

就労定着支援システム「SPIS」 セキュリティチェックシート

1. PU 公開情報

| | | | | | |
|---|------|---|----------------------------------|-----|--|
| 1 | PU-1 | 情報セキュリティについて企業としての方針を定め、取締役会等の承認を得ていますか。 また組織の内外へ周知していますか。 | <input checked="" type="radio"/> | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |

2. CT 第三者認証

| | | | | | | |
|---|------|---|----------------------------------|--|------|---|
| 2 | CT-1 | 情報セキュリティまたは個人情報保護について取得している第三者による認証や評価をすべて選択してください。 | <input checked="" type="radio"/> | ISO/IEC 27001 | 登録番号 | I-13063/25CCER02 |
| | | | | ISO/IEC 27017 | 有効期限 | 2028-11 |
| | | | | プライバシーマーク | 範囲 | インターネット関連事業 (定着支援サービスの開発、 保守、運用を含む) |
| | | | | SOC2(Type1) | | |
| | | | | SOC2(Type2) | | |
| | | | | ISMAP | | |
| | | | | ISMAP-LIU | | |
| | | | | その他 その他認証や評価の例：ISO/IEC27018、 SOC3、FedRAMP、ASPIC等 | | |
| | | | | 該当なし | | |
| | | | | 非公開 | | |

3. HS 履歴

| | | | | | |
|---|------|---|----------------------------------|-----|--|
| 3 | HS-1 | 過去2年間にホームページ等で対外的に公表もしくは監督省庁や認証機関等へ報告するレベルのセキュリティインシデントがありましたか。 | | はい | |
| | | | <input checked="" type="radio"/> | いいえ | |
| | | | | 非公開 | |

4. LG 法律

| | | | | | |
|---|------|---|----------------------------------|----------------------|-----------------------|
| 4 | LG-1 | 契約や規約等における準拠法を選択してください。 | <input checked="" type="radio"/> | 日本法 | |
| | | | | その他 | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 5 | LG-2 | 個人情報保護に関して対応しているものをすべて選択してください。 | <input checked="" type="radio"/> | 個人情報保護法 | |
| | | | | カリフォルニア州法（CCPA/CPRA） | |
| | | | | EU一般データ保護規則（GDPR） | |
| | | | | その他 | |
| | | | | 該当なし | |
| 6 | LG-3 | 政府、自治体又は公的機関から個人情報提供の命令又は要請等があった場合に実施することとしている内容をすべて選択してください。 | <input checked="" type="radio"/> | サービス利用者への速やかな通知 | 通知し、本人の同意を得ることとします。 |
| | | | <input checked="" type="radio"/> | 法的な根拠がある場合のみの対応 | 利用目的の達成に必要な情報のみ提供します。 |
| | | | <input checked="" type="radio"/> | 必要最低限の個人情報のみの提供 | |
| | | | | 対応内容の記録 | |
| | | | | 該当なし | |
| | | | | 非公開 | |

5. SU サービス利用者

| | | | | | |
|---|------|---|----------------------------------|----------------------|--|
| 7 | SU-1 | サービスの対象者は法人のみであり、個人（個人事業主を含む）での利用は不可となっていますか。 | | 法人のみ利用可能であり個人での利用は不可 | |
| | | | <input checked="" type="radio"/> | 法人だけでなく個人での利用も可能 | |
| | | | | 非公開 | |

6. SL サービスレベル

| | | | | | |
|---|------|---------------------------------------|----------------------------------|--|---|
| 8 | SL-1 | サービスレベルや責任範囲について実施していることをすべて選択してください。 | | 稼働目標を定めている | 目標復旧時間 2日 <small>詳細</small> 操作ミスなどの契約者の責によるデータの消失につきましては、復元の義務を負いません。バックアップメディアが同時に破損するなど、復元には限界があることは範囲外とします。 <small>詳細</small> 電子メール（利用責任者宛て）もしくは電話 |
| | | | | 稼働実績を開示している | |
| | | | <input checked="" type="radio"/> | 目標復旧時間(RTO)を定めている | |
| | | | <input checked="" type="radio"/> | クラウドサービス事業者の責任範囲を定めている | |
| | | | <input checked="" type="radio"/> | サービス利用者とクラウドサービス事業者間のコミュニケーション（連絡や報告）のルールや体制を定めている | |
| | | | | 損害賠償について、責任の範囲や金額の上限を定めている | |
| | | | | 該当なし | |
| | | | | 非公開 | |

| 7. DT データ利用 | | | | | |
|-------------|------|---|--|-------|---|
| 9 | DT-1 | クラウドサービスで取得する情報（預託データ）をすべて選択してください。 | <input checked="" type="radio"/> 個人を識別可能な情報 <input checked="" type="checkbox"/> 氏名やメールアドレス <input checked="" type="checkbox"/> 要配慮個人情報 <input type="checkbox"/> マイナンバー <input type="checkbox"/> その他 個人を識別可能な情報で、列挙されたものにあたらない場合は「その他」を選択の上、該当する情報を記載してください。 | | |
| | | | 個人関連情報 <input type="checkbox"/> Cookie（クラウドサービスの提供にあたり必須のCookieを除く） <input type="checkbox"/> 位置情報 <input type="checkbox"/> その他 サービス利用者（契約者）または、その他のエンドユーザーからデータを取得する場合の双方についてご検討ください。 | | |
| | | | クレジットカード情報 | | |
| | | | その他 詳細を記載してください | | |
| | | | サービスを通じての情報取得はない | | |
| | | | 非公開 | | |
| 10 | DT-2 | 預託データについて、利用規約などで定めていることをすべて選択してください。 | <input checked="" type="radio"/> データの機密性確保 <input checked="" type="checkbox"/> 秘密・機密情報としての取扱い <input checked="" type="checkbox"/> 第三者への開示の禁止 <input type="checkbox"/> 漏えい等発生時にクラウドサービス利用企業へ即時に通知 | | |
| | | | データ利用目的の規定 <input type="checkbox"/> サービス提供・保守・障害調査等 <input type="checkbox"/> サービスの改善・向上 <input type="checkbox"/> 研究・開発 <input type="checkbox"/> ニュースレターなどの情報提供（サービスの提供に係るもの以外） <input type="checkbox"/> 目的外利用の禁止 <input type="checkbox"/> その他の目的（詳細） | | |
| | | | 預託データに関する権利のクラウドサービス利用企業への帰属 | | |
| | | | その他 | | |
| | | | 利用規約などに上記のような定めはない | | |
| | | | 非公開 | | |
| 11 | DT-3 | クラウドサービスで個人を識別可能な情報を含む情報（個人データ）を取得する場合、その本人（データ主体）として当てはまる主体をすべて選択してください。 | <input checked="" type="radio"/> クラウドサービス利用企業の従業員 | 外部支援者 | |
| | | | <input checked="" type="radio"/> クラウドサービス利用企業から見た外部の個人（取引先や採用候補者など） | | |
| | | | その他 | | |
| | | | 非公開 | | |
| 12 | DT-4 | 個人データを取得する場合、取り扱いの有無について選択してください。 | <input type="checkbox"/> 取り扱う | | サービスの利用規約にて、サーバーに保存された個人情報を取り扱わない、サーバーに保存されている個人データへの適切なアクセス制御を実施する旨定めている |
| | | | <input checked="" type="radio"/> 取り扱わない | | |
| | | | その他 | | |
| | | | 非公開 | | |
| 13 | DT-5 | 個人データを取り扱う場合、その方法は以下のいずれに当たりますか。当てはまるものを全て選択してください。 | 社内利用 | | |
| | | | 第三者への移転（データの提供および、委託先等の社外の第三者によるデータアクセスを含む） | | |
| | | | その他 | | |
| | | | 非公開 | | |
| 14 | DT-6 | 個人データを取り扱う場合に、当該データを法令上規制のある形で加工しますか。当てはまる加工方法を全て選択してください。 | 匿名加工情報 | | |
| | | | 仮名加工情報 | | |
| | | | 上記の対策・設備について定期的に点検しているの固いでは加工せずに取り扱う | | |
| | | | 非公開 | | |
| 15 | DT-7 | 個人データの第三者への移転がある場合、どのような枠組みでデータを受け渡しますか。当てはまるものを全て選択してください。 | 処理の委託 | | |
| | | | 第三者提供 | | |
| | | | その他 | | |
| | | | 非公開 | | |
| 16 | DT-8 | 個人データの処理を第三者に委託する場合、関連法令の要求に従い、適切に委託先の監督を実施していますか。 | はい | | |
| | | | いいえ | | |
| | | | 非公開 | | |

