

SYSTEM QUALITY ASSESSMENT

システム品質 診断レポート

―― 技術的負債・セキュリティ・パフォーマンス・保守
性・ランニングコストの総合評価

32/100 5軸中3軸が最低評価
最も弱い領域: セキュリティ

■ **良い点**. ランニングコストは5軸で唯一「標準的な状態」です。2025年11月に月額を約4.6分の1へ削減済みで、日次バックアップも35日連続で欠けていません。

■ **最重要リスク**. 5軸中3軸が5段階の最低評価で、中でもセキュリティが最も切迫しています。個人情報を持つ本番データベースがインターネットに直接開放され、接続用のパスワードもプログラム内に平文で存在します。

■ **次の一手**. まずデータベースへの直接到達経路を塞ぎます (接続元を自社サーバーのみに限定)。設定変更が中心で、数日規模で着手できます。

対象システム		構成	
評価方式	コード静的調査+サーバー・クラウド構成確認	対象規模	自社コード 4,606 ファイル / 約 142 万行
診断基準日	2026	レポートID	RPT-20260716-



— Contents

目次

01	総括(エグゼクティブサマリー)	03
02	スコアの見方	04
03	軸別スコアの内訳	05
04	指摘の一覧	06
05	指摘の詳細 — セキュリティ	10
06	指摘の詳細 — 技術的負債	16
07	指摘の詳細 — パフォーマンス	19
08	指摘の詳細 — 保守性	21
09	指摘の詳細 — ランニングコスト	24
10	最も弱い領域の深掘り	26
11	推奨アクション	27
12	付録 — 評価基準・対象外・奥付	29

— 01 / Executive Summary

総括



診断の結果、**52 件の課題**が見つかり、うち **11 件は早期対応が必要**です。特に「セキュリティ」「技術的負債」「保守性」の3軸が5段階中**最低の評価**で、中でもセキュリティが最も切迫しています。外部から個人情報のデータベースに直接到達できる経路（インターネットに開いたデータベース接続口と、プログラム内に平文で置かれたパスワード）を塞ぐことが最優先で、サポートの切れた土台の刷新はその次に計画的に進めます。

主要な所見

- **ランニングコストは良好（標準的な状態）。**2025年11月に月額を約4.6分の1（約 \$2,175 → 約 \$473）へ削減済みで、本番2台の日次バックアップも35日連続で欠けていません。5軸で唯一、早期対応が必要な指摘がありません。
- **個人情報のデータベースが外部から直接到達可能。**本番データベースの接続口がインターネット全体に開放され、接続用のパスワード・暗号鍵もプログラム内に平文で存在します。アプリのログイン画面を経由せず、全データの読み取り・改ざん・削除が可能な状態です。
- **ログイン確認なしで他人のデータを書き換えられる窓口。**スマートフォンアプリ向けの通信窓口の多くがログイン確認を行わず、本文に書かれた利用者IDをそのまま信頼しています。ポイント残高の加算など、金銭的被害に直結する操作も含まれます。
- **土台がすべてサポート切れで更新できない。**フレームワーク（2011年版）と実行基盤（PHP 5.6）がいずれもサポート終了済みで、構造上、新しい版へ上げるとデータベースに接続できなくなります。弱点が見つかっても塞ぐ手段がありません。
- **同じ処理が14サイトに複製されている。**自社コードの約半分が他サイトからの複製で、1つの修正に最大14箇所の作業が要ります。実際に「片側にだけ修正が入った」分岐が確認されており、セキュリティ修正の反映漏れが起きやすい構造です。

重要 侵入されても記録が残らない

上記の危険性に加えて、本番Webサーバーの動作記録（誰がいつログインしたか等）が2025年3月から約1年4か月にわたって停止していることを確認しました。万一不正アクセスがあっても、その痕跡を後から確認する手段が実質的に失われており、「漏えいが無かったこと」を立証することも困難です。

