OCEANBRIDGE

当チェックシートは、Surfly B.V.（オランダ）の提供するSurflyのセキュリティについて「クラウドサービスレベルのチェックリスト」(経済産業省)に基づき回答した資料です。

最終更新日：2022年1月

No.	種別	サービスレベル項目	規定内容	測定単位	回答	備考
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	計画停止及び、定期保守を除きます。
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	定期的メンテナンススケジュールを事前にご案内します。
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	現時点でサービス提供の停止予定はございませんが、サービス停止の際は決定しだい事前に電子メールで通知いたします。
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	無	クラウドサービスとしての利用のみを想定しているため、移行ツールは提供していません。
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（%）	月間99.95%	
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	サーバーは冗長構成であり、定期的に冗長サーバーへ同期を行っています。プライマリサーバーで異常が発生した場合は、セカンダリサーバーが対応するアクティブ/パッシブ・フェイルオーバー方式を採用しています。また、ディザスタリカバリに関するプロセス規定が存在し、またそのテストが定期的（少なくとも6ヶ月ごと）に実施されています。
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	無	システムが利用できなくなった際の代替措置は準備しておりません。 冗長サーバへの切り替え/データ移行などにより早期に復旧させる構成としております。
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	代替措置で提供されるデータはありません。
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	変更管理プロセスのルールに従い、品質テストを実施した上でリリースを行っています。
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	30分	
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	0回	システム停止を伴う障害は発生しておりません。
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	規定のアクセス制御ポリシーに順守しています。ISO 27001の認定を受け、SOC 2 Type 2 報告書を保証する外部の独立した監視サービスを使用してすべてのアクセス要求を監査します。ファイアウォール、IDS/IPS、DNSなどの複数のセキュリティレイヤーを使用してDDOS攻撃などの対策を行っています。
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	登録されたメールアドレスに対して24時間365日で障害発生・復旧通知を行います。
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	1分	
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）	24時間365日	重大度の高いインシデントは24時間年中無休で監視され、サービスの停止関連するインシデントが発生した場合はSurfly B.V.エンジニアに自動的に警告が通知されます。 重大度の低いインシデントは、Surfly B.V. の業務時間内に監視をしています。
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	有	サーバーの稼働ステータスおよびインシデント履歴が確認可能です。
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	有	セッションログはユーザー情報以外（IPアドレス等クライアントを特定可能なデータやログイン情報）は保存しません。取得するにはAWS S3の利用が必要になります。 システムログは権限のある数名のみしかアクセスできません。障害調査などを行う際はシステムログを利用します。
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）	-	Surflyに該当する処理はありません。
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	無	カスタマイズすることはできません
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	有	JavascriptAPI と RESTAPIが提供されています。
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）	無	リソース環境（CPU利用率、メモリ使用量など）は定期的に監視し必要に応じてサーバスペックの拡張を実施します。これにより安定的なサービスを維持します。 サービス全体としては20万人のユーザがいます
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	ページアセットの場合は25MB、ドキュメントの場合は100MBです。
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	有	オーシャンブリッジの受付時間：平日10：00～17：00（土・日曜、祝祭日、オーシャンブリッジ休業日は除く）
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	有	オーシャンブリッジの受付時間：平日10：00～17：00（土・日曜、祝祭日、オーシャンブリッジ休業日は除く） ※ご連絡はメールでのみ受け付けております（電話でのお問い合わせは受け付けておりませんのでご了承下さい）。

