
情報セキュリティチェックシート

お問い合わせ先 情報セキュリティ委員会

情報セキュリティの資格		回答	回答に関する補足説明
1	ISMS認証を取得している	○	JIS Q 27001:2014(ISO/IEC 27001:2013) 認証登録番号 : IS 693751 有効期限 : 2024年8月10日
2	ISMSクラウドセキュリティ認証を取得している	○	CLOUD 731089/ISO27017:2015 プロセスマイニングサービス(myInvenio private cloud service)にて取得 有効期限:2024年8月10日
組織的安全措置		回答	回答に関する補足説明
3	セキュリティ管理に関する責任者を決定し、職務範囲を明確にしている	○	役職: CIO 氏名: 宮田 英一
4	情報セキュリティに関する基本方針を策定している	○	情報セキュリティ基本方針 (https://www.heartcore.co.jp/information_security/index.html)
5	セキュリティ管理を維持、継続するための方針や規程、マニュアル等を整備している	○	
6	企業秘密の取扱いにおけるリスクを定期的に分析している	○	
7	情報セキュリティインシデント発生に備えて、各種連絡体制は定められている	○	<ul style="list-style-type: none"> ・自社内外への報告体制の整備 ・関係者に対するの通知 ・原因・影響の調査体制 ・再発防止策・事後対策の検討体制

8	機密情報の取扱いに関する規程等に違反した場合の懲戒処分が定められている	○	
9	定期的な内部監査を実施している	○	
10	全従業員から守秘義務など契約書や誓約書を取得している	○	
環境的安全措置		回答	回答に関する補足説明
11	施設、執務室への入退制限、管理を行っている	○	カードキーによる入退でログを取得し、規定を定めている
12	情報媒体の保管は適切である	○	施錠管理、情報媒体の保管についての規定を定め、施錠できる書庫、キャビネットに保管している
13	書類や記録媒体は廃棄手順を定め、適切に処分している	○	書類はシュレッダーにて裁断し、装置等はデータ完全消去後に機密廃棄をしている 外部へ委託した際はデータ消去証明書を発行している
技術的安全措置		回答	回答に関する補足説明
14	データ、システムにアクセス制限を定め、情報システムを使用できる従業員を限定している	○	
15	従業員が業務で使用するPCにウイルス対策ソフトを導入している	○	ウイルス対策ソフトを導入し、業務利用のパソコンに常駐させている 1日1回ウイルス定義を更新している
16	ノートPCや携帯について紛失・盗難に備えた措置を講じている	○	管理者による動作ロックを行えるようにしている

17	ログや記録を残し、アクセス状況を確認している	○	
18	ネットワーク機器に設定している管理者用のユーザID/パスワードを適切に管理している	○	
19	情報システムの管理者の職務を複数の者に分離して内部不正を防止している	○	
人的安全措置		回答	回答に関する補足説明
20	業務を行っているすべての従業員に対して定期的な教育を実施している	○	年に一度セキュリティ教育を実施している
21	委託先との契約で情報の取り扱いに関する注意事項について合意を取っている	○	法務チェックを実施した上で締結している
22	機密情報を送付する際は情報の暗号化、ファイルストレージの使用等の措置を講じている	○	ファイル転送システムを利用している
23	情報の社外持出・持込について規定を定め記録している	-	社内外への持ち出しは行わず、ファイル転送システムを利用している
24	社内PCによる業務外利用や私物による業務データ使用について禁止は規定されている	○	
25	雇用・委託の終了または変更となった場合に、情報資産、アクセス権等の返却・削除・変更の手続きについて明確にしている	○	

テレワークに関する安全措置		回答	回答に関する補足説明
26	テレワーク時の規定を定めている	○	
27	テレワークにおいて従業員が適切に情報を扱えるよう、従業員に教育を実施している	○	