— 02 / How to Read

スコアの見方

各領域を5段階で評価しています。数字の意味と、評価に付した条件をここで説明します。

スコアの上限ルール(キャップ)について

各領域は5段階(5=非常に良好 ~ 1=早期対応が必要)で評価します。ただし、**早期対応が必要な重大の指摘がその領域に1件でもある場合、他の項目がどれだけ良くても、その領域のスコアは上限を2に制限します。**重大な入口が1つでも開いていれば、他の平均点で相殺できないためです。今回はセキュリティ・技術的負債・パフォーマンス・保守性の4領域で、この上限が適用されています。

カバレッジ(確認できた割合)

評価に用いる観点のうち、実際に確認できた割合です。例えばセキュリティは5観点中4観点を確認しました(残り1観点は、クラウド上の権限設定の中身が未取得のため評価対象外としています)。

信頼度(実測に基づく度合い)

各指摘が、実際にコードや設定を確認した「実測」に基づくか、構成からの「推測」に基づくかの比率です。今回は52件中45件が実測で、5領域すべてで信頼度「高」です。

本レポートの範囲

本レポートは、**危険箇所の特定と、その重要度の評価まで**を行うものです。何が・なぜ危険かは正確にお示ししますが、具体的な修正計画・手順は、お見積りとあわせて別途ご提案します。

— 03 / Score Breakdown

軸別スコアの内訳

5段階評価(5＝非常に良好～1＝早期対応が必要)。総合は5領域の平均を100点換算した32点です。

領域	評価	状態(お客様向け)	スコア上限	内訳(早期対応 / 計画改善 / 軽微)
● セキュリティ	1 / 5	早期対応が必要	適用(上限2)	早期対応 7 / 計画改善 6 / 軽微 1
● 技術的負債	1 / 5	早期対応が必要	適用(上限2)	早期対応 1 / 計画改善 7 / 軽微 3
● 保守性	1 / 5	早期対応が必要	適用(上限2)	早期対応 1 / 計画改善 7 / 軽微 2
● パフォーマンス	2 / 5	計画的な改善が必要	適用(上限2)	早期対応 2 / 計画改善 4 / 軽微 1
● ランニングコスト	3 / 5	標準的な状態	なし	早期対応 0 / 計画改善 4 / 軽微 6

読み取り方

セキュリティ・技術的負債・保守性の3領域が最低評価(早期対応が必要)で並びました。中でもセキュリティは、外部から到達できる重大な指摘が7件と突出しており、最も切迫した領域です。「セキュリティ以外が良好」という意味ではなく、3領域とも早期の対応を要します。パフォーマンスも重大な指摘があるため上限2が適用されています。

— 04 / Findings Index

指摘の一覧

重要度の高い順に全52件を掲載しています。各指摘の詳細は「指摘の詳細」ページ(軸別)を参照してください。

番号	重要度	領域	指摘の内容
F-201	● 早期対応	セキュリティ	データベースが世界中のどこからでも直接アクセスできる状態
F-202	● 早期対応	セキュリティ	パスワードや鍵がプログラムの中に直接書き込まれている
F-203	● 早期対応	セキュリティ	すべての権限を持つ共通の管理者アカウントがプログラムに埋め込まれている
F-204	● 早期対応	セキュリティ	スマートフォンアプリ向けの窓口がログイン確認なしで他人のデータを書き換えられる
F-205	● 早期対応	セキュリティ	入力欄に打ち込んだ文字がデータベースへの命令として解釈されうる箇所
F-206	● 早期対応	セキュリティ	利用者のパスワードが解読されやすい方式で保管されている
F-209	● 早期対応	セキュリティ	土台となる部品が古く、修正プログラムの提供が終了している
F-101	● 早期対応	技術的負債	土台のソフトウェアがすべてサポート切れで、更新できない状態になっている
F-301	● 早期対応	パフォーマンス	データ件数が増えると急激に遅くなるデータベースの使い方
F-302	● 早期対応	パフォーマンス	利用者を待たせたまま重い処理を行う作り
F-401	● 早期対応	保守性	同じ処理が14サイトに複製されており、修正がすべてに反映されていない
F-207	● 計画改善	セキュリティ	管理画面の操作が、利用者本人の意図しない形で実行されうる設定
F-208	● 計画改善	セキュリティ	画面に表示する文字の無害化処理が統一されていない

