■LANSCOPE エンドポイントマネージャー クラウド版 セキュリティチェックシート雛形

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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	メンテナンス、バージョンアップ等の理由でサーバを停止する場合を除き、 原則的には24時間365日のサービス提供となります。
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	有り 緊急時を除き、下記タイミングでユーザーページへの告知、 および管理コンソールへの通知にて連絡します。 ○ サービス停止が伴うメンテナンス：1週間前 ○ サービス停止が伴わないメンテナンス：3 日前
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	有り 本サービスの提供を中断または停止する場合、事前に利用者に通知しま す。ただし、緊急時の場合、弊社は、当該通知を行うことなく直ちに本サー ビスの提供を中断または停止することがあります。
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	無し 提供しておりません。
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(%)	2022年実績でサービス全体としては稼働率99.99%となります。 ただし、障害などで機能の一部について利用が制限されることはありまし た。
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	有り 社内の目標値に沿って復旧できる体制を構築しております。
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	無し
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	無し
9		アップグレード方針		有無	利用者への影響や、作業負担があるバージョンアップについては 事前に通知します。 バージョンアップの実施履歴はWebサイトで公開しています。
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	2022年実績で以下となります。 42分
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	SLOにて規定していますが公開しておりません。
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	2022年実績で以下となります 障害件数：27件 長時間要した障害件数：13件
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	有り 社内のシステム監視基準に基づいて監視しております。
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	有り 通知内容を利用申込時に届出のあった電子メールアドレスに送信または本 サービスの専用 webサイトに掲載する方法により行います。
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	異常検出後、4時間以内を目標に対応しています。
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)	リアルタイムで監視しています。
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	お客様向けサポートサイト「LANSCOPE PORTAL」より確認可能です。
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	有り 利用者よりアクセスログの開示要求があった場合、 アクセスログが利用者による操作から発生したものであることが 当社にて断定できる場合に限り、開示要求に関連する項目に 限定されるよう加工したうえで、アクセスログの一部を提供する場合が あります。
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)	公開しておりません。
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	無し 利用者ごとのカスタマイズは行っておりません。
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	有り 利用者の希望があれば、APIを提供しています。
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	無し 特に制約はございません。
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	アップロードできるファイルサイズなど一部の機能に上限があります。 ページビューの上限はありません。
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	原則、次の時間帯での対応(メール・電話)ですが、状況に応じてはその限り ではございません。 9:30～12:00／13:00～17:30
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	9:30～12:00／13:00～17:30 月～金曜日 ※土・日・祝祭日および当社規定の休日を除く
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	有り インベントリ情報は1日1回バックアップを取得しています。 位置情報、操作ログ情報、その他設定情報は 35日の増分バックアップを取得しています。 保管場所は日本国内です。
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	インベントリ情報は1週間 位置情報、操作ログ情報、その他設定情報は35日としております。
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	インベントリ情報は1週間保存されます。 位置情報、操作ログ情報は35日の増分バックアップを取得しています。
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	サービス利用終了日から、90日後にデータを消去します。

