番号	項目	確認內容		回答
1. 組織的対	煉	既於四十		M H
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。	0	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。	0	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。	0	映得済です。 18027001(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	被密情報を扱う全ての従業員(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・法人願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?	0	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		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、軍大な変化が発生したときに、独		毎年マネジメントレビューを実施しています。
	情報セキュリティの独立したレ ビューの実施	立したレビューを実施しているか。 内部監査・外部監査の定期的な受害や、ISMSの定期的な見直し等を実施しているか。		定期的に受審し、不適合箇所については迅速に見直しを行っています。
		内印画車・7ト印画車の定列のでは交合で、ISMSの定列のでよ光圏し等と交通しているか。		た物的に火金し、 や題 p 回 別に プレ・じは
2. 人的セキ				
	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。	0	就業規則にて明記し、入社時に全社員を対象とし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。	0	入社時にセキュリティ研修を実施、また、全社員を対象に年4回全社勉強会を実施しています。
		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。	0	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。	0	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。	0	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。	0	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。
・物理的セキ	キュリティ			
	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。	0	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圖しています。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園とセキュリティレベルを物理的に定め、区園を分離しているか。		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。
	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。機器の外部特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。	0	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。	0	社内サーバはiDCに設置しています。
・情報システ	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。	0	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。	0	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。	0	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。	0	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譲じているか。		システム開発に関するISMS規程を策定しています。
	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。
	セイエリティリ界板の収集	1前板でイエリティの配列は前板を超点収集しむ安に応じては内光行するは他のはめるか。		DPUERT が公開する認明性情報を専口機能し、必要にあして機関しています。
温用管理				
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。	0	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、ファイルをバスワード保護し、別手段や別メールでバスワードを伝えているか。	0	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しるか	0	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	0	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。	0	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るか。	0	社員全員を対象に年4回の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バッチを適宜に実施しているか。	0	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されているか。	0	即時実施しています。
5-7	パックアップ	コンピュータやソフトウェアの障害に備えたパックアップを実施しているか。		定期的なパックアップを実施しています。
	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か。 か。		
3-0	ホットリーク目 程			
		本サービスへの不正アクセスは検知・遮断されるようにしているか。		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。		PCI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。	0	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。	0	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。	0	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数します。
