Rev.1　2025/04/28

スケジュール管理システム「Skebo（スケボー）」セキュリティチェックシート

1. 公開情報					
1	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。	●	はい	
				いいえ	
				非公開	
2. 第三者認証					
2	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。	●	ISO/IEC 27001	登録番号　OSYQ01-CCER02 有効期限　2025-11 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）
				ISO/IEC 27017	
				プライバシーマーク	
				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. 履歴					
3	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	
			●	いいえ	
				非公開	
4. 法律					
4	1	契約や規約等における準拠法を選択してください。	●	日本法	
				その他	
				該当なし	
				非公開	
5	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。	●	個人情報保護法	
				カリフォルニア州法（CCPA）	
				EU一般データ保護規則（GDPR）	
				その他	
				該当なし	
				非公開	
6	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。	●	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。
				法的な根拠がある場合のみの対応	
			●	必要最低限の個人情報のみの提供	利用目的の達成に必要な情報のみ提供します。
				対応内容の記録	
				該当なし	
				非公開	
5. サービス利用者					
7	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	
			●	法人だけでなく個人での利用も可能	
				非公開	

6. サービスレベル					
8	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	
				稼働実績を開示している	
			●	目標復旧時間(RTO)を定めている	目標復旧時間　2日
			●	サービス提供者の責任範囲を定めている	詳細 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。
			●	サービス利用者とサービス提供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	詳細 電子メール（利用責任者宛て）もしくは電話
				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. データ利用					
9	1	預託データについて、定めていることをすべて選択してください。	●	秘密情報の定義	サービス利用規定および個人情報保護方針にて規定しています。
			●	第三者への開示の禁止 法令等に基づく場合は除く	サービス利用規定および個人情報保護方針にて規定しています。（法令等に基づく場合は除く）
			●	目的外利用の禁止	個人情報保護方針にて規定しています。
				その他	
				該当なし	
				非公開	
10	2	クラウドサービスで取得している情報をすべて選択してください。	●	氏名	ただしサービス上で登録された利用者の情報をシステム提供側では取得できない仕組みとなっています。
			●	メールアドレス	ただしサービス上で登録された利用者の情報をシステム提供側では取得できない仕組みとなっています。
				要配慮個人情報	
				マイナンバー	
				クレジットカード情報	
				Cookie	
				位置情報	
				その他	
				該当なし	
				非公開	
11	3	サービス利用者の個人情報に関する第三者提供について、該当するものをすべて選択してください。		個人情報を匿名化せず第三者提供している	
				個人情報を匿名化し第三者提供している	
			●	個人情報を第三者提供していない	
12	4	サービス利用者の個人情報をサービス提供以外の目的で利用していますか。該当するものをすべて選択してください。		個人情報を匿名化せず自社で利用している	
				個人情報を匿名化し自社で利用している	
			●	利用していない	
13	5	預託データを第三者提供していますか。		はい	
			●	いいえ	
14	6	預託データをサービス提供以外の目的で利用していますか。		はい	
			●	いいえ	
15	7	預託データの利用にあたり、契約や規約等にて利用目的として定めていることをすべて選択してください。		サービスの提供	
				ニュースレター等の情報提供（サービスの提供にかかるもの以外）	
				その他	
			●	該当なし	
				非公開	

16	8	Cookie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 GDPRに準拠する場合は利用するCookieの明記が必要です	
				未実施	
			●	オンライン識別子の利用なし	
				非公開	
17	9	外部委託先が預託データを取り扱うことはありますか。		はい	
			●	いいえ	
				非公開	
18	10	外部サービスの利用や外部委託等により預託データが他国に保管されることはありますか。		はい	
			●	いいえ	
				非公開	
19	11	預託データが他国からアクセスされることはありますか（外部サービスの利用や外部委託等によるアクセスを含む。利用者によるアクセスは含みません）。	●	はい	
				いいえ	
				非公開	
20	12	日本国外に所在する第三者に対して委託のため個人情報を提供する場合、当該第三者との間で合意していることをすべて選択してください。		利用目的の特定	
				目的外利用の禁止	
				違法または不当な行為につながる恐れがある方法による利用の禁止	
				第三者提供の禁止	
				利用する必要のなくなった個人情報の消去	
				安全管理措置の実施	
				従業員の監督	
				さらに他の第三者へ委託する場合の当該委託先の監督	
				漏えい等の事案が発生した場合の通知	
				さらに他の第三者へ提供する場合における各措置の実施の確保	
				合意していない	
			●	日本国外へ提供していない	
				非公開	
21	13	外部委託先や外部サービスに個人情報が委託されることはありますか。委託がある場合は委託先を公開していますか。		個人情報の委託があり委託先を公開している	
				個人情報の委託があるが委託先は公開していない	
			●	個人情報の委託はない	
				非公開	
8. データの所在地					
22	1	サービス提供のため利用しているデータセンターのリージョンやエリアをすべて選択してください（バックアップ用途を含む）。	●	日本	
				US	
				EU	
				中国	
				その他	
				非公開	