| | | | | | |
|--------------------------|-------|--|---|--|--|
| 17 | DT-9 | 個人データを第三者提供する場合、本人の同意を取得するなど、適切な手続を確認して提供していますか。 | | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 18 | DT-10 | Cookie(クラウドサービスの提供にあたり必須のCookieを除く)や位置情報、IPアドレス等のオンライン識別子の利用について、対応していることをすべて選択してください。 | | 事前の同意を得ている | |
| | | | | 利用停止の方法を明記している | |
| | | | | 利用するCookieを明記している <small>GDPRに準拠する場合は利用するCookieの明記が必要です</small> | |
| | | | | 未実施 | |
| | | | | オンライン識別子の利用なし | |
| | | | | 非公開 | |
| 8. LO データの所在地 | | | | | |
| 19 | LO-1 | データセンターやIaaSのリージョンなど、預託データを保管するために利用する施設の所在地をすべて選択してください。 | ● | 日本 | |
| | | | | アメリカ合衆国 | |
| | | | | 欧州連合（EU）および英国 | |
| | | | | 中華人民共和国 | |
| | | | | その他 | |
| | | | | 非公開 | |
| 20 | LO-2 | 預託データが日本国外の主体からアクセスされることはありますか。 | | はい | |
| | | | ● | いいえ | |
| | | | | 非公開 | |
| 21 | LO-3 | 個人データなど、法規制のかかるデータを日本国外に保管するか、または日本国外の主体がデータにアクセスする場合、法的な根拠を確認・評価して実施していますか。 | | ケースに応じ、適切な法的根拠を確認して実施している | |
| | | | | 確認せず実施している | |
| | | | ● | 対象となるデータや運用はない | |
| | | | | 非公開 | |
| 9. OR 情報セキュリティ確保のための組織体制 | | | | | |
| 22 | OR-1 | クラウドサービスのセキュリティの維持や向上、監督などの活動全般を統制する枠組みとして実施していることをすべて選択してください。 | ● | セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めている | |
| | | | ● | セキュリティ管理に関する関係部署や業務、機能を明らかにしている | |
| | | | ● | セキュリティ体制について、通常時だけでなく有事を想定した役割や責任を定めている | |
| | | | | 自社の責任範囲と外部委託先との責任範囲を明確にしている | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 23 | OR-2 | クラウドサービスのセキュリティリスク管理として実施していることをすべて選択してください。 | ● | セキュリティリスクへの対応計画を策定している | |
| | | | ● | 経営層が対応計画を承認している | |
| | | | ● | 経営層に対応進捗・結果などが報告されている | |
| | | | ● | 定期的なセキュリティリスク評価を行っている | |
| | | | | 実施していない | |
| | | | | 非公開 | |
| 10. EM 従業員に対するセキュリティ対策 | | | | | |
| 24 | EM-1 | 従業員に対するセキュリティ対策として実施していることをすべて選択してください。 | ● | セキュリティおよび重要情報の取り扱いに関する意識向上のため、定期的に教育を実施している | 頻度 年1回 最終実施日 2025-08 テーマやトピック 1. 守秘義務 2. 業務上の遵守事項 3. 建物出入口や窓の施錠及び防犯、防火について 4. 廃棄紙類等について 5. 事故報告（報告・提案・問い合わせ） 6. その他の注意事項 |
| | | | | セキュリティインシデントを想定した演習や訓練を実施している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 25 | EM-2 | 従業員および委託先・派遣契約元などの契約相手と秘密保持に関する契約や誓約書を締結をしていますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |

| | | | | | |
|---------------|------|--|---|--|--|
| 26 | EM-3 | 従業員および委託先・派遣契約先などの契約相手との契約が終了または変更となった場合、アクセス権の変更や削除、貸与資産の返却等を実施していますか。 | ● | 手続きを文書化している | |
| | | | | 定期的に文書の内容を見直している | |
| | | | ● | 実施している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 11. AS 情報資産管理 | | | | | |
| 27 | AS-1 | 情報資産の管理プロセスおよび重要度の基準を定め、管理プロセスに従い情報資産の洗い出しと評価を行い、資産一覧を作成していますか。 | ● | 管理プロセスを文書化している | |
| | | | ● | 定期的に文書内容を見直している | |
| | | | ● | 情報資産一覧を作成している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 28 | AS-2 | 契約や規約等により、サービス利用終了時のデータの取り扱いが明確になっていますか。 | | 返却や削除の取り決めが規約等に明記されている | サービス終了時ではありませんが、秘密保持契約書第7条（秘密情報の返還・破棄）にて要求があった場合には返還または破棄すると規定しています。 |
| | | | ● | 明記されていない | |
| | | | | 非公開 | |
| 29 | AS-3 | サービス利用終了時またはサービス利用者からの指示があった場合、預託データやサービス利用者が作成したデータを返却したり削除できますか。 可能なものをすべて選択してください。 | | 返却・ダウンロード サービス利用者によるダウンロードを含む | 削除までの時間 要相談 |
| | | | | 利用終了時に削除 | |
| | | | ● | サービス利用者の要望を受けた場合に削除 | |
| | | | | 削除証明書の発行が可能 | |
| | | | | 返却・削除できず残存するデータがある 残存データの内容および、法規制等に基づくものである場合は削除できない理由をご記載ください | |
| | | | | 非公開 | |
| 30 | AS-4 | 情報資産を消去または廃棄する場合は復旧できない状態にしていますか。 | | 手続きを文書化している | |
| | | | | 定期的に文書の内容を見直している | |
| | | | ● | 実施している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 31 | AS-5 | クラウドサービスの開発、保守および運用において、私用端末を利用していますか。 | ● | 利用していない | |
| | | | | 利用している 対策の例：端末へのマルウェア対策の導入、外部記録媒体の書き込み無効化、認証・認可のポリシー適用、スクリーンロック設定、紛失時の対応（端末管理システムへの登録）等 | |
| | | | | 非公開 | |
| 32 | AS-6 | 持ち運び可能な外部記憶媒体を利用していますか。 | | はい | |
| | | | ● | いいえ | |
| | | | | 非公開 | |
| 33 | AS-7 | 持ち運び可能な外部記憶媒体の保管や移動、廃棄、取扱者の範囲等の管理手順を定め、その手続きに基づき利用していますか。 | | 定められた手続きや機能に基づき利用していて、定期的に見直ししている | |
| | | | | 定められた手続きや機能に基づき利用しているものの、定期的に見直ししていない | |
| | | | | 定められた手続きや機能は存在しない | |
| | | | | 非公開 | |
| 34 | AS-8 | 持ち運び可能な外部記憶媒体について、実施しているセキュリティ対策をすべて選択してください。 | | 使用可能な媒体を制限 | |
| | | | | 持ち出し禁止もしくは持ち出し時の事前申請 | |
| | | | | 施錠 | |
| | | | | 暗号化 | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 35 | AS-9 | 持ち運び可能な外部記憶媒体の利用は禁止されていますか。該当する選択肢をすべて選択してください。 | ● | 利用禁止であることを明文化している | |
| | | | | システム上利用禁止に設定している | |
| | | | | 該当なし | |
| | | | | 非公開 | |

