当チェックシートは、Surfly B.V.（オランダ）の提供するSurflyのセキュリティについて「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9版令和2年3月版）」に基づき回答した資料です。
※Surflyが対象となる項目のみ記載しています。

最終更新日：2022年5月

統制基準

基準大項目	基準中項目	基準番号	基準小項目	基準分類	対応状況
1 内部の統制	(1)方針・計画	統1	システムの安全対策にかかわる重要事項を定めた規定を整備すること。	基礎	ISO27001の基準に準拠した情報セキュリティポリシーおよびプロセスを定義しています。
		統2	中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること。	基礎	ロードマップに基づいて開発計画を策定しています。
		統3	システム開発計画は中長期システム計画との整合性を確認するとともに、承認を得ること。	基礎	
	(2)組織体制	統4	セキュリティ管理体制を整備すること。	基礎	ISO27001の基準に準拠した情報セキュリティポリシーおよびプロセスを定義し、インシデント管理体制を整備しています。定期的に外部セキュリティ評価の監査を受け、管理体制の維持を行っています。
		統5	サイバー攻撃対応体制を整備すること。	基礎	
		統6	システム管理体制を整備すること。	基礎	
		統7	データ管理体制を整備すること。	基礎	
		統8	ネットワーク管理体制を整備すること。	基礎	
		統12	各種業務の規則を整備すること。	基礎	サービス運用に関する管理体制を定義しています。
	(3)管理状況の評価	統13	セキュリティ順守状況を確認すること。	基礎	ISO27001の基準に準拠して実施しています。
	(4)人材（要因・教育）	統14	セキュリティ教育を行うこと。	基礎	
		統15	要因に対するスキルアップ教育を行うこと。	基礎	
		統16	障害時・災害時に備えた教育・訓練を行うこと。	基礎	
		統17	防災・防犯訓練を行うこと。	基礎	
		統18	要因の人事管理を行うこと。	基礎	
		統19	要因の健康管理を行うこと。	基礎	
2 外部の統制	(1)外部委託管理	統20	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること。	基礎	サービスに関する業務の外部委託は、行っていません。
		統21	外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること。	基礎	
		統22	外部委託先の要員にルールを遵守させ、その遵守状況を確認すること。	基礎	
		統23	外部委託における管理体制を整備し、委託業務の遂行状況を確認すること。	基礎	
	(2)クラウドサービスの利用	統24	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること。	基礎	ISO27001の基準に準拠して実施しています。

実務基準

基準大項目	基準中項目	基準番号	基準小項目	基準分類	対応状況
1 情報セキュリティ	(1)データ保護	実1	他人に暗証番号・パスワード等を知られないための対策を講ずること。	基礎	Surfly社規定のアクセス制御ポリシーを定義しています。
		実3	蓄積データの漏洩防止策を講ずること。	付加	Surfly社規定のアクセス制御ポリシーを定義しています。
		実4	伝送データの漏洩防止策を講ずること。	付加	通信データはTLS1.2/1.3を使用して暗号化されます。
		実5	ファイルに対するアクセス制御機能を設けること。	基礎	Surfly社規定のアクセス制御ポリシーを定義しています。
		実6	不良データ検出機能を充実すること。	基礎	予期せぬ不正侵入試行の検知や総当たり攻撃を素早く遮断する侵入検知システム（IPS）を有効化しています。
		実7	伝送データの改ざん検知策を講ずること。	付加	
	(2)不正使用防止	実8	本人確認機能を設けること。	基礎	データセンターへのアクセスは強力なアクセスキーを使用した多要素認証またはワンタイムパスワードが必須になります。
		実9	ID の不正使用防止機能を設けること。	基礎	
		実10	アクセス履歴を管理すること。	基礎	サーバーへのアクセスはすべて監査され、ログが記録されます。
		実13	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。	付加	Surfly社規定のアクセス制御ポリシーを順守し、暗号鍵にはSSHキーを使用、管理しています。
	(3)外部ネットワークから	実14	外部ネットワークからの不正侵入防止策を講ずること。	基礎	データセンターへのアクセスは強力なアクセスキーを使用した多要素認証またはワンタイムパスワードが必須になります。
		実15	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。	基礎	
	(4)不正検知策	実16	不正アクセスの監視機能を設けること。	基礎	予期せぬ不正侵入試行の検知や総当たり攻撃を素早く遮断する侵入検知システム（IPS）を有効化しています。
	(5)不正発生時の対応	実19	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	基礎	不正アクセス発生時のプロセスが定義され、外部調査団体による分析が行われます。
	(6)不正プログラム対策	実20	コンピュータウイルス等の不正プログラムへの防御対策を講ずること。	基礎	サーバにはネットワークファイアウォールとIDSが導入されています。 また、Surfly社が規定するリスクレベルの指標に基づいて分類され、適切に処理、改善されます。
		実21	コンピュータウイルス等の不正プログラムの検知対策を講ずること。	基礎	
		実22	コンピュータウイルス等の不正プログラムによる被害時対策を講ずること。	基礎	

