情報セキュリティへの取り組み

番号	項目	確認内容	回答	
1. 組織的対策				
1-1	情報セキュリティの運営	経営者の主導で情報セキュリティの 方針を示しているか。	○	会社HP内にて経営者としての方針を公開しています。 https://www.skyarch.net/profile/security.html
		情報セキュリティ対策を実施するための体制を整備し、問題が起きたときには体制改善を行っているか。	○	社内にてISO運営委員会を設置し改善を行っています。
		ISO27001を取得済か。 またプライバシーマークの認証も取得しているか。	○	取得済です。 ・ISO27001（2005年4月8日）・プライバシーマーク 21000270（2007年2月6日）
1-2	情報セキュリティの基本方針について	秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員などに対して個人情報・法人顧客情報の取扱いに関する基本方針・規程等を定めているか。	○	情報セキュリティ基本方針や個人情報保護に関する規程を定めています。
1-3	情報セキュリティの独立したレビューの実施	情報セキュリティ確保のための、技術的対策や運用、投資状況について定期的もしくは、重大な変化が発生したときに、独立したレビューを実施しているか。	○	毎年マネジメントレビューを開催しています。
		内部監査・外部監査の定期的な受審や、ISMSの定期的な見直し等を実施しているか。	○	定期的な受審を行い、不適合箇所については迅速に見直しを行っています。
2. 人的セキュリティ				
2-1	雇用契約	従業員の雇用契約時にセキュリティ事項を定め雇用契約を実施しているか。また秘密保持契約も締結しているか。	○	実施しています。就業規則にて明記し、入社時に全社員対象で機密保持に関する誓約書を締結しています。
2-2	教育及び訓練	雇用中に業務で必要な情報セキュリティについて、定期的な教育と訓練を実施しているか。	○	入社時のセキュリティ研修及び毎年、全従業員にテスト等を用いたセキュリティ教育を実施しています。
		教育や訓練内容は世の中の情報セキュリティ及びリスクの変化に適宜対応した内容に刷新しているか。	○	コロナ過におけるテレワークのリスクなど適宜情勢に応じた研修を実施しています。
2-3	アクセス権限	雇用者のアクセス権限は、業務に必要な最小権限に限定して付与しているか。	○	アクセス権限の付与は最低限にしています。
		社員に付与した権限について、台帳等で詳細に管理し棚卸を行っているか。	○	台帳管理を行い、退職者などの不要なアカウントが残っていないか定期的な棚卸を実施しています。
2-4	退職後の秘密保持	従業員が退職する際に、退職後の秘密保持義務への合意をもとめているか。	○	退職時に誓約書の提出にて秘密保持への合意を取っています。
3.物理的セキュリティ				
3-1	オフィス管理	オフィスへの入退室管理や不正侵入防止のための対策を実施しているか。またどのように管理しているか。	○	実施しています。生体認証を用いての入室管理及び監視カメラを設置し録画しています。静脈認証のログは半年間保管しています。
		オフィスの執務室内にてセキュリティ区画とセキュリティレベルを物理的に定め、区画を分離しているか。	○	オフィス内にセキュリティエリアを構築し、分離しています。
3-2	情報管理	書類、PC、データ記録媒体を持ち出す場合は、紛失・盗難対策を講じているか。	○	PCのHDDを暗号化しています。機器の外部持出についてのルールを定めています。
3-3	廃棄管理	顧客情報がある装置の廃棄については、適切なデータ消去を実施・確認したうえで廃棄しているか。	○	HDDは初期化後、物理的に破壊して廃棄しています。
		廃棄した資産について管理・記録しているか。	○	廃棄情報は資産管理ツールに記録しています。保管期限は定めていません。
3-4	災害対策	脅威となる自然災害やインフラ災害を想定し、対応策を講じているか。	○	社内サーバはiDCに設置しています。
4.情報システムの開発と保守				
4-1	セキュリティ要求	情報システムの開発において、セキュリティ要求事項を定めているか。	○	システム開発に関するISMS規程にて要求事項を定めています。
		システムの新規開発や改修時にシステムに脆弱性がないか診断を行うことがあるか。	○	ISMS規程にて脆弱性の定期チェックを 行うことを定めています。
4-2	暗号化	インターネットを利用するシステムについては、通信およびサーバに保管するデータの暗号化を実施しているか。	○	システム開発に関するISMS規程にて実施が義務化されています。
		暗号化は電子政府推奨方式に準拠したものを採用しているか。	○	採用しています。
4-3	プロセス	開発や保守のプロセスにおいて、セキュリティを確保する手段を講じているか。	○	システム開発に関するISMS規程を策定しています。
4-4	セキュリティ情報の収集	情報セキュリティの脆弱性情報を適宜収集し必要に応じて社内共有する仕組みはあるか。	○	JPCERTが公開する脆弱性情報を毎日確認し、必要に応じて展開しています。
5.運用管理				
5-1	メール	メールの誤送信を防止するための対策を講じているか。	○	送信前確認機能を導入しています。
		重要な情報をメールで送信する場合は、ファイルをパスワード保護し、別手段や別メールでパスワードを伝えているか。	○	添付ファイルをパスワードで暗号化し、パスワードは別メールで通知しています。
5-2	変更管理	F/Wの設定変更において、変更前のセキュリティ評価と実施内容の確認を行うための事前レビューを組織として実施しているか。	○	変更作業は、上長の承認のもとで実施しています。
