セキュリティチェックシート　　対象サービス名 ：請求QUICK　　記入年月日：2025年1月30日

・本チェックシートはSBIビジネス・ソリューションズが提供するSaaSサービスついて、そのセキュリティ対策を記載したものです。
・本チェックシートの項目は「クラウドサービスレベルのチェックリスト」（経済産業省）および「ASP・SaaSの安全・信頼に係る情報開示指針（ASP・SaaS編）第３版」（総務省）を基に、任意で追加/削除を加えて作成したものです。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
サービス運用					
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（アプリケーション・サーバ・ネットワークその他必要な機器と環境の管理・運用・保守対応を行います。※定期メンテナンスのため、月に1回程度、断続的にサービスが停止いたします。）
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 月初に弊社営業担当もしくはカスタマーサポートより、お客様に予めご登録頂いたメールアドレスへの個別メール、もしくはお客様サイトへの案内掲載等にて連絡します。
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 営業からの電話連絡、メール連絡、ホームページ掲載にてご連絡いたします。
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	有 プログラム資材のバックアップ、およびシステム環境のバックアップ、DBバックアップを実施しており、有事の際に復旧できるデータは保有している。
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（ % ）	稼働率は99%以上を目標（定期、臨時メンテナンス時間を除く）とします。但し、AWS及び外部接続先に起因する障害、または天災等による全損的な損害はこれに当てはまりません。
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 災害発生時はバックアップデータからシステム復旧を予定している
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	無
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 システムに変更が発生する処置をする場合、変更内容に限らず必ず修正内容を検証環境にて確認のうえ、動作保障をする。 その後、開発会議の合意もしくはシステム管掌部門長の承認を経て商用環境へ適用する
10		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）	有無	有 冗長化・負荷分散手当済
11	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	非公開
12		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	弊社責任範囲内のサービス障害により弊社営業時間帯にサービスが停止した場合は、障害検知後、12時間以内にサービスを再開することを目標とします。
13		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	お客様がサービス利用不可となるような障害は発生なし
14		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 本サービスで使用する当社管理下のサーバ群の動作を監視するための監視システムを構築し、管理運用します。監視システムでは定期的に以下例示する項目を確認します。 例）サーバのリソース監視、サービス URL へのアクセス可否監視、など ※監視項目は上記に限らず、各サーバの役割に応じて実施します。 監視により障害その他製品利用に影響する問題を検知した場合、原因調査や接続先への問合せその他、問題解消の為の対応を実施します。

15		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 弊社営業担当もしくはカスタマーサポートより、お客様に予めご登録頂いたメールアドレスへの個別メール、もしくはお客様サイトへの案内掲載等にて連絡します。障害に関する情報が更新された場合やシステムの復旧時にも同様にメールにて連絡します。
16		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	障害の重要度により、調査後ご連絡となる可能性がございますため、一概に通知にかかるまでの時間を定義しているものはございません
17		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）	障害の重要度により、調査後ご連絡となる可能性がございますため、一概に通知にかかるまでの時間を定義しているものはございません
18		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	障害の重要度により、調査後ご連絡となる可能性がございますため、一概に通知にかかるまでの時間を定義しているものはございません
19		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	請求QUICKサービス内で、「ログ管理」という機能があり、操作ログ、ログイン履歴等がお客様環境内で表示可能です。 また、検索結果をCSVデータとしてダウンロードいただくことが可能です。 その他、システム内でアクセスログやエラーログ等は取得しており、弊社内での原因調査時には利用しておりますが、基本的には非公開となっております。
20	性能	オンライン応答時間	処理の応答時間	時間（秒）	非公開
21		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開
22		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	非公開
23	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 請求書のフォーマットで、一部出力項目の位置を変更（左右）、ロゴ、印影の設定が可能です。 請求書の発行に際し、発行方法（PDFメール、郵送代行、URLリンク付きメール、クレカ決済つきURLリンクメールなど）を請求書単位で設定することが可能です。 そのほか、銀行口座の明細取得機能（従量課金あり）、請求書買取機能（手数料課金あり）などの機能の提供がございます。 一部機能は継続利用のお申込み/審査、もしくは入金QUICKのお申込み/審査（どちらも請求QUICKユーザサイトにログインいただいたうえで実行が可能）が必要となります。
24		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	有 以下機能をご提供（有償） ・銀行口座の明細情報 ・請求書の発行についての郵送代行機能 ・AIOCR読み取り ・請求書のクレジットカード決済機能（取引先様向け）
25		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	制約条件はないが、ベストエフォート型となります
26		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	現時点では添付ファイルのアップロード上限はございませんが、今後のサービス状況により有限となる可能性がございます。
27	データセンター	データの所在地	サーバーおよびデータ保管先の所在地はどこか。	所在地	日本国内
28		データの再委託	各顧客データ・顧客が入力したデータ取扱いの第三者委託はあるか。	有無	無
29		データセンター入館管理	入退室管理されたコンピュータルームの施錠管理されたラック等、明示的に許可された者以外は触れない環境に設置されているか。	有無	非公開
30		データセンター監査	ユーザーによるデータセンター訪問、監査を受け付けるか。	可否	否

