スマート書記 セキュリティチェックシート

本チェックシートは、エピックベース株式会社が提供する スマート書記 サービスについて、そのセキュリティ対策を記載したものです。

2023年8月より提供開始した「AIアシスト」をご利用頂く場合には、必ず以下のURLから本セキュリティチェックシート記載内容の変更点をご確認くださいませ。
https://epicbaseinc.my.salesforce.com/sfc/p/2w000003MATB/a/BB000000BlA3/ygdvOPDKROeH9jfF5E7yozThQtax2AFg1tH9TR0w40c

本チェックシートの項目は、それぞれ経済産業省が公開している内容を元に作成したものとなります。
1.「クラウドサービスレベルのチェックリスト」に準拠した運用や開発体制に関するチェックシートです。
2.「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に任意で項目の追加削除を加えて作成したチェックシートです。
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

認証登録概要

認証組織	エピックベース株式会社
認証規格	ISO/IEC 27001:2013, JIS Q 27001:2014
認証番号	IS721524
取得日	2020年4月13日
認証範囲	クラウドサービスを利用した音声をテキスト化するサービスのシステム開発及び企画、販売の業務社

改定履歴

2021/06/14	初版
2021/10/20	記載表記内容の軽微な修正、機能追加による記載追加（パスワード有効期限設定）
2021/11/08	利用規約のURLを変更
2021/12/06	ユーザー認証方法に多要素認証の記載を追加
2022/02/01	サービス稼働率について2020年度から2021年度実績に変更
2022/02/18	データ所在地に関する記述の修正
2022/06/18	記述内容の軽微な修正（リンク先変更等）
2022/10/24	データ漏えい・破壊時の補償/保険に関する記述の修正
2023/04/05	サービス稼働率について2021年度から2022年度実績に変更
2023/08/03	記述内容の軽微な修正、表紙にAIアシスト利用の際のセキュリティ確認事項のURLを追加
2023/08/25	記述内容の軽微な修正

スマート書記 セキュリティチェックシート

1.「クラウドサービスレベルのチェックリスト」に準拠した運用や開発体制に関するチェックシート

No.	種別	サービスレベル項目	規定内容	測定単位	設定
アプリケーション運用					
1	可用性	サービス時間	サービスを提供する時間帯(設備やネットワーク等の点検/保守のための計画停止時間の記述を含む)	時間帯	24時間365日です。(計画停止/定期保守を除く)
2		計画停止予定通知	定期的な保守停止に関する事前連絡確認(事前通知のタイミング/方法の記述を含む)	有無	【有】計画停止については、遅くとも5営業日前までにメールで告知します。
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認(事前通知のタイミング/方法の記述を含む)	有無	【有】現時点で終了の予定はありませんが、なるべく早いタイミングでアカウント管理者のメールアドレス宛に通知します。
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	【無】現時点で終了予定はなく、プログラムやデータの預託も未定です。
5		サービス稼働率	サービスを利用できる確率((計画サービス時間-停止時間)÷計画サービス時間)	稼働率(%)	2022年(1月～12月)の実績値は99.974%でした。
6		ディザスタリカバリ	災害発生時のシステム復旧/サポート体制	有無	【有】インフラストラクチャは複数の拠点を利用し、災害発生時にもシステムを継続的に利用できるように構成しています。また、バックアップデータ等復旧に必要なデータについても、複数の拠点にて管理しています。
7		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	【有】バックアップデータを複数の拠点で管理しています。また、インフラストラクチャはコードで管理しており、バックアップデータと組み合わせることで速やかに新しい環境を構築できる体制を整えています。
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無 (ファイル形式)	【無】
9		アップグレード方針	バージョンアップ/変更管理/パッチ管理の方針	有無	【有】パッチプログラムは迅速に反映を行います。マイナーバージョンアップ以上の変更については、互換性等の確認を実施し、必要に応じて適宜反映を行います。
10	信頼性	平均復旧時間(MTTR)	障害発生から修理完了までの平均時間(修理時間の和÷故障回数)	時間	公開しておりません。
11		目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	時間	公開しておりません。
12		障害発生件数	1年間に発生した障害件数/1年間に発生した対応に長時間(1日以上)要した障害件数	回	2022年(1月～12月)の実績は、4回 / 0回 でした。
13		システム監視基準	システム監視基準(監視内容/監視・通知基準)の設定に基づく監視	有無	【有】CPU やメモリ等の使用率を監視し、あらかじめ指定した閾値を超えた場合に自動でスケーリングを行います。スケーリングが行えないリソースの場合には、システム管理者への通知を行います。
14		障害通知プロセス	障害発生時の連絡プロセス(通知先/方法/経路)	有無	【有】通知はシステムから自動的に管理者のメールアドレス宛に送信されます。また、通知のメールを受信した際に、当社で利用する業務用チャットサービスに対しても障害の発生を通知します。 運用担当者は、システムの異常が発生したことを検知した際に、あらかじめ指定された手段でお客様に障害の発生を通知します。
15		障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	当社への通知は通常数分以内に行われます。お客様への通知は、当社担当者がシステムから通知を受け取った後、可能な限り速やかに実施します。
16		障害監視間隔	障害インシデントを収集/集計する時間間隔	時間(分)	稼働するサービスからの通知は随時、外形監視は5分未満です。
17		サービス提供状況の報告方法/間隔	サービス提供状況を報告する方法/時間間隔	時間	必要に応じて、あらかじめ指定された手段で報告を行います。
18		ログの取得	利用者に提供可能なログの種類(アクセスログ、操作ログ、エラーログ等)	有無	【無】
19	性能	応答時間	処理の応答時間	時間(秒)	公開しておりません。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	公開しておりません。
21		バッチ処理時間	バッチ処理(一括処理)の応答時間	時間(分)	公開しておりません。

