JBS

マネージドセキュリティサービス

サービス仕様書

Ver 4.0 | 2022.11.18

Japan Business Systems, Inc.

【改訂履歴】

版	改訂日	改訂者	改訂内容
1.0		JBS	初版作成
1.1	2020/05/01	JBS	章構成、文言修正
2.0	2021/02/09	JBS	名称変更、章構成、文言修正
3.0	2022/03/01	JBS	章構成、文言修正
4.0	2022/11/18	JBS	下記の 5 文書の内容を本文書に統一 ・マネージドセキュリティサービス Azure Active Directory Identity Protection_サービス仕様書 ・マネージドセキュリティサービス Microsoft Defender for Cloud Apps_サービス仕様書 ・マネージドセキュリティサービス Microsoft Defender for Endpoint_サービス仕様書 ・マネージドセキュリティサービス Microsoft Defender for Identity_サービス仕様書 ・マネージドセキュリティサービス Microsoft Defender for Office 365_サービス仕様書

【目次】

1. はじめに

1.1. 本書の目的

本サービス仕様書は日本ビジネスシステムズ株式会社(以下、「当社」とする)が以下のサービスを提供するにあたってのサービス仕様を記載するものとなります。

- マネージドセキュリティサービス Microsoft Defender for Endpoint
- マネージドセキュリティサービス Microsoft Defender for Office 365
- マネージドセキュリティサービス Microsoft Defender for Cloud Apps
- マネージドセキュリティサービス Microsoft Defender for Identity
- マネージドセキュリティサービス Azure Active Directory Identity Protection

本仕様書の内容はサービス内容の更新等により、追加・変更されることがあります。

2. サービス提供概要

本サービスは、お客さま環境の Microsoft 365 E5 Security を利用して提供する、セキュリティ監視運用サービスです。

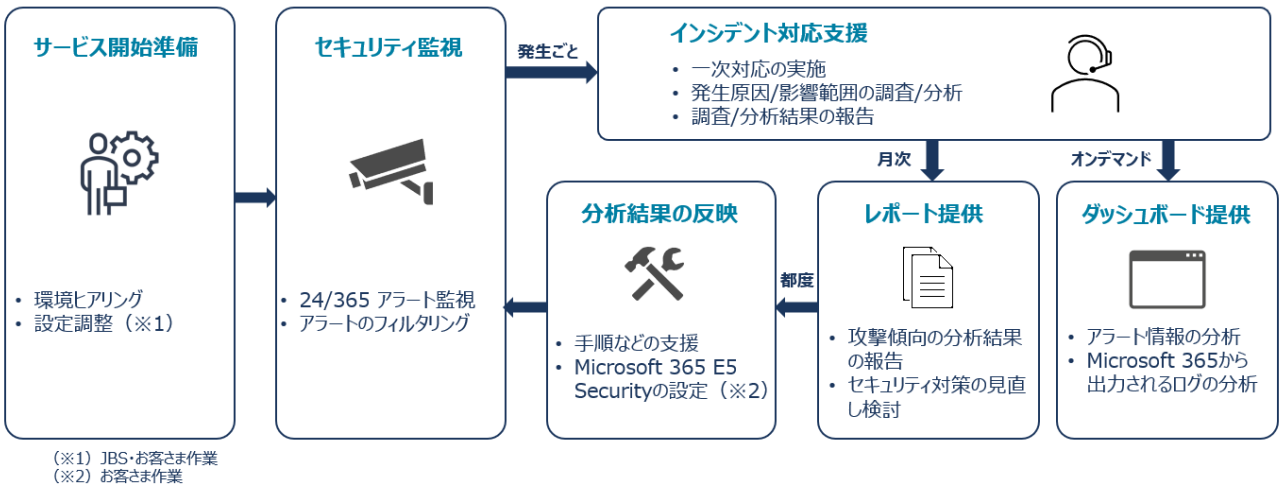
2.1. サービス提供対象製品

当社が本サービスの提供対象とする製品は以下とします。

- Microsoft Corporation 製 「Microsoft Defender for Endpoint」（以下、「MDE」とする）
- Microsoft Corporation 製 「Microsoft Defender for Office 365」（以下、「MDO」とする）
- Microsoft Corporation 製 「Microsoft Defender for Cloud Apps」（以下、「MDA」とする）
- Microsoft Corporation 製 「Microsoft Defender for Identity」（以下、「MDI」とする）
- Microsoft Corporation 製 「Azure Active Directory Identity Protection」（以下、「IdP」とする）