		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。	0	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	レニュ aussectには、自じていかが。 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。またその保管期限は何年か。	0	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	官規模は何年か。 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いるか。		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年以上保管されているか。		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	サービス設備高の節変ギーケ等	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、PASSIこよるログイン管理を行っています。
	理		Ĺ	The second secon
		移住 「「つ」」で、利用金の間で、利用製造、海切か、「っつ、「「沖血を中枢」 レン・ドロネルはものドロのではない。		接点を培心 「子を培」 イトセイ おはム鉱小戸産物師はったイナ
6-1		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。		
	特権ID管理			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ます。
	行権ID官程	また、特権口発行時の審査、定期的なバスワードの変更、廃業時の即時提示を実施しているか。	0	
	· 行使心管。24			棚卸は朱実施ですが、特権心発行は最小限に限定しています。
6-2	守権 D 官 理 アクセス権のレビュー	また、特権口発行時の審査、定期的なバスワードの変更、廃業時の即時提示を実施しているか。	0	期部は未実施ですが、特権の発行は最小限に限定しています。 定期的な棚部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。
	アクセス権のレビュー	また、特権D免行時の審査、定期的なパスワードの変更、廃業時の即時提示を実施しているか。 特権Dの定期的な棚助は実施しているか。	0	
6-3	アクセス権のレビュー	また、特権の発行時の審査、定期的なバスワードの変更、廃業時の即時提示を実施しているか。 特権Dの定期的な補助は実施しているか。 特権Dの之別的な補助は実施しているか。	0	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	アクセス権のレビュー 社内ネットワークのアクセスコント ロール	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時提示を実施しているか。 特種のの定期的な棚割は実施しているか。 特種の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割を実施しているか。 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。	0 0	定期的な棚割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。 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。
6-3	アクセス権のレビュー 社内ネットワークのアクセスコント ロール F/Wのアクセスポリシー	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時提示を実施しているか。 特種のの定期的な棚卸は実施しているか。 特種の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。 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。 外部との接続制限を行うド/Wについて基本的なアクセスポリシーを定めているか。	0 0 0	定期的な機能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。 専用ANNSアカウントを発行し、独立した環境で運用しています。 ISMS規模にて、必要最低限のポートのみを開放するよう定めています。 ISMS規模にて半角美数学記号を含めた8文学以上で設定することを義務化しています。
6-3 : 6-4 : 6-5 : 6-6 : 6-6	アクセス権のレビュー 社内ネットワークのアクセスコント ロール F/Wのアクセスポリシー パスワード	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時度示を実施しているか。 特権のの定期的な精助は実施しているか。 特権の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機動を実施しているか。 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。 外部との修練制限を行う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。 パスワード設定に関して独皮など社内ルールはあるか。	0 0 0	定期的な機能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。 専用ANNSアカウントを発行し、独立した環境で運用しています。 ISMS規模にて、必要最低限のポートのみを開放するよう定めています。 ISMS規模にて半角美数学記号を含めた8文学以上で設定することを機務化しています。
6-3 6-4 6-5 6-6	アクセス権のレビュー 登具ネットワークのアクセスコント ロール・ ア/ アクレスポリシー バスワード グリアスがリーン エリケィインケデトの智慧	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時度示を実施しているか。 特権のの定期的な精助は実施しているか。 特権の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機動を実施しているか。 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。 外部との修練制限を行う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。 パスワード設定に関して独皮など社内ルールはあるか。	0 0 0 0	定期的な機能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。 専用AMSアカウントを発行し、独立した環境で運用しています。 ISMS原程にて、必要最低限のボートのみを開放するよう定めています。 ISMS原程にて、必要最低限のボートのみを開放するよう定めています。 ISMS原程にて半角実数字配号を含めた8文字以上で設定することを機器化しています。 ISMS原程にて半角実数字配号を含めた8文字以上で設定することを機器化しています。 ンン・ルロック実施のルールを含定めています。 ・定時間(10分)でのパスワード付きスクリーンセーバーの1動ロック、離底時の ンソールロック実施のルール等を定めています。
