

情報警備 サービス仕様書

サービス名	ALSOK ホームページ改ざん 検知・復旧サービス
-------	------------------------------

1.1 版

発行日: 2024 年 4 月 1 日

目 次

1.	はじめに.....	2
1.1.	本書の位置づけ	2
1.2.	本サービス仕様書の変更.....	2
1.3.	用語・略語の定義	2
2.	本サービス仕様	3
2.1.	概要	3
2.2.	ご利用条件	4
2.3.	サービスのご利用方法.....	5
2.4.	システム要件	6
2.4.1.	利用システム.....	6
2.4.2.	Agent の通信要件	6
2.4.3.	Agent 稼働要件.....	6
2.4.4.	Agent 対応 OS	6
2.4.5.	Manager 管理画面.....	7
2.4.6.	Manager 管理画面サポートブラウザ.....	7
2.5.	機能.....	8
2.5.1.	改ざん検知・復旧機能.....	8
2.5.2.	稼働監視機能.....	9
2.5.3.	管理(Manager)サーバー仕様	9
2.5.4.	アラート通知/緊急通知仕様	9
2.5.5.	更新モード監視仕様.....	10
3.	お客様サポート.....	11
3.1.	サポート範囲	11
3.2.	サポート窓口	11
3.3.	解約について	12
4.	サービス提供条件	13
4.1.	本サービスの提供内容	13
4.2.	サービスの保証	14
4.3.	データの取扱いについて	14
5.	本サービス用設備のメンテナンス.....	15
5.1.	メンテナンス	15
5.2.	パッチ適用/アップデート対応(バージョンアップ対応含む)	15
5.3.	障害対応	15
6.	その他	16

1. はじめに

1.1. 本書の位置づけ

本書は、ALSOK株式会社(以下「ALSOK」といいます。)が、インターネットを通じて提供する「ALSOK ホームページ改ざん検知・復旧サービス」のサービス仕様をまとめたものです。

1.2. 本サービス仕様書の変更

本書は、「ALSOK ホームページ改ざん検知・復旧サービス利用約款」第 7 条および、「ALSOK ホームページ改ざん検知・復旧サービス（無料トライアル）利用約款」第 7 条の定めにより、適宜、改訂されるものとし、改訂時には最新の内容が適用されます。改訂にあたり、ALSOK のホームページへの掲出によりその内容を通知することとします。改訂された本書の効力は、ALSOK のホームページに改訂後の内容を掲載してから、30 日経過した日から有効になるものとし、お客様は、本サービスを利用する際、ALSOK から提供または ALSOK のホームページに掲載されている最新の内容をご確認いただくものとします。お客様が、本書の改訂の効力が生じた後に本サービスを利用した場合には、改訂後のすべての記載内容に同意したものとみなされます。

1.3. 用語・略語の定義

本書で使用する用語・略語の意味は、以下に定めるとおりとします。なお、本書において明示的に定めのない、その他の用語は本約款の定めに従うものとします。

用語・略語	説明
本サービス	ALSOK が提供する「ALSOK ホームページ改ざん検知・復旧サービス」
ALSOK	ALSOK株式会社および同社の指定する会社
お客様	ALSOKと契約して本サービスを利用する法人もしくは個人事業主またはその管理者
サービス利用者	お客様が本サービスの利用を認めた個人
アラート	本サービスによって検知された、改ざんに関わる警報
監視センター	本サービスの日常的な運用や、お客様からの各種問い合わせを受け付ける、ALSOK 情報警備監視センターのこと
営業日	土曜日、日曜日、国民の祝日に関する法律に定める休日、および ALSOK 所定の休日を除く日
本約款	「ALSOK ホームページ改ざん検知・復旧サービス利用約款」および、「ALSOK ホームページ改ざん検知・復旧サービス（無料トライアル）利用約款」のこと

2. 本サービス仕様

2.1. 概要

本サービスは、サーバー内の公開/非公開コンテンツ、設定ファイル、アプリケーションの改ざんを瞬時に検知して、瞬間復旧するサービスをSaaS(Software as a Service)型で提供するものです。

本サービスは、サーバー内のファイル・ディレクトリに対する予期せぬ変更やファイル追加、削除、権限変更等の改ざんを、発生と同時に検知します。また、サーバー内の設定ファイルや実行モジュール等の非公開ファイルの改ざん検知も行います。そして、改ざんを検知した場合は、復旧用バックアップデータを使って瞬時に復旧を行います。