| | | | | |
|----|-------|---------------------------|---|--|
| 36 | AS-10 | 他のユーザーとデータが混在しないようにしていますか | <div><div>●</div><div>分離している 該当するものをすべて選択してください □サーバー筐体やIaaS/テナントレベルでの分離 □データベーステーブルやスキーマレベルでの分離 ☑アプリケーションレイヤでの論理的分離 □その他</div></div> | |
| | | | 未実施 | |
| | | | 非公開 | |

| | | | | |
|---------------|------|---|--|--|
| 12. AC アクセス制御 | | | | |
| 37 | AC-1 | クラウドサービスの開発、保守および運用において利用するソフトウェア、ハードウェア、ネットワーク上で取り扱われるデータについて、アクセス制御の方針やルールを定めていますか。 | <div><div>●</div><div>定めていて、定期的に見直ししている</div></div> | |
| | | | <div><div></div><div>定めているものの、定期的に見直ししていない</div></div> | |
| | | | <div><div></div><div>定めていない</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 38 | AC-2 | 従業員やシステム管理者が預託データへアクセスすることを原則として禁止とし、アクセスする場合は、事前に承認を得たものに限定していますか。 | <div><div></div><div>手続きを文書化している</div></div> | |
| | | | <div><div></div><div>定期的に文書の内容を見直している</div></div> | |
| | | | <div><div>●</div><div>実施している</div></div> | |
| | | | <div><div></div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 39 | AC-3 | 従業員やシステム管理者が預託データにアクセスする場合は、アクセス者の操作ログをモニタリングしていますか。 | <div><div></div><div>不正や漏洩、データの改変を検出するためモニタリングの観点や手順を文書化している</div></div> | |
| | | | <div><div></div><div>定期的にモニタリングの観点や手続きの文書を見直している</div></div> | |
| | | | <div><div></div><div>モニタリングを実施している</div></div> | |
| | | | <div><div>●</div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 40 | AC-4 | クラウドサービス内のコンポーネントやデータへのアクセスを、業務上必要な従業員にのみ限定していますか。 | <div><div></div><div>手続きを文書化している</div></div> | |
| | | | <div><div></div><div>定期的に文書の内容を見直している</div></div> | |
| | | | <div><div>●</div><div>実施している</div></div> | |
| | | | <div><div></div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 41 | AC-5 | クラウドサービスの開発、保守および運用において、特権アカウントを割当および利用する際は、承認を必須とし必要最小限に制限していますか。 | <div><div></div><div>手続きを文書化している</div></div> | |
| | | | <div><div></div><div>定期的に文書の内容を見直している</div></div> | |
| | | | <div><div>●</div><div>実施している</div></div> | |
| | | | <div><div></div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 42 | AC-6 | クラウドサービスの開発、保守および運用において、特権アカウントを用いた情報資産に対するネットワークアクセスを記録し、適切な利用かどうかをモニタリングしていますか。 | <div><div></div><div>不正や漏洩、データの改変を検出するためモニタリングの観点や手順を文書化している</div></div> | |
| | | | <div><div></div><div>定期的にモニタリングの観点や手続きの文書を見直している</div></div> | |
| | | | <div><div></div><div>モニタリングを実施している</div></div> | |
| | | | <div><div>●</div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 43 | AC-7 | クラウドサービスのコンポーネントにおいて、管理者権限を保持する特権的ユーティリティおよびサービスアカウントのアクセス制限・権限管理として実施していることをすべて選択してください。 | <div><div>●</div><div>用途以上に必要な権限を付与していない（Webサーバーやアプリケーションサーバーのプロセスを管理者権限以外で起動していないなど）</div></div> | |
| | | | <div><div></div><div>サービスやデーモン、プロトコルは必要なもののみ設定および起動をしており、不要なものは起動できないようにしている</div></div> | |
| | | | <div><div></div><div>ログインが必要なサービスアカウントについて十分な認証を行い、ログインが不要なサービスアカウントについては技術的にログイン不可としている</div></div> | |
| | | | <div><div></div><div>該当なし</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |
| 44 | AC-8 | プログラムソースや仕様書等のクラウドサービスに関連する情報へアクセスできる人を業務の必要性や役割に応じて資産単位で限定していますか。 | <div><div></div><div>手続きを文書化している</div></div> | |
| | | | <div><div></div><div>定期的に文書の内容を見直している</div></div> | |
| | | | <div><div>●</div><div>実施している</div></div> | |
| | | | <div><div></div><div>未実施</div></div> | |
| | | | <div><div></div><div>非公開</div></div> | |

| | | | | | |
|----|-------|---|---|---|--|
| 45 | AC-9 | クラウドサービスのリリースもしくはローンチ作業ができる人を限定していますか。 | | 手続きを文書化している | |
| | | | | 定期的に文書の内容を見直している | |
| | | | ● | 実施している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 46 | AC-10 | クラウドサービスの開発、保守および運用において使われるアカウントについて対処していることを選択してください。 | ● | すべてのアカウントを把握している、もしくは把握が可能となっている | |
| | | | ● | 不要となった際に無効化・削除している | |
| | | | | 棚卸している 実施頻度が選択肢の間にある場合、より長い方の選択肢を選んでください（例：2か月→「四半期」を選択、4か月→「半期」を選択） 1年以上のサイクルで定期棚卸しを実施している場合は、「不定期」を選択してください | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 47 | AC-11 | サービスの開発・運用・保守・運営において共有アカウントが利用禁止であることを明文化していますか。もしくは例外的に利用する場合のルールを定めていますか。 | | はい | |
| | | | ● | いいえ | |
| | | | | 非公開 | |
| 48 | AC-12 | クラウドサービスの開発・運用・保守・運営において、共有アカウントを利用していますか。 | ● | はい | 共有アカウントの用途や利用する場合の条件 開発用サービスは個人アカウントですが、運用・保守サーバー接続時はドメインごとに共有のアカウントを利用 |
| | | | | いいえ | |
| | | | | 非公開 | |
| 49 | AC-13 | 共有アカウントを利用する際に実施していることをすべて選択してください。 | ● | 事前に承認を得た場合のみ利用可能としている | |
| | | | | 管理簿や利用ログ等で適切な利用が確認している | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 50 | AC-14 | クラウドサービス利用者がサービスを利用する際の認証機能について、該当するものを選択してください。 | ● | サービス自身が認証機能を提供している（例：サービスにID/Passwordで認証できるログイン画面がある） | |
| | | | | サービス以外のIDプロバイダーとの認証連携機能（SSOなど）を提供している | |
| | | | | その他 | |
| | | | | ログインが不要など、ユーザー認証が不要 | |
| | | | | 非公開 | |
| 51 | AC-15 | クラウドサービス利用者がサービスを利用する際の認証機能のうち、サービス自身が提供している機能について該当するものを選択してください。 | | 多要素認証が適用されている ☑パスワード+ワンタイムパスワード（OTP） | 利用者がOTPを取得する手段 メール |
| | | | ● | ☐パスワード+ユーザー個別の証明書 ☐パスワード+セキュリティキー ☐パスキー認証（多要素パスワードレス認証） ☐その他の多要素認証 | |
| | | | | パスワード以外の単一要素認証で認証されている | |
| | | | | パスワードでのみ認証されている | |
| | | | | 非公開 | |

