SB Technology

SaaS パトロール
サービス仕様書

この SaaS パトロールサービス仕様書（以下「本仕様書」といいます）は、SB テクノロジー株式会社（以下「SBT」といいます）が提供するクラウドサービス「SaaS パトロール」（以下「本サービス」といいます）の提供内容、提供範囲、提供方法、提供水準、利用時間帯その他の諸条件を定めるものです。本仕様書は「NOZ SECURITY サービス約款」の一部を構成するものとします。 なお、当該サービス約款において定義された用語は、本仕様書において別段の定めのない限り、本仕様書においても同様の意味に用いるものとします。

目次

1. サービス内容、範囲 3
   1.1 サービスの概要 3
   1.2 サービスメニュー 3
   1.3 サービス内容 3
      1.3.1 提供内容 3
      1.3.2 利用条件 4
      1.3.3 利用上の注意点 6
2. サービスレベルアグリーメント（SLA） 6
   2.1 サポートデスク受付 6
      2.1.1 サポートデスクへの問合せ担当者 6
      2.1.2 サポートデスク対応内容 6
      2.1.3 サポートデスク対応時間 7
   2.2 障害対応 7
   2.3 サービスの運用 7
   2.4 可用性 8
   2.5 計画停止 8
   2.6 補償請求 8
3. セキュリティ 10
4. クライアント機器の利用環境 10
5. ネットワーク 10
6. 耐障害性 12
7. パフォーマンス 12
8. データ 12
9. トライアル 12
   9.1 トライアル内容 12
      9.1.1 トライアル提供内容 12
      9.1.2 トライアル利用上の注意点 13

10. 利用開始 13
11. 利用終了 13
11.1 サービス停止の実施 13
11.2 サービス停止時の注意事項 13
12. その他禁止事項 13
13. その他制限事項 14
14. 契約に関する注意事項 14

1. サービス内容、範囲

1.1 サービスの概要

・ 本サービスは、社内で利用されている SaaS テナントを一元管理することにより、SaaS に関わる運用効率化やセキュリティリスクを軽減させるための一連の機能を提供いたします。

・ 本サービスは、SBT と直接または販売店（第 2 次販売店以降含む）（以下、「販売店」）を通じて利用契約を締結された契約者に提供されるものとします。

1.2 サービスメニュー

本サービスのメニューは以下のとおりになります。

■基本メニュー

メニュー		内容
基本メニュー	サービス利用料	本サービスの利用の対価

※ 最低契約期間は 1 年となります。

※ 「基本メニュー」では、下記機能をご利用いただくことができます。

- SaaS 管理台帳（サービス管理・テナント管理）
- メールによるサービス検知機能
- ユーザー別利用状況
- 棚卸し機能
- 申請・承認機能
- 一般ユーザー向け機能（サービスカタログ、部下情報）

■オプションメニュー

メニュー		内容
オプション	SKYSEA Client View 連携	SKYSEA Client View の Web アクセスログを SaaS パトロールに連携を行うことで、サービス検知を実現します。
オプション	LANSCOPE エンドポイントマネージャー 連携	LANSCOPE エンドポイントマネージャー の Web アクセスログを SaaS パトロールに連携を行うことで、サービス検知を実現します。

1.3 サービス内容

1.3.1 提供内容

・ SaaS パトロール サービス

・ マニュアル一式

・ 問合せサポート

1.3.2 利用条件

・ SaaS 型のサービス提供となる為、お客様側でサーバー実行環境をご用意いただく必要はありません。

・ **メールスキャンによるサービス検知**

- 対象となるサービスは Microsoft365 Exchange Online となります。
- メールスキャンによるサービス検知では、サービス側で一時的にメールの一部データ（件名、送信元・送信先アドレス）を保持する場合がございます。
- 365 日前より過去に実行されたメールスキャン結果は自動的に破棄されます。
- 実行にあたり、特定の権限を設定画面より、本サービスに付与頂く必要があります。

設定作業に必要となる Microsoft 365 管理者権限

- グローバル管理者

本サービスに付与する権限

- Read all users' full profiles
- Read mail in all mailboxes
- Sign in and read user profile