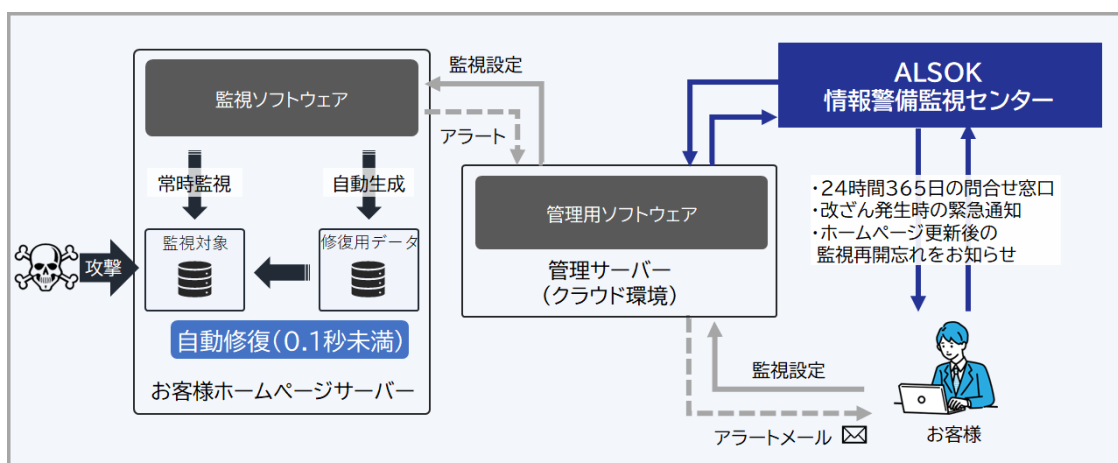


図 本サービスの提供イメージ

本サービスがファイル等の改ざんを検知した場合、以下のいずれかの動作を実行します。動作設定は、以降に記載する「Manager」の管理画面から、ディレクトリ・ファイル単位に設定することができます。

(1) 通知のみ

改ざん発生時、お客様にメールを通知します。

(2) 自動復旧と通知

改ざん発生後、0.1秒未満で復旧元データから自動復旧を行います。あわせて、本項(1)の動作を行います。

(3) 自動復旧と保全

本項(2)の動作にあわせ、改ざん(変更)されたファイルを証拠として保存します。

2.2. ご利用条件

(1) 前提条件

- ① お申込みいただき、初期監視設定が完了した後に利用可能となります。
- ② 本サービスは、AGS株式会社が管理・運用するManagerサーバー(以下、「Manager」という)とAgentソフトウェア(以下、「Agent」という)で構成されます。「Manager」は、改ざん検知・復旧の設定を行うための管理インタフェースをお客様に提供します。「Agent」は、改ざん検知・復旧を行うお客様サーバー(以下、「ホスト」という)にインストールされます。「Agent」には、「Manager」を経由してライセンス証明書が、1ホストにつき1つインストールされます。
- ③ ホストには、「Agent」と合わせJavaをインストールする必要があります。「Agent」のインストールには、管理者権限が必要となります。共用サーバー等管理者権限がない環境ではご利用いただけません。「Agent」が稼働する要件につきましては、2.5.章「システム要件」をご覧ください。

(2) お客様の利用回線

インターネット回線からのアクセスを前提としております。本サービス提供に際し、「Manager」の IP アドレスからのアクセス許可をいただきます。「Manager」の IP アドレスについては、契約後に別途ご案内します。

- ① ファイアウォールの設定によって、当サービスをご利用いただけない場合があります。このような場合、ファイアウォール設定を変更していただくことによってご利用が可能になります。
- ② 当社は、インターネット回線事業者・ISP の都合によりシステム利用に支障が発生した場合の責任を負わないものとします。

