SBテクノロジー
クラウドパトロール
サービス仕様書

2025年5月27日

SBテクノロジー株式会社

改訂履歴

改訂日	備考
2023/8/21	初版作成
2023/9/27	6.1.解約時の対応についてマニュアル参照とする旨、追記
2023/10/17	4.5.2.リソース一覧の取得間隔を 1 時間に 1 回に変更
2023/11/15	AWS だけでサービス利用可能な機能追加に伴う更新
2023/11/30	AWS 環境（独自）のリソース取得について追記
2023/12/7	Google Cloud 環境（MDfC）について追記
2023/12/21	Google Cloud だけでサービス利用可能な機能追加に伴う更新
2024/1/25	ガイドライン監査機能追加に伴う更新 サービスに関するお問い合わせのサポート範囲を更新
2024/2/1	監査機能の Azure 対応に伴う更新
2024/2/22	監査機能の Google Cloud 対応に伴う更新
2024/3/7	AWS 監査機能の CISv3.0.0 対応に伴う更新
2024/3/14	環境ごとの通知先機能追加に伴う更新 Azure 監査機能の CISv2.1.0 対応に伴う更新
2024/3/28	アタックサーフェス管理機能追加に伴う更新 AWS 監査機能のレベル 2 対応に伴う更新
2024/5/16	以下の実施を反映 ・Azure、AWS、GCP の MDfC 推奨事項を利用したポリシーを廃止 ・AWS/GCP 環境の登録（MDfC）機能を廃止
2024/5/30	以下の実施を反映 ・Azure：基本的な保護ボタンを 2 つに分割
2024/6/20	リスク通知履歴と特定リソースの検査除外機能追加に伴う更新
2024/6/27	任意の検査対象の登録、レポート一括出力対応に伴う更新
2024/7/18	ASM リスク通知機能追加に伴う更新
2024/7/26	問い合わせ対応の生成 AI モデルの GPT-4o Mini 対応に伴う更新 クラウド資産台帳対応に伴う更新
2024/8/8	Google Cloud 監査機能のレベル 2 対応に伴う更新
2024/8/23	当社営業日に関する記載を更新
2024/9/5	Azure 閲覧者ロールでの登録機能追加に伴う更新
2024/10/17	レポーティング機能追加に伴う更新
2024/10/24	アカウントレポート追加に伴う更新
2024/10/29	ASM の検査間隔変更（24 時間に 1 回）に伴う更新
2024/11/13	ポータル管理者設定の表記変更に伴う更新
2024/12/12	以下の実施を反映 ・AWS 環境の登録に、即時対策なしを追加 ・クラウド保護＞STEP4 に、重大度の追加 ・通知先を無制限に、Teams Webhook の廃止
2024/12/19	以下の実施を反映 ・リスク通知履歴の保持期間を 30→365 日に変更 ・CIS 監査 AWS v4.0.1 対応を追加
2024/12/25	即時通知の連続通知抑制について追記
2025/1/30	リスク通知履歴の保持期間を 30 日に更新

2025/3/6	リスク診断レポート B について追加 リソース一覧の取得について更新
2025/4/24	CIS 監査 Azure v4.0.0 対応を追加
2025/5/27	パトロール日報の仕様変更について更新 問い合わせ対応の生成 AI モデルの GPT-4.1 mini 対応に伴う更新 CIS 監査 AWS v5.0.0 対応を追加 CIS 監査 Google Cloud v4.0.0 対応を追加

目次

本書で使用する製品名は各社の商標または登録商標です。
本文中では、®、©マークは省略しています。

本書に記載された事項は、約款の定めに従い変更することがあります。

本書に記載された Microsoft をはじめとする各社のサービス名、機能名は予告なく変更となる場合がございますが、機能の大幅な変更がない限り本サービスの提供は名称変更後の各社サービスに対して適用されます。

1. はじめに

本書の位置づけ

本書では、SB テクノロジー株式会社（以降、当社）が提供する「クラウドパトロール」のサービス内容について、記述したものです。

本書は、お客様との契約内容の一部を構成します。

用語定義

本書で利用する用語について記載します。

以降の文書は本定義に基づいてご理解を進めてください。

・本サービス

当社が提供する「クラウドパトロール」を指します。サービスの略称として「クラパト」と記載することがあります。

・リスクポリシー

当社がお客様のパブリッククラウド（Azure、AWS、Google Cloud）に対して設定する監視ルールを指します。この監視ルールに基づき、当社がすぐに対処すべきと判断した緊急リスクに対する即時通知や即時対策を行います。

・パトロール

当社監視ルールに基づいてお客様のパブリッククラウド環境を定期的に巡回して緊急リスクが発生していないか検査することを指します。

・パトロール日報（緊急リスク有無の日次報告）

緊急リスクの発生有無に関わらず、1 日 1 回お客様が指定した時間に、登録されたクラウド環境のリスク有無を設定された宛先に通知する機能を指します。

・サービスポータル

当社が提供する本サービス契約者様専用のポータルを指します。ポータルの基盤として ServiceNow を利用しております。

・サービステナント

お客様のパブリッククラウド（Azure、AWS、Google Cloud）に対して緊急リスクの検知や対策など各種自動対応を行う当社のサービス専用に構築したテナントを指します。

・クラウド環境の登録

お客様が所有者権限を持つ Azure テナントとサブスクリプション、AWS アカウントおよび Google Cloud プロジェクトを、本サービスポータルで管理できるように登録することを指します。

・サービスプリンシパル

Microsoft 社が提供する Microsoft Entra（旧 Azure AD）上に作成するオブジェクトリソース操作用のインスタンスを指します。

・NSG（ネットワークセキュリティグループ）

Microsoft Azure の仮想ネットワーク上の Azure リソースが送受信するネットワークトラフィックに対するフィルタ処理を提供するサービスを指します。NSG のルールでは、送信元と宛先、ポートおよびプロトコルを指定することができます。

