートが設定されているが、特定のロールがこれを迂回できる設定であった。

基準: 社内変更管理手順(申請・承認・テスト・移行分離・記録保持)、J-SOXのITGC(変更管理)。

原因: (1)【整備】パイプラインの承認ゲートに迂回可能なロールが存在する。(2)【運用】緊急変更の事後承認の期限が定められておらず、対応完了後に手続が放置される。(3)【運用】テスト結果の保存場所が手順に明記されていない。

影響: 未承認変更による課金ロジックの誤りやサービス障害、財務報告の信頼性・業務効率への影響。

改善提案: 承認ゲートの迂回を技術的に不可能にし(ロール設定の是正)、チケット番号を伴わないデプロイをパイプラインで拒否する。緊急変更の事後承認に期限(翌営業日)を設け、未了を週次で検出する。テスト結果の保存場所を変更管理手順に明記する。

被監査部門の回答: 指摘に同意する。未完了の事後承認11件は2027年8月末までに遡って処理する。パイプラインのロール設定是正とチケット必須化は2027年11月末までに実装する。

改善責任者・期限: 開発責任者/運用(SRE)責任者/2027-11-30

F-05 個人情報漏えいを想定したインシデント通知手順の実効性が不十分（整備の不備） [重要度中]

事実: 【欠陥種別:整備の不備】 インシデント 27 件のタイムラインを突合した結果、検知からエスカレーションまでの記録は残っていたが、マルチテナント環境で影響テナントを特定する手順が文書化されておらず、重大 3 件のいずれも影響範囲の確定に 3 営業日以上を要していた (P-09)。個人情報漏えい時の当局報告・本人通知の要否判断基準と時限が対応手順に定められていない。対応演習は母集団期間中に 1 回のみで、個人情報漏えいシナリオを含んでいなかった。

基準: 社内インシデント対応手順、個人情報保護法(漏えい等報告・本人通知の義務)。

原因: (1) 【整備】 対応手順がシステム障害を前提に作られており、個人データの越境影響を想定した記述がない。(2) 【整備】 個人情報保護法の報告・通知の要件が手順に落とし込まれていない。(3) 【運用】 演習の年間計画が定められていない。

影響: 漏洩発生時の報告遅延による法令違反・行政対応・信用毀損・損害賠償のリスク(コンプライアンス・資産保全)。

改善提案: 影響テナントの特定手順、報告・通知の判断基準と時限、エスカレーション経路を対応手順に明記する。個人情報漏えいシナリオを含む演習を年 1 回以上実施し、記録を残す。

被監査部門の回答: 指摘に同意する。対応手順の改訂を 2027 年 11 月末までに行い、改訂後の手順に基づく演習を 2028 年 1 月までに実施する。

改善責任者・期限: セキュリティ管理責任者／コンプライアンス責任者／2027-11-30

F-06 重要委託先契約の個人情報・監査権条項と SOC 報告書評価が不十分（整備の不備） [重要度中]

事実: 【欠陥種別:整備の不備】 重要委託先 5 社の契約を全数突合したところ、2 社で監査/報告徴収条項が欠落し、1 社で再委託の事前承認条項が定められていなかった (P-12)。SOC 報告書は 5 社中 3 社から入手していたが、評価記録が残っていたのは 1 社のみで、補完的ユーザー統制 (CUEC) の自社実装確認はいずれも行われていなかった。判断抽出した その他委託先 6 社では、個人情報保護条項を欠くものが 2 社あった。

基準: 社内委託先管理規程、個人情報保護法(委託先の監督義務)。

原因: (1) 【整備】 契約ひな形に個人情報・監査/報告徴収・再委託の条項が標準搭載されていない。(2) 【整備】 SOC 報告書の入手・評価の手順が委託先管理規程に定められていない。(3) 【運用】 委託先の重要度区分がなく、評価の深さが担当者判断に委ねられている。

影響: 委託先起因の情報漏洩時に監督義務違反・責任分界不明確による損害拡大リスク(コンプライアンス・資産保全)。

改善提案: 契約ひな形に個人情報・秘密保持・監査/報告徴収・再委託承認の条項を標準搭載し、既存契約は更新時に差し替える。SOC 報告書の年次入手と評価（対象範囲・例外事項・CUEC の自社実装確認）を手順化する。委託先を重要度で区分し、評価の深さを対応づける。

被監査部門の回答: 指摘に同意する。契約ひな形の改訂を 2027 年 10 月末までに行い、条項が欠落している 3 社は 2028 年 3 月末までの更新時に差し替える。SOC 報告書の評価手順の整備と CUEC の確認は 2027 年 12 月末までに実施する。