— 04 / Findings Index

指摘の一覧

(前ページからの続き)

番号	重要度	領域	指摘の内容
F-210	● 計画改善	セキュリティ	画像アップロード時の保存先と権限の扱いが安全側になっていない
F-211	● 計画改善	セキュリティ	エラー発生時に内部の処理内容が画面に表示される設定
F-212	● 計画改善	セキュリティ	サーバーの動作記録が長期間残されておらず、問題が起きても原因を追えない状態
F-214	● 計画改善	セキュリティ	サーバーが自身のクラウド利用権限を、合言葉なしで渡してしまう設定になっている
F-102	● 計画改善	技術的負債	外部サービス連携の部品が、動作環境と噛み合わない状態で残っている
F-103	● 計画改善	技術的負債	自社コードの半分近くが他サイトからの複製で、1つの修正に最大14箇所の作業が要る
F-104	● 計画改善	技術的負債	保管されているソースコードが、稼働中のシステムの完全な写しになっていない
F-105	● 計画改善	技術的負債	1つの処理に大量の条件分岐が詰め込まれ、安全に直せる状態にない
F-106	● 計画改善	技術的負債	動作を自動で確認する仕組みが無いため、土台の更新に着手できない
F-107	● 計画改善	技術的負債	使われていない古い画面や壊れた処理が、URLから呼び出せる状態で残っている
F-108	● 計画改善	技術的負債	設置場所がプログラム内に固定されており、別の場所では動かせない
F-303	● 計画改善	パフォーマンス	同じ計算結果の使い回し(キャッシュ)がほぼ行われていない
F-304	● 計画改善	パフォーマンス	利用者が増えたときにサーバを増やして対応する手段がない

— 04 / Findings Index

指摘の一覧

(前ページからの続き)

番号	重要度	領域	指摘の内容
F-305	● 計画改善	パフォーマンス	性能の状態を後から確認する仕組みがない
F-306	● 計画改善	パフォーマンス	必要な分だけでなく、常に全件を取り出す作り
F-402	● 計画改善	保守性	プログラムの動作を自動で確認する仕組みが1件もない
F-403	● 計画改善	保守性	プログラム一式だけでは環境を再現できず、リポジトリが稼働システムの正本になっていない
F-404	● 計画改善	保守性	変更内容を自動で検査する仕組みが用意されていない
F-405	● 計画改善	保守性	1つの部品に処理が詰め込まれすぎており、読み解くのが困難
F-406	● 計画改善	保守性	同じ外部部品が二重に入って版が揃わず、実際に使われている部品の版が分からない
F-407	● 計画改善	保守性	動作記録の設定が揃っておらず、障害時に経緯を追いにくい
F-408	● 計画改善	保守性	開発・運用のための説明資料が1件も無い
F-501	● 計画改善	ランニングコスト	常時稼働のサーバーに長期利用割引が適用されていない
F-502	● 計画改善	ランニングコスト	検証用サーバーが夜間・休日も止めずに動き続けている
F-503	● 計画改善	ランニングコスト	データベースの料金を大きく下げた一方で、復旧手段が日次バックアップのみになっている
F-504	● 計画改善	ランニングコスト	定期処理の台帳が無く、111本のうち現役の3本以外の扱いが決まっていない

— 04 / Findings Index

指摘の一覧

(前ページからの続き)