5-3	性能管理	情報システムの稼働及び性能管理を実施しているか。	○	ISMSの委託先管理手順に従って管理しています。
5-6	ウィルス対策	コンピュータウィルスの対策を実施しているか。	○	全PCにウィルス対策ソフトを導入しています。
		標的型メール攻撃への対策を講じていますか。	○	社員全員を対象に訓練を実施し対策に努めています。
		ソフトウェアのセキュリティパッチを適宜に実施しているか。	○	管理サーバ経由で強制的に適用しています
		パターンファイルの更新は即時実施しているか。	○	即時実施しています。
5-7	バックアップ	コンピュータやソフトウェアの障害に備えたバックアップを実施しているか。	○	定期的なバックアップを実施しています。
5-8	ネットワーク管理	インターネットと自社ネットワークからの不正アクセスに対する防護対策を実施しており、具体的な対策が文書化されているか。	○	ISMS規定に従い、ゲートウェイにFirewallを設置しています。
		本サービスへの不正アクセスは検知・遮断されるようにているか。	○	FirewallにてIPアドレスによるアクセス制御を実施しています。
5-9	媒体の管理	USBメモリ、携帯電話、DVDなどの外部記憶メディアの利用制限を実施しているか。	○	PCに常駐した管理ソフトにて、外部メディアの接続を無効化しています。
5-10	外部からの不正行為について	インターネットに公開しているシステムへの不正アクセス、改ざんのモニターを実施しているか。	○	定期的に各サーバのログを確認しています。
		不正アクセスとして検知している通信設定内容のポリシーが一覧化されているか。	○	構成管理ツールにて管理しています。
		不正アクセスとして検知された通信は必要に応じて遮断等の防御が実施されているか。	○	自動的に遮断は実施していませんが、検知の際アラートが発動し、担当者が迅速に対応致します。
		モニタリングのルール及び不正行為への対策の定期的な見直しの実施をおこなっているか、またその見直し結果についてレビュー記録として保管しているか。	○	定期的な見直しを行い、確認結果を記録しています。
5-11	メンテナンス記録	アプリケーション、サーバ、通信機器などのITシステムに対する保守作業について作業記録を保管しているか。保管期間は何年か。	○	構成管理ツールに記録し管理しています。保管期限はありません。
5-12	障害記録	アプリケーション、サーバ、通信機器の障害ログを取得し、解析とチェックを実施してるか。	○	定期的に各サーバのログを確認しています。
		解析・チェックの結果記録が1年以上保管しているか。	○	構成管理ツールに記録し管理しています。保管期限はありません。
5-13	サービス設備面の顧客データ管理	テレワーク等、社外から情報へアクセスする場合は、セキュリティリスクを考慮した対策を講じているか。	○	接続可能なIPアドレスを限定、ID、PASSによるログイン管理を行っています。
6.アクセス制御及び認証				
6-1	特権ID管理	特権IDについて、利用者の限定、利用記録、適切なパスワード強度を実施し、かつ、使用者台帳及び使用記録を保管しているか。	○	構成管理ツールにて管理しています。記録台帳の保管期間は3年です。
		また、特権ID発行時の審査、定期的なパスワードの変更、廃棄時の即時提示を実施しているか。	○	定期的なパスワード変更は実施していませんが、解約時は即時AWSアカウントを削除している。
		特権IDの定期的な棚卸は実施しているか。	○	棚卸は未実施ですが、特権ID発行は最小限に限定しています。
6-2	アクセス権のレビュー	特権IDやネットワークのアクセスコントロール内容について適切か定期的な棚卸を実施しているか。	○	定期的な棚卸は未実施ですがお客様からのご依頼に応じて実施しています。
6-3	社内ネットワークのアクセスコントロール	サービスで利用しているネットワークと自社の業務で利用しているネットワークの分離を実施しているか。	○	専用AWSアカウントを発行し、独立した環境で運用しています。
6-4	F/Wのアクセスポリシー	外部との接続制限を行うF/Wについて基本的なアクセスポリシーを定めているか。	○	ISMS規程にて、必要最低限のポートのみを開放するよう定めています。
6-5	パスワード	パスワード設定に関して強度など社内ルールはあるか。	○	半角英数字記号を含めた8文字以上がISMS規程にて義務化されている。
6-6	クリアスクリーン	従業員が使用するパソコンについてクリアスクリーンの対策は講じているか。	○	ISMS規程にてクリアスクリーンが義務化されています。 一定時間(10分)でのパスワード付きスクリーンセーバーの 自動ロック、離席時のコンソールロック実施のルール等を定めています。
7.情報セキュリティインシデントの管理				
7-1	報告と改善	世の中のセキュリティ事故や自社で発生した事故を報告し対策実施する仕組みはあるか。	○	ISMS規程「事業継続計画書」にて策定しています。
7-2	証拠の収集	セキュリティ事故を調査し証明するため、通信記録やセキュリティシステム/サーバなどのセキュリティ・ログを保管しているか。	○	対象のログは1年以上保管しています。
7-3	事業継続	緊急事態やサイバー攻撃発生時の対応について危機管理対応手順を定めているか。また訓練も行っているか。	○	ISMS規程「事業継続計画書」にて策定しており、訓練は年1回実施しています。
8. 個人情報の取扱いについて				
8-1	個人情報の取扱い	個人番号や特定個人情報の安全管理についてルールや 手段を定め、社内周知を行っているか。	○	個人情報保護の取り扱いについて社内にてルールを定め、研修にて社員に連携しています。