Safieクラウドサービス　セキュリティチェックシート

最終更新日： 2025年1月6日

No	種別	項目	確認内容	測定単位	セーフィーの回答	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日提供しています。	
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	定期メンテナンスは基本的にサービス停止を伴わずに実施しています。 停止を伴うメンテナンスが発生した場合は、事前に当社ホームページ、Safie Viewerの「お知らせ」及びメール配信通知をメンテナンス予定の1カ月前程度に周知します。	サービス利用規約(第6条 本サービスの停止等) https://safie.link/about/terms-of-service/
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	サービス提供を終了する1か月前に、ホームページ、Safie Viewerの「お知らせ」及びメール配信にて通知します。	サービス利用規約(第6条 本サービスの停止等) https://safie.link/about/terms-of-service/
4		突然のサービス提供停止に対する対処	プログラムの預託等の措置の有無	有無	対応していません。	
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(%)	当社では正式にSLAを規定しておりませんが、独自の算出方法に基づく2024年の稼働率は100%を達成しております。	
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	データセンター、ネットワーク、サーバーなどの物理レイヤが冗長化されたクラウド環境にシステムを構築し、障害対応手順と復旧手順に従い、システム復旧が可能な体制を整えています。	災害時には本サービスは停止する可能性があることを、利用規約に明記しています。 サービス利用規約(第6条 本サービスの停止等) https://safie.link/about/terms-of-service/
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	代替措置が必要な場合は、当社の復旧手順書に従い代替対応を行います。	障害内容によって代替対応できない場合があります。 サービス利用規約(第6条 本サービスの停止等) https://safie.link/about/terms-of-service/
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)	お客様自身で画像/映像データをダウンロードできる機能を提供しています。 画像データはJPEG、動画データはMP4形式で保管可能です。	
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	機能追加や画面の変更などより高い付加価値を提供できるよう適宜実施しています。 ユーザーに影響がある場合は事前にSafie Viewerの「お知らせ」に通知します。	
10	信頼性	平均復旧時間(RTO)	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	ベストエフォートで対応します。	
11		障害発生件数	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	2024年に対応に長時間（1日以上）要した障害は発生しておりません。	
12		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	下記について監視を行っています。 ・クラウド基盤／サーバー／ネットワークの活動 ・アクセス負荷／コンピュータリソース ・不正侵入／攻撃／改ざん等のサイバー攻撃	
13		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	長時間に及ぶ障害が発生した場合、当社ホームページ、Safie Viewerの「お知らせ」でアナウンスを行い、必要に応じてメール通知を行います。 問い合わせは以下当社サポート宛にご連絡ください。 問い合わせメール： support@safie.jp 問い合わせに関するヘルプページ： https://support.safie.link/hc/ja/articles/360024699672	
14		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	営業時間内にサービス障害が発生した場合、通知まで2時間以内を目標としています。	
15		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）	監視間隔は、監視対象に応じて1～5分以内に設定しています。	
16		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	サービス障害が発生している場合には、当社ホームページ及びSafie Viewerの「お知らせ」でアナウンスを行い、必要に応じてメール通知を行います。	
17		ログの取得	利用者がログを取得できる機能があるか、または求めに応じてログを提供できるか 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	操作ログ、認証ログ、その他のアクティビティログを取得し、1年以上保管しています。 基本的に詳細ログの提供は行っていません。 お客様の状況により協力致しますのでサポート事務局宛にご連絡ください。 またお客様自身でカメラ映像の閲覧ソフトウェア（Safie Viewer）に対するログイン履歴は確認可能です。	
18	性能	応答時間	処理の応答時間	時間（秒）	具体値は非公表です。サービスの応答性を加味し設計しています。	
19		遅延	処理の応答時間の遅延継続時間	時間（分）		
20		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）		
21	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	ダッシュボードやマルチビューアーなどの機能でお客様自身でカスタマイズが可能です。	
22		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	オプションでAPI機能を利用し、外部システムとの連携機能を開発いただけます。	
23		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）	同時接続数の制限は設けていません。負荷に応じて適宜、分散を行っています。	
24		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	録画可能日数は、契約録画プランに依存します。	
サポート						
25	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	10:00-17:00 （土日祝祭日除く） 業務時間外においても障害監視システムが24時間365日稼働しています。障害を検知した場合、当社基準に則りベストエフォートで復旧対応を行います。	
26		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	10:00-17:00 （土日祝祭日除く） Safie Viewerのお問い合わせ、お客様ご相談フォームから問い合わせを受け付けています。質問／依頼に対して、メールで回答致します。	