2.2. サービス提供イメージ図

サービス提供のイメージ図です。



（※1）JBS・お客さま作業
（※2）お客さま作業

2.3. サービス提供言語

本サービスは、電話・メール・ドキュメントに関して、日本語での提供とします。

2.4. インシデント管理

当社はお客さまに対しインシデント管理システム（OpsRamp）を用意し、以下の機能を提供します。
なお、インシデントに関する連絡事項のすべてのやり取りは、インシデント管理システム上で行うものとします。

機能	説明
インシデント管理	インシデントチケットを生成し、インシデント内容の詳細や対応状況を更新し、生成および更新時に関係者に対してメールで通知します。
問い合わせ管理	製品機能・仕様やアラート抑止に対する問い合わせについてインシデントチケットを作成していただき、内容の詳細や対応状況を更新し、作成および更新時に関係者に対してメールで通知します。

3. サービス前提条件

当社が本サービスをお客さまへ提供する上で、必要となる前提条件を以下に示します。

3.1. サービス前提条件（全製品共通）

当社が本サービスをお客さまへ提供する上で、必要となる前提条件は下表の通りです。
本項は、全ての製品に共通する条件となります。

条件	内容
Azure AD のアプリ登録	当社環境から次の操作を実施するために、お客さま環境の Azure AD 上に、アプリケーションの登録が必要となります。 ■操作 • Microsoft 365 E5 Security 製品が生成するアラート情報の取得 • Advanced Hunting の実施（MDE） • ネットワーク遮断および、フルスキャンの実施（MDE） • パスワード変更の要求（IdP） • ユーザのメールアドレス・表示名の取得（IdP）
Azure サブスクリプション	後述の Microsoft Sentinel を利用するため、お客さま環境の Azure AD と紐づいた Azure サブスクリプションが必要となります。
Microsoft Sentinel	脅威情報の分析・可視化のため、お客さま環境の Azure AD と紐づいた Microsoft Sentinel が必要となります。
Azure Lighthouse	上記 Microsoft Sentinel の操作・運用のため、当社環境の Azure への権限委任を Azure Lighthouse 機能により実行します。
Azure AD B2B	当社環境からお客さま環境の Microsoft 365 E5 Security 管理画面へアクセスするために、当社が指定するユーザをお客さま環境の Azure AD にゲストユーザとして登録していただきます。 また、Microsoft 365 E5 Security の各製品ポータルおよび、Microsoft 365 Defender へのアクセスやアラート調査等に必要な権限を付与いただく必要がございます。
作業場所	本サービスはオフサイトでの提供となります。 そのため、当社のサービス担当者がお客さま環境の Microsoft 365 E5 Security の各製品ポータルおよび、Microsoft 365 Defender へアクセスするために、本サービスで指定するグローバル IP からアクセスできるよう許可していただきます。
製品の正常性	本サービスは各製品の動作状態が正常であることを前提に提供します。 Microsoft Corporation の提供する各製品、またインシデント管理に使用する「OpsRamp」の動作状態が正常でない場合、本サービスの提供状況にも不具合が

条件	内容
	生じる場合があります。

3.2. サービス前提条件（Microsoft Defender for Endpoint）

本サービスにて MDE を対応範囲とする場合に、必要となる前提条件は下表の通りです。

条件	内容
クライアント PC の OS・バージョン	次の OS・バージョンのクライアント PC を利用されているものとします。 • Windows 10 バージョン 1607 以降 • Windows 11 上記以外の OS・バージョンの場合は MDE の仕様により、機能に制限がありますが、本サービスの対象とするかは別途相談の上、対応いたします。
ライセンス	Windows 10 Enterprise E5 もしくは、Microsoft Defender for Endpoint Plan2 が含まれているライセンスおよび、単体ライセンスの契約が必要となります。
クライアント PC へのソフトウェアインストール	対象のクライアント PC に MDE が展開（オンボーディング）されているものとします。
クライアント PC の通信要件	対象のクライアント PC は MDE と通信できる必要があります。
MDE と連携するアンチウィルスソフト	基本的には Microsoft Defender Antivirus を利用しているものとします。 ※他のアンチウィルスソフトを利用している場合は、MDE の機能が制限されます

