全社的内部統制・IT 全般統制

サンプル暗号資産交換株式会社　第 3 期（2026 年 3 月期）　評価範囲：本社

1．全社的内部統制（ELC・表 I ）

No	COSO 基本的要素	評価項目（着眼点）	会社の統制状況	評価手続	評価結果	評価者・評価日
1	1. 統制環境	経営者は、資金決済法・JVCEA 自主規制規則の遵守を経営の最重要事項と位置づけ、誠実性・倫理観を重視する経営方針を全社に明示しているか。	取締役会が制定した経営理念・行動規範に「利用者保護」「法令遵守」「資金決済法・JVCEA 規則の遵守」を明記し、代表者メッセージとして全役職員に周知。行動規範には暗号資産交換業者としての受託者責任・利益相反防止を含め、年 1 回の誓約書取得と理解度確認を実施している。	行動規範規程と取締役会議事録を閲覧し、法令遵守・利用者保護の方針が明文化されていることを確かめる。全役職員からの誓約書取得状況をサンプルで突合し、未取得者がいないか網羅性を確認する。	有効	内部監査室長 田中 2025-10-20
2	1. 統制環境	コンプライアンス・リスク管理委員会が設置され、独立した立場で資金決済法・JVCEA 規則の遵守状況とリスクを審議・牽制する体制が機能しているか。	コンプライアンス・リスク管理委員会を月次開催。委員長はコンプライアンス担当役員、構成員にリスク管理部門・法務・社外専門家を含む。重要な法令違反兆候・苦情・不芳情報・新規取扱リスクを審議し、取締役会へ付議・報告する規程	委員会規程と直近の議事録を通査し、月次で開催され法令遵守・リスク事項が実質的に審議されているかを確かめる。営業部門からの独立性（委員構成・議決権）と取締役会への報告ルートの有効性を評価する。	有効	内部監査室長 田中 2025-10-20

			を整備。営業部門から独立した発言権を確保している。			
3	1. 統制環境	3 線ディフェンス（第 1 線=営業/業務、第 2 線=リスク管理・コンプライアンス、第 3 線=内部監査）が職務分掌上明確に区分され、内部監査室の独立性が確保されているか。	組織規程で 3 線の役割を定義。内部監査室は代表取締役直轄ではなく取締役会・監査役（監査等委員会）に直接報告し、営業・リスク管理部門から独立。第 2 線のリスク管理・コンプライアンス部門は営業ラインから分離した報告系統を持ち、第 1 線の業務に対する牽制機能を担う。	組織図・職務分掌規程を閲覧し、3 線が職責・報告系統で分離していることを確かめる。内部監査室の人事・予算・報告ラインを確認し、営業・経営からの独立性が担保されているかを評価する。	有効	内部監査室長 田中 2025-10-20
4	1. 統制環境	取締役会・監査役（監査等委員）は、暗号資産交換業の特性に関する十分な知見を有し、経営者の業務執行を監督・牽制しているか。	取締役会は月次開催。社外取締役・社外監査役を選任し、暗号資産・金融規制・IT の専門性を有する者を含む。監査役は内部監査・会計監査人と定期的に連携（三様監査）し、分別管理・財務健全性・サイバーセキュリティを監督対象としている。	取締役会・監査役会の議事録を閲覧し、暗号資産特有のリスク（分別管理・鍵管理・財務健全性）が監督対象として審議されているかを確かめる。役員のスキルマトリクスで専門性を評価する。	有効	内部監査室長 田中 2025-10-20
5	2. リスクの評価と対応	全社的なリスク（事業・法令・財務・オペレーショナル・流動性）を網羅的に識別・評価し、資金決済法・JVCEA 規則	リスク管理規程に基づき年 1 回・重要事象発生時にリスクアセスメントを実施し、リスクマップを更新。法改正・JVCEA	リスク管理規程と最新のリスクマップを閲覧し、暗号資産業特有のリスク（流動性・カストディ・規制変更）が識別されて	有効	内部監査室長 田中 2025-10-20