9. 情報セキュリティ確保のための組織体制					
23	1	情報セキュリティの維持や向上、監督、それら活動全般を統制する管理上の枠組みを確立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。	●	情報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	
			●	情報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	
			●	情報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	
				自社で対応する箇所、外部に委託する箇所を適切に切り分け、役割と責任を明確にしている	
				該当なし	
				非公開	
24	2	承認されていないもしくは意図しない変更や不正利用のリスクを低減するため、組織の役割と責任に応じて情報資産へのアクセスや閲覧、修正等の権限を分離していますか。	●	分離していて、定期的に見直ししている	
				分離しているものの、定期的に見直ししていない	
				分離していない	
				非公開	
10. 従業員に対するセキュリティ対策					
25	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。	●	情報セキュリティおよび重要情報の取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　2024-07 内容　社内研修資料にて全社員参加で情報セキュリティマネジメント担当者より研修を実施しました。 研修内容は以下（研修資料の目次抜粋）： 運用の手引き 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	
26	2	従業員および契約相手と秘密保持に関する契約を締結をしていますか。	●	はい	
				いいえ	
				非公開	
27	3	従業員および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. 情報資産管理					
28	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	
29	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	サービス終了時に、要求があった場合には返還または破棄します。
			●	明記されていない	
				非公開	

30	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
				利用終了後に自動削除	
			●	ユーザー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	
31	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	
32	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	
33	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	
34	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	
35	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	
36	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	
37	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	●	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	
				未実施	
				非公開	

12. アクセス制御					
38	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。	●	定めていて、定期的に見直ししている	
				定めているものの、定期的に見直ししていない	
				定めていない	
				非公開	
39	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。		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	
40	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。		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続を文書化している	
				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	
				モニタリングを実施している	
			●	未実施	
				非公開	
41	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。		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	
42	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。		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	
43	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。		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続を文書化している	
				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	
				モニタリングを実施している	
			●	未実施	
				非公開	
44	7	クラウドサービスのコンポーネントにおいて、管理者権限や特権的ユーティリティのアクセス制限として実施していることをすべて選択してください。	●	管理者権限でのログインおよびクラウドサービスへのアクセスは必要な場合のみ実施している	
			●	Webサーバやアプリケーションサーバのプロセスを管理者権限以外で起動している	
			●	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	
				該当なし	
				非公開	
45	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。		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	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	

47	10	クラウドサービスの開発、保守および運用において、不要または一定期間使用していないアカウントを無効化あるいは削除していますか。		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	
			●	都度無効化・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	
48	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	
49	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	
50	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	マネージャーに事前承認を得ている
				管理簿や利用ログ等で適切な利用か確認している	
				その他	
				未実施	
				非公開	

			●	IDは各個人に発行し、利用者を特定できる仕様としている 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	
			●	パスワード認証 該当するものをすべて選択してください ☒パスワードに最小の文字数を設定している 最小文字数を記載してください 8文字 ☒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 制御機能の詳細を記載してください ☒パスワードは利用者自身が登録する仕様となっている ☐パスワードの再発行を行う際は本人しか知りえない情報等で本人確認をしている ☐その他のパスワードポリシー 詳細を記載してください パスワードの複雑性や有効期限、世代管理等について記載してください	
51	14	サービス利用者のアカウントについて、実施していることおよび実施可能なことをすべて選択してください。	●	ワンタイムパスワード認証	
				ユーザーごとの証明書による認証	
				生体認証	
				その他の認証方法	
				指定回数続けて認証に失敗したアカウントはロックまたは一定期間認証を不可としている	
			●	セッションの有効期限を設けている	有効期限　60分
				リスクベース認証を用いることができる	
				ネットワーク経路や端末による接続制限ができる 該当するものをすべて選択してください ☐IPアドレス ☐複数のユーザーで共有されるクライアント証明書	
				IDプロバイダーを利用したシングルサインオン（SSO）を用いることができる 例：SAML、OAuth、OpenID Connect等	
				管理者権限アカウントと一般アカウントで異なる認証ポリシーを設定できる	
				未実施	
				非公開	
52	15	サービス事業者（貴社）が利用するサービス運営のための機能や管理画面等がありますか。	●	はい	
				いいえ	
				非公開	