サービス検知の実行制限

- 検知を実行できる最大の期間は 180 日間となります。
- 初回実行を含めたスキャンメール数が 10 万件を超えた場合、次回以降の実行が翌月までできなくなります。

・ **テナントユーザー連携**

- 管理対象のサービスと API 経由で連携することで、テナントのユーザーを同期・削除・無効化することができます。
- 連携対象のサービスおよび、詳細は別紙「連携 SaaS 一覧」をご参照ください。
- 本機能は Anyflow 株式会社が提供するサービス「Anyflow Embed」を利用することで実現しています。
- SaaS パトロール利用に伴い、Anyflow Embed の基盤上に下記データを保持いたします。これらの情報は、セキュアな環境のもと、厳密に管理されます。
  - ✧ SaaS の API で取得した SaaS アカウント情報のログ
  - ✧ SaaS の API 実行のための認証情報（API キーや、OAuth トークン）
- 接続対象のサービスの仕様変更や挙動について、本サービスでは一切保証いたしません。

・ **従業員マスタの SCIM 連携**

- 従業員マスタの SCIM 連携は、Microsoft Entra ID に対応しています。
- Microsoft 社の仕様により、Microsoft Entra ID から同期できないユーザー属性があります。

・

・ **SKYSEA Client View 連携**

- 本機能はクライアント端末からサービスにアクセスする際のアクセス URL を基にサービスの利用を判定します。クライアントとサービスの間にプロキシなどを挟み、アクセス時の URL を変更している場合はサービスが検知できませんのでご注意ください。
- 対象となるクライアント端末は、Windows PC となります。
- お客様オンプレミス環境に連携用のバッチプログラムを置く必要があります。下記の条件をご確認ください。
  - ✧ ログ出力実行端末をご用意いただき、弊社が用意したバッチプログラムを配置いただく必要があります。
  - ✧ ログの保存先として、ログ出力実行端末の空ドライブ、又は別サーバーのネットワークドライブを指定いただきます。
  - ✧ 対象のドライブは十分な空き容量を確保してください。

- アクセス URL は SKYSEA Client View サーバーに保持する Web アクセスログから取得します。
- 上記 Web アクセスログは毎日 0:00～7:00 の時間帯に、前日分のログのみを対象に集計されます。※2 日以上前のログが含まれていても集計対象となりません。
- 本機能で SaaS パトロールにアップロードされたオリジナルのログファイルは最大 30 日保管され、その後削除されます。※集計した検知ログは 30 日以降も残ります。
- 集計された検知ログは、ログ発生日より 180 日前までの結果を保持します。それ以前のログは自動的に破棄されます。
- SKYSEA Client View 連携機能を利用する為には、SaaS パトロールの従業員マスタに Active Directory のユーザー属性「sAMAccountName」の値を設定いただく必要があります。

  設定手段は以下をご用意しております。
  ・Microsoft Entra ID からの同期（SCIM 連携）
  ・CSV ファイルインポート

  Microsoft Entra ID から同期する場合、「sAMAccountName」属性に該当する値が、Microsoft Entra ID のユーザー属性に設定されている必要があります。

  また、その属性が SCIM 連携により同期可能な属性である必要があります。該当する属性が Microsoft Entra ID 上に存在しない場合、Microsoft Entra Connect の導入/設定変更により、Active Directory から同期することが可能です。

- Active Directory と Microsoft Entra ID の同期に関するサポートは提供いたしません。
- 連携できる SKYSEA Client View はオンプレミス版のみとなります。
- 本オプションでサポートする、SKYSEA Client View のバージョンは最新のメジャーバージョンを含め、3 世代までとなります（Sky 社のサポート対象となるバージョン）。