改善責任者・期限: コンプライアンス責任者／情報システム責任者／2027-12-31

5. 改善計画とフォローアップ

指摘 ID	改善アクション	状況	期限	備考
F-01	暫定策（テナント横断の管理者ロールを 1 名へ縮減・恒常デプロイ権限保持者の月次レビュー開始）を 3 か月後に検証する。恒久策（IAM ロールの職務単位への再設計と break-glass 手順の整備）は設計完了→本番反映→運用定着の段階で 6 か月後に再検証する。	未着手	2027-09-30	最優先。暫定策期日 2027/9/30、恒久策期日 2027/12/31。上場申請期であり、改善が遅延する場合は主幹事証券への説明が必要になるため監査役会へ即時報告する。 F-02 の権限昇格方式への移行と一体で確認する。
F-02	root の MFA 必須化（2027 年 8 月中に是正予定）を 3 か月後に証跡で確認する。共有 ID の廃止と権限昇格方式への移行、特権操作ログの月次レビュー開始を 6 か月後に検証する。	未着手	2027-09-30	暫定策期日 2027/9/30、恒久策期日 2027/12/31。未返却 7 件の是正状況もあわせて確認する。
F-03	失効 SLA の規程化と異動時の旧権限削除の手順化を 3 か月後に確認する。人事と IdP の連携実装は 6 か月後に検証し、実装後に退職者を再サンプルして失効経過日数を分析する。	未着手	2027-10-31	期日 2027/10/31（規程・手順）、2028/3/31（連携実装）。残存アカウント 2 件は指摘当日に失効済みのため証跡のみ確認する。
F-04	未完了の事後承認 11 件の遡及処理を 3 か月後に確認する。パイプラインのロール設定是正とチケット必須化は 6 か月後に、デプロイログと変更チケットの再突合により検証する。	未着手	2027-11-30	期日 2027/8/31（遡及処理）、2027/11/30（技術的抑止）。技術的抑止の実装後は、チケットを伴わないデプロイがゼロになることを再分析で確かめる。
F-05	対应手順の改訂（影響テナント特定手順・報告通知の判断基準と時限・エスカレーション経路）を 3 か月後に閲覧で確認	未着手	2027-11-30	期日 2027/11/30（手順改訂）、2028/1/31（演習）。演習は個人情報漏えいシナリオを含むことを要件とする。

指摘 ID	改善アクション	状況	期限	備考
	し、改訂後の手順に基づく演習の実施記録を6か月後に確認する。			
F-06	契約ひな形の改訂を3か月後に確認する。条項が欠落している3社の差し替えは更新時期に合わせて6か月後以降に追跡し、SOC 報告書の評価手順の整備と CUEC の自社実装確認を6か月後に検証する。	未着手	2027-12-31	期日 2027/10/31（ひな形）、2027/12/31（評価手順・CUEC）、2028/3/31（既存契約の差し替え）。差し替えは相手方との交渉を伴うため進捗を四半期で確認する。

改善状況は暫定策（早期に運用で止血）と恒久策（システム改修・契約更改のリードタイムを考慮）の二段階で管理し、本報告の3か月後（2027年11月）と6か月後（2028年2月）にフォローアップ監査を行う。重要度「高」の指摘が期限を超過した場合は監査役会へ報告する。

6. 監査役会・取締役会への付議事項

- ・ 上場審査への影響：F-01（開発者の恒常的な本番アクセス）は内部管理体制の根幹に関わるため、恒久策の本番反映時期が申請スケジュールに間に合うかを経営者と確認する必要がある
- ・ 第二線の体制：委託先管理（F-06）とインシデント対応（F-05）は第二線の自己点検でカバーされてきた領域であり、自己点検の設計そのものを見直すかを経営者に諮りたい
- ・ 内部監査の資源：当年度は内部監査室2名＋外部専門家0.2で情報セキュリティに25人日を配分したが、翌期は決算・財務報告プロセスとBCPの独立的評価を予定しており、体制の増強が必要になる見込み
- ・ 会計監査人との連携：F-04（変更管理）はJ-SOXのITGC評価にも影響するため、評価範囲と結論の共有時期を協議する

7. 監査の実施記録

調書番号	種別	タイトル	実施日	状況
ITGC-AC-01	全件分析（CAAT）	本番アクセス権の全数突合と緊急アクセスの追跡	2027-07-08	査閲済
ITGC-AC-02	全件分析（CAAT）	特権IDの全数検証と特権操作ログの突合	2027-07-09	査閲済
ITGC-AC-03	全件分析（CAAT）	退職者・異動者のアカウント失効の適時性検証	2027-07-10	査閲済
ITGC-AC-04	全件分析（CAAT）	アクセス権の定期棚卸の実効性検証	2027-07-11	査閲済
ITGC-CM-01	全件分析（CAAT）	本番変更の承認・テスト・移行分離の検証	2027-07-14	査閲済

調書番号	種別	タイトル	実施日	状況
ITGC-CM-02	全件分析（CAAT）	脆弱性・パッチ対応の適時性検証	2027-07-15	査閲済
REV-01	サンプルテスト	契約データと課金・請求・会計上の整合性検証	2027-07-16	査閲済
REV-02	全件分析（CAAT）	課金システム外の手作業仕訳の条件抽出と証憑突合	2027-07-17	査閲済
SEC-IR-01	サンプルテスト	インシデント対応の実効性検証	2027-07-18	査閲済
SEC-PII-01	サンプルテスト	顧客個人データの取扱いと暗号化の検証	2027-07-21	査閲済
OPS-BK-01	全件分析（CAAT）	バックアップ取得と復旧テストの検証	2027-07-22	査閲済
TP-01	文書レビュー	重要委託先の契約条項とSOC 報告書評価の検証	2027-07-23	査閲済
CMP-01	サンプルテスト	研修受講・内部通報・利益相反管理の検証	2027-07-24	査閲済
REV-03	全件分析（CAAT）	SLA 測定とサービスクレジットの処理検証	2027-07-25	査閲済