53	16	サービス事業者（貴社）従業員が利用するサービス運営のためのアカウントについて、実施していることをすべて選択してください。	●	パスワード認証 該当するものをすべて選択してください ☒パスワードに最小の文字数を設定している 最小文字数を記載してください 8文字 ☒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 制御機能の詳細を記載してください ☒パスワードは利用者自身が登録する仕様となっている ☐パスワードの再発行を行う際は本人しか知りえない情報等で本人確認をしている ☐その他のパスワードポリシー 詳細を記載してください パスワードの複雑性や有効期限、世代管理等について記載してください	
				ワンタイムパスワード認証	
				ユーザーごとの証明書による認証	
				生体認証	
				その他の認証方法	
				指定回数続けて認証に失敗したアカウントはロックまたは一定期間認証を不可としている	
			●	セッションの有効期限を設けている	有効期限　60分
				リスクベース認証を用いることができる	
				ネットワーク経路や端末による接続制限ができる 該当するものをすべて選択してください ☐IPアドレス ☐複数のユーザーで共有されるクライアント証明書	
				IDプロバイダーを利用したシングルサインオン（SSO）を用いることができる 例：SAML、OAuth、OpenID Connect等	
				管理者権限アカウントと一般アカウントで異なる認証ポリシーを設定できる	
				未実施	
				非公開	

			●	パスワード認証 該当するものをすべて選択してください ☒パスワードに最小の文字数を設定している 　最小文字数を記載してください 　どの業務を行うかによって異なる （基本的には8文字以上） ☐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 　制御機能の詳細を記載してください ☒パスワードは利用者自身が登録する仕様となっている ☐パスワードの再発行を行う際は本人しか知りえない情報等で本人確認をしている ☐その他のパスワードポリシー 　詳細を記載してください パスワードの複雑性や有効期限、世代管理等について記載してください	
54	17	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インフラやデータベース、IaaS等のアカウントについて、実施していることをすべて選択してください。		ワンタイムパスワード認証 スマートフォンのアプリ等、利用する媒体を記載してください メール	
				ユーザーごとの証明書による認証	
				生体認証	
				その他の認証方法	
				指定回数続けて認証に失敗したアカウントはロックまたは一定期間認証を不可としている	
				セッションの有効期限を設けている	
				リスクベース認証を用いることができる	
				ネットワーク経路や端末による接続制限ができる	
				IDプロバイダーを利用したシングルサインオン（SSO）を用いることができる 例：SAML、OAuth、OpenID Connect等	
				未実施	
				非公開	
13. 暗号					
55	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	
56	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	

57	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	
58	4	預託データ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。	●	安全な暗号化方式と十分な鍵長により、預託データが格納されたデータベースやファイルを暗号化している	個人情報に該当する入力項目のみ暗号化
			●	パスワードはソルト付きでハッシュ化し保管している	
				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. 物理及び環境的セキュリティ					
59	1	データセンターの利用形態について、 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	
				IaaS/PaaS等	
			●	そのほか自社以外のデータセンター	ハウジング等具体的なデータセンター形態 ホスティング
				非公開	
60	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	詳細
				非公開	

61	3	自然災害や事故への対策として、サーバ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	詳細
				非公開	
62	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. 運用のセキュリティ					
63	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	
64	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	
65	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	
			●	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	通知のタイミングや通知方法 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。
			●	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	通知のタイミングや通知方法 緊急メンテナンスと同様です。
				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	
66	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	
67	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	バックアップの頻度と保存世代数、保存期間 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	

68	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	自社での日次バックアップ分は不定期で確認 サーバー委託会社でも日次バックアップ実施 頻度　不定期年1回 最終実施日　非公開
			●	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	
			●	適切に復旧できるかリストアテストを行っている	
				該当なし	
				非公開	
69	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	
70	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	
				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	
71	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	
				非公開	
72	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	
73	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	
74	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	
75	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	

76	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	
				設定診断（セキュリティポスチャーアセスメント）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	
77	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	
78	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ウィルス対策を選択してください。	●	ウィルス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. 監視					
79	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	
80	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. ネットワークのセキュリティ					
81	1	サーバ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	