番号	重要度	領域	指摘の内容
F-213	● 軽微	セキュリティ	Web サーバーに、外部からの通信を中継する機能が不要に有効化されている
F-109	● 軽微	技術的負債	使っていない外部部品が大量に同梱され、更新対象が実態より膨らんでいる
F-110	● 軽微	技術的負債	リアルタイム配信部分の外部部品が、一覧として記録されていない
F-111	● 軽微	技術的負債	集計結果が正しいか開発者自身が確信を持ってないまま、そのコードが 6 サイトで動いている
F-307	● 軽微	パフォーマンス	データベースの設計図がプログラムと一緒に管理されていない
F-409	● 軽微	保守性	障害が起きたときの対応手順が用意されていない
F-410	● 軽微	保守性	サービス品質の目標値が定められていない
F-505	● 軽微	ランニングコスト	停止したサーバーのディスクと IP アドレスは止めても料金がかかり続ける
F-506	● 軽微	ランニングコスト	振り分け装置が 3 台あり、通信量に関係なく台数分の基本料金がかかっている
F-507	● 軽微	ランニングコスト	古いバックアップイメージと、廃止済みデータベースの監視設定が残っている
F-508	● 軽微	ランニングコスト	画像をデータの中に文字として埋め込んで送っており、通信量が増える作りになっている
F-509	● 軽微	ランニングコスト	ログの保管費用は発生していないが、消す仕組みが決まっていない
F-510	● 軽微	ランニングコスト	定期処理の作りは適切だが、常時待ち受けが必要なサーバーの所在が記録されていない

— 05 / Security · Detail

指摘の詳細 — セキュリティ

セキュリティ 1/5・早期対応が必要／重大な指摘があるため上限2としています

外部から個人情報のデータベースへ直接到達できる経路が実在し、早期対応が必要な指摘が7件あります。以下は早期対応が必要な指摘(前半)と計画的な改善が必要な指摘(後半)です。

● 早期対応 データベースが世界中のどこからでも直接アクセスできる状態 実測・F-201

何が起きているか。個人情報を持つ本番データベースの接続口(3306番)が、3つの接続許可設定すべてでインターネット全体から接続できる状態になっています。データベースが実際に全アドレスで接続を待ち受けていること、OS側の遮断も無いことをサーバー内で実測しました。管理用の接続口(SSH)も、固定IP制限に「全世界許可」が併記されて無効化された状態で、稼働中3台がインターネットに開いています。

なぜ危険か。入口は「インターネット上の任意の端末」です。データベース接続に必要な接続先・利用者名・パスワードの3点はすべてプログラム内に平文で存在するため(F-202)、アプリのログイン画面を一切経由せず、個人情報を含むデータベース全体の読み取り・改ざん・全削除に到達できます。情報漏えい時は個人情報保護法上の報告義務が生じ、事業停止・契約解除・損害賠償に発展し得ます。接続口への探索はインターネット上で常時自動的に行われており、外部から無条件に到達できるため「早期対応が必要」に分類しています。

対処の方向性。データベースへの接続元を自社サーバーのみに限定し、管理用接続口の全世界開放を撤廃する。開放期間中の漏えいを前提に、パスワード・鍵は再発行する。

規模感: 設定変更が中心・3つの接続許可設定/稼働中3台・数日規模(接続先の切替を伴う場合は1~2週間規模)

● 早期対応

[Redacted text block]

[Redacted text block]

[Redacted text block]

規模感: 設定変更+コード修正(設計変更不要)・14サイト/約60ファイル/クラウド関数4本・1～2週間規模

[Redacted text block]

(注)

● 計画改善 サーバーの動作記録が長期間残されておらず、問題が起きても原因を追えない状態 実測・F-212

本番Webサーバーで、誰がいつログインしたか・システムに何が起きたかを記録する仕組みが、2025年3月から約1年4か月にわたって止まっています。この間の認証・システム・定期処理の記録は残っていません。このサーバーは、外部開放されたデータベース (F-201) や固定管理者 (F-203) を抱えるシステムの中核です。万一これらを悪用した不正アクセスがあっても痕跡を後から確認できず、「漏えいが無かったこと」を立証することも影響範囲を特定することもできません。報告要否の判断や取引先への説明にも支障します。

対処の方向性: 動作記録の仕組みを復旧し、記録を外部に集約して監視できる状態にする。

● 計画改善 サーバーが自身のクラウド利用権限を、合言葉なしで渡してしまう設定になっている 実測・F-214

クラウド上のサーバーが、自分に与えられたクラウド利用権限 (一時的な鍵) を、単純な取得要求1回で取り出せる旧方式のままです (全7台)。新方式では事前の合言葉が必須となり、この種の取り出しを構造的に防げます。これ単独では情報が漏れませんが、他の弱点の被害を桁違いに大きくします。サーバー内部から意図しない要求を送らせ得る弱点や、任意処理を実行され得る弱点が本システムに複数あるため、それらと組み合わせるとクラウド権限の乗っ取りに増幅し得ます。