| | | | | | |
|----|-------|---|---|---|---|
| 52 | AC-16 | サービス自身が提供しているクラウドサービス 利用者の認証機能について、該当するものを すべて選択してください。 | ● | パスワードを利用する場合に安全性を 確保する機能がある ☒パスワードに最小の文字数を設定している ☒パスワードに英数字だけでなく記号も使用 可能である □脆弱なパスワードを制御する機能がある ☒パスワードはソルト付きハッシュで保管さ れる | 最小文字数 10 英数記号をそれぞれ1文字以上使用 Bcryptとランダムソルトとストレッチングによる暗号 化 回数 20回 |
| | | | | リスクベース認証が導入されている | |
| | | | | 管理者権限アカウントと一般アカ운 トで異なる認証ポリシーを設定できる | |
| | | | ● | 複数回認証に失敗した場合はアカ운 トをロックする | |
| | | | | 認証情報の再発行時に本人確認する | |
| | | | | その他 | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 53 | AC-17 | クラウドサービス利用者のアクセス制御について、実施 可能な機能をすべて選択してください。 | ● | アカウントはユーザー毎に発行可能 | 発行済のIDを他の人に重複して払い出しできない仕様 としている場合を含む 60分 |
| | | | ● | IPアドレスによるアクセス制限 | |
| | | | | 利用者共通の証明書によるアクセス端 末制限 | |
| | | | ● | アプリケーションのセッションタイム アウト | |
| | | | | その他 | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 54 | AC-18 | クラウドサービス事業者が利用するサービス 運営のための機能や管理画面などがありますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 55 | AC-19 | クラウドサービス事業者が利用するサービス運営の ためのアカウントについて、SSOログイン認証を 含めて、認証として該当するものを選択してください。 | | 管理画面や管理ツールのすべてのユー ザーアカウントに対して多要素認証が 適用されている 該当する認証要素の組み合わせを選択して ください □パスワード+ワンタイムパスワード (OTP) □パスワード+ユーザー個別の証明書 □パスワード+セキュリティキー □パスキー認証（多要素パスワードレス認 証） □その他の多要素認証 | 認証要素が適用されているアカウントの範囲 アプリ管理者、インフラ管理者 管理画面や管理ツールのユーザーがOTPを取得する手 段を記載してください（例：メール、スマホの認証ア プリ等） アプリ管理者：メール、インフラ管理者：スマート フォンの認証アプリ |
| | | | ● | 管理画面や管理ツールのユーザーアカ ountの一部に多要素認証が適用され ている 該当する認証要素の組み合わせを選択して ください ☒パスワード+ワンタイムパスワード (OTP) □パスワード+ユーザー個別の証明書 □パスワード+セキュリティキー □パスキー認証（多要素パスワードレス認 証） □その他の多要素認証 | |
| | | | | 管理画面やツールを利用するすべての ユーザーアカウントが単一認証で認証 されている 該当する認証要素を選択してください □パスワード □その他の単一認証 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| | | | | | |

| | | | | | |
|-----------|-------|--|---|--|---|
| 56 | AC-20 | クラウドサービス事業者が利用するサービス運営のためのアカウントのアクセスについて、追加で制御していることをすべて選択してください。 | ● | IPアドレスによるアクセス制限 | 60分 最小文字数 10 英数記号をそれぞれ1文字以上使用 |
| | | | ● | 利用者共通の証明書によるアクセス端末制限 | |
| | | | ● | アプリケーションのセッションタイムアウト | |
| | | | ● | パスワードを利用する場合に最小文字数を設定している | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 57 | AC-21 | クラウドサービスの開発、保守および運用に携わる要員が利用するインフラやデータベース、IaaSなどのアカウントについて、SSOログイン認証を含めて実施していることを選択してください。 | | 緊急用アカウントなどの例外を除き、適用可能なすべてのユーザーアカウントに対して多要素認証が適用されている 該当する認証要素の組み合わせを選択してください <input type="checkbox"/> パスワード+ワンタイムパスワード（OTP） <input type="checkbox"/> パスワード+ユーザー個別の証明書 <input type="checkbox"/> パスワード+セキュリティキー <input type="checkbox"/> パスキー認証（多要素パスワードレス認証） <input type="checkbox"/> その他の多要素認証 | 認証要素が適用されているアカウントの範囲 アプリ管理者、インフラ管理者 管理画面や管理ツールのユーザーがOTPを取得する手段を記載してください（例：メール、スマホの認証アプリ等） アプリ管理者：メール、インフラ管理者：スマートフォンの認証アプリ |
| | | | ● | ユーザーアカウントの一部に多要素認証が適用されている 該当する認証要素の組み合わせを選択してください <input checked="" type="checkbox"/> パスワード+ワンタイムパスワード（OTP） <input type="checkbox"/> パスワード+ユーザー個別の証明書 <input type="checkbox"/> パスワード+セキュリティキー <input type="checkbox"/> パスキー認証（多要素パスワードレス認証） <input type="checkbox"/> その他の多要素認証 | |
| | | | | すべてのユーザーアカウントが単一認証で認証されている 該当する認証要素を選択してください <input type="checkbox"/> パスワード <input type="checkbox"/> その他の単一認証 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| | | | | | |
| | | | | | |
| 58 | AC-22 | クラウドサービスの開発、保守および運用に携わる要員が利用するインフラやデータベース、IaaSなどのアカウントのアクセスについて、追加で制御していることをすべて選択してください。 | ● | IPアドレスによるアクセス制限 | 60分 最小文字数 10 |
| | | | ● | 利用者共通の証明書によるアクセス端末制限 | |
| | | | ● | アプリケーションのセッションタイムアウト | |
| | | | ● | パスワードを利用する場合に最小文字数を設定している | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 13. CR 暗号 | | | | | |
| 56 | CR-1 | 暗号化および鍵管理の方針やルールについて、該当することをすべて選択してください。 | | 文書で定めている | 暗号化鍵のパスフレーズは8文字以上 |
| | | | | 定期的に見直している | |
| | | | ● | 定めていない | |
| | | | | 非公開 | |
| 57 | CR-2 | 暗号鍵について、実施していることをすべて選択してください。 | | 必要なときに許可された管理者のみアクセスできるよう制御している | |
| | | | | 鍵管理システムを利用している | |
| | | | | 鍵の利用をモニタリングしている | |
| | | | ● | 用途に応じ、適切に鍵を分類している | |
| | | | | 鍵のライフサイクルを適切に管理し、必要に応じ更新・破棄している | |
| | | | | インフラ提供者が鍵管理を実施している | |
| | | | | 未実施 | |
| | 非公開 | | | | |