31	ネットワーク	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	有無	有
32		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	有無	有 EDR
33		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	時間	エンドユーザとの間の障害は弊社では検知できません。
34		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	有無	有 SSLサーバ証明書の導入及び、https通信の必須化
35		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）	対応状況	IDS、IPS、FW、アンチウィルス、EDR導入
サポート					
36	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	弊社営業日（年末年始、土日、祝祭日を除く）9:00～17:45
37		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	弊社営業日（年末年始、土日、祝祭日を除く）9:00～17:45
38		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）	有無	無
データ管理					
39	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	日時でバックアップを取得し、遠隔地でのバックアップデータの保管を実施。
40		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	・システム基盤_OS／ミドルウェア：アプリケーション更新時など ・システム基盤_アプリケーション：アプリケーション更新時など ・業務データ_データベース全体：日次
41		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	・システム基盤_OS／ミドルウェア：期限なし ・システム基盤_アプリケーション：期限なし ・業務データ_データベース全体：直近7日分
42		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	利用契約が終了した場合、利用者は、本サービスの利用を直ちに終了するものとし、当社は、利用者の全てのデータを削除します。
43		バックアップ世代数	保証する世代数	世代数	・システム基盤_OS／ミドルウェア：最新状態の1世代前 ・システム基盤_アプリケーション：最新状態の1世代前 ・業務データ_データベース全体：直近7日分
44		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 各サービスへのアクセスはTLS1.2を使用したHTTPS暗号化通信で行います。
45		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
46		データ漏えい・破壊時の補償／保険	データ漏洩・破壊時の補償／保険の有無	有無	無 当社は、本サービスを提供する設備等の故障等によりデータ等が滅失した場合に、復元する目的で利用者に関する情報を一定期間保管します。ただし、当社がそれらの情報を復元する義務を負うものではありません。
47		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	有 解約後社内ワークフローでの承認を経て、データ削除作業を実施しております。
48		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	無
49		機密性の高いデータの要件	個人情報や機密性の高い情報が含まれている場合、それぞれの取扱い規則との整合性を確認できること	有無	無

50		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 それぞれの入力項目について、必要と想定される文字以外は値が入力できないように制御を行っている
セキュリティ					
51	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	弊社はプライバシーマークを取得し、これに基づいた業務管理を実施しております。 【認定番号】第10822526号
52		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 第三者セキュリティ検査機関によって、共通脆弱性評価システム:CVSS等に準拠した脆弱性診断を定期的に実施しています。 脆弱性診断を実施した結果、Web サービス上に情報漏洩、改ざん、なりすまし等の指摘事項が発生した場合には、検知の都度、適切に対処しています。
53		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 プライバシーマークを取得し、これに基づいた業務管理を実施しております。
54		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 TLS1.2以上の通信のみを許可
55		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監査基準に対する資料提供・監査受入れができるか。監査報告書の公開できるか	有無	無
56		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	無
57		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 弊社では製品サービスごとに定められた作業担当者のみ、サーバへのアクセス及び作業を許可しており、特定のアクセス用端末からのみアクセスできる構成になっております。 アクセスに必要なログイン ID、パスワードは、作業担当者と別の運用管理者にて厳重に管理しています。
58		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	有 IDをログ検索で利用することが可能 詳細内容は社外非公開
59		ウイルススキャン	ウイルススキャンの頻度	頻度	リアルタイムファイル保護を実施
60		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 バックアップデータや業務データは暗号化を実施
61		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	日本国内にデータを保管しており、個人情報保護法に則り運用している
62		脆弱性への対応	セキュリティパッチを適用する等、サーバの脆弱性対策を遅滞なくかつ定期的に実施しているか。	頻度	四半期に一度パッチ適用を実施。緊急度の高いものは随時適用を実施。
63		アクセス経路の制限	ファイアウォール等のアクセス制御を行い、公開する必要のない通信ポートは閉じているか。	有無	有
64		不正なアクセスに対する対策	侵入・改ざん・Dos攻撃を検知し制御する仕組みがあるか。	有無	有
65		不要な表示の有無	公開する必要のないディレクトリ・ファイル・設定情報は外部から不可視とし、必要のない機能は、停止する等の措置がされているか。	有無	有
66		セキュリティ検査	公開前にセキュリティ検査を実施し、提供に適した状態であることを確認し報告を提出できるか。	有無	無 診断結果は非公開のため提出不可 外部の脆弱性診断会社を利用し、セキュリティ診断を通過したのちサービスリリースを行っている
67		ログの保持	利用者の活動、セキュリティ事象と関連するログ期間はどのくらいか。	期間	1年間保管
68	基本機能	パスワード定期変更	パスワードに有効期限を設け、再発行を強制する仕組みがあるか。	有無	無
69		パスワード強度	十分な強度のパスワード文字列が設定できるか。	有無	有 一定以上の文字数および、複数種類の文字種を組み合わせて設定する必要があります。
70		多要素認証	ID/PW以外の本人認証の仕組みを設けているか。	有無	無
71		多要素認証（クラウド基盤）	クラウド認証基盤との連携機能（AzureAD連携等）	有無	有 オプション機能として、希望した場合にSSO認証機能を提供可能
72		スマートフォンアプリ	スマートフォンアプリでサービス利用ができるか。利用制約について特記事項はあるか。	有無	無（ブラウザにてご利用いただきます。）

