作成日：2024年4月5日

「Smart BTM」 ASP・SaaS 安全・信頼性に係る情報開示指針

項目は「ASP・SaaSの安全・信頼性に係る情報開示指針（ASP・SaaS編）第3版」（総務省）から一部抜粋しております。

【情報開示項目】			【内容】	必須/選択	【回答項目】
1	開示情報の時点	開示情報の日付	開示情報の年月日（西暦）	必須	2024年4月5日
サービス基本特性					
35	サービス内容	サービス名称	本ASP・SaaSのサービス名称	必須	Smart BTM
36		サービス開始時期	本ASP・SaaSのサービス開始年月日（西暦）	必須	2021年10月1日
			サービス開始から申請時までの間の大規模な改変等の有無と、「有り」の場合は改変年月日（西暦）		無し
37		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴	必須	出張時の航空券やホテル、Wi-Fiなどを初期費用・月額費用不要でオンライン予約できるシステムです。 更に24時間365日チャットや電話で自社のオペレーターが対応しており、手配担当者の方も、出張に出かける方もいつでも安心してご利用いただけるサービスになります。
			他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容		無し
38		サービス提供時間	サービスの提供時間帯	必須	24時間365日です。(計画停止/定期保守を除く)
39		サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲（契約内容に依存する場合はその旨記述）	必須	無し
40		移行支援	本サービスを利用する際における既存システムからの移行支援の有無（契約内容に依存する場合はその旨記述）	必須	無し
41		マネージド・サービスやコンサルティング・サービスの提供	本サービスのシステム動作環境の設定や運用支援などをマネージド・サービスやコンサルティング・サービスとして提供しているか、または第3者の当該サービスを紹介しているかの有無。「有り」の場合はその概要	選択	無し

42	サービスの変更・終了	サービス（事業）変更・終了時等の事前告知	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	必須	無し・利用規約第１１条 https://www.iace.co.jp/all/yakkan/smartbtm.html
			告知方法		
43		サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無と、「有り」の場合はその概要	必須	有り サービス終了前に、お客様自身が一部のデータを CSV ファイル等でエクスポート可能。
44	契約の終了等	情報の返却・削除・廃棄	契約終了時等の情報資産（利用者データ等）の返却責任の有無と、受託情報の返還方法・ファイル形式・費用等	必須	無し
			情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等		不可 サービス解約時にデータを削除します。データはサーバサイドで抹消されているため、復旧は不可能です。
			削除又は廃棄したことの証明書等の提供		サービスとしては提供していません。別途、契約者からの申込みにてデータ消去証明書の発行が可能です。
45	サービス料金	料金体系	初期費用額	必須	料金については、下記のURLを参照ください。 https://www.iace.co.jp/smartbtm/#sec_6
			月額利用額		
			最低利用契約期間		1年間
46		解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	必須	無し
47		利用者からの解約事前受付期限	利用者からのサービス解約の受付期限の有無と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	必須	有り： 3ヶ月・利用規約第１５条 https://www.iace.co.jp/all/yakkan/smartbtm.html

48	サービス品質	サービス稼働設定値	サービス稼働率の目標値	必須	非開示
			サービス稼働率の実績値		非開示
			サービス停止の事故歴		非開示
49		サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	選択	有り（詳細は非開示）
			ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要		有り（詳細は非開示）
50		認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1 等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準 ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称。また、組織の方針に基づく内部システム監査等を実施している場合はその概要	選択	有り ISMS認証(ISO27001)　認証番号 GIJP-0946-IC プライバシーマーク(JIS Q 15001準拠)　認定番号　第10450050号
51		脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	選択	有り （アプリケーション診断・ネットワーク診断）
52		システム動作環境の設定・診断に係る支援ツール等の提供	システム動作環境の設定や設定値の診断に係る支援ツール等提供の有無。「有り」の場合は、ツールの概要。	選択	無し
53		学習コンテンツや学習機会の提供	システム動作環境そのものや設定に係る学習コンテンツもしくは講習会等の学習機会の提供有無。「有り」の場合はその概要	選択	有り お客様からのご希望があれば初期設定完了後にユーザー向け講習会を実施しています。
54		バックアップ対策	利用者データのバックアップ実施インターバル	必須	日次
			世代バックアップ（何世代前までかを記述）		7世代
55		サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	必須	有り 冗長化およびフルバックアップ
			DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要		無し
56		受賞・表彰歴	ASP・SaaSに関連する各種アワード等の受賞歴	選択	無し
57		SLA（サービスレベル・アグリーメント）	本サービスに係るSLAが契約書に添付されるか否か	必須	無し

58	契約者数	契約者数	本ASP・SaaSサービスの契約企業数等	選択	非開示
アプリケーション等					
59	連携	他のサービス・事業との連携状況に関する情報提供	他のサービスや事業との連携の有無と、「有り」の場合は情報提供の条件等	必須	無し
60	セキュリティ	死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	必須	有り（サーバーに死活監視を設定しています。）
61		時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	必須	有り（AWSの規格に準じます。）
62		ウイルス対策	ウイルス対策の有無	必須	有り
63		管理者権限の運用管理	システム運用部門の管理者権限の登録・登録削除の手順の有無	必須	有り
64		ID・パスワードの運用管理	事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の状況	必須	利用者のユーザー管理は、利用者の管理者に行っていただきます。 弊社にて、管理、アクセスは行いません。
65		記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、その保存期間及び利用者への提供可否	必須	有り（保管期間1年） ※利用者への提供は不可
			システム運用に関するログの取得の有無と、「有り」の場合は保存期間		有り（保管期間1年）
			ログの改ざん防止措置の有無		有り
66		セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	必須	有り
67		暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	必須	非開示
68		設定不備防止対策	申請したサービスが該当する「クラウドサービス利用・提供における適切な設定のためのガイドライン」における「【評価項目】 a. クラウドにおけるセキュリティ設定項目の類型と対策」それぞれに対する設定不備防止対策の有無。「有り」の場合は、該当項目と設定不備防止対策の概要	必須	「【評価項目】 a. クラウドにおけるセキュリティ設定項目の類型と対策」全項目において推奨設定と同等の設定、対策を行っております。