対処の方向性: 権限の取り出しに合言葉を必須とする新方式へ切り替える。

この領域の評価を上げるには

外部から到達できる入口 (データベース接続口・認証なしの窓口・命令文への直接連結) を先に塞ぎ、続いて認証とパスワード保管の作り直し、土台の更新を進めることで、上限2の制約が外れます。

— 06 / Tech Debt ・ Detail

指摘の詳細 — 技術的負債

技術的負債 1/5・早期対応が必要／土台が更新不能なため上限2としています

土台（フレームワーク・実行基盤）がサポート切れかつ構造的に更新できず、自社コードの約半分が複製、自動テストは0件です。

- **早期対応** 土台のソフトウェアがすべてサポート切れで、更新できない状態になっている 実測・F-101

何が起きているか。

ータアクセスの実装

タベースに接続でき

なぜ危険か。入口を

る」運用が成立せず

環境を組み直すこと

ており、復旧が長期

応が必要」としてい

対処の方向性。デー

着手する。

規模感: 設計変更を伴う・14サイト/4,606ファイル・約142万行・1ヶ月以上規模（段階実施で複数四半期）

● 計画改善 外部サービス連携の部品が、動作環境と噛み合わない状態が残っている 実測・F-102

外部サービス連携(SMS認証・Googleログイン・SNS連携)に使う部品が、実行環境のPHPでは読み込めない構成で同梱されています。宣言だけでなく実装の書き方も、現在の実行基盤とは噛み合いません。これらの機能は現在動いていないか、呼び出された瞬間に停止するかのいずれかで、コードを読むだけでは判別できません。改修担当者が「動かないコード」を動くものと誤認したまま設計を進める危険があります。

対処の方向性: 使われていない部品を撤去し、生きている連携経路を切り分けて明確にする。

● 計画改善

自社コードの約
ます。とりわけロ
も中身が同一で
に分かれた処理

対処の方向性: 共通部分と差分部分を抽出し、共通部分は共通ライブラリで実装し、差分部分は個別実装とする。

● 計画改善 保管されているソースコードが、稼働中のシステムの完全な写しになっていない 実測・F-104

稼働に必須の構成物(クラウド連携・SMS送信・決済のライブラリ等)が変更管理の外にあり、保管されているソースコードが稼働中システムの完全な写しになっていません。リポジトリから検証環境を立ち上げても、決済・クラウド連携・SMS送信は動かない形でしか組み上がらず、土台の更新(F-101)の第一歩で行き詰まります。管理外のファイルは変更履歴も残らず、決済の異常時に「いつから変わったか」を追えません。

対処の方向性: 稼働に必要な構成物を変更管理下に置き、リポジトリを稼働システムの正本にする。

● 計画改善 1つの処理に大量の条件分岐が詰め込まれ、安全に直せる状態にない 実測・F-105

1つの関数が最大2,557行・条件分岐161という規模に膨らんでおり、100行を超える関数が全体の11.2%(1,555件)あります。対象には学習進捗の更新・月次集計・研修データ取り込みといった業務の中核処理が含まれます。全体を理解したうえで安全に直すことが現実的に不可能な規模で、改修は「該当しそうな箇所だけ直す」形にならざるを得ず、他の分岐への影響は運任せになります。自動テストが無いため、影響は本番で発覚するまで分かりません。

対処の方向性: 巨大な処理を役割ごとに分割し、あわせて自動検査の仕組みを導入する。まず中核処理から着手する。

● 計画改善 動作を自動で確認する仕組みが無いため、土台の更新に着手できない 実測・F-106

動作を自動で確認する仕組み(自動テスト・自動検査)が1件もありません。修正が他の機能を壊していないかを確認する手段が、人手での画面操作しかない状態です。この状態は他の特性(48.4%の重複・9版に分かれた認証・巨大関数・サポート切れの土台)と組み合わせると特に厳しくなります。土台の更新は全機能に影響しますが、壊れていないことを確認する手段が無いため、更新そのものに着手できません。