1.「クラウドサービスレベルのチェックリスト」に準拠した運用や開発体制に関するチェックシート

No.	種別	サービスレベル項目	規定内容	測定単位	設定
22	拡張性	カスタマイズ性	カスタマイズ(変更)が可能な事項/範囲/仕様等の条件とカスタマイズに必要な情報	有無	【有】サービス画面上から一部の項目で新規登録や変更、削除が可能です
23		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様(API、開発言語等)	有無	【無】
24		同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無(制約条件)	【有】ご契約のユーザー数を上限とした同時接続を保障します。
25		提供リソースの上限	ディスク容量の上限/ページビューの上限	処理能力	【有】ご契約毎に提供機能の利用上限を設けています。
サポート					
26	サポート	サービス提供時間帯(障害対応)	障害対応時の問合せ受付業務を実施する時間帯	時間帯	土日祝日、年末年始を除く平日の10時～18時 ※緊急時は、障害復旧まで上記時間帯に限らず対応予定
27		サービス提供時間帯(一般問合せ)	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	土日祝日、年末年始を除く平日の10時～18時
データ管理					
28	データ管理	バックアップの方法	バックアップ内容(回数、復旧方法など)、データ保管場所/形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無/内容	【有】データベースは最低1日1回のバックアップ、またはバックアップと同等のデータを取得します。バックアップデータは冗長化されたストレージに保管し、データの閲覧者は運用上必要な人員に限定を行っています。
29		バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	時間	バックアップは1日1回、サービスのオフピーク時間で指定された1時間の間に取得されます。これにより、データの復元は25時間前までを保証します。
30		バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	データベースのバックアップは30世代を保存します。およそ30日前までのデータに相当します。ログは 180 日間保存を行います。
31		データ消去の要件	サービス解約後の、データ消去の実施有無/タイミング、保管媒体の破棄の実施有無/タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	【有】データ削除は解約後1ヶ月以内に実施します。
32		バックアップ世代数	保証する世代数	世代数	データベースのバックアップは30世代を保存します。およそ30日前までのデータに相当します。ログは 180 日間の保存を行い、世代数の上限を設けません。
33		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	【有】AES-256方式で暗号化しています。
34		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無/内容	【無】マルチテナントストレージは全顧客で単一のキーを利用します。
35		データ漏えい・破壊時の補償/保険	データ漏えい・破壊時の補償/保険の有無	有無	【有】損害賠償保険に加入しております。
36		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	有無/内容	【無】
37		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	【有】通信は TLS 1.2 以上、データは AES-256 方式以上の堅牢性を持つプロトコルで暗号化を行っています。
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	【有】顧客から提供されるデータについては、値が適切なものかどうかの検証を行った後にデータストアへ保存を行います。不正なデータを検出した場合には、メッセージを表示します。
セキュリティ					
39	セキュリティ	公的認証取得の要件	JIPDECやJQA等で認定している情報処理管理に関する公的認証(ISMS、プライバシーマーク等)が取得されていること	有無	【有】ISMS認証(ISO27001)を取得しています。(認証番号:IS721524) https://help.smartshoki.com/ja/articles/6048940/
40		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無/実施状況	【有】第三者によって提供される脆弱性診断を1年～1.5年周期で実施しています。
41		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	有無	【有】データの取扱は最小限の権限付与を徹底するとともに、社内ネットワークのみのアクセス制限や多要素認証の導入等でアクセスを制限しています。