		改正や金商法移管などの環境変化を継続的にリスク評価へ反映する仕組みがあるか。	通知・金商法移管動向は法務・コンプライアンス部門がモニタリングし、コンプライアンス・リスク管理委員会で評価・対応方針を決定。リスクオーナーと対応計画を明確化している。	いるかを確かめる。法改正モニタリングの記録と委員会での対応決定を突合し、環境変化が適時に反映されているかを評価する。		
6	2. リスクの評価と対応	不正リスク（横領・秘密鍵の不正利用・インサイダー取引・相場操縦・利用者資産の流用）を評価し、不正の機会・動機・正当化を低減する対応策が講じられているか。	年次の不正リスク評価で、秘密鍵アクセス権限者による不正出庫、自己ポジションを利用した不正取引、インサイダー情報を利用した取引等のシナリオを評価。職務分離・複数承認・取引モニタリング・売買審査により不正の機会を低減し、評価結果を委員会・監査役へ報告している。	不正リスク評価の文書を閲覧し、暗号資産業に固有の不正シナリオ（鍵不正利用・利用者資産流用・インサイダー）が網羅されているかを確かめる。各シナリオに対する統制（職務分離・複数承認）の有無を業務プロセス統制と突合する。	有効	内部監査室長 田中 2025-10-20
7	2. リスクの評価と対応	新規取扱暗号資産（および新商品・新サービス）の取扱可否を審査する新規取扱審査委員会が、営業部門から独立した立場でリスク評価・JVCEA 審査を実施しているか。	新規取扱審査委員会を設置し、技術的特性・流動性・AML/CFT リスク・法的性質・利益相反を評価。委員長はリスク管理またはコンプライアンス担当役員とし、営業部門は提案者として参加するが議決権を持たない。JVCEA の新規取扱審査ルールに沿った社内審査	審査委員会規程と直近の審査案件の議事録・審査シートを閲覧し、リスク評価項目が網羅され営業部門が議決から排除されているかを確かめる。JVCEA 審査手続および取締役会承認との整合を突合する。	有効	内部監査室長 田中 2025-10-20

			を経て取締役会が最終決定する。			
8	2. リスクの評価と対応	経営者は、財務健全性（自己資本規制・流動性・履行保証）に係るリスク指標を設定し、日次でモニタリングする体制を整備しているか。	財務・リスク管理部門が、利用者預り暗号資産と分別管理残高の一致、履行保証暗号資産の充足率、自己資本規制比率、法定通貨の分別管理残高等の健全性指標を日次で算定し、経営者・リスク管理部門へ報告。閾値超過時のエスカレーション基準を定めている。	日次健全性レポートをサンプル日付で入手し、分別管理残高一致・履行保証充足率・自己資本規制比率が算定・報告されているかを確かめる。経営者の確認証跡と閾値超過時の対応記録を検証する。	有効	内部監査室長 田中 2025-10-20
9	3. 統制活動	全社的な統制活動として、規程体系（コンプライアンス・リスク管理・分別管理・鍵管理・AML/CFT・会計方針等）が整備・承認され、定期的に見直されているか。	規程管理規程に基づき、業務全般を網羅する規程・マニュアルを文書管理。各規程は所管部門が起案し、委員会・取締役会の承認を経て制定・改訂。法改正・JVCEA 規則変更時には適時に改訂し、版数管理と全社周知を実施している。	規程一覧と規程管理規程を閲覧し、重要業務を網羅する規程が整備され、承認・改訂・周知のプロセスが機能しているかを確かめる。直近の法改正に対応した改訂が適時に行われているかをサンプル検証する。	有効	内部監査室 主査 佐藤 2025-10-20
10	3. 統制活動	利用者資産の分別管理および履行保証に係るガバナンス（職務分離・複数承認・定期照合・第三者管理）が全社方針として確立されているか。	利用者資産分別管理規程に基づき、利用者預り暗号資産・金銭を自己資産と区分管理。日次で利用者帳簿残高とウォレット/信託残高を照合し差異を調査。履行保証暗号資産を自社の固有財産とし	利用者資産分別管理規程と照合表をサンプル期間で閲覧し、利用者資産と自己資産の区分・照合・差異調査が運用されているかを確かめる。分別管理監査報告書・信託契約により外部牽制を確認	有効	内部監査室 主査 佐藤 2025-10-20