2.3. サービスのご利用方法

(1) お申込み(ご注文/トライアル)からご利用開始までの流れ

本サービスの開始までの、手順の概要を以下に示します。

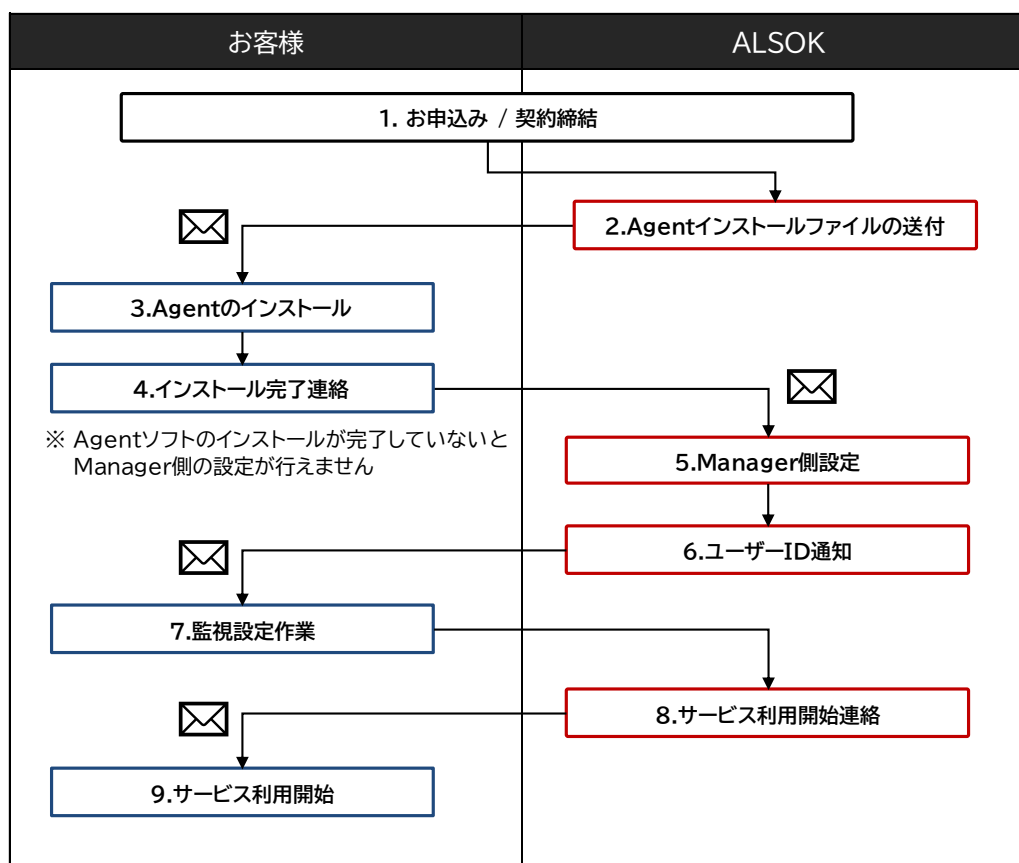


図 サービス開始までの流れ

1. お申込み/契約の締結(お客様/ALSOK)
2. Agent インストールファイルをメールにて送付(ALSOK)
3. Agent のインストール作業を実施(お客様)
4. Agent インストールの完了連絡(お客様)
5. Agent インストール完了連絡を受領後、Manager 側の初期設定を実施(ALSOK)
6. ユーザーID をメールにて通知(ALSOK)
7. 監視設定作業(お客様)
8. サービス利用開始連絡(ALSOK)
9. サービス利用開始

2.4. システム要件

2.4.1. 利用システム

改ざん検知・復旧機能は、以下のシステムにより実現しております。

AGS 株式会社

「SaaS 型 WebARGUS サービス」

2.4.2. Agent の通信要件

「Agent」は、「Manager」との通信のため、ファイアウォール等がある場合は、これらの通信の許可が必要です。詳細な通信条件については契約後に別途ご案内します。また、「Agent」がプライベートアドレス空間にある場合は、インターネット側から通信を確立できるようグローバル IP アドレス(および必要に応じてポート番号)との NAT の調整も必要です。

2.4.3. Agent 稼働要件

権限	管理者権限が必要となります。
IP アドレス	固定グローバル IP アドレスが必要となります。
必須ソフトウェア	Java Runtime Environment(JRE)1.8 以降(Java11 対応済)
CPU	Intel® Xeon® CPU E5-2650 0 @2.00GHz(1Core)相当以上
メモリー	空き 256MB 以上を推奨 ※復旧対象データサイズによっては、推奨以上に空きメモリが必要になる場合があります。
HDD	空き 20MB 以上 ※インストール時に必要な空き容量となります

2.4.4. Agent 対応 OS

- Red Hat Enterprise Linux 9.x, 8.x, 7.x, 6.x
- CentOS 7.x
- Amazon Linux 2
- SUSE Linux Enterprise Server 15, 12, 11