82	2	外部および内部からの不正アクセスを防止するためにファイアウォールを設置していますか（WAFは除く）。		設置していて、定期的に設定を見直している	
			●	設置しているものの、定期的に設定を見直していない	
				設置していない	
				非公開	
83	3	不正なパケットを自動的に発見または遮断するためにIPSやIDSを導入していますか。		導入していて、定期的に設定を見直している	
			●	導入しているものの、定期的に設定を見直していない	サーバー会社に委託しており、見直し等の詳細については非公開となっております。
				導入していない	
				非公開	
84	4	Webアプリケーションの脆弱性を悪用した攻撃等を防止するため、WAFを導入していますか。		導入していて、定期的に設定を見直している	
			●	導入しているものの、定期的に設定を見直していない	
				導入していない	
				非公開	
85	5	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　サーバー会社に委託しており、詳細については非公開となっております。
				いいえ	
				非公開	
86	6	各サーバ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サーバがWebサーバ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. システムの取得、開発及び保守					
87	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。	●	明確にしていて、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	
88	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	
89	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 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	

90	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	
91	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	
92	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	
93	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. 外部委託先管理					
94	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	
			●	いいえ	
				非公開	
95	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	
96	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	
				非公開	
97	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	

98	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	
				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	
99	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	
21. インシデント管理					
100	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。	●	明確にしていて、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	
101	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。	●	確立していて、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	
102	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	
22. 事業継続マネジメントにおける情報セキュリティ					
103	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。		策定していて、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	
				策定していて、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	
104	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ーゾーン・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	
				いいえ	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
				非公開	
23. 法令遵守					
105	1	サービス提供者およびクラウドサービスが満た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	

106	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	
107	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	
108	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　2024/09
			●	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　2024/10
				未実施	
				非公開	
24. アカウント					
109	1	サービス利用者側のアカウントについて、一般的な利用者権限と、管理者権限等の特権を分離していますか。	●	はい	
				いいえ	
				非公開	
110	2	サービス利用において利用者権限とユーザーアカウント管理権限等の特権アカウントでどのような管理機能を分離していますか。	●	アカウントの追加、削除、利用停止（ロック）等	
			●	アカウントの一覧出力	
				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	
				ログのダウンロード	
				その他	
				該当なし	
				非公開	
111	3	サービス利用者のログイン情報について、利用者側の管理者権限を有するユーザーが利用する管理画面や、監査ログのダウンロード機能などにより提供可能な情報や制約を選択してください。		ログイン関連 該当するものをすべて選択してください □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	
				アクセス元	
				ログの提供期間を規定 利用者がログにアクセスできる期間を記載してください（例：ログイン日時から1年間保管など）	
				その他	
			●	該当なし	
				非公開	
112	4	サービス利用者の操作について、利用者側の管理者権限を有するユーザーが利用する管理画面や、監査ログのダウンロード機能などにより提供可能な情報や制約を選択してください。		データの作成・更新・削除記録	
				データの閲覧・検索記録	
				アカウントの作成・更新・削除記録 該当するものをすべて選択してください □操作権限（ロール）変更履歴 □管理権限の付与・はく奪 □パスワード変更（履歴）	
				データのアップロード履歴	
				データのダウンロード履歴	
				ログの提供期間を規定 利用者がログにアクセスできる期間を記載してください（例：閲覧日から遡って1年分のログにアクセス可能など）	
				その他	
			●	該当なし	
				非公開	

25. ファイルアップロード					
113	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。		暗号化	
				バックアップ	
				マルウェアスキャン	
				未実施	
			●	ファイルのアップロード機能なし	
				非公開	
26. 独自ドメイン					
114	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）。	●	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。
				いいえ	
				非公開	
27. 機能制限					
115	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	
116	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	
28. API					
117	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	
				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	
118	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	
119	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	
29. スマートデバイスアプリ					
120	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	
30. 電子メール					
121	1	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と招待メール機能があります。
				いいえ	
				非公開	
122	2	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	
				非公開	

123	3	サービス利用者が電子メールを送信する機能について、どのように送信ドメインの詐称（なりすまし）を防いでいますか。	●	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	
31. AI					
124	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。		利用している	
				開発している	
			●	いいえ	
				非公開	
125	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。		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	
				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	
				預託データを学習利用する	
				その他	
			●	該当なし	
				非公開	
126	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。		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	
				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	
				その他	
			●	該当なし	
				非公開	