実務基準					
基準大項目	**基準中項目**	**基準番号**	**基準小項目**	**基準分類**	**対応状況**
2 システム運用共通	(1)マニュアルの整備	実23	通常時マニュアルを整備すること。	基礎	サービス運用に関する管理体制を定義しています。
		実24	障害時・災害時マニュアルを整備すること。	基礎	ディザスタリカバリに関するプロセスが定義され、定期的にテストが実施されています。
	(2)アクセス権限の管理	実25	各種資源、システムへのアクセス権限を明確にすること。	基礎	Surfly社規定のアクセス制御ポリシーを定義しています。
		実26	パスワードが他人に知られないための措置を講じておくこと。	基礎	
		実27	各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること。	基礎	
	(3)データ管理	実28	データファイルの授受・管理方法を明確にすること。	基礎	すべてのデータはSurfly社の方針に基づいて分類、管理されています。
		実29	データファイルの修正管理方法を明確にすること。	基礎	
		実30	暗号鍵の利用において運用管理方法を明確にすること。	基礎	
	(4)オペレーション習熟	実31	オペレーション習熟のための教育及び訓練を行うこと。	基礎	情報セキュリティポリシーを定義し、すべての従業員の教育はそれらに基づいて維持されます。
	(5)コンピュータウイルス対	実32	コンピュータウイルス対策を講ずること。	基礎	アンチウイルスソフトを導入しており、WAFを超えるアクセスは監視されています。
	(6)外部接続管理	実33	接続契約内容を明確にすること。	基礎	各端末上にアンチウイルスソフトを導入しており、WAFを超えるアクセスは監視されています。
		実34	外部接続における運用管理方法を明確にすること。	基礎	
3 運行管理	(2)データファイル管理	実39	データファイルのバックアップを確保すること。	基礎	DBのバックアップを外部サーバへ取得しています。
	(3)プログラムファイル管理	実40	プログラムファイルの管理方法を明確にすること。	基礎	定期的に冗長サーバーへ同期を実施しています。
		実41	プログラムファイルのバックアップを確保すること。	基礎	
	(4)ネットワーク設定情報	実42	ネットワークの設定情報の管理を行うこと。	基礎	ネットワーク設定情報の管理及び、設定内容の監視を行っています。
		実43	ネットワークの設定情報のバックアップを確保すること。	基礎	
	(5)運用時ドキュメント管	実44	運用時のドキュメントの保管管理方法を明確にすること。	基礎	ディザスタリカバリに関するプロセス規定が存在しています。
		実45	災害時の復旧対応に必要なドキュメントのバックアップを確保すること。	基礎	
	(6)運行監視	実46	システムの運行状況の監視体制を整備すること。	基礎	稼働サーバ及び冗長サーバの稼働状態を常時監視しています。
4 各種設備管理	(1)資源管理	実47	各種資源の能力及び使用状況の確認を行うこと。	基礎	リソース環境（CPU利用率、メモリ使用量など）は定期的に監視しています。
	(2)機器の管理	実48	ハードウェア及びソフトウェアの管理を行うこと。	基礎	Surfly社規定のポリシーを規定し、デバイスマネージャーによる管理がされています。
	(2)入出力管理	実66	出力情報の作成、取扱いについて、不正防止及び機密保護対策を講ずること。	基礎	Surflyにはデータ出力機能を有していません。
	(3)帳票管理	実67	未使用重要帳票の管理方法を明確にすること。	付加	
		実68	重要な印字済帳票の取扱方法を明確にすること。	基礎	
	(4)顧客データ保護	実69	顧客データの保護策を講ずること。	基礎	アカウントの認証情報はハッシュ化されています。
6 緊急時の対応	(1)障害時・災害時対応策	実70	障害時・災害時の関係者への連絡手順を明確にすること。	基礎	ディザスタリカバリに関するプロセス規定が存在しています。
		実71	障害時・災害時復旧手順を明確にすること。	基礎	
		実72	障害の原因を調査・分析すること。	基礎	
	(2)コンティンジェンシープ	実73	コンティンジェンシープランを策定すること。	基礎	
7 システム開発・変更	(1)システム開発・変更	実75	システムの開発・変更手順を明確にすること。	基礎	変更管理プロセス定義に従い、品質テストを実施しています。
		実76	テスト環境を整備すること。	基礎	
		実77	本番への移行手順を明確にすること。	基礎	
	(2)開発・変更時ドキュ	実78	開発・変更時のドキュメントの作成手順を明確にすること。	付加	
		実79	開発・変更時のドキュメントの保管管理方法を明確にすること。	基礎	
	(3)パッケージの導入	実80	パッケージの評価体制を整備すること。	付加	変更管理プロセスのルールに従い、品質テストを実施した上でリリースを行っています。
		実81	パッケージの運用・管理体制を明確にすること。	付加	
	(4)システムの廃棄	実82	システムの廃棄計画を策定するとともに、廃棄手順を明確にすること。	基礎	アカウント情報は契約終了後、速やかに削除します。
		実83	システム廃棄時の情報漏洩防止対策を講ずること。	基礎	お客様専用環境をご利用の場合は、解約後すみやかに環境消去を実施します。