2.4.5. Manager 管理画面

「Manager」管理画面には、2.4.6.章「管理画面サポートブラウザ」に示すブラウザを用いてアクセスしてください。「Manager」管理画面の URL については、契約後に別途ご案内します。また、管理画面は発信元のグローバル IP アドレスによる接続制限を行っております。

2.4.6. Manager 管理画面サポートブラウザ

Microsoft Edge	バージョン 42.x 以降
Google Chrome	バージョン 68.x 以降
Mozilla Firefox	バージョン 60.x 以降

2.5. 機能

サーバー内のファイル、ディレクトリに対して「変更、追加、削除、属性情報の変更」が発生したか否かで改ざん有無を判断します。あらかじめ、監視対象のファイル・ディレクトリ情報をハッシュ値※で取得しておき、サーバー内部で新旧比較を行います。チェックのタイミングはリアルタイムで、改ざん状態を復旧することができます。主な機能を以下に記載します。

※ ファイルのデータ(ビット列)を、ハッシュ関数という特別な関数を使って計算すると決まった長さのビット列になります。これを、ハッシュ値といいます。

2.5.1. 改ざん検知・復旧機能

改ざん検知頻度	24時間365日 常時監視により改ざん発生と同時に検知	
監視対象	設定ファイルを含むサーバー内のすべてのコンテンツ監視が可能	
自動復旧速度	改ざん検知後、0.1秒未満での自動復旧が可能	
アラート通知	改ざん発生時 / 復旧時 / Agent異常停止時にメール通知を実施	
緊急通知	監視センターにてアラート通知を受信すると、通知内容を確認してお客様へメールにて詳細レポートを送付	
証拠保全	改ざんされたファイルを証拠として保存する機能を搭載(変更ファイルのみ)	
監視モード	「監視のみ」 / 「通知&自動復旧」 / 「通知&証拠保全&自動復旧」の3種類	
更新モード	意図的なホームページコンテンツの更新のため、コンテンツ更新モード(アラート通知あり、ログの記録)のON/OFFが可能	
更新モード監視	お客様からホームページコンテンツ更新の連絡を受け付け、終了予定時間を過ぎても更新モードがOFF状態となっている場合に、監視センターよりお客様へ連絡を行う	
問い合わせサポート窓口	監視センターによる問い合わせの24時間365日受付・対応	
復旧元データ	監視設定都度、最新復旧元データを自動生成 電子署名を付与することで、原本の真正性を担保	
	ライセンスファイル	電子証明書;X.509 Version 3
	電子署名	署名アルゴリズム:SHA(256(256bit) with RSA(2048bit) 署名フォーマット:CMS (Cryptographic Message Syntax)(signed-data format)