・VNet（仮想ネットワーク）

Microsoft Azure において、他ネットワークと論理的に分離されたプライベートなネットワークを構築できるサービスです。

・PAL（Partner Admin Link）

パートナー管理リンクと呼ばれ、当社がお客様の Azure 環境においてサービス提供していることを示すフラグです。クラウド環境の登録時に自動処理されますが、PAL 登録した状態の維持が本サービス提供の前提条件となります。

・緊急リスク

お客様がすぐに対処すべきリスクを指します。

・インシデント

お客様の環境下において、不正な活動が行われたという事実・事案を指します。

・保護対象

お客様のパブリッククラウド環境（Azure、AWS、Google Cloud）を指します。

・お客様

本サービスが監視対象とするパブリッククラウドを所有・管理されるユーザー様を指します。

・当社営業日

原則、暦に準拠していますが、年末年始などについては弊社サイトのお知らせにて公開いたします。

https://www.softbanktech.co.jp/news/topics/info

2. サービス概要

当社が提供する本サービスは、パブリッククラウド（Azure、AWS、Google Cloud）の設定不備およびインシデント発生を検知するセキュリティ監視サービスです。

2.1. サービスの提供項目およびサービス提供時間

本サービスでは、お客様と以下の役割分担でサービス提供いたします。

■ 初期作業

#	提供サービス・機能	お客様	当社	自動化	提供時間	補足
1	申込サイトに必要情報を登録	○	-	○	24/365	申込サイトで受付
2	サービスポータル受入作業 ～お客様への Welcome メール送付	-	○	△	営業日 9-17	お客様情報の登録と開設
3	STEP1:クラウド環境の登録	○	-	○	24/365	
4	STEP2:保護の適用	○	-	○	24/365	AWS、Google Cloud は不要
5	STEP4:即時通知、対策対象のリスク選択	○	-	○	24/365	
6	STEP5:通知先の設定	○	-	○	24/365	

凡例：○実施主体 - 主体ではない

[自動化]列の凡例：○サービス提供の自動化　△一部自動化　×手動

■ 運用サービス

#	提供サービス・機能	お客様	当社	自動化	提供時間	補足
1	危険な設定の検知、即時通知、対策	-	○	○	24/365	
2	リスク診断、監査やアタックサーフェス管理のレポート出力	-	○	○	24/365	レポート発行指示はお客様にて実施
3	準拠や修復対応	○	△	△	24/365	結果を踏まえた対応
4	サービスに関する問い合わせ対応	-	○	○	24/365	サービスポータルから実施
5	サービス監視	-	○	○	24/365	負荷や処理状況の監視
6	サービス改修対応	-	○	△	営業日 9-17	高負荷や不具合時の対応
6	サービスの機能追加・更新	-	○	△	営業日 9-17	機能やマニュアルの更新時はお知らせに掲載

※凡例は初期作業と共通

■ 解約時

#	提供サービス・機能	お客様	当社	自動化	提供時間	補足
1	契約に関する連絡窓口に連絡	○	-	×	営業日 9-17	メール
2	クラウド環境の削除	○	-	○	24/365	サービスポータルからお客様セルフでいつでも実施可能
3	サービスポータル削除作業	-	○	△	営業日 9-17	お客様情報の削除

※凡例は初期作業と共通

2.2. サービス提供対象環境

本サービスの監視対象となるパブリッククラウド環境は、以下となります。

Microsoft Azure

AWS (Amazon Web Services)

Google Cloud

2.3. サービス提供言語

本サービスは、日本語での対応とさせていただきます。お客様向けのサービスポータルにおいても日本語表記を基本としておりますが、機能名の表記など分かりやすさの観点から英語表記としている箇所がございます。

2.4. サービス提供条件

本サービスを提供する上で必要な条件を以下に示します。

2.4.1. Azure 向けサービス提供条件

(1)クラウド環境を登録する Azure ユーザーには、以下 2 つの権限が必要です。確認方法はマニュアルを参照ください。

①Microsoft Entra テナントを管理するロールとして、グローバル管理者

②サブスクリプションを管理する Azure リソースロールにおいて、所有者

(2)上記テナントに対して、サービス提供に必要な資格情報（サービスプリンシパル）の作成を承諾頂けること

(3)上記サブスクリプションに共同作成者ロール（即時対策あり）あるいは閲覧者ロール（即時対策なし）の作成を承諾頂けること

(4)当社がお客様の Azure 環境においてサービス提供していることを示すフラグである PAL（パートナー管理リンク）について、クラウド環境の登録時に自動処理されますが、PAL 登録した状態を維持していただけること。なお、クラウド環境を削除することで、PAL も削除されます。

(5)インシデント発生した可能性の高いアラートを出力するためには、MDfC の各種有償機能の有効化が必要であり、本サービス費用とは別にお客様の Azure 費用が発生することを承諾いただけること（ご利用は任意となります）

2.4.2. AWS 向けサービス提供条件

(1) クラウド環境を登録する AWS アカウントには、CloudFormation 実行権限および IAM ロール作成権限が必要です。具体的には以下のロールとなります。

iam:CreateRole

iam:DeleteRole

iam:DetachRolePolicy
iam:AttachRolePolicy
iam:PutRolePolicy
iam:ListAttachedRolePolicies
iam:ListRolePolicies
iam:GetRolePolicy
iam:GetRole
cloudformation:CreateStack
cloudformation:DeleteStack
cloudformation:DescribeStacks
cloudformation:ListStacks
cloudformation:DescribeStackEvents
cloudformation:GetTemplateSummary

(2)お客様の AWS 環境に対して AWS の標準マネージドポリシーの一つである、ReadOnlyAccess を適用します。これは AWS のほとんどのサービスに対して読み取り専用のアクセス権を付与することを意味します

(3)AWS アカウントを即時対策ありで登録した場合、お客様の AWS 環境に対して、ec2:ModifySecurityGroupRules というアクションを許可することで､セキュリティグループのルールを変更する権限を適用します。即時対策なしで登録した場合、この権限は適用されません。