			て確保し、信託会社・分別管理監査（公認会計士による法定の分別管理監査）を通じた外部牽制を受けている。	し、履行保証暗号資産の充足を検証する。		
11	3. 統制活動	秘密鍵管理およびサイバーセキュリティに係る統制（コールドウォレット管理・鍵の分散保管・出庫の複数承認・アクセス権限管理）が全社的に確立されているか。	鍵管理規程・情報セキュリティ規程に基づき、利用者預り暗号資産の一定割合以上をコールドウォレットで保管。秘密鍵はマルチシグ/分散保管し、出庫は複数名承認・閾値超過は上位承認を要する。鍵アクセス権限者を限定し、職務分離と定期的な権限棚卸を実施。重大インシデント時のJVCEA・当局報告手順を整備している。	鍵管理・情報セキュリティ規程を閲覧し、コールド保管割合・マルチシグ・複数承認・権限管理の方針を確かめる。出庫承認ログと権限棚卸記録をサンプル検証し、職務分離が運用されているかを評価する。	有効	内部監査室 主査 佐藤 2025-10-20
12	3. 統制活動	インサイダー情報・利益相反の管理（新規上場情報・自己勘定取引・役職員の暗号資産売買）に係る統制が全社的に整備・運用されているか。	インサイダー情報管理規程に基づき、新規取扱予定情報等の重要情報を特定・管理し、情報隔壁（チャイニーズウォール）を設定。役職員の暗号資産売買は事前届出・禁止期間を設定し、自己勘定取引と顧客取引の利益相反を管理。違反時の懲戒を規定している。	インサイダー情報管理規程と重要情報リストを閲覧し、新規上場情報等が管理対象とされ情報隔壁が設定されているかを確かめる。役職員の売買届出記録をサンプル検証し、運用状況を評価する。	有効	内部監査室 主査 佐藤 2025-10-20
13	3. 統制活動	反社会的勢力の排除およ	反社排除規程・AML/	AML/CFT 規程と統括責	有効	内部監査室 主査 佐藤 2025-10-20

		び AML/CFT（取引時確認・取引モニタリング・疑わしい取引の届出）に係る統制が全社方針として確立されているか。	CFT 規程に基づき、口座開設時の取引時確認・反社チェック、継続的顧客管理、取引モニタリングによる疑わしい取引の検知・届出を実施。AML/CFT 統括責任者を任命し、リスクベース・アプローチで管理。JVCEA・FATF 基準を踏まえた手続を整備している。	任者の任命を確認し、リスクベースの管理体制を確かめる。取引時確認・反社チェック・モニタリング検知記録をサンプル検証し、運用の有効性を評価する。		
14	4. 情報と伝達	財務報告に関連する重要な情報（取引・残高・分別管理・健全性指標）が適時・正確に識別・集約され、経営者・取締役会・監査役に伝達される仕組みが整備されているか。	経営会議・取締役会・コンプライアンス・リスク管理委員会の階層的会議体を通じ、財務状況・分別管理・健全性指標・重要リスク事象を定期報告。月次決算・日次健全性指標を経営者へ報告し、重要事象は即時エスカレーションする報告ルートを規程化している。	報告ルート図と会議体への報告資料を閲覧し、財務・分別管理・健全性情報が経営層へ適時に伝達されているかを確かめる。重要事象のエスカレーション事例があれば、規程どおりに伝達されたかを検証する。	有効	内部監査室 主査 佐藤 2025-10-20
15	4. 情報と伝達	内部通報制度が整備され、役職員が法令違反・不正・利用者保護上の問題を経営者・監査役・外部窓口に通報でき、通報者保護と適切な調査・是正が確保されているか。	内部通報規程に基づき社内窓口および社外（弁護士等）窓口を設置。通報は監査役・コンプライアンス・リスク管理委員会へ報告され、通報者の不利益取扱いを禁止。受領	内部通報規程と窓口周知記録を閲覧し、社内外の通報ルートと通報者保護が整備されているかを確かめる。通報受付・調査・是正の記録をサンプル検証し、適切に処理さ	有効	内部監査室 主査 佐藤 2025-10-20

			した通報は調査・是正し、結果を取締役会・監査役へ報告する仕組みを整備している。	れているかを評価する。		
16	4. 情報と伝達	資金決済法・JVCEA 規則に基づく当局・JVCEA への報告・届出（変更届・不祥事件・システム障害・漏洩等）が適時・正確に行われる体制が整備されているか。	コンプライアンス部門が当局・JVCEA への法定報告・届出事項を一元管理し、報告期限・要否を判断する手続を整備。システム障害・情報漏洩・分別管理上の問題等は社内エスカレーション基準に基づき所定期限内に報告。報告内容は委員会・取締役会で確認している。	報告管理台帳と届出控えを閲覧し、法定の報告・届出が期限内に網羅的に行われているかを確かめる。システム障害等の事象が発生していれば、適時報告の運用を検証する。	有効	内部監査室 主査 佐藤 2025-10-20
17	5. モニタリング	内部監査室が、リスクベースの年次監査計画に基づき、分別管理・鍵管理・AML/CFT・財務健全性・各業務プロセスを監査し、結果を取締役会・監査役へ報告してフォローアップしているか。	内部監査規程に基づき年次監査計画を策定し、暗号資産業の重要リスク領域（分別管理・鍵管理・AML/CFT・新規取扱・財務健全性）を網羅的に監査。指摘事項は是正計画を求め、フォローアップで改善を確認。監査結果を取締役会・監査役会へ直接報告している。	内部監査計画と報告書を閲覧し、重要リスク領域がリスクベースで監査対象に含まれているかを確かめる。指摘事項のフォローアップ記録を検証し、是正が完了しているか、報告ラインの独立性が確保されているかを評価する。	有効	内部監査室長 田中 2025-10-20
18	5. モニタリング	全社的内部統制および業務プロセス統制の有効性を経営者が日常的・独立的にモニタリングし、不	コンプライアンス・リスク管理委員会が統制の運用状況・KRI・苦情・インシデントを継続的にモ	モニタリング指標レポートと不備管理台帳を閲覧し、統制不備が識別・追跡・是正される仕組みが	有効	内部監査室長 田中 2025-10-20

