

カテゴリ	No	設問	回答
I. 組織体制・ガバナンス	1	ISMS（ISO27001）の取得状況	IS 97518（初回登録日：2005年10月14日・次回更新日：2029年10月07日）
I. 組織体制・ガバナンス	2	プライバシーマーク（JIS Q 15001）の取得状況	登録番号：10860069（取得日：2004年7月8日・更新日：2028年7月22日）
I. 組織体制・ガバナンス	3	ISO/IEC27017、SOC2、PCI DSS等の認証取得状況	無し
I. 組織体制・ガバナンス	4	情報セキュリティ基本方針を策定し周知していますか。	はい。 https://www.dip-net.co.jp/files/1805
I. 組織体制・ガバナンス	5	プライバシーポリシーを策定して周知していますか。	はい。 https://www.dip-net.co.jp/privacy_policy
I. 組織体制・ガバナンス	6	情報セキュリティ管理責任者（または個人情報保護管理者）を任命していますか？	任命しています。
I. 組織体制・ガバナンス	7	セキュリティポリシーや関連規定は、定期的に見直しを行っていますか？	はい。見直しを実施しています。
I. 組織体制・ガバナンス	8	情報セキュリティに関する監査（内部監査または外部監査）を定期的に実施していますか？	内部監査を年1回実施するほかに外部認証機関の監査が年1回以上あります。
I. 組織体制・ガバナンス	9	個人情報保護法など、業務に関連する法令や契約上の要求事項を特定し、遵守していますか？	はい。
I. 組織体制・ガバナンス	10	保有する情報資産（個人情報・機密情報）を特定し、管理台帳等で管理していますか？	はい。管理しています。
II. 人的セキュリティ	11	全従業員（パート・アルバイト含む）に対し、年1回以上の情報セキュリティ教育を実施していますか？	年4回実施しています。
II. 人的セキュリティ	12	従業員の採用時（または雇用期間中）に、秘密保持に関する誓約書を取得していますか？	取得しています。
II. 人的セキュリティ	13	退職者からの資産返却、アクセス権削除、秘密保持誓約の回収等の手続きを定めていますか？	細則にて詳細を定めています。
II. 人的セキュリティ	14	セキュリティ規定に違反した場合の罰則規定（懲戒処分等）を就業規則等で定めていますか？	就業規則に定められています。
III. 外部委託・再委託管理	15	業務を再委託する場合、委託元への事前通知や承諾を得る運用になっていますか？	はい。
III. 外部委託・再委託管理	16	再委託先に対して、自社と同等のセキュリティレベルであることを確認・監督していますか？	はい。委託先管理の規定に基づき実施しています。
III. 外部委託・再委託管理	17	再委託先との間で、秘密保持契約を含む業務委託契約を締結していますか？	はい。締結しています。
IV. アクセス制御・認証	18	アクセス権限は、業務上必要な最小限の範囲・期間で付与していますか？	はい。
IV. アクセス制御・認証	19	ユーザーID（アカウント）の登録・削除・棚卸しを定期的に実施していますか？	実施しています。
IV. アクセス制御・認証	20	パスワードの複雑性（桁数、文字種）や有効期限などのルールを設けていますか？	はい。設けています。
IV. アクセス制御・認証	21	外部からの接続や管理者アカウントには、多要素認証（MFA）を利用していますか？	現状、多要素認証は設定されておりませんが、導入を目指しております。
IV. アクセス制御・認証	22	原則として、IDの共有（使い回し）を禁止し、個人を特定できるIDを付与していますか？	はい。
V. 技術的セキュリティ対策	23	PCやサーバーにウイルス対策ソフトを導入し、定義ファイルを常に最新にしていますか？	実施しています。
V. 技術的セキュリティ対策	24	OSやアプリケーションに最新のセキュリティパッチ（修正プログラム）を適用していますか？	適用しております。
V. 技術的セキュリティ対策	25	インターネット経由で重要情報を送受信する際、通信経路を暗号化（SSL/TLS等）していますか？	TLS1.2を採用しております。
V. 技術的セキュリティ対策	26	保存されている重要情報（DB、PCのHDD等）は暗号化されていますか？	はい。
V. 技術的セキュリティ対策	27	ファイアウォール（FW）やWAF等を設置し、外部からの不正アクセスを遮断していますか？	はい。
V. 技術的セキュリティ対策	28	定期的にシステムに対する脆弱性診断（プラットフォーム診断やWebアプリ診断）を実施していますか？	はい。
VI. 運用・ログ・物理対策	29	アクセスログや操作ログを取得し、一定期間保管していますか？	はい
VI. 運用・ログ・物理対策	30	セキュリティ事故発生時の連絡体制・緊急連絡先（24時間365日等）を整備していますか？	はい。整備しています。
VI. 運用・ログ・物理対策	31	重要情報を扱うエリア（執務室・サーバ室）は施錠し、入退室の記録を行っていますか？	はい。実施しております。
VI. 運用・ログ・物理対策	32	機器や媒体を廃棄・返却する際、データを復元不可能な状態で完全消去していますか？	はい。規程に定められています。
VI. 運用・ログ・物理対策	33	重要データのバックアップを定期的に取得し、復旧可能な状態で保管していますか？	はい。