2.4.3. Google Cloud 向けサービス提供条件

(1)クラウド環境を登録する Google Cloud プロジェクトには、オーナー権限が必要です

(2)お客様の Google Cloud 環境に対して

①特定の権限（compute.firewalls.update および compute.networks.updatePolicy）を持つカスタムロール（CloudPatrolRole）の作成を承諾いただけること

②2 つのサービス（cloudresourcemanager.googleapis.com と compute.googleapis.com）の有効化を承諾いただけること

ⅰ）Google Cloud Resource Manager サービスによって、プロジェクト内のリソースにアクセス権を設定できるようになります。

ⅱ）Google Compute Engine サービスによって、仮想マシンの作成、ネットワーキングの構成、ストレージの管理など、さまざまなタスクを実行できるようになります。

③特定のロール（viewer、cloudasset.viewer および①で作成した CloudPatrolRole）を持つ cloud-patrol という名前のサービスアカウントの作成を承諾いただけること

④cloud-patrolサービスアカウントにiam.serviceAccountTokenCreatorロールの付与を承諾いただけること。これはサービスアカウントトークンの作成権限を持つロールです。サービスアカウントトークンとは、Google Cloudリソースにアクセス権を委任するために使用される一時的な認証情報です。

3. クラウド環境の登録から保護開始まで

3.1. クラウド環境の登録から保護開始までの流れ

以下に本サービス利用時のクラウド環境の登録から保護開始までの流れの概要を示します。具体的な手順はマニュアルを参照ください。

STEP	項目	必須 任意	内容
1	クラウド環境の 登録	必須	（1）Azure テナントのグローバル管理者によってサブスクリプションに共同作成者ロール／閲覧者ロールを付与 （2）AWS ①本サービスに登録したいAWSアカウントにIAMロールを作成 ②本サービスにAWSアカウントを追加 （3）Google Cloud ①本サービスに追加したGoogle Cloudプロジェクトに IAMロールを作成 ②本サービスにGoogle Cloudプロジェクトを追加 上記によって登録した環境がSTEP2以降の適用対象となる
2-1	保護の適用	任意	Azureのみ選択可能。チェックすると、以下対象となる ①リソース一覧の取得（レポーティング配下で取得） ②定期検査ポリシーの対象
2-2	有償機能の適用	任意	
3	リスク診断レポート	任意	現在発生している緊急リスクの一覧を環境ごとにレポート
4	緊急リスクの選択	必須	緊急リスクごとに即時通知・対策有無をチェック
5	通知先の設定	必須	リスク発生時の各種通知・パトロール日報の送付先を設定

3.1.1. 登録や設定の単位

各 STEP における登録や設定の選択単位について以下に示します。

STEP	Azure	AWS	Google Cloud
1：クラウド環境の登録	テナント単位 ※対策あり/なしはポータル単位で切り替え	アカウント単位	プロジェクト単位
2：保護の適用	サブスクリプション単位	選択不可	選択不可
3：リスク診断レポート	同上	アカウント単位	プロジェクト単位
4：リスクの選択	ポータル単位		
5：通知先設定	サブスクリプション単位	アカウント単位	プロジェクト単位
6：リソースの検査除外	リソース単位	リソース単位	リソース単位

3.1.2. 複数ポータルについて

本サービスでは、事業部やグループ会社ごとにポータルを複数発行して、管理を分けることが可能です。複数ポータルを利用希望の際は、追加問い合わせからご依頼ください。

なお、グループ会社様もご利用になる際は、1社1契約をお願いしております。

	シナリオ例	システム仕様
複数ポータルを希望	・事業部やグループ会社ごとに管轄が異なり、環境やレポートを見せたくない ・Azureテナントや AWS アカウントによって対策ありなしを分けたい	・サービスポータルの右上にポータルを選択するプルダウンが表示され、利用するポータルを選択 ・同一ユーザーが複数ポータルの管理者になることが可能

3.2. STEP1：クラウド環境の登録（Azure）

本サービスでは利用開始時にお客様がグローバル管理者権限を持つ Azure テナントが一覧で表示されますので、本サービスに登録したいクラウド環境をテナント単位で選択可能です。

3.2.1. STEP1-1：Azure 環境の登録

サービスポータルに用意されている「Azure 環境の登録」ボタンを押下することで、登録作業を開始できます。なお、このボタンを右クリックからリンクコピーして社内ユーザーにリンク共有、押下してもらうことで、本サービスポータルにアクセス権限のない社内ユーザーがグローバル管理者権限を持つクラウド環境についても登録作業を開始することができます。

リンクを社内に共有する機能がないため、本サービスだけでは完結しませんが、この機能によって、社内で本サービス契約者以外の方が所有者権限を持つ環境を、契約者が把握し、監視対象とすることが可能となるため、必要に応じて活用をご検討ください。

3.2.2. STEP1-2：登録可能なテナント一覧表示

STEP1-1 で「Azure 環境登録の開始」ボタンを押下したユーザーは、次に以下のアクションが必要です。

①「ホームテナント」は本登録完了

②「ゲストテナント」は仮登録ステータスのため、「本登録/更新」ボタンを押下

③本サービスポータルへのアクセス権限を持たない「ゲストテナント」ユーザーには、「本

登録/更新」リンクを共有、押下

※ホームテナントとは、ユーザーが所属している Microsoft Entra テナントのことです。ゲストテナントとは、ユーザーが招待されてアクセスできる他の Microsoft Entra テナントのことです。

また、本サービスから登録した環境は、登録時と同じテナント単位で本サービスから削除可能です。

クラウド	表示される情報
Azure	①テナント名 ②テナント ID ③Azure ポータルへのサインインアドレス ④利用機能（対策あり/なしを識別） ⑤登録ステータス（本登録/仮登録） ⑥アクション/社内へのリンク共有（右クリックでリンクコピー可） ⅰ）本登録/更新 ⅱ）削除