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	バックアップ方法：外部サーバへのスナップショットの保存 バックアップ対象：user-db 実行頻度：日次 保管場所：非公開 暗号化強度：AES 鍵長：256bit
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	日次	セッションデータは保存されません。
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	720時間	30日間
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	セッションデータは不揮発性ディスク上に一切保存されません。アカウント情報は契約終了後、速やかに削除いたします。 お客様専用環境をご利用の場合は、解約後すみやかに環境消去を実施いたします。
32		バックアップ世代数	保証する世代数	世代数	30世代	日次バックアップデータは720時間（30日間）保存されます。
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	セッションデータは不揮発性ディスク上に一切保存されません。セッションの間のみ有効かつ常に暗号化されています。 ユーザーDBは、氏名、メールアドレスなどの詳細およびセッションの参加者数、時間などセッションのメタデータのみを保持します。
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	有	規定のアクセス制御ポリシーに順守しています。暗号鍵にはSSHキーを使用し、IPアドレスによるアクセス制限と組み合わせて、サーバーへのアクセス制御に必要な最小限のSSHキーを管理します。すべてのパスワードはPKBDF2暗号化を使用して暗号化され解読不能となっています。また、すべての通信データは、TLS1.2/1.3を使用して暗号化されます。当サービスにおいて契約者側へのキーの提供及び認識事項はありません。
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	サイバー保険はありませんが、専門職賠償責任保険は、顧客情報などの特定の種類のデータ侵害をカバーしています。
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	有	セッションデータは不揮発性ディスク上に一切保存されません。アカウント情報は契約終了後、速やかに削除いたします。 お客様専用環境をご利用の場合は、解約後すみやかに環境消去を実施いたします。
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	Surflyはプロキシサーバとして機能し、元のWebサイトのコンテンツを書き換えますが、変更はしません。 セッション中のユーザーからのデータ入力は、監査ログを使用して記録できます。
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	ダッシュボードの設定値に想定外のデータが入力された場合は、保存処理時に警告を表示します。 ゴブラウズ中では元のWebアプリ（閲覧しているWebアプリ）の動作をシミュレートします。
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	開発元（Surfly B.V.）は、ISMS認証(ISO27001)を取得しています。
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	ポリシーの一環として、毎年、独立したサードパーティの脆弱性評価/侵入テストを委託しています。
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	規定のリモート作業ポリシーおよびプロセスに順守しています。データセンターへの物理的なアクセスは有効な認証を持つ従業員に限定されているほか、仮想的なアクセスは限定されたIP範囲かつ認証済み従業員からのアクセスのみに制限されています。また強力なアクセスキーを使用した多要素認証またはワンタイムパスワードが必須になります。
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	すべての通信データは、TLS1.2/1.3を使用して暗号化されます。
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	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は行っていません。 ISO27001の認証を受けており、その監査を受けています。
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	契約者（企業）ごとで登録情報を論理的に分離しています。
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	規定のリモート作業ポリシーおよびプロセスに順守しています。データセンターへの物理的なアクセスは有効な認証を持つ従業員に限定されているほか、仮想的なアクセスは限定されたIP範囲かつ認証済み従業員からのアクセスのみに制限されています。また強力なアクセスキーを使用した多要素認証またはワンタイムパスワードが必須になります。
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	有	規定のアクセス制御ポリシーに順守しており、アカウントは個人を識別できるよう1人に1つのアカウントを交付し、共有アカウントは認めておりません。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	自動更新	自動管理、更新を行うデバイスマネージャーがすべての端末にインストールされています。
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	バックアップデータは、AES（鍵長256bit以上）で暗号化されています。 ポータブルストレージメディアの使用は許可していません。
49		データの外部保存方針	データ保存時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	把握しています	オランダのKVK（商工会議所）に登録されており、法制度に従います。 GDPRに準拠しています。また、事業国の現地規制を遵守するよう努めています。