・ **LANSCOPE エンドポイントマネージャー連携**

- 本機能はクライアント端末からサービスにアクセスする際のアクセス URL を基にサービスの利用を判定します。
  - ✧ 対象となるクライアント端末は、Windows PC となります。
  - ✧ クライアントとサービスの間にプロキシなどを挟み、アクセス時の URL を変更している場合はサービスが検知できませんのでご注意ください。
- アクセス URL は LANSCOPE 統合マネージャーサーバーに保持する Web アクセスログから取得します。
- Web アクセスログは連携用バッチプログラムを定期実行することで SaaS パトロールへ連携されます。
- 連携用バッチプログラムの利用条件は下記をご確認ください。
  - ✧ お客様の LANSCOPE 統合マネージャーサーバーに弊社が用意した連携用バッチプログラムを配置いただき、定期実行していただく必要があります。
  - ✧ Web アクセスログの一時保存先として、LANSCOPE 統合マネージャーサーバーに十分な空き容量を確保したドライブをご用意いただくか、別サーバーのネットワークドライブを指定いただきます。
  - ✧ 本機能で SaaS パトロールに連携された Web アクセスログは最大 30 日保管され、その後削除されます。※集計した検知ログは 30 日以降も残ります。
- SaaS パトロールへ連携された Web アクセスログは毎日 3:00～7:00 の時間帯に、集計されます。
  - ✧ 3:00 以降に連携された Web アクセスログは当日の集計対象にならず、翌日の集計対象になります。
  - ✧ 集計されたログはログ発生日より 180 日前までの結果を保持します。それ以前のログは自動的に破棄されます。
- LANSCOPE エンドポイントマネージャー連携機能を利用する為には、SaaS パトロールの従業員マスタに Active Directory のユーザー属性「sAMAccountName」の値を設定いただく必要があります。

  設定手段は以下をご用意しております。

・Microsoft Entra ID からの同期（SCIM 連携）
・CSV ファイルインポート

Microsoft Entra ID から同期する場合、「sAMAccountName」属性に該当する値が、Microsoft Entra ID のユーザー属性に設定されている必要があります。

また、その属性が SCIM 連携により同期可能な属性である必要があります。該当する属性が Microsoft Entra ID 上に存在しない場合、Microsoft Entra Connect の導入/設定変更により、Active Directory から同期することが可能です。

- Active Directory と Microsoft Entra ID の同期に関するサポートは提供いたしません。
- 連携できる LANSCOPE エンドポイントマネージャーはオンプレミス版のみとなります。
- 本オプションでサポートする LANSCOPE エンドポイントマネージャーのバージョンは MOTEX 社がサポート対象とするバージョンに準じます（リリースから 5 年後を目安に旧バージョンのサポートを廃止）

・ **棚卸機能**
- 以下の棚卸機能はそれぞれ 1 か月あたり 50,000 件までを上限とします。
  - ✧ サービス利用許可棚卸
    【カウント例】500 ユーザーに対し 2 回棚卸を実施した場合 1,000 件とカウント
  - ✧ テナント棚卸
    【カウント例】10 テナントに対し 2 回棚卸を実施した場合 20 件とカウント
  - ✧ テナント利用者棚卸
    【カウント例】500 人のテナント利用者に 2 回棚卸を実施した場合 1,000 件とカウント

1.3.3 利用上の注意点

・ ユーザー向けのマニュアル等は含まれません。
・ 提供するマニュアルは本サービス に関する部分のみ記載します。Microsoft Entra ID に関する仕様や設定など Microsoft 社が提供するサービスについては、Microsoft 社提供のドキュメントをご参照ださい。

2. サービスレベルアグリーメント（SLA）

2.1 サポートデスク受付

2.1.1 サポートデスクへの問合せ担当者

ご契約時に登録していただいた、契約者の管理責任者及び運用担当者（3 名以内）からの問合せのみの受付となります。

2.1.2 サポートデスク対応内容

本サービス範囲内における以下の内容をサポートデスクにて提供いたします。

■ 問合せ受付（サポートデスク：saas-patrol-support@tech.softbank.co.jp）
- 以下の問合せ内容をメールにて受付いたします。
  - 仕様に関するお問合せ
  - 動作不具合に関するお問合せ

・ 連携先サービスの仕様や問題については、お客様にてサービス提供企業にお問合せいただく場合がございます。
・ サポートデスクへの問合せ受付は『2.1.1 サポートデスクへの問合せ担当者』様からのみお受付いたします。

■ サービス情報の配信
・ 以下の情報をメールにて配信いたします。
➢ 障害情報およびメンテナンス情報
➢ サービス仕様や機能に関する追加、変更、廃止の情報
・ サポートデスクからの情報は『2.1.1 サポートデスクへの問合せ担当者』へ配信いたします。