3.2.3. STEP1-3：本登録完了

STEP1-2 のアクションにより、Azure 環境の登録は完了です。なお登録完了後に、テナント内のサブスクリプション情報が更新された際も「本登録/更新」ボタン押下することで、更新が反映されます。

3.3. STEP1：AWS 環境の登録

[AWS 環境の登録]ボタンから環境登録できます。即時対策の有無によって、登録ボタンが異なります。具体的な手順はマニュアルを参照ください。

3.4. STEP1：Google Cloud 環境の登録

[Google Cloud 環境の登録]ボタンから環境登録できます。

3.5. STEP2-1：保護の適用

「独自ポリシー」ボタンは、Azure サブスクリプション単位で適用要否を選択可能です。STEP2 において「独自ポリシー」適用時の動作は以下となります。

（1） クラウド保護＞STEP4：独自ポリシーの適用

（2） アタックサーフェス管理＞STEP3：リスクの検査

（3） リソース一覧の取得

ボタンのアンチェック時には上記の適用除外となります。

STEP2 において「MDfC 有償機能」適用時の動作は以下となります。

（1） MDfC セキュリティ警告の適用(STEP2 で各有償機能ボタンが選択可能となります)

（2） クラパト専用リソースグループ(RG)を東日本リージョンに作成

sbt-cloudpatrol-rg

（3） クラパト専用 Log Analytics ワークスペース(WS)を専用 RG 内に作成

（4） MDfC セキュリティ警告のログを専用 WS に出力開始（既定の 30 日間ログ保管）

ボタンのアンチェック時には、クラパト専用 RG および WS が削除され、上記の適用除外となります。

※参考 URL

Azure Monitor ログでのデータ保持とアーカイブ - Azure Monitor | Microsoft Learn

3.5.1. 危険な設定からの保護

緊急リスクは、リスクカテゴリとして「危険な設定」を対象としており、クラウドパトロール独自ポリシーでは、ポリシーに該当した場合に即時通知や対策を実施します。

3.6. MDfC 有償機能の適用

本サービスでは、サービスポータルから MDfC の有償機能を適用可能です。

本 STEP において、MDfC 有償機能を有効化する保護対象（サブスクリプション）が一つでもあれば、STEP4 で該当する有償機能のリスクポリシーを選択可能となります。このため、お客様の Azure 環境においてすでに MDfC 有償機能を有効化されていた場合もサービスポータル上で適用頂く必要がございます。その際、お客様の Azure 環境には影響はございません。

各種有償機能の説明については Microsoft 社のサイトを参照ください。
Microsoft Defender for Cloud とは - Microsoft Defender for Cloud | Microsoft Learn

また、有償機能利用によって発生する Azure 費用は以下を参照ください。
価格 — Microsoft Defender | Microsoft Azure

上記 MDfC の有償機能について、サービスポータルから有効化だけでなく、無効化も可能です。

3.7. STEP3：リスク診断レポートの発行

環境ごとに現在発生しているリスク状況と過去 30 日間の通知／修復履歴について、レポートいたします。レポート一括取得においては、双方作成します。

（1）リスク診断レポート A 仕様
・現在発生しているリスクのみをレポート
・Azure：テナントリスクは全環境のレポートに出力

（2）リスク診断レポート B 仕様
・レポート A の内容に加えて、過去 30 日間のリスク通知／修復履歴をレポート
・A.現在の状態／B.通知・修復履歴列において、A でフィルタすると、レポート A
・通知日時は STEP6：リスク通知履歴から情報取得するため、STEP4 を有効化しないと、通知履歴はレポートされない
・リスク検知されなくなったことを修復と判断し、最終検知日時の 1 時間後を修復日時

として記載

・過去 30 日間にリスク通知し、すでに修復済みのリソースを行追加

・通知未設定のポリシーは、通知日時列に、通知未設定（STEP4 の即時通知を有効化してください）と記載

・意図しない国からのログインなど、通知のみのポリシーもレポート

・STEP4 で個別設定のリスクポリシーは指定した値、検知した値を入れたうえでレポート

・同一リソースが過去 30 日間で通知/修復を繰り返した場合は最後の通知/修復のみ記載

・Azure：テナントリスクは STEP6 参照のため、通知先に指定された環境のレポートのみ出力

・STEP3 の条件では不合格だが、STEP4 の個別設定列の通知基準に達しない場合、通知日時列に、「即時通知の設定した基準に達しないため、通知履歴なし」と表示

◆リスク診断レポートのスコア（A,B 共通）

計算式：[合格]判定数／（[不合格]判定数＋[合格]判定数）

※リスクがないことを意味するため、診断対象なしも合格と判定

3.8. STEP4：緊急リスクの選択（監視・即時通知・対策）

本サービスでは、サービスポータル上に掲載された個別のリスクポリシーについて、お客様が任意でチェックすることで、STEP2 で保護対象としたお客様のクラウド環境に該当リスクが発生していないか定期的に監視し、リスク発生時に即時通知や対策が可能です。

