金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
統 1	情報セキュリティ管理規程を策定し、定期的に見直しを行っております。
統 2	ロードマップに作成し、開発・運用の計画や必要なリソースの確保を行っております。
統 3	経営陣の承認を得る運用となっております。
統 4	情報セキュリティ代表者・責任者・管理者を設置し、情報セキュリティ管理体制を運用しております。
統 5	AWS Inspectorによるセキュリティ評価の実施、IDS/IPSの導入等セキュリティ担当部署にて対策を行っております。
統 6	各開発単位に管理者を設置し、それぞれの管理者の間で連携ができる体制に整備しております。
統 7	各開発単位に管理者を設置し、それぞれの管理者の間で連携ができる体制に整備しております。
統 8	ネットワーク管理者を設置し、ネットワーク管理手順および利用承認手続き等定め整備しております。
統 9	業務組織の分離および分担を行い、相互チェックできる体制を整備しております。
統 10	コーポレート部門で災害時マニュアルを整備し、全社員に周知徹底しております。 システム資源についてはクラウド上（AWS）で稼働しており、クラウド事業者において防災対策を行なっております。 https://aws.amazon.com/jp/compliance/data-center/data-centers/
統 11	オフィスの入退室管理を実施しております。 システム資源についてはクラウド上（AWS）で稼働しており、クラウド事業者において防災対策を行なっております。 https://aws.amazon.com/jp/compliance/data-center/controls/
統 12	情報セキュリティ管理規定で整備されております。
統 13	年1回のセキュリティ教育の実施、人員異動や退職等によるアカウント削除・権限確認を行なっております。
統 14	年1回のセキュリティ教育を実施しております。
統 15	開発メンバーに対して定期的に研修を行なっております。
統 16	障害時の対応手順を整備し、定期的に訓練を行なっております。
統 17	定期的に防災訓練を実施しております。
統 18	半期毎に開発状況に応じて人員配置を行なっております。
統 19	年1回健康診断の実施しております。
統 20	委託先選定基準に基づき、責任者の承認を得て決定しております。
統 21	機密保持契約を締結しております。
統 22	セキュリティポリシーや開発ルールの遵守を定期的に確認しております。

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
統 23	委託作業内容において、定期的に作業報告を受けております。
統 24	AWSの責任共有モデルに沿って、アクセス管理や暗号化など必要なセキュリティ対策を行なっております。 https://aws.amazon.com/jp/compliance/shared-responsibility-model/
統 25	対象外
統 26	対象外
統 27	対象外
実 1	対象外
実 2	対象外
実 3	データベースに保存されるデータはAES256で暗号化されており、限られた保守メンバーのみアクセスできるようアクセス管理しております。
実 4	通信はHTTPS(SSL)で暗号化されております。
実 5	添付ファイルはAmazon S3というオブジェクトストレージサービスに保存されており、アクセス範囲を限定しております。
実 6	バリデーションチェックを行なっております。
実 7	Amazon GuardDutyという改ざん検知サービスを導入しております。
実 8	ID・パスワード認証のほかOAuthの認証連携に対応しております。 また、Azure-ADのOpenID-Connectに対応しており、SSOが可能です。
実 9	セッションタイムアウトや10回以上サインインに失敗した場合、アカウントロックする仕組みとなっております。
実 10	アクセスログを取得し、無期限で保存しております。 また定期的に不正なアクセスログがないか確認しております。
実 11	対象外
実 12	対象外
実 13	AWS KMSというマネージド型鍵管理サービスで管理しており、年1回ローテーションを行なっております。
実 14	IDS/IPS、WAF、ファイアウォールを導入し不正アクセス対策を行なっております。
実 15	接続が許可された機器のみ、不要なポートを閉じるなど必要最小限に設定しております。
実 16	IDS/IPS、WAF、ファイアウォールを導入し不正アクセス対策を行なっております。
実 17	対象外