| | | | | | |
|----------------------|------------------------------------|--|----|--|----------------------------|
| 58 | CR-3 | サービスの通信に関する暗号化について実施していることをすべて選択してください。 | ● | サービスへのアクセス時の通信を暗号化している | |
| | | | ● | 安全なプロトコルのバージョンのみを使用して暗号化している 対策の例：TLS1.1などの古いバージョンを制限している | |
| | | | ● | 安全な暗号アルゴリズムと十分な鍵長の組み合わせのみを利用している 対策の例：適切な暗号スイートを設定している | |
| | | | ● | 有効期限が切れていない、信頼できる認証局が発行したサーバ証明書を利用している | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| | | | 59 | CR-4 | |
| ● | 安全な暗号方式と十分な鍵長により、バックアップデータを暗号化している | | | | |
| | 該当なし | | | | |
| | 非公開 | | | | |
| | | | | | |
| 14. PH 物理及び環境的セキュリティ | | | | | |
| 60 | PH-1 | クラウドサービスのITインフラストラクチャについて、該当するものをすべて選択してください。 | | 自社データセンター | ハウジング等具体的なデータセンター形態 AWS |
| | | | ● | AWS、Azure、Google CloudなどのIaaS/PaaS等 | |
| | | | | そのほか自社以外のデータセンター | |
| | | | | 非公開 | |
| 61 | PH-2 | データセンターについて、実施している物理的セキュリティ対策をすべて選択してください。 | | 情報資産の重要度に基づいて、物理的セキュリティ対策の位置や強度を定めている | |
| | | | | データセンターへの入館および情報資産が保管されている区画への入室は承認にもとづき許可され、ICカード認証や生体認証等の認証により制御している | |
| | | | | 入退館ログおよび入退室ログを定期的に確認し、不正アクセスがないか確認している | |
| | | | | 特に重要な場所には監視カメラを設置したり、立会人を同行させる等の対策を講じている | |
| | | | | 情報資産のある区画へは、持ち込み品および持ち出し品の制限を行なっている | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| | | | | | |
| 62 | PH-3 | 自然災害や事故への対策として、サーバー室やデータセンター等の重要度に応じて実施していることをすべて選択してください。 | | 電力設備と電力ケーブルを損傷および破壊から保護している | |
| | | | | 主電源が失われた場合に備え非常用電源や無停電電源装置（UPS）を導入している | |
| | | | | 免震や耐震等の地震対策を導入している | |
| | | | | 消火および火災検知のための装置や仕組みを導入している | |
| | | | | 雷対策を導入している | |
| | | | | 温度と湿度を保つための装置や仕組みを導入している | |
| | | | | 防水措置や漏水防止対策を導入している | |
| | | | | 代替通信サービスを確立している | |
| | | | | 代替拠点を用意している | |
| | | | | 上記の対策・設備について定期的に点検している | |
| | | | | 該当なし | |
| | | | | 非公開 | |

| | | | | | |
|------------------|------|---|---|--|---|
| 63 | PH-4 | 利用しているIaaS/PaaS等、そのほか自社以外のデータセンターの選定にあたり、データセンターの入退室管理や自然災害への対策等の物理的なセキュリティ対策を確認していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 15. OP 運用のセキュリティ | | | | | |
| 64 | OP-1 | クラウドサービスの運営に必要な情報を定め文書化していますか。 | ● | 手続きを文書化している | |
| | | | ● | 定期的に文書の内容を見直している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 65 | OP-2 | 構成管理や変更管理により、システム構成やネットワーク構成、変更状況を可視化していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 66 | OP-3 | サービス利用者への通知について、該当するものをすべて選択してください（実施予定のものを含む）。 | | サービスを提供する時間帯もしくはメンテナンス時間を定め、通知もしくは開示している | <div>通知のタイミングおよび通知方法</div> メンテナンス実施の2週間以上前に、システムログイン画面に設けたお知らせ画面にて事前通知を掲載しています。 <div>通知のタイミングおよび通知方法</div> 緊急メンテナンスと同様です。 <div>通知までの目標時間：発生から2時間以内（営業時間内）もしくは翌営業日（営業時間外）</div> <div>通知方法：電子メールまたは電話</div> |
| | | | ● | 緊急もしくは不定期なメンテナンスが必要な場合について、事前に通知している | |
| | | | ● | サービスの大きな変更や終了について、事前に通知している | |
| | | | | サービス提供に関わる障害やパフォーマンス低下等が発生した場合について、速報や追加報告（復旧予測時刻等）を実施している | |
| | | | ● | セキュリティインシデントが発生した場合は速やかに通知している | |
| | | | | アクセス権限設定の仕様を変更する場合は事前に通知している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 67 | OP-4 | 現状だけでなく将来必要となるリソースを考慮し、キャパシティプランニングを実施していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 68 | OP-5 | 障害や災害からあらかじめ定められた目標時間やポイントで復旧できるようクラウドサービスのデータやアプリケーション、環境構成情報のバックアップを取得していますか。 | ● | はい | <div>バックアップの頻度と保存世代数、保存期間</div> 毎日バックアップを取得し、7世代分を一週間保存しています。 |
| | | | | いいえ | |
| | | | | 非公開 | |
| 69 | OP-6 | バックアップから適切に復旧可能とするために実施していることをすべて選択してください。 | ● | バックアップが取得できていることを定期的に確認している | <div>サーバー委託会社では日次バックアップ実施し定期的に取得を確認</div> 自社での日次バックアップ分は不定期で確認 <div>頻度 不定期年1回</div> <div>最終実施日 非公開</div> |
| | | | ● | バックアップデータをクラウドサービスが設置してある場所とは物理的に離れた場所で保管している | |
| | | | ● | バックアップデータを論理的に分離した環境やオフラインストレージ、不変ストレージに保存している | |
| | | | ● | 適切に復旧できるカリスタテストを行っている | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 70 | OP-7 | 関連法令や規制、契約上の要求事項を満たすことができるよう、データやログの保管期間と管理要件を定め、その定めに従って管理していますか。 | ● | 手続きを文書化している | |
| | | | | 定期的に文書の内容を見直している | |
| | | | ● | 実施している | |
| | | | | 未実施 | |
| | | | | 非公開 | |

| | | | | |
|----|-------|---|---|--|
| 71 | OP-8 | 取得しているログをすべて選択し、保管期間を記載してください。 | ● 例外処理や誤操作によるエラー、システム障害、セキュリティインシデントに関するイベントログ ● 該当するものを選択してください。 ☒アプリケーションのログ ☒インフラ（ネットワークやIaaS環境など）のログ □その他 | アプリケーションログの保管期間 2年 インフラ（ネットワークやIaaS環境など）のログの保管期間 2年 保管期間 2年 保管期間 2年 |
| | | | ● サービス利用者の認証ログやアクセスログ、操作ログ | |
| | | | ● システム管理者の認証ログやアクセスログ、操作ログ | |
| | | | ログは取得していない | |
| | | | 非公開 | |
| 72 | OP-9 | 取得したログが不正アクセスおよび改ざんされないよう、アクセス制御や暗号化等により保護していますか。 | 手続きを文書化している | サーバー自体にIPによる管理者のアクセス制御は実施 |
| | | | 定期的に文書の内容を見直している | |
| | | | ● 実施している | |
| | | | 未実施 | |
| 73 | OP-10 | 取得したログが不正アクセスおよび改ざんされないよう、アクセス制御や暗号化等により保護していますか。 | ● はい | |
| | | | いいえ | |
| | | | 非公開 | |
| 74 | OP-11 | クラウドサービスの開発、保守および運用において利用する端末に対するセキュリティ対策を選択してください。 | ● マルウェア対策ソフトやEDRの導入 | |
| | | | ● セキュリティパッチやソフトウェア・OS等のアップデートの適用 | |
| | | | ネットワーク経由（Webやメール）での情報の持ち出し対策 | |
| | | | Webフィルタリングの実施 | |
| | | | その他の対策 | |
| | | | 未実施 | |
| | | | 非公開 | |
| 75 | OP-12 | クラウドサービスの開発、保守および運用において利用する端末へインストールするソフトウェアについて、禁止したソフトウェアが利用されないよう制限やモニタリングをしていますか。 | ● 手続きを文書化している | |
| | | | 定期的に文書の内容を見直している | |
| | | | ● 実施している | |
| | | | 未実施 | |
| | | | 非公開 | |
| 76 | OP-13 | 脆弱性を管理するための方針を定め、その方針に従って脆弱性に対処していますか。 | ● 手続きを文書化している | |
| | | | 定期的に文書の内容を見直している | |
| | | | ● 実施している | |
| | | | 未実施 | |
| | | | 非公開 | |
| 77 | OP-14 | 脆弱性診断やペネトレーションテストについて、実施していることをすべて選択してください。 | プラットフォーム（OS、ミドルウェアやネットワーク）に対する脆弱性診断を実施している ● 実施状況 □定期的に実施 頻度 ☒不定期に実施 最終実施年月 非公開 | |
| | | | 設定診断（セキュリティポスチャアセスメント）を実施している | |
| | | | アプリケーションに対して脆弱性診断を実施している 実施状況 □定期的に実施 頻度 ☒不定期に実施 最終実施年月 非公開 診断対象 ☒Webアプリケーション全体 □API、特定機能や画面当に限定 | |
| | | | サービスに対して第三者によるペネトレーションテストを実施している | |
| | | | その他 | |
| | | | 未実施 | |
| | | | 非公開 | |
| | | | | |