3.3. サービス前提条件（Microsoft Defender for Office 365）

本サービスにて MDO を対応範囲とする場合に、必要となる前提条件は下表の通りです。

条件	内容
ライセンス	サービス利用人数分の Microsoft Defender for Office 365 Plan2 が含まれるライセンスの契約が必要となります。
監視するポリシーのカテゴリ	次のカテゴリのポリシーのみ監視対象とします。 • 脅威の管理 • アクセス許可
Exchange Online 機能の有効化	Exchange Online の監査ログ機能が有効化済み、または有効化に同意済みである必要があります。
Exchange Online Protection の展開	Exchange Online Protection が既に展開済みである必要があります。
メールフィルタリング製品との連携	Exchange Online Protection 以外のメールフィルタリング製品と連携されている場合は、MDO の動作に制限が掛かる可能性があるため、本サービス内容についても制限が掛かる可能性があります。

3.4. サービス前提条件（Microsoft Defender for Cloud Apps）

本サービスにて MDA を対応範囲とする場合に、必要となる前提条件は下表の通りです。

条件	内容
ライセンス	サービス利用人数分の Microsoft Defender for Cloud Apps が含まれるライセンスの契約が必要となります。
監視するポリシーのカテゴリ	次のカテゴリのポリシーのみ監視対象とします。 • Cloud Discovery • 共有制御 • 脅威検出
監視するサービス（接続アプリ）	Office 365、Microsoft Azure のみ監視するものとします。

3.5. サービス前提条件（Microsoft Defender for Identity）

本サービスにて MDI を対応範囲とする場合に、必要となる前提条件は下表の通りです。

条件	内容
ライセンス	サービス利用人数分の Microsoft Defender for Identity が含まれるライセンスの契約が必要となります。
Agent（センサー）のインストール	全てのオンプレミス Active Directory サーバに MDI の Agent（センサー）がインストールされている必要があります。
Microsoft Defender for Cloud Apps との連携	当社環境より、MDI からアラート情報を定期的に取得するために、お客さま環境 Microsoft Defender for Cloud Apps ポータル上で MDI データ統合が有効になっている必要があります。

3.6. サービス前提条件（Azure AD Identity Protection）

本サービスにて IdP を対応範囲とする場合に、必要となる前提条件は下表の通りです。

条件	内容
ライセンス	サービス利用人数分の Azure Active Directory Plan 2 が含まれるライセンスの契約が必要となります。
機能の有効化（※）	次の機能が有効および設定されている必要がございます。 • 保護対象ユーザの Azure Multi-Factor-Authentication (MFA) • 保護対象ユーザの SSPR（セルフパスワードリセット）機能 • Azure AD パスワードライトバック

（※）機能の有効化および設定が行えない場合は、別途サービス内容を相談の上、対応させていただきます。

4. サービス提供準備事項

本サービスを提供するにあたり、必要な準備事項を以下に示します。

4.1. 準備事項（全製品共通）

本サービスをお客さまへ提供するにあたり、必要となる準備事項は下表の通りです。

項目	内容	担当
管理者アカウント登録（※1）	当社が指定するユーザをお客さま環境の Azure AD にゲストユーザとして登録していただきます。 また、Microsoft 365 E5 Security 管理画面へのアクセスやアラートの調査等に必要な権限を付与いただきます。	お客さま
グローバル IP アドレスのアクセス許可	当社からお客さま環境にアクセスするために、条件付きアクセス等でアクセスを制御している場合は、本サービスで利用するグローバル IP アドレスを登録します。	お客さま
CSP 新規契約（※2）	Direct CSP Azure サービス（お客さまの既存テナントに Azure サブスクリプションを追加）を新規に契約します	お客さま・当社
Azure リソースグループの権限委任（※3）	Microsoft Sentinel の操作・運用のため、本サービスが保持しているテナントの Azure AD セキュリティグループに対して、Azure Lighthouse を設定していただき、当社環境の Azure テナントへ権限を委任していただきます。	お客さま・当社
Microsoft Sentinel の構築（※2）	本サービスで利用する Microsoft Sentinel を構築します。	当社
Azure AD のアプリ登録	アラート・サインイン情報の取得、およびネットワーク遮断・フルスキャンなどの操作を当社の仕組みから実行するために、Azure AD のアプリ登録を実施します。	お客さま
独自システムの構築	次の動作をする独自システムを当社環境上に構築します。 • Microsoft 365 E5 Security 製品が生成するアラート情報の取得 • Advanced Hunting の実施（MDE） • ネットワーク遮断および、フルスキャンの実施（MDE） • パスワード変更の要求（IdP） • ユーザのメールアドレス・表示名の取得（IdP）	当社
インシデント管理システム(OpsRamp)	インシデントを管理するために必要なアカウント登録と設定を行います。	当社
担当者の連絡先提供	インシデント発生時のご担当者さまの連絡先を当社にご提供していただきます。当社はお客さまからご提供いただいた担当者情報を「セキュリティ監視仕様書」の「2. 連絡体制」に記載します。	お客さま