1.「クラウドサービスレベルのチェックリスト」に準拠した運用や開発体制に関するチェックシート

No.	種別	サービスレベル項目	規定内容	測定単位	設定
42		通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	有無	【有】通信は TLS 1.2 以上のプロトコルで保護します。
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	有無	【無】
44		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	【有】契約毎に割り当てられる ID により、データを論理的に分離して管理しています。
45		情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無/設定状況	【有】データの取扱は最小限の権限付与を徹底するとともに、社内ネットワークのみのアクセス制限や多要素認証の導入等でアクセスを制限しています。利用者のデータについては、運用上必要な者のみへのアクセス権限付与を行っています。
46		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	保管しているログから調査可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	アプリケーションのビルドを行う都度、スキャンを実施しています。スキャンは、オープンソースの Clair プロジェクトの共通脆弱性識別子 (CVEs) データベースを使用しています。
48		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	【有】冗長化されたクラウドストレージ上に保管しており、オブジェクト毎に暗号化を行っています。USB ポートを利用した記録メディアの使用は禁止しています。
49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しています。

2.「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に作成したチェックシート

	確認事項	実施有無	備考
1	情報セキュリティのための方針群		
1	経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	○	当社代表取締役によって承認されたクラウドサービスに関するセキュリティの基本方針を定めています。 当方針は、従業員に対しては社内規定として周知、利用者には当社HP(https://www.epicbase.co.jp/policy/)に公開しています。
2	情報セキュリティに関する基本方針を定めた文書は、定期的またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	○	情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。また、セキュリティ基本方針はISMSにおいて重大な変化が発生した際に見直しています。
2	情報セキュリティのための組織		
1	内部組織		
1	経営陣は、情報セキュリティに関する取り組みについての責任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	○	「情報セキュリティ方針」を定め、以下の目的を達成すべく、業務に携わる役員、社員が継続的に情報セキュリティ対策を推進することを宣言しています。また、ISMSの整備・運用方法を明記した文書（以下、ISMSマニュアル）にて責任およびコミットメントを明記しています。
2	情報セキュリティ責任者とその役割を明確に定めること。またクラウドサービスの情報セキュリティに関する窓口を明確にし、外部に公開すること。	○	情報セキュリティ責任者は代表取締役と定めており、サービスページ内よりサポート窓口を公開しています。
3	情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化すること。	○	ISMSマニュアルにて、情報セキュリティ対策を明記しています。
4	クラウドサービス利用者がクラウドサービスの受け入れを行うために必要な資料を作成し、提供すること。また、提供するクラウドサービスSLA などサービス開始前の合意事項をクラウドサービスの利用を検討する者に明示すること。	○	本チェックシートにて利用者に対し、明示しています。
5	クラウドサービスのサポート窓口、苦情窓口を明確にし、外部に公開すること。	○	土日祝、年末年始を除く平日の10時～18時にて、サービスページ内よりサポート窓口を公開しています。
3	人的資源のセキュリティ		
1	雇用前		
1	従業員のセキュリティの役割及び責任は、情報セキュリティ基本方針に従って定め、文書化すること。また該当文書を雇用予定の従業員に対して説明し、この文書に対する明確な同意をもって雇用契約を結ぶこと。	○	ISMSマニュアルにて、従業者が守るべきセキュリティの役割及び責任を明記しています。 また雇用時に、誓約書を締結しています。
2	雇用期間中		
1	すべての従業員に対して、情報セキュリティに関する意識向上のための教育・訓練を実施すること。	○	入社、新規従事のタイミングで必ず教育・研修を実施し、以後も教育計画に基づいて実施しています。
2	セキュリティ違反を犯した従業員に対する対応手続きを備えること。	○	所定のルールに沿って、懲戒手続きを行うことになっています。
3	雇用の終了又は変更		
1	従業員の雇用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すること。	○	ISMSマニュアルに基づき、適切にアカウントやアクセス権の削除、情報資産の回収を行っています。
4	資産の管理		
1	情報資産について明確にし、重要な情報資産の目録及び各情報資産の利用の許容範囲に関する文書を作成し、維持すること。また情報資産について管理責任者を指定すること。	○	情報資産管理台帳にて情報の分類、リスクレベル、責任者を明記し管理しています。なお下記に分類に対する基本的な考え方を記載しています。 https://www.epicbase.co.jp/policy/