		備を是正・改善するプロセス（PDCA）が機能しているか。	ニタリング（日常的モニタリング）し、内部監査・分別管理監査が独立的評価を担う。識別された不備は是正計画を策定し、委員会・取締役会で進捗を管理する PDCA を運用している。	機能しているかを確かめる。委員会での是正進捗管理をサンプル検証する。		
19	5. モニタリング	利用者からの苦情・トラブル、システム障害・サイバーインシデントを集約・分析し、再発防止と統制改善に反映する仕組みがあるか。	苦情・インシデント管理規程に基づき、苦情・障害・セキュリティインシデントを一元管理し、原因分析・再発防止策を委員会へ報告。重大インシデントは JVCEA・当局報告と連動。傾向分析の結果をリスク評価・統制改善へフィードバックしている。	苦情・インシデント台帳を閲覧し、収集・分析・再発防止のプロセスが運用されているかを確かめる。重大事案について原因分析・是正・当局報告との連動をサンプル検証する。	有効	内部監査室長 田中 2025-10-20
20	6. IT への対応	IT に関する全社的な統制方針（IT 全般統制：アクセス管理・変更管理・運用管理・外部委託管理）が整備され、財務報告に関わる主要システム（取引・残高・ウォレット・会計）に適用されているか。	情報システム管理規程・IT 全般統制方針に基づき、取引システム・残高管理システム・ウォレット管理システム・会計システムについて、アクセス権限管理・プログラム変更管理・ジョブ運用管理・障害管理を整備。外部委託・クラウド利用は委託先管理規程に基づき統制している。	IT 全般統制方針とシステム一覧を閲覧し、財務報告に関連する主要システムが特定され、アクセス・変更・運用・委託管理の方針が適用対象とされているかを確かめる。	有効	内部監査室 主査 佐藤 2025-10-20

21	6. IT への対応	ブロックチェーン・ウォレット基盤および暗号資産の保管・出入庫に係る IT 統制（秘密鍵の技術的保護・トランザクション署名・残高オンチェーン照合）が全社的に確立されているか。	ウォレット管理基盤について、コールド/ホットの分離、HSM・マルチシグによる秘密鍵保護、出庫トランザクションのシステム的な複数承認、オンチェーン残高と内部帳簿の自動照合を実装。システム変更・鍵生成は厳格な権限管理と証跡保存の下で実施している。	ウォレット基盤の設計書と設定記録を閲覧し、秘密鍵の技術的保護・出庫の複数承認・残高自動照合が実装されているかを確かめる。出庫操作ログ・照合ログをサンプル検証する。	有効	内部監査室 主査 佐藤 2025-10-20
22	6. IT への対応	情報セキュリティ・サイバー攻撃対策（不正アクセス・DDoS・標的型攻撃・内部不正）に係る全社的 IT 統制と、有事の事業継続・復旧体制が整備されているか。	情報セキュリティ規程に基づき、多層防御・脆弱性診断・ペネトレーションテスト・ログ監視（SOC）・特権 ID 管理を実施。CSIRT を設置し、インシデント対応・JVCEA/当局報告・利用者通知の手順を整備。BCP・DR により重要システムの復旧目標（RTO/RPO）を定めている。	情報セキュリティ規程と診断報告書を閲覧し、サイバー攻撃対策とインシデント対応体制が整備されているかを確かめる。脆弱性診断・特権 ID 管理・BCP 訓練の記録をサンプル検証し、運用状況を評価する。	有効	内部監査室 主査 佐藤 2025-10-20
23	6. IT への対応	会計方針（実務対応報告第 38 号「資金決済法における暗号資産の会計処理等に関する当面の取扱い」）に基づく暗号資産の評価・自己/預り区分の会計処理が、IT シス	経理規程・会計方針に実務対応報告第 38 号に基づく暗号資産の期末時価評価、活発市場の有無の判定、利用者預り暗号資産と自己保有暗号資産の区分、預り資産・見合い	会計方針書を閲覧し、実務対応報告第 38 号に準拠した評価・区分・計上方法が定められているかを確かめる。時価評価のシステム算定ロジックと自己/預り区分の自動仕	有効	内部監査室 主査 佐藤 2025-10-20