※本サービスにて提供するサポート・資料は全て日本語での提供とします。

2.1.3 サポートデスク対応時間

・ サポートデスクの対応は以下の時間帯で行われます。
➢ 問合せ受付：24 時間 365 日（閏年 366 日）
➢ 受付に対する対応および返信：SBT 営業日の 10:00 － 17:00
・ 問合せ担当者からの問合せに SBT が対応する時間は 1 ヶ月あたり 20 時間までとします。ただし、SBT の責めに帰すべき事由による障害対応時間は含めません。
・ 問合せ受付後は速やかに受付の回答及びその後の対応を開始するよう努めますが、保証値はベストエフォートとなります。
・ 問合せに対し商業上合理的な範囲で問題解決ができるよう努めますが、全ての問題解決を保証するものではありません。

2.2 障害対応

・ 本サービスの障害の対応は以下の時間帯で行います。
➢ 土、日、祝日および SBT 指定休日を除く平日 10：00～17：00
・ 障害対応時間内に、SBT にて状況の確認を行うものとし、本サービスが提供する機能の利用可否を通知するものとします。
・ SBT プログラムの障害の場合は、SBT にて復旧まで対応するものとします。
・ 障害が発生した場合、商業上合理的な範囲でデータの復元ができるよう努めますが、データの復元が可能であることおよびすべてのデータを完全に復元することを保証するものではありません。
・ SBT は、本サービスにおいて、障害等によりデータが失われた場合、速やかに原因を追求し、復旧に努めるものとしますが、このことは復旧を確約するものではありません。なお、販売店および契約者の責に帰すべきデータ消失について、SBT は復旧対応について何らの義務および責任を負うものではありません。
・ SBT は、システム障害などで販売店および契約者のデータを確認する必要があると判断した場合に、当該データを確認することがあります。販売店および契約者は SBT が当該データその他必要情報の提供を求めた場合、すみやかに応じるものとします。

2.3 サービスの運用

SBT は、本サービスにアクセスされた方の履歴「アクセスログ」を記録し、保守管理や利用状況に関する統計分析、機能開発・機能改善のために利用することがあります。SBT は、アクセスログを保守管理や利用状況に関する統計分析以外の目的で利用しないものとします。

2.4 可用性

SBT は、本サービスの可用性を 99.5%（ただし努力目標とし、保証値は「2.6 補償請求」に定める）とします。算定の際には計画停止時間は含まれないものとします。

2.5 計画停止

SBT がアプリケーションの更新が必要であると判断した場合、バージョンアップおよびメンテナンスを SBT 指定の時間で行います。メールにて事前に登録頂いたメールアドレス宛に通知します。予定されているバージョンアップおよびメンテナンスは下記通知期限を目標に、事前にお客様へ通知する努力を尽くしますが、緊急時のメンテナンスについては事前に通知することができない場合があります。

区分	リリース内容	連絡期限
計画	機能追加/バグフィックス/機能改善（サービス停止あり）	2 週間前
計画	機能追加/バグフィックス/機能改善（サービス停止なし）	1 週間前
計画	メジャーバージョンアップ/業務に影響のある UI 変更	2 週間前
計画	機能の廃止	1 ヶ月前
計画	システム要件の追加	2 週間前
計画	システム要件の削除	1 ヶ月前
緊急	サービス継続に必要な緊急メンテナンス	即日都度
緊急	メンテナンス後に問題が発生した切り戻し	即日都度

2.6 補償請求

請求の前提条件	SBT は、本仕様書に規定されているサービスレベルを達成しない場合、本項の定めに従い、契約者に対して補償を行います。契約者への補償は、契約者が SBT に請求した場合に限り実施するものとします。 契約者が本仕様書に基づく補償請求を行う場合、「障害」の発生後 3 営業日以内に SBT に補償請求の意思を報告し、障害発生の翌月 15 日までにその請求の内容を裏付ける根拠となる資料を提示するものとします。 また、契約者は、補償請求を行い得ることとなった日から 3 ヶ月を経過する日までに請求をしなかった時は、本規定に基づく権利を失うものとします。
補償の対象となる障害定義	① ダウンタイムの定義 本サービスへの接続不能状態（以下（ア）に定める基準に従う）が 10 分以上継続した状態の 1 請求月間の合計累積時間（分）をダウンタイムと定義します。なお、同じ障害が原因で、以下に定める基準の複数のダウンタイムが発生した場合、契約者は、補償請求を行うダウンタイムを 1 つだけ選ぶ必要があるものとします。 (ア) 本サービスの Web アプリケーションへの接続の試行が 10 分間連続して接続が失敗した場合に、本サービスは 10 分間使用できなかったとみなされます。