| | | | | | |
|----------------------|-------|--|---|---|-------------------------------|
| 78 | OP-15 | サービスを提供するシステムのOSやミドルウェア、ライブラリ、ファームウェア等すべてのソフトウェアの脆弱性およびEOL, EOS, EOAに関する情報を定期的に収集し、適宜セキュリティパッチの適用やソフトウェアのアップデートを行っていますか。 | | 手続きを文書化している | |
| | | | | 定期的に文書の内容を見直している | |
| | | | ● | EOL, EOS, EOAや脆弱性の情報を把握している | |
| | | | ● | セキュリティパッチやソフトウェアのアップデートを適用している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 79 | OP-16 | クラウドサービスを構成する本番サーバに対して行なっているマルウェア対策を選択してください。 | ● | マルウェア対策ソフトを導入し、リアルタイムスキャン、定期的なウィルススキャンやパターンファイルの最新化を行なっている | |
| | | | | その他の対策を行なっている（EDR利用、その他の総合対策を含む） 脆弱性対応やマルウェア感染の検知、不正アクセスの検知といった代替対策で対応している場合は具体的な対策を記載してください | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 16. MN 監視 | | | | | |
| 80 | MN-1 | セキュリティインシデントやシステム障害を検知するために実施していることをすべて選択してください。 | ● | クラウドサービスおよびネットワークに対するパフォーマンス監視 | |
| | | | ● | クラウドサービスの死活や障害監視、外形監視（運用監視） | |
| | | | | 社内ルール違反等の挙動監視 | |
| | | | | 内部および外部からの不正アクセスや不正利用の監視 | |
| | | | | サイバー攻撃の兆候監視 | |
| | | | ● | 不正なパケットに関する監視 | |
| | | | | サーバーへのリモートアクセスやサービスの環境、IaaS・PaaSの管理画面等へのアクセスの監視 | |
| | | | | 該当なし | |
| | | 非公開 | | | |
| 81 | MN-2 | セキュリティインシデントの兆候検知、発生予防および被害最小化のためにログを効率的に分析する仕組みを導入していますか。 | | はい | CPU、メモリ等の負荷、容量の使用状況等は監視しています。 |
| | | | ● | いいえ | |
| | | | | 非公開 | |
| 17. NW ネットワークのセキュリティ | | | | | |
| 82 | NW-1 | サーバーへのリモートアクセスやサービスの環境、IaaS・PaaSの管理画面等へのアクセスを制限していますか。実施していることをすべて選択してください。 | | アクセスの都度、承認を必要としている | |
| | | | ● | 特定の部署や人からのアクセスに制限している | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 83 | NW-2 | クラウドサービスのネットワークセキュリティ対策について、採用しているツールやサービスを選択してください。 | ● | ファイアウォールまたは類似の通信制御 見直しまたは最新化の実施有無 ○ルールの定期見直しまたは自動的な最新化を実施している ●定期的な見直しや最新化は実施していない | |
| | | | ● | IPSもしくはIDS、または類似の機能 | |
| | | | ● | WAF | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| | | | | | |
| 84 | NW-3 | DDoS等のサービスの維持運用を妨害する攻撃への対策をしていますか。 | ● | はい | 対策内容 Amazon CloudFrontを利用 |
| | | | | いいえ | |
| | | | | 非公開 | |

| | | | | | |
|-----------------------|------|--|---|--|--|
| 85 | NW-4 | 各サーバーの用途に応じた論理的分離により境界を保護していますか。実施していることをすべて選択してください。 | ● | DBサーバーがWebサーバーと分離された構成になっており、WebサーバとDBサーバ間の通信経路が必要最低限になるようアクセスを制御している | |
| | | | ● | DBサーバーは外部から直接アクセスできないようにアクセスを制御している オンプレ環境の場合はDMZにWebサーバを設置、クラウド環境の場合はDBサーバをプライベート環境に設置し、パブリック環境のサーバ経由での通信のみにアクセスを制御している等 | |
| | | | ● | 不要なポートを閉じている | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 18. SY システムの取得、開発及び保守 | | | | | |
| 86 | SY-1 | クラウドサービスの開発、保守および運用において、セキュリティ対策の要求事項を明確にしていますか。 | ● | 明確にしている、定期的に見直ししている | |
| | | | | 明確にしているものの、定期的に見直ししていない | |
| | | | | 明確にしていない | |
| | | | | 非公開 | |
| 87 | SY-2 | クラウドサービスの開発、保守および運用の各工程において、セキュリティや品質を確保するために実施していることをすべて選択してください。 | ● | 機能要件や非機能要件、セキュリティ要件のレビュー | |
| | | | | 各工程における承認プロセスの整備 | |
| | | | | データ修正の承認プロセス、作業手順の整備 | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| 88 | SY-3 | クラウドサービスの開発工程において安全なサービス開発のために実施していることを選択してください。 | ● | コーディング規約などを定め、セキュアコーディングを実施している | |
| | | | ● | ソースコードのレビューをしている 実施状況 <input type="checkbox"/> 人による確認 <input checked="" type="checkbox"/> SASTなどのツールを用いた自動検証 SAST(Static Application Security Testing) : コードの静的解析 | |
| | | | ● | サービスで利用しているOSSを把握している | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| | | | | | |
| 89 | SY-4 | クラウドサービスの開発、保守および運用において、環境やデータの分離について実施していることをすべて選択してください。 | ● | 開発環境と本番環境の分離 | |
| | | | ● | 本番データについて、本番環境以外での利用禁止 | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 90 | SY-5 | アプリケーションを変更する場合は、事前にテストし変更後の影響や不具合がないか確認していますか。実施していることをすべて選択してください。 | ● | 機能要件のテスト | |
| | | | | 非機能要件のテスト 非機能要件テストとは、サービスにおけるセキュリティ要件、性能要件などの非機能要件、および運用プロセスや障害対応プロセス等が想定通りであるかどうかを確かめることを言います | |
| | | | | 該当なし | |
| | | | | 非公開 | |
| | | | | | |
| 91 | SY-6 | アプリケーションを変更する場合は、事前に本番環境と同等の開発環境でテストを実施していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 92 | SY-7 | クラウドサービスのインフラやネットワークを変更する場合に実施していることをすべて選択してください。 | ● | 機能要件のテスト | |
| | | | | 非機能要件のテスト 非機能要件テストとは、サービスにおけるセキュリティ要件、性能要件などの非機能要件、および運用プロセスや障害対応プロセス等が想定通りであるかどうかを確かめることを言います | |
| | | | | 該当なし | |
| | | | | 非公開 | |