2	組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から情報資産を分類すること。	○	
5	物理的及び環境的セキュリティ		
1	重要な情報資産がある領域を保護するために、物理的セキュリティ境界(例えば、有人受付、カード制御による入口)を用いること。	○	重要な情報資産がある領域(入室制限スペース)は、キー制御を用いて物理的な境界を設けております。
2	重要な情報資産がある領域へ許可された者のみがアクセスできるように入退室等を管理するための手順、管理方法を文書化すること。	○	重要な情報資産がある領域は、許可された者のみがアクセスできるように制御をしております。
6	運用のセキュリティ・アクセス制御		

2.「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に作成したチェックシート

1	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	○	運用管理の手順については文書を作成しており、変更が発生するごとに更新しております。
2	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	○	メンテナンス等、ご利用者様に影響を及ぼすものについては、 事前にメールで通知しております。
3	クラウドサービスを利用できるオペレーティングシステムやウェブブラウザの種類とバージョンを明示すること。利用できるOSとブラウザに変更が生じる場合は事前に通知すること。	○	利用できるウェブブラウザの種類・バージョンは、HP（ https://help.smartshoki.com/ja/articles/6009070/ ）に公開しております。
4	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	脆弱性情報について日次で収集するとともにIPAからの情報を随時受け影響について確認をしております。またパッチの適用についても手順に則り適用作業を実施しております。
5	クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	○	クラウドサービスの利用状況については監視を実施しております。
6	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	○	1～1.5年のペースで第三者機関による脆弱性診断を行っています。 診断結果を踏まえて、計画を立てて対策を行っています。
7	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また、認可されていないモバイルコードを実行できないようにすることが望ましい。	○	自社で作成し配布するモバイルコードについては、自社内で定めたルールに沿って開発が行われております。
8	クラウドサービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	○	日次でデータベースとログのバックアップデータを取得しています。
9	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	○	死活監視、パフォーマンス監視、エラー監視を行っており、サービス停止の検知した場合は、お客様への通知は必要に応じてメールで行います。
10	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	○	死活監視、パフォーマンス監視、エラー監視を行っており、障害を検知した場合は、お客様への通知は必要に応じてメールで行います。
11	システムの運用担当者の作業については記録すること。	○	運用管理者の作業はすべて記録しております。
12	利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログについては定期確認し、改竄、許可されていないアクセスがないように保護する。	○	日次で該当ログのアラートについて取得をしております。また該当のログについては運用管理者及びアクセスが許可されたものがアクセスできる場所に保管しております。
13	クラウドサービス上で取得する利用者の活動、例外処理及びセキュリティ事象を記録した監査ログについて明示すること。また監査ログの保持する期間、提供方法、提供のタイミングについて明示すること。	○	監査ログにつきましては、最低7年間保有しておりますが、現在ログについては外部への提供を行っておりません。 有事の際には、弊社内で確認しご報告いたします。
14	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	○	NTPを利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期を実施しております。
15	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	○	システムのアカウントについては当社規定に則り、各個人にアカウントを付与しております。またシステムにアクセスする際にはVPN網もしくはオフィスネットワークから許可しており、さらにアクセスが許可されていない者がアクセスできないように制御しております。アカウントや暗号化方針については当社規定にて定めております。
16	クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	○	システムへのアクセス権限の追加・削除・変更の方法については手順の文書化を行なっております。特権については業務上必要な一部の開発者のみに制限しています。
17	システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	○	英数字（大文字小文字）と記号を含む8文字以上で設定しています。また多要素認証が設定可能な場合は、設定を行っています。