具体的に適用可能なポリシーの一覧については、本仕様書の範囲外としております。サービスポータルにてご確認ください。

リスクポリシーの仕様について、以下に示します。

項目	仕様
検査対象	Azure：STEP2 で独自ポリシー適用したサブスクリプション AWS：登録されているすべての環境 Google Cloud：登録されているすべての環境
リスクポリシー一覧	すべてのお客様共通 ・カスタムポリシーの作成不可だが、一部ポリシーは任意の設定が可能
リスクポリシー設定単位	ポータル単位で共通 ・Azure サブスクリプションごとに異なるポリシー設定不可 ・ポータルを分ければ Entra テナントや AWS アカウント、Google Cloud プロジェクトごとに異なるポリシー設定可能
リスクポリシー名	緊急リスクのポリシー名称を記載
クラウド	Azure、AWS、Google Cloud から選択可能
ポリシー種別	・クラウドパトロール独自（危険な公開、不十分なアカウント管理、意図しない事象、異常な使用、コンプライアンスなど） ・MDfC 各種有償機能
重大度	修復対応の優先度付けを目的として重大度を定義 緊急：単独でインシデントにつながる危険な設定や状態 高：場合によってはインシデントにつながるリスクの高い設定や状態
個別リスク説明	リスクポリシーの具体的な内容を記載。 STEP4 でリスクポリシー名をクリックすることで表示
即時通知	該当リスクが発生した際に、設定した宛先に通知
即時対策	該当リスクが発生した際に、実装した内容を実施し、完了した旨を通知
監視間隔 ①独自ポリシー	60 分：ポリシー違反しているリソースがないか、保護対象の環境をすべてチェック
監視間隔 ②MDfC 有償機能	60 分：MDfC セキュリティ警告の新規に発生したアラートをチェック ・アラートの状態（アクティブ、進行中、却下済み、解決済み）判定はしていない

項目	仕様
	・MDfC がリスク検出し、Log Analytics ワークスペースにログ出力したセキュリティ警告のログがないか、60 分間隔で本サービスが検査
連続通知の抑制	・CSPM、ASM とも 1 週間（24h×7d）以内に、同一のリソースが同じリスクを複数回検知した場合は再通知しない ※リスク状態が変わらないリソースについては 1 時間ごとに検査し、リスク検知をし続けるため、継続的に通知しない ※違反リソースが修復後、1 週間以上経過して、再度リスク発生した場合は新規リスクとして通知 ※異なるリソースや条件と判定できる場合は、新規リスクとして通知
外部サービス利用	AWS 向けの緊急リスクポリシー W050：意図しない国からのマネジメントコンソールへのログイン において、Console Login イベント内の送信元 IP アドレスからの国名参照には、オープンソースで提供されている IP2Location Lite を利用 https://lite.ip2location.com/edition-comparison

3.9. STEP5：通知先の設定（リスク発生時の各種通知・パトロール日報）

本サービスでは、リスク発生時や対策完了時の即時通知とは別に、1 日 1 回緊急リスクの有無に関わらず報告する「パトロール日報」機能があります。

これらの各種通知や日報は、サービスポータルからお客様自身で通知先を設定可能です。

以下にリスク発生時の各種通知とパトロール日報の仕様について、示します。

項目	仕様
通知タイミング	①即時通知：リスク発生時 ②即時対策：リスク対策完了時 ③パトロール日報：1 日 1 回（送付時間は 30 分単位でお客様が任意で選択）
通知先	①②③共通（種別ごとに異なる通知先設定は不可）
通知対象	①②ポータルでお客様が有効化したリスクポリシーのみ ③即時通知が有効となっているリスクポリシーのみ
通知手段	メール、Teams、Slack を任意で追加 ※Teams はチャネルのメールアドレスを取得して登録ください
通知先上限	無制限
通知先設定単位	通知先ごとに以下の単位で通知対象とする環境を追加 Azure：サブスクリプション単位 AWS：アカウント単位 Google Cloud：プロジェクト単位
FROM アドレス	patrol-noreply@tech.softbank.co.jp 表示名：クラウドパトロール
パトロール日報仕様	新規発生および修復可能なリスク A,B の一覧 A.過去 24 時間に発生した新規発生リスク （意図しない国からのサインインなど、修復不可の通知のみリスクも掲載） B.過去に発生した修復可能なリスクのうち、未修復のリスク ※通知のみのリスクや MDfC セキュリティ警告は対象外 C.当月のコスト情報（Azure、AWS のみ） ：「想定外の高額課金請求」ポリシーを有効化している場合に記載 D.国内/海外リージョンのリソース数（Azure、AWS、Google Cloud） ：「海外リージョンの利用」ポリシーを有効化している場合に記載

項目	仕様
	E.環境ごとのユーザー数と前日の作成（Azure、AWS、Google Cloud） ：「不審なユーザー名の追加（日報）」ポリシーを有効化している場合に記載 リスクがある場合だけでなく、リスクがない場合も毎日レポート
不要な通知抑制	リソースやアラート単位の抑制不可。該当ポリシーの無効化による対応のみ

3.10. STEP6：リスク通知履歴と特定リソースの検査除外（通知・対策）

本サービスでは、過去 30 日間の緊急リスクの即時通知・対策完了通知の履歴を確認できます。リソースごとに通知/対策除外にチェックすることで、該当リソースを即時通知や対策の検査対象から除外できます。

以下に、通知・修復履歴に関する仕様について、示します。

項目	仕様
通知・対策除外	リソース単位で、検査除外
通知履歴の保持期間	表（ポータル画面上）：過去 30 日間 裏（基盤側）：過去 37 日間 検査除外リソース：永続 ※30 日間経過して表通知履歴から削除後、次の定期検査で再検知して掲載
通知履歴のレポート B への出力	検査リソース：過去 37 日間 検査除外リソース：永続
メモ	上限 1000 文字まで記載可能

4. ガイドライン監査機能仕様

4.1. STEP1：監査機能

本サービスでは、クラウド保護の STEP1 で登録した環境に対して、最新の CIS ベンチマークへの準拠状況を監査することができます。

以下に監査機能の仕様について、示します。

項目	仕様
監査対象環境	（1）登録したテナント配下の Azure サブスクリプション （2）AWS 環境の登録から登録した AWS アカウント （3）GCP 環境の登録から登録した Google Cloud プロジェクト
監査基準	監査可能な項目 （1）CIS Azure Foundations Benchmark v2.1.0/v3.0.0/v4.0.0 レベル 1,2 （2）CIS AWS Foundations Benchmark v3.0.0/v4.0.1/v5.0.0 レベル 1,2 （3）CIS Amazon Elastic Kubernetes Service Benchmark v1.5.0 レベル 1 （4）CIS Google Cloud Foundations Benchmark v3.0.0/v4.0.0 レベル 1,2
監査結果	CSV ファイルで出力