ネットワーク					
69	センター側ネットワーク	回線	専用線（VPNを含む）、インターネット等の回線の種類	必須	インターネット回線
70		帯域	データ通信速度の範囲、帯域保証の有無	必須	AWSの規格に準じます。
71	セキュリティ	ファイアウォール	ファイアウォール設置等の不正アクセスを防止する措置の有無	必須	有り
72		不正侵入検知	不正パケット、非権限者による不正なサーバ侵入に対する検知等の有無と、「有り」の場合は対応方法	必須	有り
73		ネットワーク監視	事業者とエンドユーザとの間のネットワーク（専用線等）において障害が発生した際の通報時間	選択	監視対象外　（責任範囲外のインターネット回線のため）
74		ユーザ認証	ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法等	必須	パスワード認証、二要素認証をご利用いただけます。
75		なりすまし対策（事業者サイド）	第三者によるなりすましサイトに関する対策の実施の有無と、「有り」の場合は認証の方法	必須	非開示
76		暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	必須	有り サービスとの通信はTLS 1.2以上を強制しています。
77		その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（情報漏洩対策等）	選択	
78	ＰＣ側ネットワーク	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類	必須	インターネット回線
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲		インターネット回線はお客様環境に準じるため、弊社では責任を負いかねます。
79		推奨帯域	推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲	必須	無し
端末					
80	ＰＣ等 （操作端末）	推奨端末	パソコン、スマホ、タブレット、シンクライアント等の端末の種類、OS等	必須	下記にて詳細を記載しております。 「よくあるご質問」→「セキュリティ」→「利用する環境に制限はありますか」 https://www.iace.co.jp/smartbtm/#sec_8
			利用するブラウザの種類		同上

ハウジング（サーバ設置場所）					
81	施設建築物	建物形態	データセンター専用建物か否か	必須	専用ではございません。AWSの国内リージョンを利用しております。
82		所在地	国名、日本の場合は地域ブロック名（例：関東、東北）	必須	日本・関東
			特筆すべき立地上の優位性があれば記述（例：標高、地盤等）	選択	AWSの規格に準じます。 https://aws.amazon.com/jp/compliance/data-center/environmental-layer/
83		耐震・免震構造	耐震数値	必須	有り AWSの規格に準じます。 https://aws.amazon.com/jp/compliance/data-center/controls/
			免震構造や制震構造の有無		同上
84	非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間	必須	同上
85		給電ルート	異なる変電所を経由した給電ルート（系統）で２ルート以上が確保されているか否か	必須	同上
			（自家発電機、UPSを除く）		同上
86		非常用電源	非常用電源（自家発電機）の有無と、「有り」の場合は連続稼働時間の数値	必須	同上
87	消火設備	サーバルーム内消火設備	自動消火設備の有無と、「有り」の場合はガス系消火設備か否か	必須	同上
88		火災感知・報知システム	火災検知システムの有無	必須	同上
89	避雷対策設備	直撃雷対策	直撃雷対策の有無	必須	同上
90		誘導雷対策	誘導雷対策の有無	必須	同上
91	空調設備	空調設備	空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容	必須	同上
92	セキュリティ	入退室管理等	入退室記録の有無と、「有り」の場合はその保存期間	必須	同上
			監視カメラの有無		同上
			個人認証システムの有無		同上
93		媒体の保管	紙、磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットの有無	選択	同上
			保管管理手順書の有無		同上
94		その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（破壊侵入防止対策、防犯監視対策等）	選択	同上

サービスサポート					
95	サービス窓口 （苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	必須	サービス内のチャット及びお問い合わせフォームにて受付 https://www.iace.co.jp/bts/inquiry/smartbtm/
			代理店連絡先の有無と、「有り」の場合は代理店名称、代理店の本店の所在地と連絡先		無し
96		営業日・時間	営業曜日、営業時間（受付時間）	必須	平日10時～17時30分
97		サポート範囲・手段	サポート範囲	必須	・サービス利用／操作方法 ・障害等トラブル対応
			サポート手段（電話、電子メールの返信等）		チャット/メールにてサポート可能です。
98	サービス通知・報告・インシデント対応	メンテナンス等の一時的サービス停止時の事前告知	利用者への告知時期（1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）	必須	緊急時を除き1週間以上前
			告知方法		サービス内及びサービスサイトのお知らせに掲示して通知を行います。また管理者さまへはメールでの通知を行います。
99		障害・災害発生時の通知	障害発生時通知の有無と、「有り」の場合は通知方法及び利用者への通知時間	必須	有り 管理者権限アカウントのメールアドレス宛にメールで通知いたします。
100		セキュリティ・インシデント対応	セキュリティに関するインシデントが発生した場合の対応（通知、被害の拡大防止、暫定対処、本格対処など）	必須	インシデント種別ごとにインシデント対応手続を規定し、連絡経路、被害拡大防止方法、対応方法などを定めております。
101		定期報告	利用者への定期報告の有無（アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等）	必須	無し