| 19. OS 外部委託先管理 | | | | | |
|----------------|------|---|---|--|--------------------------|
| 93 | OS-1 | クラウドサービスの開発、保守および運用において、外部委託先を利用していますか。 | ● | はい | 委託業務 サーバー管理 |
| | | | | いいえ | |
| | | | | 非公開 | |
| 94 | OS-2 | 外部委託先の選定および管理について、方針や基準を定めていますか。 | | 定めていて、定期的に見直している | |
| | | | ● | 定めているものの、定期的に見直していない | |
| | | | | 定めていない | |
| | | | | 非公開 | |
| 95 | OS-3 | 外部委託先に対する要求事項として合意し、文書化していることを選定してください。 | | セキュリティ対策 | |
| | | | | セキュリティインシデント発生時の報告や対処 | |
| | | | | 情報の消去 | |
| | | | | 関連法令の遵守 | |
| | | | | 監査権 | |
| | | | | サービスレベル | |
| | | | | 機能要件や非機能要件 | |
| | | | | 検収基準 | |
| | | | ● | 該当なし | 委託先のセキュリティポリシーを確認するに留まる |
| | | | | 非公開 | |
| 96 | OS-4 | 外部委託先との合意内容が履行されているか定期的に確認していますか。 | | 文書化された手続きや機能に基づき実施していて、定期的に見直ししている | |
| | | | | 文書化された手続きや機能に基づき実施しているものの、定期的に見直ししていない | |
| | | | | 実施しているものの、文書化された手続きや機能は存在しない | |
| | | | ● | 未実施 | |
| | | | | 非公開 | |
| 97 | OS-5 | 外部委託先を定期的に評価していますか。 | ● | 文書化された手続きや機能に基づき実施していて、定期的に見直ししている | 頻度 年一回 最終実施年月 2025-09 |
| | | | | 文書化された手続きや機能に基づき実施しているものの、定期的に見直ししていない | |
| | | | | 実施しているものの、文書化された手続きや機能は存在しない | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 98 | OS-6 | 外部サービスやツールを利用する場合、セキュリティ水準を確認していますか。 | | 文書化された手続きや機能に基づき実施していて、定期的に見直ししている | |
| | | | | 文書化された手続きや機能に基づき実施しているものの、定期的に見直ししていない | |
| | | | | 実施しているものの、文書化された手続きや機能は存在しない | |
| | | | ● | 未実施 | |
| | | | | 非公開 | |

| 20. IM インシデント管理 | | | | | |
|-------------------------------|------|--|---|---|--|
| 99 | IM-1 | セキュリティインシデントやシステム障害に対して迅速かつ効果的に対応するために役割および責任を明確にしていますか。 | ● | 明確にしている、定期的に見直ししている | |
| | | | | 明確にしているものの、定期的に見直ししていない | |
| | | | | 明確にしていない | |
| | | | | 非公開 | |
| 100 | IM-2 | セキュリティインシデントやシステム障害へ対応するための手順を確立していますか。 | ● | 確立している、定期的に見直ししている | |
| | | | | 確立しているものの、定期的に見直ししていない | |
| | | | | 確立していない | |
| | | | | 非公開 | |
| 101 | IM-3 | セキュリティインシデント対応や訓練、他社事例から学んだ教訓をセキュリティインシデント対応手順に取り入れて改善につなげていますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 21. BC 事業継続マネジメントにおける情報セキュリティ | | | | | |
| 102 | BC-1 | 地震や火災等の災害または大規模なシステム障害に備えてリカバリ計画およびコンティンジェンシープランを策定し、定期的な訓練または見直しで実現性を確認していますか。 | | 策定している、定期的に見直しおよびそれに応じた実機訓練をしている | |
| | | | | 策定している、定期的に見直しもしている 机上訓練も含む | |
| | | | ● | 策定しているものの、見直ししていない | |
| | | | | 策定していない | |
| | | | | 非公開 | |
| 103 | BC-2 | 地震や火災等の災害または大規模なシステム障害に備えて複数の拠点や地域にまたがって冗長化されたシステム構成となっていますか。 | | はい マルチリージョン、マルチアベイラビリティゾーン・マルチゾーン構成等を含む。単一DC内での冗長化は、「いいえ」を選択ください | サーバー自体は国内のデータセンターにありバックアップデータは遠隔地に保存し復旧できるようにしています |
| | | | ● | いいえ | |
| | | | | 非公開 | |
| 22. CP 法令遵守 | | | | | |
| 104 | CP-1 | クラウドサービスの提供にあたって順守すべき関連法令や規制、契約上の要求事項を整理し、これらを満たすための取り組みを継続的に実施していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 105 | CP-2 | 個人情報保護に関連する法令や規制上の要求に従って対応していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 106 | CP-3 | プライバシーポリシーを定め、サービス利用者に開示していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 107 | CP-4 | セキュリティ対策が正しく実装され意図したとおり運用されているか、関連法令や規制、契約上の要求事項を満たしているかを独立した評価部門により定期的に評価していますか。実施していることをすべて選択してください。 | ● | 内部監査もしくは内部評価 ISO 27001等のISMS認証を取得している場合は内部監査の実施が必須となります。審査の対象に本サービスを含むかご確認ください | 実施頻度 年一回 最終実施年月 2025-09 |
| | | | ● | 外部監査もしくは外部評価 ISO 27001等のISMS認証を取得している場合は認証取得および更新時に審査が行われます。当該審査の実施時期や審査の対象に本サービスを含むかご確認ください | 実施頻度 年一回 最終実施年月 2025-10 |
| | | | | 未実施 | |
| | | | | 非公開 | |
| | | | | | |