◆監査レポートのスコア

計算式：[準拠]判定数／（[非準拠]判定数＋[準拠]判定数）

※監査対象なしは計算から除外

4.2. STEP2：準拠対応

STEP1 で監査を実施した結果、非準拠となったリソースについて、監査項目ごとに準拠に必要な手順をまとめています。

5. アタックサーフェス管理機能仕様

5.1. STEP1：攻撃面の発見

クラウド保護の STEP1 で登録した環境に対して、クラウド環境内部から公開状態のリソースを発見し、公開資産を含むクラウド資産台帳として出力します。

以下に **STEP1** でクラウド資産台帳を出力する仕様について、示します。

項目	仕様
対象環境	（1）登録したテナント配下の Azure サブスクリプション （2）AWS 環境の登録（独自）から登録した AWS アカウント （3）GCP 環境の登録（独自）から登録した Google Cloud プロジェクト
検出対象	検出対象の一覧は、ASM＞STEP1 のページにて情報更新 ・パブリック IP を持つリソース A ・A が持つプライベート IP ・プライベート IP のみのリソース B ※公開している可能性のあるリソースも含む
出力フォーマット	CSV ファイルで出力

5.2. STEP2：攻撃面の情報収集

クラウド保護の STEP1 で登録した環境や任意の検査対象に対して、公開資産（パブリック IP や FQDN）に紐づく OS、ソフトウェア、バージョン、脆弱性情報、ポート、バナー情報などを公開情報（OSINT）から収集し、ASM レポートとして出力します。

以下に **STEP2** で **ASM** レポートを出力する仕様について、示します。

項目	仕様
対象環境	（1）登録したテナント配下の Azure サブスクリプション （2）AWS 環境の登録（独自）から登録した AWS アカウント （3）GCP 環境の登録（独自）から登録した Google Cloud プロジェクト （4）任意の検査対象（IP,FQDN）
連携する公開情報	（1）Shodan　Shodan Search Engine （2）CISA KEV （3）JVN iPedia ※連携する公開情報(OSINT)は今後予告なく変更する可能性があります
情報収集方	公開情報（OSINT）が収集・保持している情報を、クラパトが API 連携や

項目	仕様
法	JSON/XML を取得 ※レポート出力時に、OSINT が新たにスキャン実行しないため、新規リソース作成直後など、タイミングによって情報が取得できない場合があります
出力フォーマット	CSV ファイルで出力
脆弱性関連	CVE 番号は、以下の条件を満たした際に表示されます。 ・OSINT（公開情報）から CPE が取得できる ・CPE に紐づく CVE がある ※CPE は、ハードウェア、OS、ソフトウェアなどを識別するためのユニークな ID です。 cpe：/{種別}：{ベンダ名}：{製品名}：{バージョン}：{アップデート}：{エディション}：{言語} ・KEV：OSINT が取得した CVE-ID に対して、既知の悪用された脆弱性一覧（KEV カタログ）と突合し、合致する CVE のみを掲載 ・脆弱性情報：OSINT が取得した CVE-ID に対して、JVN から関連する脆弱性情報を取得 ※OSINT が収集した CPE に関連付けている未確認の脆弱性を含みます。セキュリティパッチ適用によって CPE のバージョン番号が変更されないケースでは、パッチ適用後も脆弱性が修復済みと判定されません
任意の環境の登録数	ASM＞STEP2 のレポート一括出力では IP、FQDN の登録上限に制限は設けておりません。 単体のレポート発行処理は最大 230 秒のため、処理時間を超過し、レポート発行に失敗する場合は、トップページ＞レポーティング＞レポート一括出力から ASM レポートを発行してください

参考）CPE について

[共通プラットフォーム一覧 CPE 概説 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構]

（１）ASM レポート B 仕様

・任意の環境のみ、ASM レポート B の発行に対応

・ASM レポート A の内容に加えて、過去 30 日間のリスク通知履歴をレポート

・shodan が任意のタイミングでスキャン後に、クラパトが日次検査しており、時刻の精度が低いため、リスク解消日時は対象外とする

・A.現在の状態／B.通知履歴列において、A でフィルタすると、レポート A

・通知日時は STEP5：リスク通知履歴から情報取得するため、STEP3 を有効化しないと、通知履歴はレポートされない

・同一リソースの通知が複数回ある場合は、過去 30 日間で最も古い通知をレポート出力

・STEP3 で個別設定のリスクポリシーは指定した値、検知した値を入れたうえでレポート

5.3. STEP3：攻撃面のリスク評価

クラウド保護の STEP1 で登録した環境や任意の検査対象に対して、ASM リスクへの該当有無を定期的にチェックします。リスクポリシーに合致した際に、STEP4：リスクの通知先設定で指定した宛先に通知します。

リスクポリシーの仕様について、以下に示します。

その他の仕様は、クラウド保護＞STEP5：即時通知・対策のポリシーと同様です。

項目	仕様
検査対象	Azure：クラウド保護＞STEP2 で独自ポリシー適用したサブスクリプション AWS：登録されているすべての環境 Google Cloud：登録されているすべての環境 任意の環境：登録されているすべての環境
検査間隔	24 時間に 1 回

アタックサーフェス管理＞STEP4：リスクの通知先設定には、パトロール日報機能がありませんが、その他はクラウド保護＞STEP5：通知先設定と同じ仕様となります。

5.4. STEP5：リスク通知履歴

CSPM の緊急リスク同様、ASM においても、過去 30 日間の緊急リスクの即時通知の履歴を確認できます。リソースごとに通知除外にチェックすることで、該当リソースを即時通知の検査対象から除外できます。

6. レポーティング

6.1. レポート一括作成

クラパトポータルに登録した複数環境のレポートを一括で作成します。複数のポータルを利用している際も、自分が権限を持つポータルのみ、作成します。

各レポートを 1 つの Excel ファイルのシートごとに表示することで、大量に環境がある場合でも、公開状態にあるストレージなど、特定の要件に合致したリソースを見つけやすくなります。