2.5.2. 稼働監視機能

稼働監視	Manager側で Agent の稼働を定期的に監視
異常検知時の処置	Agentが停止した際にメール通知

2.5.3. 管理(Manager)サーバー仕様

管理(Manager)サーバーは、以下の操作インタフェースを提供します。

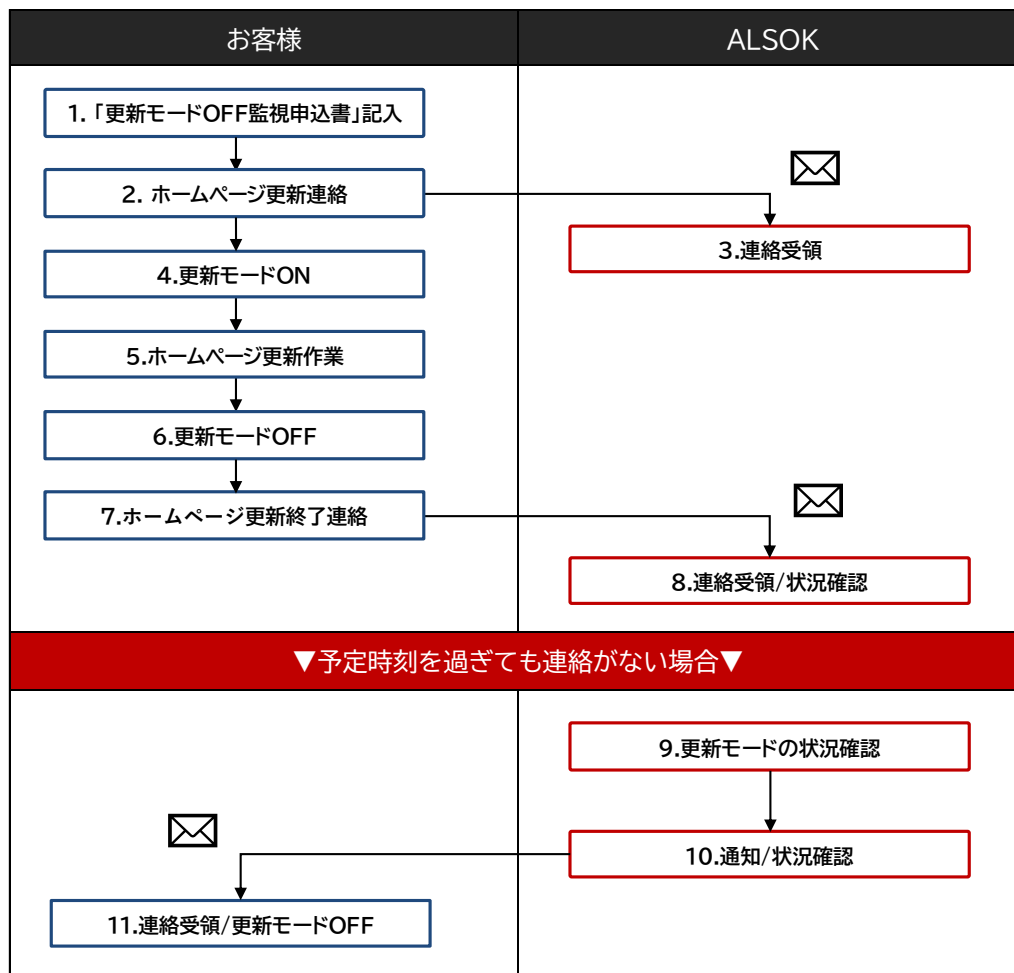
エージェント管理	更新モード機能、再設定機能、改ざん検知・復旧動作対象範囲の設定、動作の OFF/ON、改ざん検知時の通知設定
テンプレート管理	監視設定のテンプレート設定

2.5.4. アラート通知/緊急通知仕様

本サービスが、監視対象の改ざんを検知した場合は、速やかに指定連絡先へメールにて、システムによるアラート通知(自動送信)を行います。また、監視センターから改ざん箇所が記載されたレポートを添付した緊急通知を行います。

2.5.5. 更新モード監視仕様

お客様からホームページ更新の連絡を受領後、終了予定時刻を過ぎても更新モードが ON 状態の場合、監視センターよりお客様へ状況確認の連絡を行います。本機能の概要を以下に示します。



1. 「更新モード OFF 監視申込書」に必要事項を記入(お客様)
2. ホームページの更新連絡をメールにて送付(お客様)
3. 連絡受領(ALSOK)
4. 更新モードを ON に切り替える(お客様)
5. ホームページの更新作業を実施(お客様)
6. 更新モードを OFF に切り替える(お客様)
7. ホームページ更新の終了連絡をメールにて送付(お客様)
8. 連絡受領後、更新モードが OFF 状態であることを確認し作業完了(ALSOK)
- ※ 予定時刻を過ぎても連絡がない場合
9. 更新モードの状況を確認(ALSOK)
10. お客様へ状況確認(ALSOK)
11. 連絡受領、更新モードを OFF に切り替え、監視を再開させる(お客様)

3. お客様サポート

本サービスをご利用のお客様には、以下のサポートを提供します。

3.1. サポート範囲

内容	説明
各種手続きおよび手続き方法に関するお問い合わせ	更新モード OFF 監視等の各種手続きおよび、手続き方法についてのお問い合わせ
操作方法のお問い合わせ	管理画面の操作方法についてのお問い合わせ
障害確認のお問い合わせ	本サービスが正常に利用できない等、サービス状態に関するお問い合わせ
仕様確認のお問い合わせ	各種ドキュメントの内容についてのお問い合わせ
その他	サービスの内容等、その他のお問い合わせ

3.2. サポート窓口

内容	説明
サポート窓口	ALSOK 情報警備監視センター
受付時間	24 時間/365 日 ※お問い合わせ内容によっては、翌営業日での対応となる場合があります。
連絡方法	メールおよび電話 ※メールアドレスおよび電話番号については、契約後に別途ご案内します
お問い合わせに必要な情報	・サービス名:ALSOK ホームページ改ざん検知・復旧サービス ・お客様番号(監視センターからのメール冒頭に記載しています) ・お客様会社名 ・お客様担当者名