		テム上で全社一貫して適用されているか。	負債の計上方法を明文化。取引・残高システムから会計システムへの自動連携と時価ソースの一元管理により、全社的に一貫した会計処理を確保している。	訳設計を検証し、全社一貫適用を評価する。		
24	1. 統制環境	金融商品取引法への移管（暗号資産の規制枠組み変更）に備えたガバナンス・対応体制が経営レベルで構築され、必要な体制整備が計画的に進められているか。	金商法移管対応のプロジェクト/委員会を設置し、移管に伴う業規制・開示・内部管理態勢の変更点を法務・コンプライアンス部門が分析。対応計画・ロードマップを取締役会で承認し、進捗を定期報告。制度動向はJVCEA・当局情報を継続モニタリングして反映している。	金商法移管対応の計画書と取締役会報告を閲覧し、影響分析・対応計画・進捗管理が経営レベルで実施されているかを確かめる。制度動向のモニタリングが対応計画へ反映されているかを評価する。	有効	内部監査室長 田中 2025-10-20

2．IT 全般統制（ITGC・表IX）

No	区分	対象システム	リスク	統制活動	頻度	整備評価	評価日
ITGC-AC-01	アクセス権限管理	全対象システム(取引システム / 勘定系・預金管理システム / 信託保全管理システム / 分別管理システム / 残高突合システム / 会計システム /	対象システムへのアクセス権限が職務分掌に基づき適切に付与・剥奪されず、単独者が取引・分別管理・会計処理や秘密鍵操作・出金実行を	全対象システムのアクセス権限について、申請・承認・付与を分離した正式なワークフローで管理し、付与時は職務分掌マトリクスと照合	随時(権限申請の都度)	有効	2025-10-20

		顧客管理システム (KYC) / AML スクリーニングシステム / 全銀 EB システム / ウォレット管理システム / 署名承認ワークフロー / HSM / 利用者預り台帳システム / ワークフロー・承認システム / 料率マスタ管理システム / ログ管理(SIEM)システム / デリバティブ取引システム / ステーキング管理システム / 暗号資産審査管理システム / 時価評価システム)	完結できることで、内部不正や誤処理による顧客資産の不正流出・財務報告の誤謬が発生する。	する。ウォレット管理システム・署名承認ワークフローではコールド/ホット・出金起票者/署名者/承認者を相互排他に設定し、秘密鍵を保持・操作する権限はマルチシグ(複数署名者)を必須として単独完結を技術的に排除する。退職・異動時は当日中に剥奪する。			
ITGC-AC-02	アクセス権限管理	ウォレット管理システム / HSM / 取引システム / KYC システム / AML システム / 会計システム / ブロックチェーンノード / 信託保全管理システム / 料率マスタ管理システム / 利用者預り台帳システム / ワークフロー・承認システム	退職者・異動者や特権 ID(管理者・root アクセス)の権限が定期的に棚卸されず、不要・過剰な権限が残存することで、不正アクセス・なりすましによる暗号資産や顧客資産の不正操作リスクが生じる。	全対象システム(ウォレット、HSM、取引システム/マッチングエンジン、KYC、AML、会計、ブロックチェーンノード、信託保全管理)のユーザー ID・特権 ID について、四半期ごとに権限棚卸を実施。退職・異動者の ID 無効化を人事情報と突合し、特権 ID の利用	四半期(秘密鍵関連システムは月次)	有効	2025-10-20

				ログをレビュー。秘密鍵関連システムは月次で棚卸を実施。差異は是正し承認記録を残す。			
ITGC-AC-03	アクセス権限管理	認証基盤(IdP) / ウォレット管理システム / HSM / 取引システム / 会計システム / 全銀EB システム / 信託保全管理システム / KYC システム / AML スクリーニングシステム / ワークフロー・承認システム / 利用者預り台帳システム	認証基盤が脆弱で、多要素認証や強固なパスワードポリシーが適用されず、外部からの不正ログイン・認証情報窃取により基幹システムへ侵入され、暗号資産の流出や取引改ざんが発生する。	全対象システムへのアクセスに多要素認証(MFA)を強制し、特権アクセス・秘密鍵関連操作にはハードウェアトークン/ FIDO 等のフィッシング耐性認証を適用。パスワードポリシー(長さ・複雑性・有効期限・ロックアウト)を統制設定で強制し、設定内容を定期的に検証。認証失敗・異常ログインは SIEM で監視・アラートする。	随時(認証時)/ 設定検証は四半期	有効	2025-10-20
ITGC-AC-04	アクセス権限管理	HSM / ウォレット管理システム / 署名承認ワークフロー	HSM・署名承認ワークフローの特権ID(鍵操作権・送金実行権)が不適切に付与・共用され、秘密鍵の不正操作や不正送金が可能になる。	特権 ID は利用者ごとに個別発行し、鍵操作権と送金実行権を同一 ID に付与しない。特権操作は多要素認証と操作ログの記録を必須とし、付与・変更はシステム部が承認ワークフ	随時(付与・変更の都度)	有効	2025-10-20