レポート一括取得の仕様について、以下に示します。

環境種別	レポート種別	レポート/台帳	環境ごとのスコア
Azure AWS Google Cloud	CSPM	リスク診断レポート	有
		CIS 監査レポート レベル 1	有
		CIS 監査レポート レベル 2	有
		クラウド資産台帳	-
上記および 任意の環境	ASM	ASM レポート	-

環境数によってはレポート作成に時間がかかるため、後日ログインしてご確認ください。

6.2. アカウント台帳作成

ポータルに登録した環境に対して権限のあるユーザーアカウントを一覧で出力します。複数のポータルを利用している際も、自分が権限を持つポータルのみ、作成します。

アカウント情報は、各パブリッククラウドのコンソールからも確認できますが、登録されたすべてのアカウントを 1 つの Excel ファイルで表示することで、大量に環境がある場合でも、

・招待されたが未ログイン
・長期間利用のない特権アカウント
・MFA 未適用

など、特定の要件に合致したユーザーアカウントを見つけやすくなります。

アカウント台帳の仕様について、以下に示します。出力内容は随時更新いたします。

環境種別	レポート内容（抜粋）
Azure	クラウド保護＞STEP1 に登録した Microsoft Entra ID テナント上のアカウントの表示名、ユーザープリンシパル名、メールアドレス、ユーザーの種類（メンバー／ゲスト）、招待の状態、アカウント作成日時 等
AWS	クラウド保護＞STEP1 に登録した AWS アカウント上のユーザーアカウント一覧、ARN、MFA 有無、アカウント作成日時 等
Google Cloud	クラウド保護＞STEP1 に登録した Google Cloud プロジェクト上のアカウントのタイプ（サービスアカウント／ユーザー）、プリンシパル、ロール 等

6.3. リソース一覧の作成

ポータルに登録した環境におけるリソース一覧を出力します。複数のポータルを利用している際も、自分が権限を持つポータルのみ、作成します。

[AWS 環境の登録]から登録した AWS 環境からのリソース取得には事前作業が必要となります。手順はサービスポータルやユーザーマニュアルを参照ください。

取得可能なリソースタイプに制限がありますが、それぞれ取得元の Azure、AWS、Google Cloud の仕様に準じます。

項目	仕様
取得元	①Azure：Azure ポータル＞[すべてのリソース]から取得 ②AWS：AWS Resource Explorer＞[リソースの検索]から取得 ③Google Cloud：[IAM と管理]＞[アセットインベントリ]内の[リソース]から取得
取得条件	①Azure：クラウド保護＞STEP2 の独自ポリシーにチェックを入れていること ②AWS：AWS リソース取得の事前作業を実施し、Resource Explorer が有効化されていること ③Google Cloud：とくになし

7. その他のサービス仕様

7.1. サービスポータル機能

以降の項目では、これまで紹介していないサービスポータルの機能について記載します。

メニュー	機能
お知らせ	ご案内（お知らせ）やメンテナンス情報などの提示
ポータル管理者設定	・サービスポータルの管理者の作成 ・ポータル管理者とポータルの紐づけ変更
お問い合わせ/ マニュアル	・サービス仕様に関するお問い合わせ ・修復対応や準拠対応に関するお問い合わせ ・サービスに関する改善要望、苦情の受付 ・サービスのマニュアルを提供

7.1.1. サービスポータルのログイン

サービスポータルへのログインについて、以下に示します。

項目	仕様
接続 URL	すべてのお客様共通の URL となります。 https://monolith.service-now.com/cp_portal
ログイン	ID、PW および MFA を一律で強制適用 ※ID/PW のみでのログイン不可
PW	Welcome メールに記載。初回ログイン時に変更を強制
PW 要件	・最小 8 文字、最大 40 文字 ・少なくとも 1 文字の小文字 ・少なくとも 1 文字の大文字 ・少なくとも 1 文字の数字
MFA 対応アプリ	スマートフォン用のアプリである Microsoft Authenticator を利用 App Store や Google Play から入手可能

7.2. サービスポータルのお知らせ

サービスポータルのトップページでは、以下内容をお客様に伝えるため、お知らせ機能を利用いたします。

①サービスの機能やポータル内容の更新

②メンテナンス予定

③障害や不具合

7.3. サービスポータルの管理者設定

お客様がご利用するサービスポータルの管理者について、以下に示します。

項目	仕様
上限	上限なし。お客様にて無制限でポータル内で作成可能
権限	設定変更を含む、ポータルにおけるすべての操作が可能
管理者とポータルの紐づけ変更	不要となったユーザーのポータルへのログイン権限をはく奪します

7.4. サービスポータルからのお問い合わせ

本項目では、問い合わせに関するサービス内容について説明しています。

7.4.1. サービスに関するお問い合わせ対応

サービスポータルでは、サービスに関連したお問い合わせ対応をしております。

項目	条件
受付時間	24 時間 365 日
サポート範囲	・サービス仕様に関するお問い合わせ ・修復や準拠対応に関するお問い合わせ
サポート範囲外	・サービス内容と関連がないお問い合わせ ・環境に依存した設定変更時の影響や手順に関するお問い合わせ ・現在構築不可のレガシーリソースの手順に関するお問い合わせ ・弊社側で再現や確認ができない事象や手順のお問い合わせ
受付方法	サービスポータルからの受付
回答方法	生成 AI による即時回答
お問い合わせ回数上限	なし

