データセンター		
建屋等		
1	データセンターの所在地はどこですか？	東京リージョン（AZ：アベイラビリティーゾーン 4箇所）で管理しています。 各リージョンは「AZ」と言われるローカルリージョンで構成されます。
2	データセンター専用建物ですか？ （耐震・免震構造など）	AWS社のデータセンター専用建物となっております。
3	給電ルートは冗長化されていますか？	電力システムは、24時間365日、運用に影響を与えないよう、完全な冗長化と保守が可能な設計になっています。
4	無停電電源（UPS）や、非常用電源の用意はありますか？	無停電電源装置とバックアップ発電機を設置し、停電時の負荷をサポートしています。
5	火災感知・報知システムはありますか？	火災または煙の被害リスクを軽減するために自動火災検知・消火設備が設置されています。
6	不正侵入対策はされていますか？	データセンターのサイトへの立ち入りは、ビデオ監視、侵入検知、およびアクセスログモニタリングシステムを使用して継続的に監視されています。入口はデバイスで保護されており、ドアがこじ開けられた場合や開け放したままの場合にアラームが鳴るようになっています。
マシンルーム等		
7	サーバーマシンルームとオペレーションルームは分離されていますか？	分離されております。 サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。
8	入退室管理はされていますか？	AWSのデータセンターの境界防御レイヤーへの立ち入りは、管理されています。入口ゲートには警備員を配備し、監視カメラで警備員と訪問者を監視する監督者を雇用しています。
9	入退室記録は保存されていますか？保管期間は？	権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ（CCTV）カメラで録画されています。録画は 90 日間保存されます。ただし、法的または契約義務により 30 日間に制限される場合もあります。
10	社員証やバッチなどにより、構内従業者と訪問者の区別は外見から行えるような措置が取られていますか？	立ち入りを許可された人はバッジを渡されます。このバッジにより、多要素認証が実行され、アクセスが事前に承認されたエリアに制限されます。
11	サーバールーム内を監視するカメラ設備はありますか？	有ります。 監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。
12	十分な空調設備は備わっていますか？	サーバーなどのハードウェアの動作温度を一定に保つための制御により、過熱を防ぎ、サービス停止の可能性を低減します。データセンターは、大気の状態を指定されたレベルに維持するように条件付けされています。人員やシステムが温度や湿度を適切なレベルで監視し、制御しています。
13	サーバルーム内消火設備はありますか？	有ります。 火災または煙の被害リスクを軽減するために自動火災検知・消火設備が設置されており、AWSでは火災発生時に緊急対応者に連絡するプロセスが定められています。
その他		
14	第三者セキュリティ認証は何を取得していますか？	2024年8月にISO27001、27017を取得しています。
15	ユーザ企業の監査の受け入れは可能ですか？	不可となります。 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。
	CHROFYサービスは、『Amazon QuickSight』サービス上で稼働しております。 Amazon QuickSight は、フルマネージド型のクラウドベースのサービスとして、エンタープライズグレードのセキュリティ、 グローバルな可用性、組み込みの冗長性を提供します。 より詳細な情報確認は下記情報をご参照ください。 https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/welcome.html	
安全管理措置		
サーバー		
16	サーバーに対するウィルス対策や不正アクセスなどに対する対策は施されていますか？	CHROFYが利用する各種AWSサービス（S3、Lambda、QuickSightなど）を構成するサーバについては定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCIDSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。
17	OSのセキュリティパッチの適用を実施していますか？	CHROFYが利用しているS3、Lambda、QuickSight、CloudFrontの各種サービスについてはAWSのマネジメントサービスとなり、AWSポリシーに従い、またISO27001、NIST、およびPCIの要件に準拠して、AWSのポリシーに従い実行されます。
18	ソフトウェアのセキュリティパッチの適用を実施していますか？	CHROFYが利用しているS3、Lambda、QuickSight、CloudFrontの各種サービスについてはAWSのマネジメントサービスとなり、AWSポリシーに従い、またISO27001、NIST、およびPCIの要件に準拠して、必要に応じて実行されます。
19	不正アクセスに対する防御および監視を実施していますか？	GuardDutyを利用して、S3やLambdaの異常な動き、認証情報の抽出、コマンドおよびコントロールインフラストラクチャ（C2）通信などの潜在的な悪意のあるアクティビティの監視を行います。