対処の方向性: まず中核領域(認証・決済・月次集計)から自動確認の仕組みを整える。

● 計画改善 使われていない古い画面や壊れた処理が、URL から呼び出せる状態で残っている 実測・F-107

使われていない古いコピー・退避ファイル・壊れた処理が、URLから呼び出せる状態で残っています(連番コピー33系統・壊れた読み込み4件・到達不能コード10件等)。個々のファイルへのアクセスを制限する記述がありません。改修担当者が対象ファイルを開いても、現行版か・古いコピーか・そもそも動かないものかを判断できず、修正すべき版を取り違える危険が構造的に存在します。古い版・壊れた版が公開面に残ることで、意図しない画面表示やエラー露出の原因になります。

対処の方向性: 不要ファイルを撤去し、公開してよい画面を明示的に制限する。

● 計画改善 設置場所がプログラム内に固定されており、別の場所では動かせない 実測・F-108

設置場所を指す固定パスが185ファイルに直書きされており(実効51種)、「独立した14サイト」が一部のサイトを隠れた中継点として結合しています。システムは特定の場所に置かれている前提で書かれており、それ以外では動きません。このため本番と同じ検証環境が作れず、土台の更新やコード整理が進められません。隠れた結合により、1サイトの整理が他サイトに波及することを構成から知る術がありません。

対処の方向性: 設置場所を設定値として外に出し、サイト間の共有物の配置を整理する。

この領域の評価を上げるには

サポートされる土台への段階的な載せ替えと、複製の共通化・自動確認の仕組みの導入により評価が上がります。まず本番と同じ検証環境を作れる状態にすることが起点です。

— 07 / Performance ・ Detail

指摘の詳細 — パフォーマンス

パフォーマンス 2/5・計画的な改善が必要／重大な指摘があるため上限2としています

データ件数に比例して重くなる作りと、利用者を待たせる処理が中核です。ただし性能の実測はスコープ外のため、指摘はすべて構造上の事実に基づきます。

● 早期対応 データ件数が増えると急激に遅くなるデータベースの使い方 実測・F-301

何が起きているか。データ件数に比例して問い合わせ回数が増える作り（繰り返し処理の中でのデータベース問い合わせ）が、299ファイル・2,728箇所分布しています。問い合わせが掛け算で増える三重の入れ子も実在します。一括取得の仕組みがそもそも無く、個々の実装で手作業の回避に頼っています。

なぜ危険か。入口は「利用者・データ量の増加」です。グループ学修や管理画面は、参加者やグループが増えるほど問い合わせが掛け算で増えるため、利用が増えたときに画面表示が急激に遅くなると想定されます。データベースは1台に集約され負荷を逃がす先がなく、処理が途中で時間切れになると一部だけ更新済みという中途半端な状態が残り、手作業での復旧が必要になります。事業機会の損失につながる構造ですが、外部から悪用される種類ではなく業務停止の実測も無いため、この領域は最低評価ではなく1段上（計画的な改善）としています。

対処の方向性。件数に比例して増える問い合わせを一括取得へ改め、主要導線から順に是正する。

規模感: コード修正（一部は設計変更を伴う）・299ファイル/2,728箇所・全面対応は1ヶ月以上規模、主要導線に絞れば1～2週間規模

— 08 / Maintainability ・ Detail

指摘の詳細 — 保守性

保守性 1/5・早期対応が必要／修正が全サイトに届かないため上限2としています

同一処理が14サイトに複製され、同じ変更が一部のコピーにしか入っていない分岐を実測で確認しました。自動テスト・自動検査・説明資料はいずれも0件です。

● 早期対応 同じ処理が 14 サイトに複製されており、修正がすべてに反映されていない 実測・F-401

何が起きているか。14サイトは共通のひな型をディレクトリごと複製して作られており、同一内容のファイルが多数あります。今回、同じコードの「片側にだけ変更が入った」分岐を32ファイル分、実測で確認しました。認証を担う部品も14サイトで9種類に枝分かれています。