実務基準					
基準大項目	**基準中項目**	**基準番号**	**基準小項目**	**基準分類**	**対応状況**
8 システムの信頼性向	(2)ソフトウェア等の品質向上対策	実89	必要となるセキュリティ機能を取り込むこと。	基礎	ISO27001の基準に準拠してセキュリティ対応を実装し、変更管理プロセス定義に従った、品質テストを実施することで、ソフトウェア品質を維持しています。
		実90	設計段階におけるソフトウェアの品質を確保すること。	基礎	
		実91	プログラム作成段階における品質を確保すること。	基礎	
		実92	テスト段階におけるソフトウェアの品質を確保すること。	基礎	
		実93	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	基礎	
		実94	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	基礎	
		実95	定型的な変更作業時の正確性を確保すること。	基礎	
		実96	機能の変更、追加作業時の品質を確保すること。	基礎	
		実97	ファイルに対する排他制御機能を設けること。	付加	
		実98	ファイル突合機能を設けること。	付加	
	(3)運用時の信頼性向	実99	オペレーションの自動化、簡略化を図ること。	付加	可能な限りオペレーションの自動化を実施しています。
		実100	オペレーションのチェック機能を充実すること。	基礎	
		実101	負荷状態の監視制御機能を充実すること。	基礎	リソース環境（CPU利用率、メモリ使用量など）は定期的に監視しています。
	(4)障害の早期発見・[	実102	システム運用状況の監視機能を設けること。	基礎	稼働サーバ及び冗長サーバの稼働状態を常時監視しています。
		実103	障害の検出及び障害箇所の切り分け機能を設けること。	付加	アクティブ/パッシブ・フェイルオーバー方式を採用しています。
		実104	障害時の縮退・再構成機能を設けること。	付加	
		実105	障害時の取引制限機能を設けること。	付加	
		実106	障害時のリカバリ機能を設けること。	基礎	

監査基準					
基準大項目	**基準中項目**	**基準番号**	**基準小項目**	**基準分類**	**対応状況**
1 システム監査	(1)システム監査	監1	システム監査体制を整備すること。		Surflyは、定期的に外部セキュリティ評価の監査を受けています。