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 18	対象外
実 19	情報セキュリティ管理規定にてインシデント発生時の対応フローを定義しております。
実 20	業務端末について、ウイルス対策ソフトの導入、定期的なOSのアップデートなど必要なセキュリティ対策を実施しております。
実 21	業務端末にウイルス対策ソフトについて、スキャン・パターンファイルの最新化など日次で実施しております。
実 22	情報セキュリティ管理規定にてインシデント発生時の対応フローを定義しております。
実 23	システム運用・開発に必要なマニュアルを整備、最新化を行なっております。
実 24	障害時・災害時の対応フローマニュアルを整備、最新化を行なっております。
実 25	各個人にアカウントを発行しており、必要最低限のアクセス権を付与するよう管理しております。 また定期的に見直しを行なっております。
実 26	パスワードポリシー（大小英数字記号含む12桁以上）を定義しております。
実 27	各個人にアカウントを発行しており、必要最低限のアクセス権を付与するよう管理しております。 また定期的に見直しを行なっております。
実 28	データファイルはクラウド上に保管し、適切にアクセス権限設定を行なっております。
実 29	データファイルの修正が必要な場合、対応内容が問題ないか複数人でレビューを行なっております。
実 30	AWS KMSというマネージド型鍵管理サービスで管理しており、年1回ローテーションを行なっております。
実 31	開発メンバーに対して定期的に研修を行なっております。
実 32	業務端末について、ウイルス対策ソフトの導入、定期的なOSのアップデートなど必要なセキュリティ対策を実施しております。
実 33	対象外
実 34	対象外
実 35	対象外
実 36	システムの変更は事前にレビューを実施し承認を得てからリリースされる仕組みとなっております。
実 37	開発組織体制として明確化されております。
実 38	リリース実施予定・進捗状況などを記録し確認を行なっております。
実 39	バックアップの取得、世代管理を行なっております。
実 40	作業内容の履歴、本番リリース前レビュー・承認を得て本番リリースを実施しております。

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 41	バックアップの取得、世代管理を行なっております。
実 42	ネットワーク設定情報はすべてコード化され、適切に管理しております。
実 43	バックアップの取得、世代管理を行なっております。
実 44	システム運用・開発に必要なマニュアルを整備、最新化を行なっております。
実 45	バックアップの取得、世代管理を行なっております。
実 46	Datadogによるリソース監視、サービス監視、死活監視、エラーログ監視を行なっております。
実 47	Datadogによるサーバリソースの使用状況監視を行なっております
実 48	各種ソフトウェアのサポート終了予定日の確認、バージョンアップ、脆弱性対策を行なっております。
実 49	執務室は関係者のみ入室が可能。また持ち出しが容易な機器については鍵付きキャビネットに保管しております。
実 50	ネットワーク設定情報はすべてコード化され、適切に管理しております。
実 51	対象外
実 52	対象外
実 53	対象外
実 54	対象外
実 55	対象外
実 56	対象外
実 57	対象外
実 58	対象外
実 59	対象外
実 60	対象外
実 61	対象外
実 62	対象外
実 63	対象外
実 64	対象外

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 65	入力データのチェック、承認を得るプロセスとなっております。
実 66	出力結果について不正データが存在しないか日次でチェックを行なっております。
実 67	対象外
実 68	対象外
実 69	実3～7の通り対策を行なっております。
実 70	障害時・災害時の対応フローマニュアルを整備、最新化を行なっております。
実 71	障害時・災害時の対応フローマニュアルを整備、最新化を行なっております。
実 72	障害発生の原因を分析し、適切に対策を行なっております。
実 73	緊急対応の体制を組み、対応手順書を作成しております。
実 74	サービスはAWS上で運用しており、リージョン障害の場合は別リージョンでサービスが継続できるよう対策を行なっております。
実 75	新規開発・既存システムにおける変更において、企画、設計、コードレビュー、テスト環境でのテストの実施、リリース前には承認を得ております。
実 76	本番環境とは別にネットワークレベルで分離したテスト環境を整備しております。
実 77	リリース手順書が整備されております。
実 78	開発・変更時のドキュメントはテンプレート化され、必要な情報が入力される仕組みになっております。
実 79	ドキュメントツールに保存・管理されております。
実 80	パッケージの有効性、信頼性、生産性などを評価しております。
実 81	パッケージ供給元の問い合わせ窓口や、各種設定、有効期限などを整理しております。
実 82	社内規定に則り廃棄対応を行なっております。
実 83	社内規定に則り廃棄対応を行なっております。
実 84	対象外
実 85	対象外
実 86	対象外
実 87	対象外
実 88	対象外