6-3 6-4 6-5 6-6 7-1	アクセス権のレビュー 社項ネットワークのアクセスコント ロール F7Mのアクセスポリシー バスワード グリアスクリーン エリケインシブントの管理 報告と改善	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時度示を実施しているか。 特権のの定期的な精節は実施しているか。 特権のの定期的な精節は実施しているか。 特権の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標節を実施しているか。 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。 外部との接続制限を行うF/Mについて選本的なアクセスポリシーを定めているか。 パスワード設定に関して強度など社内ルールはあるか。 従業員が使用するパソコンについてグリアスクリーンの対策は講じているか。	0 0 0 0	定期的な機能は未実施ですがお客格からのご依頼に応じて実施しています。 専用AMSアカウントを発行し、独立した環境で選用しています。 ISMS規模にて、必要最低限のボートのみを開放するよう定めています。 ISMS規模にて、必要最低限のボートのみを開放するよう定めています。 ISMS規模にて非角英数字配号と含めた8文字以上で設定することを義体化しています。 ISMS規模にて非角英数字配号と含めた8文字以上で設定することを表体化しています。 ISMS規模にてクリアスクルーンを最外にされています。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II動ロック、超底時の ンソールロック実施のルール希を定めています。 ISMS規模にで見なりないます。 ISMS規模に事業機械基本規模」にで定めています。
6-3 6-4 6-5 6-6 7-1 7-2	アクセス権のレビュー 柱頂表かり一クのアクセスコント ロール ドバのアクセスポリシー バスワード クリアスクリーン 2リティインシザントの管理 報答と改善 証拠の収集	また、特権の発行時の審査、定期的なパスワードの変更、農業時の即時度示を実施しているか。 特権のの定期的な精制は実施しているか。 特権の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精制を実施しているか。 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。 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。 パスワード設定に関して強度など社内ルールはあるか。 従業責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。 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。 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。 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。	0 0 0 0	定期的な離削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。 専用AMSアカウントを発行し、独立した環境で運用しています。 ISMS膜標にて、必要量低限のボートのみを開放するよう定めています。 ISMS膜標準にて、必要量低限のボートのみを開放するよう定めています。 ISMS膜膜でエキ角英数を記号を含めた8文字以上で設定することを義務化しています。 ISMS膜膜でエクリアスクリーンが儀務化されています。一定時間(16分)でのパスワード付きスクリーンセーバーの1動ロック、離席時の ンナールロック実施のルール等を定めています。 ISMS膜膜である実践を表現程」にて定めています。 対象のログは1年以上保管しています。 対象のログは1年以上保管しています。
6-3 : 6-4 : 6-5 : 6-6 : 7.16 t t t t t t t t t t t t t t t t t t t	アクセス様のレビュー 社内ネッドワークのアクセスコント ロール FWのアクセスポリシー バスワード グリアスクリーン コリティインシデントの管理 報告と改善 証拠の収集 事業組続	また、特種の発行時の審査、定期的なパスワードの変更、廃業時の即時度示を実施しているか。 特権のの定期的な精節は実施しているか。 特権のの定期的な精節は実施しているか。 特権の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標節を実施しているか。 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。 外部との接続制限を行うF/Mについて選本的なアクセスポリシーを定めているか。 パスワード設定に関して強度など社内ルールはあるか。 従業員が使用するパソコンについてグリアスクリーンの対策は講じているか。	0 0 0 0	定期的な機能は未実施ですがお客格からのご依頼に応じて実施しています。 専用AMSアカウントを発行し、独立した環境で選用しています。 ISMS規模にて、必要最低限のボートのみを開放するよう定めています。 ISMS規模にて、必要最低限のボートのみを開放するよう定めています。 ISMS規模にて非角英数字配号と含めた8文字以上で設定することを義体化しています。 ISMS規模にて非角英数字配号と含めた8文字以上で設定することを表体化しています。 ISMS規模にてクリアスクルーンを最外にされています。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II動ロック、超底時の ンソールロック実施のルール希を定めています。 ISMS規模にで見なりないます。 ISMS規模に事業機械基本規模」にで定めています。
6-3 6-4 6-5 6-6 7-1 7-2 7-3 7-3	アクセス権のレビュー 柱頂表かり一クのアクセスコント ロール ドバのアクセスポリシー バスワード クリアスクリーン 2リティインシザントの管理 報答と改善 証拠の収集	また、特権の発行時の審査、定期的なパスワードの変更、農業時の即時度示を実施しているか。 特権のの定期的な精制は実施しているか。 特権の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精制を実施しているか。 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。 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。 パスワード設定に関して強度など社内ルールはあるか。 従業責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。 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。 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。 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。	0 0 0 0	定期的な離削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。 専用AMSアカウントを発行し、独立した環境で運用しています。 ISMS膜標にて、必要量低限のボートのみを開放するよう定めています。 ISMS膜標準にて、必要量低限のボートのみを開放するよう定めています。 ISMS膜膜でエキ角英数を記号を含めた8文字以上で設定することを義務化しています。 ISMS膜膜でエクリアスクリーンが儀務化されています。一定時間(16分)でのパスワード付きスクリーンセーバーの1動ロック、離席時の ンナールロック実施のルール等を定めています。 ISMS膜膜である実践を表現程」にて定めています。 対象のログは1年以上保管しています。 対象のログは1年以上保管しています。