20	各種脆弱性攻撃への対策は行っていますか？	IPAで設定されているセキュリティ基準に基づき、各種対策を実施しています。
21	脆弱性診断を実施していますか？	機能開発時に内部脆弱性診断、年1回の外部脆弱性診断を実施しております。 また、CHROFYサービス提供で利用しているLambdaについてはAmazon Inspectorを利用してコードおよび利用パッケージの定期的な脆弱性スキャンを実施しています。
22	インターネットとの境界にファイアウォールが設置されていますか？	ファイアウォールについては未設置となります。 CHROFYのサービスとしてログインページ自体は一般公開されておりますが、ログイン後のサービスコンテンツはAWSの認証認可の仕組みにより企業・IPアドレスといった情報でのアクセス制限機能を設けています。
23	必要な通信ポートのみに制限されていますか？	利用ポートは443にのみに制限され、不要な通信ポートは閉塞しております。
24	ファイアウォールの設定内容や設定ファイルは定期的に確認管理されていますか？	ファイアウォール未設置となります。 各種リソースへの認証認可のアクセスポリシーについて定期的に設定ポリシー管理を実施しています。
25	DMZは設置されていますか？	DMZは設置していません。

ネットワーク		
26	通信の安全性は実装されていますか？	CHROFYへの通信はすべてTLS1.2による暗号化を行っています。
27	なりすまし対策はされていますか？	ID/PWの知識認証以外にSMS通知による所有物認証を適用させることで、なりすましによる不正アクセスのリスク低減措置をとっています。 ※SMS通知による認証の追加はオプションです。
データ保管		
28	データの暗号化は実施されていますか？	個人情報を含むデータについては所属企業のユーザ以外は閲覧できないようにKMSを利用して暗号化しています。
29	バックアップは取得されていますか？またその取得周期、世代数、保管場所は？	S3とDynamoDBのバックアップを取得・保管しています。 S3 ・周期：日次（定期） ・世代数：62 ・保管場所：同一リージョン ・保管単位：ご契約の法人単位のバケット単位でバックアップ取得、保管を実施 DynamoDB ・周期：日次（定期） ・世代数：30 ・保管場所：同一リージョン ・保管単位：テーブル単位でバックアップ取得、保管を実施（法人単位のではなくシステム単位）
30	遠隔バックアップは取得されていますか？またその取得周期、世代数、保管場所は？	遠隔バックアップは未実施となります。 S3の各ファイル単位で同一リージョン内の複数AZにレプリケーションされ管理されるため1つのAZで障害が発生した場合でも残りのAZでサービスが継続されるためCHROFYのサービス提供に影響はありません。 別リージョンへの遠隔バックアップが要件として必要になる場合は、以下のような設定で法人単位でのバックアップの取得も可能です。 ・周期：毎日夜間 ・世代数：設定次第 ・保管場所：別リージョン ・保管単位：企業単位
31	解約後、復元不可能な状態で環境の削除を行っていますか？行っている場合、削除までの期間は？	復元不可能な状態で環境を削除しております。 削除までの期間は解約後30日以内です。
32	環境削除の証明書の発行は可能ですか？	環境削除証明書の発行を希望される場合は、CHROFY社で発行します。
障害対策		
33	システム機器は冗長化されていますか？	CHROFYではAWSのマネージドサービスを利用したSaaSサービスの構築・提供を行っており、各マネージドサービスに対して明示的な機器の冗長化は行っておりません。 各種サービスの冗長化についてはAWSの設計・管理に依存します。 ※ご参考：AWSのデータセンター（インフラストラクチャー・レイヤー） https://aws.amazon.com/jp/compliance/data-center/infrastructure-layer/
34	障害を監視していますか？	AWS Health Dashboard は、AWS サービスの可用性と運用について知ることができます。AWS サービスの全体的なステータスを表示することができ、特定の AWS アカウントまたは組織の一部であるアカウントに関する個別化された通信を表示するには、サインインすることができます。アカウントビューは、リソースの問題、今後の変更、および重要な通知に関するインサイトを提供します。
35	障害発生時に通知はされますか？またその手段は？	AWS Health Dashboardを参照する運用となっています。
36	どのようなログを取得していますか？またその保管期間は？	ログ種類：アクセスログ、エラーログ、ウイルス検知イベントログ 保管期間：無期限（ウイルス検知イベントは最大30日間）
37	ログの正当性を担保するため、時刻の同期をしていますか？	NTPサーバとクロック同期しております。
その他		
38	ID/PW以外に、ログインに必要なものはありますか？	ID/PWの知識認証以外にSMS通知による所有物認証が利用可能です。 ※SMS通知による認証の追加はオプションです。
39	CHROFY株式会社として取得している認証はありますか？	2024年8月にISO27001、27017を取得しています。