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 89	監査ログや権限設定などセキュリティ機能を実装しております。
実 90	設計作業の標準化（作業。内容、ドキュメント、レビュー）を行い品質確保しております。
実 91	作成したソースコードのレビューを社内ルールに基づき実施しております。
実 92	QAチームよりテスト計画およびテスト仕様書を作成しテストを実施しております。
実 93	動作推奨環境（OS、ブラウザ）を設定し、テストを実施しております。
実 94	機能及び自社システムとの整合性を確認しております。
実 95	変更内容のレビュー及び、作業手順のドキュメント化を実施しております。
実 96	QAチームよりテスト計画およびテスト仕様書を作成しテストを実施しております。
実 97	ファイルレベルで排他制御を実装しております。
実 98	不整合を検知する仕組みを実装しております。
実 99	運用作業はできる限り自動化を行なっております。
実 100	システムによるチェック機能の利用や、複数人によるチェックを実施しております。
実 101	Datadogによるサーバリソースの使用状況監視を行なっております。
実 102	Datadogによるリソース監視、サービス監視、死活監視、エラーログ監視を行なっております。
実 103	Datadogによるリソース監視、サービス監視、死活監視、エラーログ監視を行なっており、エラー内容から切り分けを行なっております。
実 103-1	AWSの機能を使った冗長構成（複数のアベイラビリティゾーンを使った構成）や自動バックアップを設定しております。
実 104	負荷状況によってサーバー台数が自動的に増減する設定を行なっております。
実 105	対象外
実 106	修正バージョンのリリースに時間がかかる場合は、前バージョンに切り戻す等仕組み化されております。
実 107	対象外
実 108	対象外
実 109	対象外
実 110	対象外
実 111	対象外

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 112	対象外
実 113	現時点でログイン・ログアウトなど確認できる機能はございません。
実 114	Assuredにて安全対策状況を開示しております。
実 115	利用規約にて定められております。
実 116	不正アクセス対策や不正侵入防止策など運用管理方法を定めております。
実 117	対象外
実 118	業務端末と携帯電話は個人毎に貸与しており、公衆無線LANに接続しないなどルール化されております。
実 119	対象外
実 120	対象外
実 121	対象外
実 122	対象外
実 123	対象外
実 124	対象外
実 125	対象外
実 126	対象外
実 127	対象外
実 128	対象外
実 129	対象外
実 130	対象外
実 131	対象外
実 132	対象外
実 133	対象外
実 134	対象外
実 135	対象外

金融機関等コンピュータシステムの安全対策基準・解説書（第11版）対応

※ガイドラインで対象の項目のみ記載しております。

※作成時点の内容であり、予告なしに変更される場合があります。

2023年7月4日時点

基準番号	対応状況
実 136	対象外
実 137	対象外
実 138	電子メールの利用に関して、不正アクセス防止策や機密情報漏洩策などルール化されております。
実 139	業務に関係のないメール送受信・ホームページ閲覧はしないようルール化されております。
実 140	対象外
実 141	対象外
実 142	対象外
実 143	対象外
実 144	対象外
実 145	テレワークで利用する業務端末は個人毎に貸与しており、OSやソフトウェアを定期的にアップデートするよう周知しております。
実 146	クラウドサービスや社内システム利用時に接続する際は多要素認証を必須としております。
実 147	機密性が求められるデータを取り扱う場合はVPNによる接続を実施しております。 また業務端末のストレージの暗号化を検討しております。
実 148	カフェなど不特定多数がいる場所でのWeb会議を禁止しており、会議室で行うよう周知徹底しております。
監1	システム監査体制の整備を行い、年1回内部・外部監査を実施しております。