なぜ危険か。不具合修正やセキュリティ対応を行っても、同じ処理を持つ他サイトに反映されず、一部のサイトだけ問題が残ります。これは仮定ではなく、すでに32ファイル分の分岐が生じている事実です。認証が9通りに分かれているため、ログイン周りの弱点が見つかる9箇所すべてを個別に直す必要があり、1箇所でも漏らすとそのサイトだけ弱いまま公開され続けます。緊急のセキュリティ対応時に「どのサイトが直っていないか」を誰も即答できないため「早期対応が必要」としています。

対処の方向性。同一処理を1本に集約し、修正が全サイトへ確実に届く状態へ段階的に寄せる。上位のセキュリティ是正を全サイトに届かせる前提となる。

規模感: 設計変更を伴う・14サイト全体(共通化候補81ファイル/分岐済み19ファイル)・1ヶ月以上規模(段階実施)

● 計画改善 プログラムの動作を自動で確認する仕組みが 1 件もない 実測・F-402

自社コード約139万行に対し、動作を自動で確認するテストが1件もありません。テストの質以前に、成果物自体が存在しない状態です。変更が既存機能を壊していないかを機械的に確認する手段が一切なく、確認は担当者の記憶と勘に依存します。14サイトへの複製(F-401)と組み合わせ、修正の反映漏れが「起きたことに誰も気づけない」構造になっています。

対処の方向性: まず中核経路(認証・金銭処理・一括取込)から自動確認を用意する。

● 計画改善 プログラム一式だけでは環境を再現できず、リポジトリが稼働システムの正本 実測(一部推測を含む)・F-403
になっていない

プログラムの複数箇所が稼働中サーバー上の固定パスを直接指して外部部品を読み込んでおり、一部は指定先がリポジトリにも除外設定にも無く、リポジトリが稼働システムの写しになっていません。このリポジトリだけではシステムを動かすことも作り直すこともできず、新しい担当者は手元で起動できません。サイト間が固定パスで相互依存しているため、あるサイトのフォルダを移動・改称しただけで他サイトの機能が停止します。

対処の方向性: 稼働に必要な構成物を管理下に置き、固定パス依存を解消してリポジトリを正本にする。

● 計画改善

コードの変更時
規約検査のいす
コードでも本番
が検出されない

対処の方向性:

● 計画改善

1つのファイル・
ピーが本番と同
しないまま部分
取り違える危険

対処の方向性:

— 09 / Running Cost ・ Detail

指摘の詳細 — ランニングコスト

ランニングコスト 3/5・標準的な状態／早期対応が必要な指摘は無く上限は適用していません

2025年11月に月額を約4.6分の1へ削減済みで基礎は良好です。残るのは長期割引の未適用・検証環境の常時稼働・削減の代償として縮小した復旧手段の3点で、いずれも計画的な改善で詰められます。

● 計画改善 常時稼働のサーバーに長期利用割引が適用されていない 実測・F-501

常時稼働している本番2台が、4年間オンデマンド単価のまま長期利用割引が適用されていません。本番2台分の約\$199/月は月額総計\$473の約42%にあたり、割引が効いていないことを直近8か月の請求実績で確認しました。使い方も性能も一切変えず、契約形態を変えるだけで下げられる支出が残り続いています。年額では約\$2,400の支出が割引対象になり得る状態で放置されています。

対処の方向性: 常時稼働が確定した本番2台に長期利用割引を適用する(設定変更のみ)。

● 計画改善 検証用サーバーが夜間・休日も止めずに動き続けている 実測・F-502

検証用サーバー1台が2025年10月末の起動以来、夜間・休日も止めずに24時間365日動き続けています。月\$89.28(月額請求の約19%)に相当します。検証用は通常、作業を行う時間帯にしか使いません。止まらず動き続けているため、使っていない時間にも同じ料金が発生しています。金額は事業を脅かす規模ではありませんが、削減後に残る最大の単一削減余地です。