73		アカウントロック	一定回数ログインに失敗した場合に、アカウントを無効化またはロックする機能が提供されているか。	有無	有
74		アクセス制限	利用環境において、第三者がアクセス出来ない仕組みがあるか。IPアドレス制限ができるか。	有無	有 標準機能として、2段階認証機能を提供 オプション機能として、シングルサインオン機能を提供
75		アクセス権限管理	管理者毎のアクセス権限を制御する機能があるか。	有無	有
76		個人情報・企業秘密情報	個人情報や機密性の高い情報がシステム内に保管されるか。	有無	有
77		暗号化対策	暗号化措置（データベース）への対応の有無	有無	有
組織運営					
78	体制	内部不正についての対策1	人的な対策はどのようなものを行っているか。	対応状況	弊社ではすべての従業員と機密保持契約を取り交わしています。また、すべての従業員に対して定期的にコンプライアンスマニュアルを元に教育研修を行っています。
79		内部不正についての対策2	従業員が契約者のデータへ不必要に、許可なくアクセスすることへの抑止力はあるか。	対応状況	商用サービスへの本番データアクセスするためには、社内ユーザ管理者に社内申請をしたのち、承認を受けないと作業ができないように制御されている
80		内部事故についての対策	データの持ち出し・紛失への対策はあるか。	対応状況	MDM（モバイルデバイス管理）を導入
81		ユーティリティ表示	現在のシステム稼働状況を視認できるページは準備されているか。	有無	有
82		セキュリティ領域の確保	オフィスの物理的セキュリティ領域を設け、出入りを管理しているか。	有無	有 執務室全体がセキュリティ領域となり、入退室を管理している
83		セキュリティに関する外部からの指導	契約者の指示による情報管理体制の改善等の指導を受け入れられるか。	可否	否
84		事故発生時の外部監査	セキュリティインシデント発生時、契約者による外部監査を受け入れられるか。	可否	否
85	教育	従業員に対するセキュリティ教育の実施状況	従業員に対するセキュリティ教育実施に関する取り組み状況	対応状況	毎年定期的にeラーニングなどによる研修を全社員に実施
86	規定等	情報セキュリティに関する規程等の整備	情報セキュリティに関する基本方針・規程・マニュアル等の状況と文書名	有無	有 情報ｾｷｭﾘﾃｨ基本規程
87		事業継続に関する規程の整備	事業継続に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	有無	有 危機管理規定
88			BCP対応計画及び運用手順等の開示の可否と、可能な場合の条件等	可否	開示不可
89		リスク管理に関する規程等の整備	リスク管理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	有無	有 個人情報保護基本規定／個人情報保護危機管理規程／情報ｾｷｭﾘﾃｨ基本規程等
90		ASP・SaaSの苦情対応に関する規程等の整備	ASP・SaaSの苦情処理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合はそれらの文書名	有無	有 お客様苦情相談窓口受付書
91			ASP・SaaS事業者の事故責任の範囲と補償範囲が記述された文書の有無と、「有り」の場合は文書名	有無	有 利用規約
92		利用者による設定不備の抑止・防止に係る規程等の整備	サービス提供の際の利用者による設定不備を起こさせないための基本方針・規程・マニュアル等の有無と「有り」の場合は文書名方針等の文書の作成においては、「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」における対策項目を参照すると良い。	有無	有 ユーザサイトメニューとしてWEBマニュアルを提供