7.4.2. 生成 AI について

サービスポータルからのお問い合わせは、生成 AI による対応となります。本サービスについては予告なく変更する場合がございます。予めご了承ください。

項目	仕様
サービス名称	DocsBot AI
サービス提供企業	UglyRobot, LLC
サービスの仕組み	本サービスの仕様書、紹介資料やマニュアル等を学習したプライベートなチャットボットがユーザーからの質問に回答
API 連携	Open AI
Open AI モデル	GPT-4.1 mini
入力したデータの利用	入力されたデータは本サービスの改善のみに利用し、外部には共有されない。ただし、Open AI の API キーを使用しているため、Open AI が提供する API にデータが渡され、Open AI のシステム上に一時的に保存される場合がある
DocsBot AI の SLA	規定なし
入力したデータの保管場所	米国
データ保管の準拠法	EU-U.S.プライバシーシールドフレームワークおよびスイス-米国プライバシーシールドフレームワークに従い、ヨーロッパ連合およびスイスから米国に転送された個人情報の収集、使用、および保有に関する米国商務省の規定に準拠
利用規約	DocsBot AI - 利用規約
プライバシーポリシー	DocsBot AI - Privacy Policy

お問い合わせ履歴は適宜当社で確認し、学習データを追加することで回答内容の改善をいたします。入力いただいた内容は、本サービスの改善以外で利用することはありませんが、上記仕様および以下ご了承いただけることをご利用の前提条件といたします。

・AI で生成されているため、誤りを含む可能性があります
・お客様の機密情報や個人情報を入力しないでください
・生成 AI サービスや Open AI 社の仕様変更により、本サービス仕様も影響を受ける可能性があります

7.4.3. サービスに関する追加問い合わせ

サービスについて追加のお問い合わせやご要望について、サービスポータルに窓口をご

用意しております。

・生成 AI で適切な回答が得られなかった、その他ご要望
・追加のポータルを発行してほしい
・その他改善してほしいこと、苦情

7.5. サービス監視

本項目では、サービス監視の内容について説明しています。

本サービスではシステムおよびサービスの稼働状態について監視は行いません。サービスの稼働状態や提供機能に異常が認められた場合、異常を確認した時点でサービスポータルの「お知らせ」に発生した事象について記載いたします。

なお、サービスポータル自体に障害が発生した場合は、「お知らせ」の更新が遅れる、またはお客様がポータルにログインできない時間が発生する可能性があるため、その際は、サービス申込時にご連絡頂いている契約者様のメールアドレスにご連絡いたします。

サービスの稼働状態や提供機能の異常は以下の場合を指します。

・サービスポータルの障害や各種通知機能の利用不可
・サービステナントの障害による緊急リスクの検知や対策不可
・上記以外の、サービス仕様書に記載の本サービス機能の提供不可

サービス仕様書に記載の本サービス機能以外の異常については障害とはみなしません。

・お客様クラウド環境の障害による監視不可
・お客様環境の回線障害によるポータル閲覧不可

8. 解約について

8.1. 解約時の対応について

解約する際は、契約窓口に解約連絡をお願いします。お客様のクラウド環境をご利用前の状態に戻すための手順についてはユーザーマニュアルをご参照ください。

契約を解約する際の規定については「クラウドパトロール　サービス利用約款」もあわせてご確認ください。

項目	内容
解約連絡	契約窓口に解約連絡をお願いします。 無料トライアル期間を経過した際は、ご利用環境は弊社にて停止するため、解約連絡は不要です。 クラウドパトロール契約窓口 Mail：cloudpatrol-offer@tech.softbank.co.jp

9. 注意事項

9.1. 障害時の影響について

本サービスはお客様環境のパブリッククラウドと API 連携し、当社の Azure サービステナントを活用して監視を行うものです。

お客様のパブリッククラウド、Microsoft Defender for Cloud（有償機能利用時）、サービステナントおよびサービスポータルの障害時にはサービスをご提供することができません。

9.2. その他

・本サービスはお客様環境で発生する全てのセキュリティインシデントに対する検知、抑制を保証するものではありません。
・本サービスは緊急リスクの認知を中心としたサービスのため、すべてのリスクの通知や抑制は提供範囲外となります。
・本サービスはセキュリティインシデントに関する防御を保証するものではありません。
・本サービスは対象製品である Microsoft Defender for Cloud の完全な動作を保証するものではありません。
・本サービスの対象製品である Microsoft Defender for Cloud とお客様が所有する他製品との問題切り分けは含まれません。
・本サービスはサービステナントによる即時対策機能の完全な動作を保証するものではありません。障害発生時は、当社営業時間内で復旧対応を実施します。
・当社独自の監視ルールによる即時対策(NSG の変更、仮想マシンの停止)の動作により、お客様業務等へ影響を及ぼす可能性があります。貴社システムへの即時対策の有効化是非は当社では判断いたしかねます。まずは即時通知で運用したうえで、即時対策を適用してもシステムや業務上問題ないか、貴社にてご判断ください。
・本サービスには対象製品の仕様に関するお問い合わせは含まれておりません。
・本サービスの全部または一部を当社外部へ再委託する場合があります。

10. 契約に関する連絡窓口

本サービスにおける連絡窓口は以下の通りです。サービス仕様や不具合に関するお問い合わせ、改善要望や苦情は、サービスポータルからお願いいたします。

10.1. 当社サービスの契約・解約に関する連絡窓口

メールアドレス	cloudpatrol-offer@tech.softbank.co.jp
メールアドレス表示名	クラウドパトロール申込
受付内容	・契約、解約、支払いに関する相談 ・サービスポータルに初回ログインができない ・ログインできていたサービスポータルにログインできない

お問い合わせの際は以下の内容をお伝えください。

・企業名
・お名前
・内容の詳細

11. 情報セキュリティ順守事項

SBテクノロジー株式会社（以下、SBT）ではISMS認証(JIS Q 27001)、およびプライバシーマーク認証(JIS Q 15001)を取得しております。お客様にソリューションやサービスを安心してご利用いただくため、SBT全ての従業員は、以下の方針に従って、情報の適切な取り扱い、管理、保護、維持に努めていくものとします。

■情報セキュリティポリシー
https://www.softbanktech.co.jp/security/

■個人情報保護方針
https://www.softbanktech.co.jp/privacy/privacy01/