対処の方向性: 検証用サーバーを使用しない時間帯に停止する運用へ改める(本番経路に不参加のため本番影響なし)。

● 計画改善 データベースの料金を大きく下げた一方で、復旧手段が日次バックアップのみになっている 実測(一部推測を含む)・F-503

データベースの料金を大きく下げた(マネージド構成の廃止で月約\$1,255削減)一方、その代償として復旧手段が1日1回のイメージ取得のみになっています。以前あった「任意の時点まで巻き戻す」復旧と自動切り替えが失われています。料金は正しく下がりましたが、障害が起きたタイミング次第で最大24時間分のデータが戻らない状態です。安全装置が縮小したこと自体は、経営判断として把握しておく必要があります。

対処の方向性: 現在の復旧手段で許容できる範囲を明確にし、必要なら復旧手順の整備と実地確認を行う。

— 11 / Recommendations

推奨アクション(1/2)

優先度順。P1は外部からの侵入経路の封鎖、P2は認証と土台の作り直し。金額は記載せず、判断材料として作業の種類・影響範囲・期間の目安を添えています。

P1 データベースへの直接到達経路を塞ぐ

接続元を自社サーバーのみに限定し、管理用接続口の全世界開放を撤廃する。開放期間中の漏えいを前提に、パスワード・鍵を再発行する。順序に注意し、先に接続先を自社内の経路へ切り替えてから閉じる。

規模感： 設定変更が中心・接続許可3件/約60ファイル・数日～1～2週間規模 対象： セキュリティ 2 件

P1 入力からの侵入経路を塞ぐ

画面入力の値と命令文を分けて渡す方式に統一し、エラーの詳細が画面に表示される設定を止める。退避された古いファイルは撤去する。

規模感： コード修正のみ・16箇所/実質3ファイル・数日規模 対象： セキュリティ（命令文連結ほか）

P2 認証・認可を作り直す

すべての重要な窓口でログイン確認を必須化し、プログラムに埋め込まれた固定管理者を廃止、パスワードの保管を解読に耐える方式へ移行する。

規模感： 設計変更を伴う・213窓口/14サイト・1ヶ月以上規模（アプリ改修・審査を伴う） 対象： セキュリティ 3 件

P2 14サイトの共通化を進める

同一処理を1本に集約し、修正が全サイトへ確実に届く状態にする。上位のセキュリティ是正を全サイトに届かせる前提となる。

規模感： 設計変更を伴う・14サイト全体・1ヶ月以上規模 対象： 保守性・技術的負債

P2 土台を載せ替える

サポートの切れたフレームワーク・実行基盤を、更新可能な構成へ計画的に移行する。封鎖策の完了を待たず、並行して計画に着手する。

規模感： 設計変更を伴う・14サイト/約142万行・1ヶ月以上規模（年単位の計画） 対象： 技術的負債・セキュリティ

— 11 / Recommendations

推奨アクション(2/2)

P3は業務継続と支出に関わる改善。外部から悪用される種類ではないため、封鎖策の後段で計画的に進めます。

P3 性能構造を是正する

データ件数に比例して増える問い合わせや、利用者を待たせる重い処理を見直す。まず主要導線から着手する。

規模感: コード修正・主要導線に絞れば1~2週間規模 対象: パフォーマンス

P3 運用の可視化とコストを最適化する

停止している動作記録を復旧して監視できる状態にし、長期利用割引の適用・検証環境の稼働見直しで支出を絞る。

規模感: 設定変更が中心・数日~1~2週間規模 対象: 保守性・ランニングコスト

着手順の考え方

まず外部からの侵入経路の封鎖(P1)を先行させます。土台の載せ替え(P2)は完了までに年単位を要するため、封鎖の完了を待たず並行して計画に着手します。14サイトの共通化は、上位の是正を全サイトへ確実に届かせる前提になります。

具体的な修正計画・手順は、お見積りとあわせて別途ご提案します。本レポートは危険箇所の特定と重要度の評価までを行うもので、対処は方向性の提示に留めています。