（※1）お客さま環境のポリシー上、ゲストユーザへの権限付与が困難な場合は、お客さま環境の Azure AD に本サービス用のユーザを作成していただき、本サービスを提供するにあたり必要な権限を付与していただきます。
（※2）お客さまの Azure AD と紐づいた Microsoft Sentinel が存在しない、または新規に Microsoft Sentinel を構築する場合に限ります。
（※3）お客さま環境のポリシー上、ゲストユーザへの権限付与が困難な場合は、この項目は対応不要となります。

4.2. 準備事項（Microsoft Defender for Endpoint）

本サービスにて MDE を対応範囲とする場合に必要となる準備事項は下表の通りです。

項目	内容	担当
ライセンスの割り当て	エンドユーザに Windows 10 Enterprise E5 もしくは、Microsoft Defender for Endpoint Plan2 の単体、および含まれているライセンスを割り当てます。	お客さま
MDE の導入	お客さま環境に MDE を導入し、設定します。	お客さま
MDE の展開	対象のクライアント PC に MDE を展開（オンボーディング）します。	お客さま

4.3. 準備事項（Microsoft Defender for Office 365）

本サービスにて MDO を対応範囲とする場合に必要となる準備事項は下表の通りです。

項目	内容	担当
ライセンスの割り当て	エンドユーザに Microsoft Defender for Office 365 Plan2 ライセンスを割り当てます。	お客さま
MDO の導入	お客さま環境に MDO を導入し、設定します。	お客さま
Exchange Online 機能の有効化	Exchange Online の監査ログ機能を有効化、または有効化に同意します。	お客さま
Exchange Online Protection の展開	Exchange Online Protection を展開します。	お客さま
監視対象ポリシーの有効化	本サービスで監視する対象ポリシーを有効化します。	当社

4.4. 準備事項（Microsoft Defender for Cloud Apps）

本サービスにて MDA を対応範囲とする場合に必要となる準備事項は下表の通りです。

項目	内容	担当
ライセンスの割り当て	エンドユーザに Enterprise Mobility + Security E5 または Microsoft 365 E5 ライセンスを割り当てます。	お客さま
Microsoft Defender for Cloud Apps の導入	お客さま環境に Microsoft Defender for Cloud Apps を導入し、設定します。	お客さま
監視対象ポリシーの有効化	本サービスで監視する対象ポリシーを有効化します。	当社

4.5. 準備事項（Microsoft Defender for Identity）

本サービスにて MDI を対応範囲とする場合に必要となる準備事項は下表の通りです。

項目	内容	担当
ライセンスの割り当て	エンドユーザに Enterprise Mobility + Security E5 または Microsoft 365 E5 ライセンスを割り当てます。	お客さま
Microsoft Defender for Cloud Apps の導入	お客さま環境に Microsoft Defender for Cloud Apps を導入し、設定します。	お客さま
MDI の導入	お客さま環境に MDI を導入し、設定します。	お客さま
Agent（センサー）のインストール	全てのオンプレミス Active Directory サーバに MDI の Agent（センサー）をインストールします。	お客さま
Microsoft Defender for Cloud Apps と MDI の連携	Microsoft Defender for Cloud Apps と MDI を連携します。	お客さま

4.6. 準備事項（Azure AD Identity Protection）

本サービスにて IdP を対応範囲とする場合に必要となる準備事項は下表の通りです。

項目	内容	担当
ライセンスの割り当て	エンドユーザに Azure Active Directory Plan 2 が含まれているラインセンスを割り当てます。	お客さま
IdP の導入	お客さま環境に IdP を導入し、設定します。	お客さま
ユーザーリスクポリシーの作成	IdP により資格情報が漏洩した可能性が高いと判断されたユーザに対して、自動でパスワード変更を要求するように設定します。	お客さま