				ローで記録する(棚卸は ITGC-AC-02 による)。			
ITGC-BK-01	バックアップ・DR(事業継続)	HSM / ウォレット管理システム / コールドウォレット鍵保管	秘密鍵・シードのバックアップが適切に分散保管・暗号化されず、または鍵の単一障害点が存在することで、災害・機器故障・保管者の有事に暗号資産へアクセス不能となり、顧客資産が永久に喪失する。	コールドウォレットの秘密鍵/シードを Shamir 秘密分散等で分割し、地理的に分離した複数の堅牢保管場所(耐火金庫/貸金庫等)に暗号化して保管。鍵バックアップからの復元手順を文書化し、年次で実際の鍵復元リハーサルを実施して復元可能性を検証。アクセスは複数人立会いを必須とし、保管・持出・復元を記録する。	年次(復元リハーサル)/ 随時(保管・持出記録)	有効	2025-10-20
ITGC-BK-02	バックアップ・DR(事業継続)	署名承認ワークフロー / HSM / 取引システム / ウォレット管理システム / 会計システム / KYC・AML システム / 利用者預り台帳システム / 顧客管理システム(KYC) / AML スクリーニングシステム / 分別管理システム /	コールド署名者・鍵保持者の不在・退職・有事に代替体制が機能せず、出金や顧客払戻が長期間停止する、または基幹システムの被災時にデータ復旧・サービス復旧ができず、事業継続が困難となる。	コールド署名者の有事代替者(バックアップ署名者)を複数指名し権限を事前付与、署名定足数を代替者でも満たせる構成にして年次で代替署名の発動訓練を実施。基幹システム(取引・ウォレット・会計・KYC/AML)のデータ	年次(訓練)/ 日次(バックアップ取得)	有効	2025-10-20

		残高突合システム		バックアップを定期取得し遠隔地保管、RTO/RPO を定めた BCP/DR 計画に基づき年次でフェイルオーバー/復旧訓練を実施・評価する。			
ITGC-CM-01	プログラム変更管理	ウォレット管理システム / 署名承認ワークフロー	ウォレット管理システム・署名承認ロジック・出金処理に対する変更が、テスト・承認を経ずに本番反映され、署名検証の欠陥や出金制御の不備により暗号資産の不正流出・喪失が発生する。	秘密鍵を扱うウォレット管理システム・署名承認ワークフローの変更は、変更要求・設計レビュー・テスト・複数承認(IT 責任者+セキュリティ責任者)を経た正式な変更管理プロセスを必須化。本番リリースには開発者と異なる担当者による独立リリースを適用し、署名検証ロジック等の重要変更はソースコードレビューを実施。緊急変更は事後承認を必須とする。	随時(変更の都度)	有効	2025-10-20
ITGC-CM-02	プログラム変更管理	取引システム / マッチングエンジン / 時価情報サービス連携 / 分別管理システム / 信託保全管理システ	取引システム/マッチングエンジン・ロスカット執行ロジック・時価取込ロジックの変更が十分に検	取引システム/マッチングエンジン、ロスカット自動執行、時価取込処理、分別管理・信託保全・残高	随時(変更の都度)	有効	2025-10-20

		ム / 残高突合システム / ウォレット管理システム / 会計システム / 利用者預り台帳システム / ワークフロー・承認システム / 料率マスタ管理システム / デリバティブ取引システム / 時価評価システム / ステーキング管理システム / 暗号資産審査管理システム / BI レポーティングシステム / 収益計算エンジン	証されず本番反映され、約定・建玉・損益計算の誤り、ロスカット未執行・誤執行による顧客損害や財務報告の誤謬が発生する。	突合の計算ロジック、会計連携の変更について、本番同等環境での回帰テスト・業務部門による UAT 承認を経て本番反映する変更管理を運用。本番・開発環境を分離し、開発者の本番アクセスを制限。リリース後の初回稼働を業務部門がモニタリングし結果を記録する。			
ITGC-CM-03	プログラム変更管理	KYC システム / AML スクリーニングシステム / 会計システム / 取引システム / ワークフロー・承認システム / 利用者預り台帳システム	KYC・AML スクリーニング・会計システムのプログラム/設定変更(スクリーニングルール、勘定マッピング等)が無統制に行われ、制裁対象者の検知漏れや会計仕訳の誤りにより、コンプライアンス違反や財務報告の重要な虚偽表示が生じる。	KYC・AML システムのスクリーニングルール/閾値変更、会計システムの勘定科目マッピング・自動仕訳ロジック変更について、変更要求・テスト・コンプライアンス部/財務経理部の承認を経る変更管理を適用。ベンダー提供パッケージの更新適用も影響評価と承認の対象とし、本番反映前に検証す	随時(変更の都度)	有効	2025-10-20