	② ダウンタイムの除外要件 以下の場合はダウンタイムとみなしません。 ・ SBT よりあらかじめ通知されたサービス停止 ・ 10 分未満の断続的な接続不能 ・ 契約者のネットワーク障害など契約者環境に起因する場合 ・ 利用者の故意又は過失に起因するサービス停止 ・ 本サービスと外部サービスを API 連携する機能の停止 ・ 天災地変その他の不可抗力によるサービス停止 ・ 本サービスのサービス約款第 12 条（本サービスの停止）に該当する場合 ③ 障害起点定義 事前に告知がない状態でダウンタイムが発生した時間 ④ 復旧定義 SBT でサービスが正常に稼働していることの確認が取れた時間
月間稼働率	本サービスの利用があった暦月の総時間に利用者の総数を乗じ、当該暦月に請求事由となる障害の影響を受けた全利用者のダウンタイムの総時間を差し引いた数値を当該暦月の総時間に利用者の総数を乗じて得られた数値で除すことにより算出されます。
補償内容	月間稼働率が 99.5%を下回った場合、影響を受けた当該暦月の月額料金の 10%を返還します。 ※ 複数月一括払いを行っている契約者の場合、一括払いの料金を定められた一括払いの月数で除した金額（小数点以下の端数は四捨五入）を当月の月額料金とします。 【例】 [補償対象] 一か月（31 日×24h=744）の間に利用者数 3,000 の内、2,000 利用者が 8 時間の間利用不可になった。 （744h×3,000－8h×2,000）÷（744h×3,000） ≒99.28%（影響を受けた暦月の月額料金の 10%の補償対象） [補償対象外] 一か月（31 日×24h=744）の間に利用者数 1,000 の内、100 利用者が 24 時間の間利用不可になった。 （744h×1,000－24h×100）÷（744h×1,000） ≒99.67%（補償対象外）

3. セキュリティ

・ SBT は、本サービスにおいて、以下のセキュリティ管理を行うものとします。
  - ID（メールアドレス）とパスワードの認証により制御されています。
  - システム管理者権限を持つユーザーにより設定いただくことで以下の機能が提供されます。
    - ✓ Microsoft Entra ID と連携した SAML 認証
    - ✓ IPv4 アドレスによるアクセス制限
  - SSL/TLS により通信データが暗号化されています。
  - データベースの保存データは暗号化されています。
  - アプリケーションは脆弱性診断を行っています。
  - Web Application Firewall によって攻撃から守られています。

・ 以下は Microsoft Azure のサービスに準拠します。
  - データセンターの敷地、建物、サーバー室、機器に関する事項
  - データセンターの管理や運用に関する事項

4. クライアント機器の利用環境

・ クライアント機器の端末は以下を満たしている必要があります。

端末	PC ※タブレットおよびスマートフォンは対象外となります。
画面サイズ	推奨サイズ：1920 x 1080 最低サイズ：1440 x 1080 ※最低サイズより小さい画面でも表示されますが画面が崩れる可能性があります。
OS	Windows OS（最新世代および 1 世代前までのメジャーバージョンの最新パッチ適応済）
ブラウザ	Edge および Chrome（最新バージョン） ※上記ブラウザおよびバージョン以外でも利用可能ですが、動作保証はいたしかねます。

5. ネットワーク

・ インターネットに接続できる環境である必要があります。

・ ファイアウォール等によって、当サービスにアクセスでき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頂くことによってご利用可能になります。本サービスはポート 443 の HTTPS プロトコルで、下記ドメインと通信可能である必要があります。
  - https://saaspatrol.jp