■LANSCOPE エンドポイントマネージャー クラウド版 セキュリティチェックシート雛形

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
32		バックアップ世代数	保証する世代数	世代数	インベントリ情報は1世代、 位置情報、操作ログ情報、その他設定情報は差分35日分を保証します
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	有り 個人情報や、業務において重要かつ 暗号化せねば信頼性に欠けるデータを対象としています。
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	無し
35		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	有り 利用規約23条(損害賠償の制限)に準じます。
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	有り サービス利用終了日から、90日後にデータを消去します。
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	無し
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	有り
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	有り ・認証基準:ISO/IEC 27001:2013 / JIS Q 27001:2014 認証登録番号:IS 656320 ・認証基準:ISO/IEC 27017:2015 認証登録番号:CLOUD 756417
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	有り AWS ファウンデーショナルテクニカルレビューを取得しています。
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	有り 適切に管理しています。 物理的なデータの取り扱いはAWSの基準に準拠します。
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	有り TLSで暗号化しています。
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	無し 弊社は監査法人によるSAS70Type2監査自体は受けておりません。 紛失時のリモート操作代行[24/365サービス]をご契約いただく場合のみ、業務委託を行っております。 お預かりするデータについては全てAWSを利用しており、弊社内のデータ保管はありません。 AWSのSAS70Type2監査報告書は次に記載があります。 https://aws.amazon.com/jp/compliance/soc-faqs/
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	有り 物理的な情報隔離は行っておりませんが、 データごとの識別IDを付与しており、 論理的に情報隔離をしています。
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	有り 特定のアカウントでのみデータにアクセスできるよう、制限を施しています。このアカウントはデータ管理に携わる一部の社員にのみ発行されます。
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	当社からログの提供は行っておりませんが、管理コンソールでの画面閲覧や設定変更などを操作履歴として1年間保存し、閲覧・CSV出力できます。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	頻度は公開しておりませんが、計画的に実施しております。
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	有り 適切に管理しています。 物理的なデータの取り扱いはAWSの基準に準拠します。
49		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	データの保存地、取り扱いについてはAWSの基準に準拠します。 https://aws.amazon.com/jp/compliance/data-center/controls/ 管理コンソールのアカウント情報の取り扱いについてはAuth0の基準に準拠します。 https://auth0.com/jp/security
その他					
50	その他	サービス規約の有無	サービス規約が定義されているか。	有無	有り LANSCOPE エンドポイントマネージャー クラウド版 利用規約 https://www.lanscope.jp/an/terms.html
51		データの所在地	サーバー、データは日本国内にあるか。	有無	有り LANSCOPE エンドポイントマネージャー クラウド版は、 AWSの東京リージョンを利用しています。
52		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	有り 有償オプション「24/365紛失サポート」へご加入の場合、あります。加入に際しては事前に再委託にご同意いただきます。 利用規約 https://www.lanscope.jp/an/24365_terms.html
53		脆弱性対策	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	システムへの影響度を確認した後に対策を適宜実施しています。
54		情報漏洩に関しての 対策、対応	人的、システム的な対応はどのようなものを 行っているか。	対応状況	ISMSの教育を実施しております。また、インシデントに対するCSIRTを設けています。
55		内部不正についての対策	従業員が利用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	特定のアカウントでのみデータにアクセスできるよう、制限を施しています。このアカウントはデータ管理に携わる一部の社員にのみ発行されます。 サーバーにてアクセスログを取得していることを周知しており、抑止力としております。
56		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	ISO27001 (情報セキュリティ)に基づく監査を定期的に実施しております。
57		パスワードについての対策	簡単なパスワードを不許可とする仕組みがあるか。	有無	有り パスワードの強度、有効期間、以前仕様したパスワードの再使用の制限を設定できます。
58		ログイン認証についての対策	多要素認証など、パスワード以外に 本人確認する手段があるか。	有無	有り ログイン時に認証用のモバイルアプリで生成された確認コードの入力を要求できます。(二要素認証)

■LANSCOPE エンドポイントマネージャー クラウド版 セキュリティチェックシート雛形

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
59		アカウントロック	一定回数ログインに失敗した場合に、アカウントのロックアウトが可能か。	有無	有り 同一アカウントや同一IPアドレスからのログインが一定回数失敗するなど、セキュリティの異常を検出した場合に、アカウントをロックアウトします。
60		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、デバイス制限等)	有無	有り コンソールへのアクセスについて、IPアドレス制限が可能です。
61		アクセス権限管理	一般ユーザーのアクセス権限は管理者からのみ 権限付与などの制御が可能か。	有無	有り コンソール内にて設定が可能です。
62		アカウント管理	管理者で一般権限アカウントの追加削除など処理が可能か	有無	有り コンソール内にて設定が可能です。
63		管理者権限管理	管理者毎のアクセス権限を設定する機能があるか。	有無	有り コンソール内にて設定が可能です。
64		法的要求事項	下記、MOTEXが遵守する法令、国が定める指針及びその他の規範を遵守しているか。 (「規範一覧表」シート参照)	対応状況	ISMSに基づいた遵守確認を実施しています。