当社補足事項						
50	データセンター	データ所在地	サーバ及びデータ保管先の所在地はどこか	所在地	AWS　東京リージョン	東京リージョンでのSurflyサービスの提供は当社のみとなります。
51		立ち入り調査	インシデント発生時の立ち入り調査は可能か	有無	無	AWS リスクおよびコンプライアンス より抜粋 https://aws.amazon.com/jp/compliance/resources/ 「AWS のデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポートの一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。」
52	セキュリティ	パッチの適用	仮想サーバに対するパッチの適用及び管理	有無	有	おおよそ週2回の頻度で、安定版のセキュリティパッチをチェックして通知・適用する自動ジョブを実行しています。
53		証拠保全	インシデント発生時のデジタルフォレンジック対応はされているか	有無	有	セキュリティインシデントの記録、対処、再発防止策に関するプロセスおよびポリシーを定義し、順守しています。 保護されたデータや機密データを含む盗難、データ侵害、暴露が確認され次第、そのリソースへのすべてのアクセスを削除するプロセスが開始されるほか、クライアントには盗難やデータ違反があったことが直ちに通知されます。続いて外部のフォレンジック調査団の助けを借りて、根本原因を特定するために侵害や漏洩の分析を行います。 なお現在までに上記の対応が必要となるような事例は発生していません。
54		NDAの締結	サービス上に保管されたデータに対する秘密保持契約(NDA)の締結が可能か。	有無	有	契約者とオーシャンブリッジ間でNDA締結可能です。Surfly B.V. の機密保持については、Surfly B.V.・オーシャンブリッジ間で厳格なNDAを締結しており、オーシャンブリッジを介してSurfly B.V. が受領する営業秘密には機密保持義務が課されています。
55	アプリケーション	パスワード管理	ID/パスワード認証において一定の複雑性を備えるパスワードのみを認める機能を設けているか	有無	有	・パスワードの桁数（８文字以上） ・使用する文字の種類（英字、数字、記号のうち２種類以上）
56		アカウント管理	不要となったアカウントは管理されているか	有無	有	非アクティブなアカウントは90日後に無効化されます。
57		アクセス認証	アクセス認証の有効期限が設定されているか	有無	有	アクセス認証Cookieの期限は2週間です。 セッションはリーダーからの通信を検知できない際に一時停止し、その後120秒以内（初期設定値）に再接続されない場合無効となります。
58		アクセス制限	サービスへのアクセス制限機能を有しているか	有無	有	設定により、許可されたIPアドレスまたはサブネットに一致するネットワークからのみログイン可能になるようアクセス制御ができます。
59	サービス	問い合わせ	通常時の問合せ対応について、問い合わせを受付してから回答までの、以下それぞれの平均的な所要時間	時間	左記	問合せ受付（メール）：以下対応方法 SurflyB.V. で規定されている問題に対する重大度レベルによって回答及び、対応までの時間が異なります。 通常時の問い合わせの多くは重大度S3もしくはS4レベルとして扱われます。 【レベル】 S3：ほとんどの機能が引き続き機能する実稼働環境で生じたエラー S4：サービス自体に特定の影響がない問い合わせ 【対応】 S3：最善の努力を尽くして可能な限り迅速に解決されます。 S4：六か月以内のソフトウェアの定期メンテナンスリリースで解決されます。 ※詳細に関しては「Surfly support guide.pdf」(英文)をご確認ください。
60	契約	影響法令	サービスの提供が行われる国・地域、及び適用される法令	準拠法	オランダ法	お客様とSurfly B.V.との間の契約に適用される法令はオランダ法となり、 アムステルダム裁判所が専属的合意管轄裁判所となります。
61		責任範囲	責任範囲の明確化	有無	有	Surfly B.V. との関係についてはSurfly クラウドライセンス契約書に従います。 当社提供の保守サポートに関してはSurfly 保守サポートサービス利用規約に従います。 https://www.oceanbridge.jp/info/agreement_surfly.html

付録		
分類	**文書名**	**資料**
契約書	Surfly クラウドライセンス契約書	https://www.surfly.jp/wp-content/uploads/2021/07/surfly_user_license_contract.pdf
利用規約	Surfly 保守サポートサービス利用規約	https://www.surfly.jp/wp-content/uploads/2021/07/surfly_service_terms_and_conditions.pdf
個人情報の取り扱い	オーシャンブリッジの個人情報の取り扱いについて	https://www.oceanbridge.jp/info/privacypolicy.html