5. サービス内容

本サービスのメニュー及び内容について本項に記載します。
本サービスは本項に記載のある内容となり、記載の無い内容はサービス範囲外となります。

5.1. サービスメニュー・提供時間

本サービスのメニューと提供時間は下表の通りです。

分類	項目	サービス内容	対応時間
標準	セキュリティ監視	アラート監視、通知	24 時間 365 日
	インシデント対応支援	調査結果報告・一次対応・問い合わせ対応	9:00～17:30 (土日祝日・当社指定の休日を除く)
	再発防止・対策支援	月次アドバイザリレポート提供	
		ダッシュボード提供	
	ログ分析	アクティビティの監視・通知	24 時間 365 日
		脅威分析・通知	
オプション	月次報告会	月次報告会の開催	9:00～17:30 (土日祝日・当社指定の休日を除く)

5.2. セキュリティ監視

本サービスは、対応範囲内のセキュリティアラートを監視します。
また、一定以上の基準のアラートはインシデントとして管理・通知を実施します。

項目	内容	通知タイミング
監視対象	本サービスが監視を行うアラート全て	月次
インシデント対象	監視対象アラートの中でも早急な対応が求められるアラート	即時

インシデント通知メールに記載されている内容については下表の通りです。

項目	内容
チケット番号	インシデント単位で当社が発行する管理番号
重大度	当該インシデントの重大度
アラート件名	アラートの件名

5.2.1. セキュリティ監視（Microsoft Defender for Endpoint）

本サービスにて MDE を対応範囲とする場合、以下の項目を事前協議し、監視対象とインシデント対象を決定します。
決定した事項は「セキュリティ監視仕様書」の「4.サービスごとの監視基準」に記載し管理します。

項目	内容
デバイスグループ	監視対象とするデバイスグループを定義します。 当該デバイスグループ内のデバイスから発せられたすべてのアラートが監視対象となります。
アラートレベル	インシデント対象とするアラートの重大度を定義します。

5.2.2. セキュリティ監視（Microsoft Defender for Office 365）

本サービスにて MDO を対応範囲とする場合、以下の項目を事前協議し、監視対象とインシデント対象を決定します。
なお、監視対象及びインシデント対象は「3.2.サービスの前提条件」に記載されている「監視するポリシーのカテゴリ」に該当するポリシー内に限定します。
決定した事項は「セキュリティ監視仕様書」の「4.サービスごとの監視基準」に記載し管理します。

項目	内容
アラートポリシー	監視対象、インシデント対象とするアラートポリシーを定義します。

5.2.3. セキュリティ監視（Microsoft Defender for Cloud Apps）

本サービスにて MDA を対応範囲とする場合、以下の項目を事前協議し、監視対象とインシデント対象を決定します。
なお、監視対象及びインシデント対象は「3.2.サービスの前提条件」に記載されている「監視するポリシーのカテゴリ」に該当するポリシー内に限定します。
決定した事項は「セキュリティ監視仕様書」の「4.サービスごとの監視基準」に記載し管理します。

項目	内容
アラートポリシー	監視対象、インシデント対象とするアラートポリシーを定義します。

5.2.4. セキュリティ監視（Microsoft Defender for Identity）

本サービスにて MDI を対応範囲とする場合、MDI から発せられる全てのセキュリティアラートを監視し、インシデントとして通知します。セキュリティアラートの他に正常性アラートも発せられますが、そちらは監視・通知の対象外となります。

項目	内容
セキュリティアラート	Microsoft Defender for Identity によって検出された、攻撃の兆候を示すアラートです。 Microsoft Defender for Identity はオンプレミスの Active Directory シグナルを監視し、組織を対象とする高度な脅威、侵害された ID、および悪意のあるインサイダーによるアクションを検出します。
正常性アラート	Microsoft Defender for Identity インスタンスがどのように実行されているかを把握し、問題が発生した際に発報されるアラートです。

5.2.5. セキュリティ監視（Azure AD Identity Protection）

本サービスにて IdP を対応範囲とする場合、IdP から発せられる全てのセキュリティアラート（サインインリスク）を監視します。また、以下の項目を事前協議し、監視対象とインシデント対象を決定します。
決定した事項は「セキュリティ監視仕様書」の「4.サービスごとの監視基準」に記載し管理します。