3.3. 解約について

- (1) 解約の際は、解約希望月の2か月前までに「解約同意書」を担当営業員へ提出してください。「解約同意書」については担当営業員または、監視センターまでお問い合わせください。
- (2) 解約の際は、お客様にて「Agent」のアンインストール作業をお願いします。詳細な「Agent」のアンインストール方法については別途、監視センターよりご案内します。
- (3) 監視センターで保存しているログおよびお客様の情報は、解約後に削除します。

4. サービス提供条件

4.1. 本サービスの提供内容

以下の条件にてサービスを提供します。

項目	内容
サービス提供時間	24 時間 365 日(計画停止/定期保守は除く)
サービス停止	<p>1.計画サービス停止</p> <p>サービスの安定稼働ならびに維持を目的とした計画停止を行います。計画停止作業中は、サービスを一時的に停止または、アクセスが制限される場合があります。計画サービス停止で実施するメンテナンス内容につきましては、5.1.章「メンテナンス」に記載します。</p> <p>2.計画外サービス停止</p> <p>障害やセキュリティインシデント等による緊急なサービス停止、ならびに、事前に通知したうえで実施するメンテナンス作業のためのサービス停止。</p>
お知らせ	<p>サービス停止や障害時等の連絡は、メールにて通知します。</p> <p>通知の条件につきましては、5.1.章「メンテナンス」に記載します。</p>
障害時のデータ復旧	<p>障害発生により、本サービス提供のためのシステム、ソフトウェアにデータ破損等が発生し、復元の必要性があると判断した場合、前日の状態に復元します。ただし、データの破損状態によっては、前日以前の状態に復元する場合があります。</p>

4.2. サービスの保証

本サービスは、第三者からのあらゆる不正な改ざんを完全に防止するサービスではありません。

4.3. データの取扱いについて

本サービスにより検知した、改ざん情報等のログは、お客様を特定できないようにデータを加工したうえで、以下の用途に二次利用することを承諾したものとします。

- (1) サービス利用者への分析結果の情報提供
- (2) 本サービスの販売促進データとしての活用
- (3) 本サービスの品質向上のための活用
- (4) セキュリティに関する脅威トレンドの調査・分析
- (5) 新たなサイバー攻撃等の被害未然防止に資する目的での第三者(報道関係者含む)への提供

5. 本サービス用設備のメンテナンス

当社では、本サービスを安心してご利用いただけるよう、「Manager」の定期メンテナンスを実施します。

5.1. メンテナンス

(1) 本サービスは、メンテナンス等のために一時停止する場合があります。この場合には、以下のよう
な条件のもとに申込み時のメールアドレスへ通知します。

① 計画停止

システム停止を必要とするメンテナンス作業の場合は、事前に通知します。

② 緊急メンテナンス

お客様がサービスを利用するうえで重要な問題が発生し、サービス提供時間中にメンテナンスを
実施する必要がある場合は、速やかに通知します。

(2) メンテナンス中に改ざんが発生した場合でも、改ざんの検知復旧は行います。ただし、お客様への
通知が遅れる場合があります。

5.2. パッチ適用/アップデート対応(バージョンアップ対応含む)

本サービスを提供するための環境において、「Manager」のソフトウェアのパッチ適用やアップデートが
必要であると判断した場合、その作業を当社が行います。

「Agent」が稼働するお客様サーバーのパッチ適用やアップデートは、当社は実施しないものとします。

(1) OS やミドルウェアのパッチ適用/アップデート対応については、当社にて適用の判断を行い、必要
に応じて実施します。

(2) パッチ適用/アップデート対応実施時は、メンテナンスの通知を行います。

5.3. 障害対応

本サービスの「Manager」が稼働する設備は監視運用を行っております。万が一障害を検知した場合、
切り分けのうえ障害対応を行います。

6. その他

- (1) 本サービスで提供する資料以外の個別のご要望には対応しないものとします。
- (2) お客様の要件にあわせた個別機能の追加は実施しないものとします。
- (3) お客様の過失により消失したデータの復旧サービスは提供しないものとします。
- (4) Manager 側のログの開示、提供はしないものとします
- (5) 個人情報の取り扱いについては、ALSOK ホームページ記載の「個人情報の取扱い
(<https://www.alsok.co.jp/policy/>)」に準ずるものとします。

以上

本書は著作権上の保護を受けています。本書の一部あるいは全部について、著作者からの許諾を得ずに、いかなる方法においても無断で複写、複製することは禁じられています。

本サービスの仕様、および本書に記載されている事柄は、将来予告なしに変更することがあります。