2.「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に作成したチェックシート

18	クラウド事業者は、クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう、クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	○	ご利用者様からのお問い合わせ時に必要な情報を提示させていただいております。
19	提供するクラウドサービスにおいてアクセス制御機能を提供すること。	○	アカウントごとのID/パスワード、IPアドレス制限、多要素認証によるアクセス制御をおこなっております。
20	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。ネットワーク若しくはインタフェースの分離がなされていない場合、クラウド事業者は、アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。クラウド事業者は、クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために、クラウド環境における情報セキュリティについて評価を実施することが望ましい。	○	登録されたデータについては利用されているお客様以外アクセスできないようにアクセス制限を行っております。
21	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	○	利用者IDの登録・削除の機能を提供しております。
22	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	○	特権の割り当て等の管理する機能を有しておりますが、利用者には提供しておりません。特権アカウントについてはISMSマニュアルに沿って適切に管理しております。
23	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	○	パスワードの有効期限設定機能を提供しています。 英大文字、英小文字、数字、記号を全て含む8文字以上のパスワードが必須となります。
24	提供するクラウドサービスで提供している情報セキュリティ対策及び機能を列記し、明示すること。	○	本チェックシートにて利用者に対し、明示しています。
25	一定の使用中断時間が経過したときには、使用が中断しているセッションを遮断すること。またリスクの高い業務用ソフトウェアについては、接続時間の制限を利用すること。	○	使用中断時間が、ブラウザ36時間、アプリ14日間を経過すると再度ログイン画面が表示されるようにしております。ただしお客様の使用環境により時間に差異がある場合がございます。
26	ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	○	ネットワークを適切に管理し、アクセス制御を行っています。
27	ネットワーク管理者の権限割り当て及び利用は制限し、管理すること。またネットワーク管理者もアクセスを管理するためにセキュリティに配慮したログオン手順、認証技術によって制御すること。	○	ネットワークへのアクセス権限の追加・削除・変更の方法については手順の文書化を行なっております。特権については業務上必要な一部の開発者のみに制限しています。
28	外部及び内部からの不正なアクセスを防止する装置(ファイアウォール等)を導入すること。また利用することを許可したサービスへのアクセスだけを提供すること。	○	ファイアウォールと同等の機能（セキュリティグループ）を導入しています。
29	クラウドサービスへの接続方法に応じた認証方法を提供すること。クラウドサービスへの接続方法に応じた認証方法を、クラウドサービスの利用を検討するものに明示すること。	○	ユーザーのID/パスワード、または多要素認証（ソフトウェアトークン）により、クラウドサービスへの接続が可能です。 その他の認証方法についても今後順次対応予定です。
7	供給者関係		
1	外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること。	○	情報セキュリティマネジメント規定に基づき、適切に運用しております。
8	情報セキュリティ事象・情報セキュリティインシデント		
1	すべての従業員は、システムまたはサービスの中で発見したまたは疑いをもったセキュリティ弱点はどのようなものでも記録し、報告するようにすること。	○	ウィルス感染の疑いや利用しているサービスから情報漏えい等の事故の疑いがあった場合の報告連絡手段、対応手続を定めております。
2	情報セキュリティインシデントに対する迅速、効果的で毅然とした対応をするために責任体制及び手順書を確立すること。	○	ISMSマニュアルにて、責任体制および手順書を明記しています。
3	情報セキュリティインシデントの報告をまとめ、定期的にクラウド利用者に明示すること。	○	情報インシデント発生時には報告をまとめて必要な利害関係者に提示できるようにしています。
9	事業継続マネジメントにおける情報セキュリティの側面		
1	業務プロセスの中断を引き起こし得る事象は、中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに特定すること。	○	事業継続計画書・事業継続計画手順書を作成しております。