Safieクラウドサービス　セキュリティチェックシート

最終更新日： 2025年1月6日

データ管理						
27	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	システムバックアップは、日次で取得し保管しています。バックアップデータにはアクセス制限を設け、システム管理者のみアクセス可能です。 データの保管にはイレブンナインの耐久性を有するクラウドストレージを利用しています。	バックアップ体制は整えていますが、利用規約にデータの保証をしていないことを明記しています。 サービス利用規約(第9条 映像データの利用権限等) https://safie.link/about/terms-of-service/
28		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	日次バックアップは夜間に実施しています。	
29		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	映像データの保存期間は、契約録画プランに依存します。	
30		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	削除対象データを解約日から3営業日以内に削除します。 削除されるデータはユーザー退会またはプラン解約によって異なります。	
31		バックアップ世代数	保証する世代数	世代数	システムバックアップは7世代保管しています。	
32		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	256bitの暗号処理を施し、保管しています。	
33		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	カメラ単位で暗号鍵を保持します。暗号鍵は当社システムにて管理しています。	
34		データ漏洩・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	個人情報漏洩保険に加入しています。 尚、利用者による過失について当社は責任を負いません。	サービス利用規約 (第4条 パスワード及びユーザーIDの管理) (第13条 保証の否認及び免責) https://safie.link/about/terms-of-service/
35		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、外部への漏洩の懸念のない状態が構築できていること	有無／内容	データの返却は行いません。利用者が解約前に必要なデータをダウンロードする必要があります。 当社からデータの廃棄処理や証明書の発行はできませんが、データは暗号化しており、消去と同時に暗号鍵を削除しますのでデータの復元はできません。	
36		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	当社のサービスには該当しません。	
37		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	当社のサービスには該当しません。	
セキュリティ						
38	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	・ISMS （JIS Q 27001:2014） ・ISMSクラウドセキュリティ （ISO/IEC 27017:2015） ・プライバシー情報マネジメントシステム （ISO/IEC 27701:2019）	ISO/IEC 27001:2013 (JIS Q 27001:2014) 認証登録番号: IS 650319 ISO/IEC 27017:2015 認証登録番号: CLOUD 767639 ISO/IEC 27701:2019 認証登録番号: PM 767640
39		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	年に1回以上、第三者専門機関による脆弱性診断を実施しています。 指摘事項については重要度の高いものから、影響度を考慮し対策を実施しております。	直近の実施時期：2024年10月
40		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	開発、保守におけるIT基盤へのアクセスは当社のオフィスにのみ限定されています。 当社の執務スペースへの出入口には顔認証システムを採用しており、関係者外の人間が立ち入れないようにしています。またオフィス内には当社のカメラを複数設置しており、不正行為への抑止対策を講じています。	
41		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	HTTPS(TLS1.2以上)で通信を暗号化しています。	
42		システム監査への資料提供	システム監査時に、担当者へ以下の資料を提供する旨明示「SAS70認定の取得有無」「18号監査報告書の提示可否」	有無	第三者監査機関による評価は受けていません。	利用者による監査についても対応していません。
43		マルチテナント下でのセキュリティ	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	カメラ単位で録画データを暗号化しています。 障害の影響を局所化すべく、一定数のカメラごとにネットワーク環境を分離しています。	
44		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	職務分掌を明確にし、最小権限の原則を徹底しています。	
45		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否か	設定状況	アカウント毎にIDを付与します。 IDをログ検索に利用可能です。	
46		ウィルススキャン	ウィルススキャンの頻度	頻度	業務用端末にはパターンマッチ方式のウィルス対策ソフトを全台に導入し、統合管理できる仕組みで運用を行っています。 ファイルに対するリアルタイム保護を設定し、最新の定義ファイルを自動で更新しています。	