| 23. AT アカウント | | | | | |
|-----------------------------------|-----------------------------|---|-----------------------------------|--|--|
| 108 | AT-1 | クラウドサービス利用者側のアカウントについて、利用企業側で追加や削除、権限変更などが可能ですか。また、それらが可能はロールを限定していますか。 | <div><div></div><div></div></div> | クラウドサービス利用者がアカウントの追加、削除、権限変更などを実施可能 ● 当てはまるものを選択してください。 ● 特定のロール（権限）を持つアカウントのみが当該処理を実施可能 ○ 処理の実施にあたり特定のロール（権限）は不要（通常アカウントで実施可能） | |
| | | | <div><div></div><div></div></div> | クラウドサービス事業者が管理する | |
| | | | <div><div></div><div></div></div> | その他 | |
| | | | <div><div></div><div></div></div> | 非公開 | |
| 109 | AT-2 | クラウドサービス利用者が用いる管理者アカウントには、どのような管理機能が設定されていますか、また設定可能ですか。 | <div><div></div><div></div></div> | アカウントの追加、削除、利用停止（ロック）等 | |
| | | | <div><div></div><div></div></div> | アカウントの一覧表示またはファイル出力 | |
| | | | <div><div></div><div></div></div> | アカウントやグループ単位でのデータアクセスや実行可能機能の制御 | |
| | | | <div><div></div><div></div></div> | ログイン情報や操作ログのダウンロード | |
| | | | <div><div></div><div></div></div> | その他 | |
| | | | <div><div></div><div></div></div> | 該当なし | |
| | | | <div><div></div><div></div></div> | 非公開 | |
| 110 | AT-3 | クラウドサービス利用者のアクセスやログイン記録について、利用者が選択可能な項目や、記録の制約などをすべて選択してください。 | <div><div></div><div></div></div> | ダウンロード機能などにより、利用者がアクセスログを確認可能 ログに含まれる項目を選択してください ☑ ログインID ☑ ログイン日時 ☑ ログアウト日時 □ ログイン認証の成否 | 期間 2年 サーバーのアクセスログは利用者が常時確認できる機能はなく、何らかの重大な事由があり依頼があった場合のみ提供する 詳細を記載してください 利用者名、操作画面名、操作 |
| | | | <div><div></div><div></div></div> | ログや記録を提供可能な期間が限定されている | |
| | | | <div><div></div><div></div></div> | 提供機能はないが、利用者の要請に応じて提供・受渡が可能 | |
| | | | <div><div></div><div></div></div> | その他 | |
| | | | <div><div></div><div></div></div> | 該当なし | |
| | | | <div><div></div><div></div></div> | 非公開 | |
| | | | 111 | AT-4 | |
| <div><div></div><div></div></div> | ログや記録を閲覧可能な期間が限定されている | | | | |
| <div><div></div><div></div></div> | 提供機能はないが、利用者の要請に応じて提供・受渡が可能 | | | | |
| <div><div></div><div></div></div> | その他 | | | | |
| <div><div></div><div></div></div> | 該当なし | | | | |
| <div><div></div><div></div></div> | 非公開 | | | | |

| 24. UP ファイルアップロード | | | | | |
|-------------------|------|--|-----------------------------------|-------------------|--|
| 112 | UT-1 | ファイルをアップロードする機能がある場合、そのファイルに対して実施していることをすべて選択してください。 | <div><div></div><div></div></div> | 暗号化 | |
| | | | <div><div></div><div></div></div> | バックアップ | |
| | | | <div><div></div><div></div></div> | マルウェアスキャン | |
| | | | <div><div></div><div></div></div> | 未実施 | |
| | | | <div><div></div><div></div></div> | ● ファイルのアップロード機能なし | |
| | | | <div><div></div><div></div></div> | 非公開 | |

| 25. DN 独自ドメイン | | | | | |
|---------------|------|---|-----------------------------------|------|---|
| 113 | DN-1 | サービス利用者がアクセスする際に利用するURLは、利用企業毎に異なりますか（利用企業の独自ドメインを使用可能な場合やaaa.example.com、bbb.example.comのようにサブドメインのみ異なる場合も含みます）。 | <div><div></div><div></div></div> | ● はい | 詳細 企業ごとにサブディレクトリが異なるURLになります。 |
| | | | <div><div></div><div></div></div> | いいえ | |
| | | | <div><div></div><div></div></div> | 非公開 | |

| 26. RT 機能制限 | | | | | |
|--------------------|------|---|---|--------------------------------------|---|
| 114 | RT-1 | 他サービスとの連携する機能がある場合、その機能の使用可否はサービス利用者の管理者権限で設定できますか。 | | はい | |
| | | | | いいえ | |
| | | | ● | 該当する機能はない | |
| | | | | 非公開 | |
| 115 | RT-2 | 預託データを公開または外部ユーザへ共有する機能がある場合、それらの機能の使用可否はサービス利用者の管理者権限で設定できますか。 | | はい | |
| | | | | いいえ | |
| | | | ● | 該当する機能はない | |
| | | | | 非公開 | |
| 27. AP API | | | | | |
| 116 | AP-1 | 他サービスとAPI連携していますか。 該当するものをすべて選択してください。 | | 他サービスへAPIを提供している | 詳細 気象データをAPIで取得 オプションでOpenAI API連携機能あり |
| | | | ● | 他サービスのAPIを利用している | |
| | | | | API連携していない | |
| | | | | 非公開 | |
| 117 | AP-2 | 他サービスへのAPI提供について、実施していることをすべて選択してください。 | | API利用者の認証を行なっている | |
| | | | | API認証に利用する情報をアクセス制御や暗号化等により適切に管理している | |
| | | | | API通信を暗号化している | |
| | | | | APIリクエスト数による利用制限を行なっている | |
| | | | | アクセストークンに有効期限を設定している | |
| | | | | APIを対象とした脆弱性診断を実施している | |
| | | | | その他 | |
| | | | | 未実施 | |
| | | | | 非公開 | |
| 118 | AP-3 | 他サービスのAPI利用について、API認証に利用する情報を業務上必要な従業員のみアクセスできるよう制限していますか。 | ● | はい | |
| | | | | いいえ | |
| | | | | 非公開 | |
| 28. SA スマートデバイスアプリ | | | | | |
| 119 | SA-1 | スマートデバイスで利用するアプリが提供されている場合、デバイス経由でのデータ漏えい対策を実施していますか。 | | はい | |
| | | | | いいえ | |
| | | | ● | アプリの提供はない | |
| | | | | 非公開 | |
| 29. EF 電子メール | | | | | |
| 120 | EF-1 | クラウドサービス利用者が電子メールを送信する機能はありますか。 | ● | はい | パスワードリマインダー、招待メール、データ更新のお知らせ |
| | | | | いいえ | |
| | | | | 非公開 | |
| 121 | EF-2 | クラウドサービス利用者が電子メールを送信する機能について、その機能の使用可否は利用者が設定できますか。 | ● | はい | データ更新のお知らせについてのみ、送信の可否を設定できます。設定できるのは、利用企業の管理者権限を持った利用者になります。 |
| | | | | いいえ | |
| | | | | 非公開 | |
| 122 | EF-3 | クラウドサービスから送信される電子メールについて、送信ドメインの詐称（なりすまし）対策を選択してください。 | ● | メールの送信ドメインや送信元アドレスが固定されている | |
| | | | ● | SPFレコードの設定が可能 | |
| | | | ● | DKIMの利用が可能 | |
| | | | ● | DMARCの利用が可能 | |
| | | | | その他 | |
| | | | | 未実施 | |
| | 非公開 | | | | |

| 30. AI AI | | | | | |
|-----------|------|--|----------------------------------|---|--|
| 123 | AI-1 | AIを開発していますか、または既存のAIを利用したサービスを提供していますか。 | <input checked="" type="radio"/> | 利用している | |
| | | | <input type="radio"/> | 開発している | |
| | | | <input type="radio"/> | いいえ | |
| | | | <input type="radio"/> | 非公開 | |
| 124 | AI-2 | AIに関するガバナンス・管理として実施していることを選択してください。 | <input checked="" type="radio"/> | AIサービスの利用者等にむけたサービス規約を作成、明示している | |
| | | | <input type="radio"/> | 学習データの収集・利用について、法令遵守のためのルールを定めている | |
| | | | <input type="radio"/> | 預託データを学習利用する | |
| | | | <input type="radio"/> | その他 | |
| | | | <input type="radio"/> | 該当なし | |
| | | | <input type="radio"/> | 非公開 | |
| 125 | AI-3 | AIに関する品質管理およびセキュリティ対策として実施していることを選択してください。 | <input type="radio"/> | 学習データ、AIの出力結果・判断根拠などを定期的に評価し、バイアス等を継続的にモニタリングしている | |
| | | | <input type="radio"/> | AIに関する攻撃手法や動向について情報収集し、対応している | |
| | | | <input type="radio"/> | その他 | |
| | | | <input checked="" type="radio"/> | 該当なし | |
| | | | <input type="radio"/> | 非公開 | |