				る。			
ITGC-EX-01	外部委託管理	信託保全管理システム / KYC システム (eKYC) / AML スクリーニングシステム / 時価情報サービス / ブロックチェーンノード(バリデータ) / クラウド基盤 / トラベルルール対応システム	重要な外部委託先(信託銀行、eKYC ベンダー、AML スクリーニングベンダー、レート配信、バリデータ/ステーキング委託先、クラウド事業者、トラベルルール対応 SaaS ベンダー)の内部統制が評価されず、委託先の統制不備・障害・情報漏洩が自社の財務報告・顧客資産保全・コンプライアンスに重大な影響を及ぼす。	重要委託先を一覧管理し、年次で SOC1/SOC2 報告書(または ISMS/同等の保証報告)を入手・レビューして委託先の統制有効性と CUEC(利用会社側統制)の充足を評価。報告書未入手先は代替手続(質問書・現地監査)を実施。例外事項・除外事項を識別し、自社で補完する統制を整備して影響を評価・記録する。	年次	有効	2025-10-20
ITGC-EX-02	外部委託管理	信託保全管理システム / KYC システム / AML スクリーニングシステム	信託保全管理(顧客区分管理金銭・暗号資産の信託)に係る委託先報告と自社記録の突合が行われず、信託保全額の過不足や報告誤りが検知されないことで、顧客資産の分別管理・保全義務違反や財務報告の誤りが生じる。	信託銀行からの信託残高報告と自社の信託保全管理システム上の必要保全額・拠出額を日次/週次で突合し、差異を調査・是正。eKYC/AML ベンダーの処理結果(本人確認完了・スクリーニングヒット)についても自社記録と件数・結果を照合し、連携漏れ・処理	日次/週次(突合)	有効	2025-10-20

				不整合を検知する手続を運用し記録する。			
ITGC-IF-01	インターフェース管理	AML スクリーニングシステム / トラベルルール対応システム / 時価情報サービス(外部) / 流動性管理システム(LP 接続) / 当局電子届出システム	制裁リスト・チェーン分析・時価情報・LP 気配など外部データの取込が欠落・遅延・改変され、スクリーニングや評価が不完全なデータで行われる。また当局電子届出の送信が未達・エラーとなり届出義務を履行できない。	外部データ連携ジョブは受信件数・更新日時・ハッシュをコントロールトータルで検証し、欠落・遅延・不整合を検知した場合は自動アラートのうえ再取込する。当局電子届出の送信は送信件数と受付通知(受付番号)を突合し、未達・エラー時は再送して記録する。取込・送信ログを保存し、月次でシステム部が完全性を点検する。	日次(自動)・月次(点検)	有効	2025-10-20
ITGC-IF-02	インターフェース管理	勘定系・預金管理システム / 取引システム / 信託保全管理システム / 全銀 EB システム / 会計システム / デリバティブ取引システム / 時価評価システム / ステーキング管理システム / 暗号資産審査管理システム	勘定系・預金管理システム／取引システム／信託保全管理システム／会計システム間の日次連携で、データの欠落・重複・変換誤りが生じ、預り金・必要保全額・信託残高の算定が誤る。	システム間連携は件数・金額のコントロールトータルを送信側・受信側で自動照合し、不一致はジョブを停止してエラーキューへ振り分ける。再処理はシステム部の承認を要し、連携ログ・エラーログを保存す	日次(自動)	有効	2025-10-20