Safieクラウドサービス　セキュリティチェックシート

最終更新日： 2025年1月6日

セキュリティ						
47	セキュリティ	装置のセキュリティを保った処分又は再利用	・利用してる装置の破棄及び再利用時の方針や取り組みに関する情報提供 ・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	有無	データの保管先はクラウド上のストレージとなる為、データストレージの廃棄はデータ保管先の方針に従って廃棄されます。 業務で利用した業務端末の廃棄は専門の機密処理業者に依頼しています。データ消去装置で電磁波破壊後にさらに専用破壊機で複数穿孔を行いデータ復旧を不可能な状態とします。またすべての端末の機密抹消処理の証明書はエビデンスとして保管しています。 業務端末のUSBポートはソフトウェアでストレージを制限する仕組みを実装しています。	
48		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	概要	データ取扱い及び利用に関する制約条件を把握し、映像データは、AWSの東京リージョンで保管しています。	
49		暗号化による管理策	・システムとやりとりされる通信の暗号化強度 ・暗号化の実施状況および暗号化方式の情報提供	方針	最新の電子政府推奨暗号リストに記載されている暗号技術を利用しています。 インターネット通信はHTTPS(TLS1.2以上)で暗号化されます。 映像データは256暗号化を施した状態で保管されます。 パスワードは非可逆情報に変換し保持しています。	
50		クロックの同期	ログのクロックに関する情報提供	設定内容	タイムゾーンはJSTで設定しています。 NTPサーバはAWSまたは、NTP Pool Projectを利用しています。	
51		技術的脆弱性の管理	脆弱性の管理状況に関する情報提供	方針	システムで利用している OSやミドルウェア等に関する脆弱性情報を定期的に収集しています。 システムで利用しているコンポーネントに対する脆弱性パッチが公開されると、重要度の確認とテスト環境での検証を行い、適宜適用します。	
52		セキュリティに配慮した開発のための方針	利用している開発ガイドライン、開発方針に関する情報提供	方針	Webアプリケーションの開発にあたり、IPAの「安全なウェブサイトの作り方」に記載されているセキュリティ対策を基本方針としています。 またソフトウェアの開発においては、確実なコードレビューを実施しています。	
53		インシデント通知	インシデント通知手順に関する情報提供 - 通知方法(Web、メール、電話など) - 通知目標時間	方針	セキュリティインシデント発生時には、社内のインシデント対応フローに則り、速やかに利用者へ通知します。	
54		ICTサプライチェーン	サービス内で利用している外部クラウドサービス/PIIに関する情報提供	サービス名	IT基盤にAWSを利用しています。 利用者からの問い合わせ管理にService Cloudを利用しています。 当社サービスのサポート業務において、業務委託および派遣社員が対応する場合があります。	
セーフィー追記						
55	ー	パスワードポリシー	パスワードの複雑性や桁数、有効期限などのポリシー内容	有無／設定状況	パスワードポリシーは以下の通りです。 ・8文字以上32文字以下（2種別混合） ・英数記号利用可能 ・英数はそれぞれ最低1文字必須 ・大文字小文字は区別 ・ユーザー自身でパスワードの変更が可能 ・時間内一定の失敗回数でアカウントロックする仕組みを実装	以下には対応していません。 ・管理者によるユーザーのパスワード変更 ・独自のパスワードポリシー作成 ・パスワードの有効期限設定 ・パスワードの履歴管理
56		多要素認証	多要素認証に対応しているか	有無	対応しています。	
57		シングルサインオン	SSO(SAML,OpenID Connect)に対応しているか	有無	Safie Managerをご導入いただくことにより対応可能です。	
58		IPアドレス制限	グローバルIPアドレスの接続制限に対応しているか	有無	Safie Managerをご導入いただくことにより対応可能です。	