・ SBT は、インターネット回線事業者・ISP の都合により本サービス支障が発生した場合の責任は負わないものとします。

・ 端末のネットワーク帯域が遅い回線をご用すると、本サービスの利用に支障をきたす場合があります。

6. 耐障害性

- Web アプリケーションおよびデータベースは 2 つ以上の異なるインスタンスで冗長構成されているため、特定のインスタンスで物理的故障が発生してもサービスを継続することが可能です。ただし、異なるリージョン間においては冗長化されていない為、リージョン全体で障害が発生した場合はサービスを継続することができなくなります。
- データのバックアップは geo 冗長ストレージに格納されるため、リージョン全体で障害が発生しても復旧することができます。

7. パフォーマンス

- 画面は 3 秒以内に描画が行われることを目標としますが、ベストエフォートでの提供となります。
  ※大量のデータを扱う機能や長時間の処理が必要な特定機能においてはその限りではありません。

8. データ

- 契約期間終了日の翌日よりデータベース内のすべてのデータを削除します。
- Web サーバーのログおよび、アプリケーションのトレースログは最低 1 年保存しますが、基本的には開示しません。ただし、不正アクセス等、セキュリティ関連の特別な事象が発生した場合のみ、ご相談に応じて対応させて頂きます。
- 資料の提出等、お客様個別の監査依頼には対応しないものとします。
- 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ていません。

9. トライアル

- 本番契約前に利用いただけるトライアルメニューになります。

メニュー
基本機能

※ トライアルは 1 社 1 回、30 日間限定となります。

9.1 トライアル内容

9.1.1 トライアル提供内容

トライアルでは基本機能すべてをご利用いただくことができます。

9.1.2 トライアル利用上の注意点

- トライアルの利用は、申込書の管理者、運用担当者欄に記載の 3 ユーザー限定です。
- トライアル環境には SLA の適用はありません。
- トライアル環境には SLA が適用されない為、ご利用に際して情報の消失等があった場合でも、当社は責任を負うことができません。
- トライアル環境をそのまま本番環境として利用開始することが可能です。
- トライアル環境を本番環境として利用継続する場合以外を除いて、トライアル終了翌日にデータは削除いたします。

10. 利用開始

- あらかじめ同意された利用開始日までに、開通通知を送付します。利用開始日をもってサービスの利用開始となります。
- サービスの利用開始の際は申込書の記載が必要です。その他、契約方法、課金についての重要事項、注意事項の詳細については、「NOZ SECURITY サービス約款」をご確認ください。

11. 利用終了

- 契約期間の終了をもってサービス利用の終了となります。

11.1 サービス停止の実施

- 契約終了日の翌日より下記の対応を実施します。
  - お客様データの削除

11.2 サービス停止時の注意事項

- 削除したデータはいかなる場合も復元できません。
- サービス停止時にお客様環境での作業が必要となる場合は、管理責任者及び運用担当者へ作業内容をご連絡します。
- 終了時の契約方法、課金についての重要事項、注意事項の詳細については、「契約ガイド」をご確認ください。

12. その他禁止事項

- サービスの利用にあたり禁止事項を設けています。違反を確認した場合、サービス利用を停止します。
  - 本ソフトウェアの複製を作成すること。
  - 第三者に対して譲渡、貸与、もしくは再許諾すること。
  - リバースエンジニアリング、逆コンパイル、または逆アセンブルを行うこと。

13. その他制限事項

・ その他、下記については SBT では対応いたしかねますので、あらかじめご了承ください。
  - ➢ お客様個別の監査対応。
  - ➢ SBT の提供するサービスに、SBT 以外の第三者から何らかのサービス等を受けた場合、当該サービス等について一切の責任を負わないものとします。

14. 契約に関する注意事項

・ トライアル、本番（新規、変更、解約/終了時）の契約方法、課金方法の詳細については別紙「契約ガイド」をご確認ください。

・ 申込書の注意事項をよくご確認ください。

以上

2024 年 5 月 27 日 初版発行

2024 年 8 月 30 日 ver2.0 改定

2024 年 11 月 13 日 ver3.0 改定

2025 年 3 月 6 日 ver4.0 改定