2.「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に作成したチェックシート

	2	クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	○	インフラストラクチャは複数の拠点を利用し、災害発生時にもシステムを継続的に利用できるように構成しています。また、バックアップデータ等復旧に必要なデータについても、複数の拠点にて管理しています。
	3	事業継続計画については定期的に試験・更新すること。	○	事業継続計画書を作成し、定期的に試験及び見直しを行なっております。
	4	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	○	全てクラウドサーバを提供する事業者が管理するデータセンターに設置しており、停電・電力障害が発生した場合も電力が供給されるようになっております。
	5	クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	○	全てクラウドサーバを提供する事業者が管理するデータセンターに設置しており、火災検知・通報システム及び消火設備を用意しております。
10	順守			
	1	関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を明確に定め、文書化し、維持すること。また重要な記録については消失、破壊及び改ざんから保護し、適切に管理すること。	○	ISMSに影響を及ぼす可能性のある変更は確認することになっております。またISMSマニュアルは、文書ごとに管理者、承認者、版番号を定め、適切に管理しております。
	2	クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。	○	当社のサービス提供に利用するクラウドサービスは、東京リージョンを基本として、日本国内に位置するデータセンターを利用するように設定しています。準拠法および裁判管轄については、利用規約において定めております。
	3	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい	○	利用規約において定めております。
	4	認可されていない目的のための情報処理施設の利用は阻止すること。	○	利用規約において定めております。
	5	個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、契約事項の中の要求にしたがって確実に保護すること。	○	HPに公開している利用規約に従って取り扱っています。 https://www.smartshoki.com/terms/
	6	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、脆弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。 また、クラウド事業者は、クラウド利用者の個別の監査要求に応える代わりに、クラウド利用者との合意に基づき、独立したレビュー及び評価の結果を提供することが望ましい。	○	スマート書記は、1～1.5年のペースで第三者機関を含む脆弱性診断を行っています。 診断結果を踏まえて、リスク分析を行い適宜計画を立てて対策を行っています。
11	その他			
	1	記録媒体(書類、記録メディア)の保管管理については適切に行うこと。また廃棄する際には記録された情報を復元できないように安全に処分すること。また再利用の際には機密情報の漏えい等につながらないように対処すること。	○	ISMSマニュアルにて記録媒体の情報取扱方法を定め、適切に対応しています。
	2	重要な情報資産については、机の上に放置せず安全な場所に保管すること（クリアデスク）。また離席時には情報を盗み見られないように情報端末の画面をロックすること(クリアスクリーン)。	○	従業者が守るべきセキュリティマニュアルに基づき適切に対応しています。
	3	従業員のパソコンにウィルス対策を行うこと。また技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	従業者が守るべきセキュリティマニュアルに基づき適切に対応しています。
	4	サービス提供を終了する場合は、利用者に対して事前に通知を行うこと。	○	なるべく早いタイミングでアカウント管理者のメールアドレス宛に通知することになっております。