				る。			
ITGC-IF-03	インターフェース管理	取引システム / 分別管理システム / KYC システム / ウォレット管理システム	取引システム→分別管理システム／eKYC→顧客管理システムの連携で、約定・入出庫・本人確認結果が欠落・遅延し、分別管理や顧客管理が不完全なデータで行われる。	連携対象データは取引 ID・申込 ID で送受信件数を突合し、未着・重複を検知した場合は自動再送する。連携遅延は SLA(30 分)を超えた時点でアラートし、システム部が原因を記録する。	日次(自動)	有効	2025-10-20
ITGC-OP-01	運用管理(バッチ・ジョブ)	ウォレット管理システム / ジョブスケジューラ / ブロックチェーンノード	出金バッチ処理の異常・エラー・改ざん・二重実行が検知・対応されず、誤った宛先・数量への出金や承認外出金が実行され、暗号資産の不正流出・喪失が発生する。	出金バッチの実行を専用ジョブスケジューラで自動制御し、実行結果(成功/失敗/件数/金額)を運用担当が日次でモニタリング。出金前にホワイトリスト・上限額・署名承認完了の自動チェックを実施し、未承認・閾値超過はジョブを停止。バッチログとブロックチェーン上のトランザクションを突合し、異常・エラーはエスカレーション手順に従い対応・記録する。	日次(出金バッチ実行の都度)	有効	2025-10-20
ITGC-OP-02	運用管理(バッチ・	取引システム / マッ	ロスカット自動執行	ロスカット自動執	日次(随時監視)	有効	2025-10-20

	ジョブ)	チングエンジン / 時価情報サービス連携	バッチ・建玉評価バッチが正常に稼働せず(遅延・停止・誤判定)、必要なロスカットが未執行となり証拠金不足・追証回収不能・顧客と自社の損失拡大が発生する。	行・建玉評価ジョブの稼働状況をリアルタイム監視し、ジョブ遅延・停止・時価取込断をアラート検知。執行結果(発動件数・金額)を日次でレビューし、想定外の未執行・誤執行がないか検証。監視アラート発報時は即時対応する運用手順を整備し、対応結果を記録する。			
ITGC-OP-03	運用管理(バッチ・ジョブ)	時価情報サービス(外部) / 取引システム / 会計システム / 信託保全管理システム / 分別管理システム / 残高突合システム / ブロックチェーンノード / 顧客管理システム(KYC) / AMLスクリーニングシステム / 利用者預り台帳システム / ワークフロー・承認システム / デリバティブ取引システム / 時価評価システム / ステーキング管理システム	外部時価情報サービスからの時価取込バッチが異常値・配信断・遅延を検知せず取り込み、評価損益・ロスカット判定・会計時価評価が誤った価格に基づいて行われ、財務報告の虚偽表示や顧客損害が生じる。また分別管理・残高突合の日次バッチが未実行・異常終了のまま気づかれず、分別管理の不足や残高差異の検知が遅れる。	時価取込バッチに対し、複数ソース比較・前回値乖離チェック・配信タイムスタンプ鮮度チェック・ゼロ/欠損値チェックの異常値検知ロジックを組込み、閾値超過時は取込停止・代替ソース切替・アラート発報。取込結果を日次でレビューし、異常検知時の対応を記録。会計システムへの連携値の整合性を突合する。必要保全	日次(取込の都度)	有効	2025-10-20

		/ 暗号資産審査管理システム		額算定・分別管理計算・残高突合などの日次バッチについても、ジョブスケジューラで完了を監視し、異常終了時は原因を記録のうえ承認を得て再実行する。			
ITGC-SEC-01	サイバーセキュリティ・物理セキュリティ	ホットウォレット / 取引システム / ブロックチェーンノード / ネットワーク基盤 / SIEM	外部からのハッキング・標的型攻撃・不正アクセスが検知・防御されず、ホットウォレットや取引システムが侵害され、暗号資産の大規模流出や顧客情報漏洩が発生する。	ネットワーク分離(ホット/コールド/管理系セグメンテーション)、WAF/IDS/IPS、EDR、SIEM による 24 時間監視を整備し、ホットウォレット保有量の上限管理とコールド比率の維持をモニタリング。脆弱性診断・ペネトレーションテストを年次以上で実施、重要パッチを適時適用。出金の異常検知(宛先/数量/頻度)アラートとインシデント対応(CSIRT)手順を運用し、検知・対応を記録する。	随時(常時監視)/ 年次(脆弱性診断・ペネトレ)	有効	2025-10-20
ITGC-SEC-02	サイバーセキュリティ・物理セキュリ	HSM / コールドウォレット署名端末 /	HSM・コールドウォレット鍵保管設備・	HSM・コールド署名端末・鍵保管庫を施	随時(入退室記録)/ 四半期(ログレビュー)	有効	2025-10-20

	ティ	データセンター・サーバ室 / 鍵保管設備	データセンター/サーバ室への物理アクセスが統制されず、機器の物理的窃取・改ざん・不正操作により秘密鍵が侵害され、暗号資産が流出する。	錠区画/耐タンパ環境に設置し、入退室をIC カード+生体認証+複数人立会で制限。入退室ログとカメラ映像を取得し、定期的にアクセスログをレビューして許可者のみのアクセスを検証。署名端末はオフライン(エアギャップ)を維持し、機器の持込/持出・封印を管理・記録する。			