項目	内容
アラート（リスク）レベル	インシデント対象とするアラートの重大度を定義します。

5.3. インシデント対応支援

本サービスのメニュー「インシデント対応支援」の内容を以下に示します。

5.3.1. 調査結果報告

インシデント（「5.2.セキュリティ監視」に記載の「インシデント対象」に該当するアラート）発生時に、当社が早急な対応が必要と判断した場合、当該インシデントの対応支援として、対応範囲内の製品機能を利用してインシデントの原因・経緯・影響などを調査します。
調査した結果はインシデント管理システムを通じてお客さまの担当者に報告します。
調査時の報告内容は下表の通りです。

項目	内容
ユーザ名	当該インシデントのユーザ名
インシデント内容	当該インシデントの内容
関連検知情報	当該インシデントに関連する情報
対応推奨事項	当該インシデントに対して、本サービスがお客さまに推奨する対応事項

5.3.2. 一次対応

インシデント発生時に当該インシデントの対応支援として、対応範囲内の製品機能を利用した一次対応を実施いたします。
製品毎の対応内容を以下に示します。

5.3.2.1. 一次対応（Microsoft Defender for Endpoint）

インシデントの対応支援として、MDE の機能を利用して下表の対応を実施します。

項目	内容
対象クライアント PC のネットワーク遮断・フルスキャン（※）	当社の独自システム、もしくは MDE の管理コンソールより、対象のクライアント PC をネットワークから論理的に切り離し、フルスキャンを実施します。

（※）OS の種類および MDE の仕様により、ネットワーク遮断・フルスキャンは実施できない場合がございます。

（※）対象クライアント PC のネットワーク遮断の解除は、次の場合に実施します。

- お客さまの担当者からの解除依頼があった場合
- 当社による調査で脅威がなくなったと判断した場合

5.3.2.2. 一次対応（Microsoft Defender for Office 365）

インシデントの対応支援として、MDO の機能を利用して下表の対応を実施します。

項目	内容
自動調査結果の承認	自動調査機能（※）の対象であるアラートを検知した場合に、修復作業の承認を当社がお客さまの代わりに実施します。

（※）MDO がメールボックスの状態や関連する設定を自動で調査し、実行すべき修復作業を提案する機能です。

承認処理を明示的に行うことにより、MDO が提案する修復作業（メールの論理削除等）が実施されます。

5.3.2.3. 一次対応（Microsoft Defender for Cloud Apps）

MDA の機能を利用した一次対応は、本サービスの内容には含まれません。

5.3.2.4. 一次対応（Microsoft Defender for Identity）

MDI の機能を利用した一次対応は、本サービスの内容には含まれません。

5.3.2.5. 一次対応（Azure AD Identity Protection）

インシデントの対応支援として、IdP の機能を利用して下表の対応を実施します。

項目	内容
パスワード変更の要求	対象ユーザのリスクレベルを high（高）に変更し、IdP の機能（ユーザリスクポリシー）により、パスワード変更を要求します。

5.3.3. 問い合わせ対応

対応範囲内の製品仕様やアラート対応に対する不明点など、お客さまから問い合わせを頂いた場合に調査・回答します。調査に要する時間と回答内容は一定の品質を保証するものではなく、ベストエフォートの対応となります。
問い合わせの分類を下表に記します。

項目	説明	一次回答までの目安
一般問い合わせ	本サービスや対象製品の機能・仕様、インシデント対応での不明点相談など	3 営業日以内
業務影響が生じている問い合わせ	製品の不具合等により業務影響が生じている事象に関する問い合わせ	平日の 17:00 までに受け付けたものは当日中、平日の 17:00 以降や土日祝日に受け付けたものは翌営業日以内

5.4. 再発防止・対策支援

本サービスのメニュー「再発防止・対策支援」の内容を以下に示します。

5.4.1. 月次アドバイザリレポート提供

対象期間を月末締めとし、翌月 10 営業日までを目安にレポート（報告書）を作成し、お客さまに提供いたします。
レポートに記載する内容は次の通りとなります。

- アラート監視の結果総評
- 検知アラート数
- インシデントの発生状況
- 各種ログのグラフ化
- お客さまのセキュリティ運用維持・改善のための提案

※分析結果に応じて、内容が異なる場合がございます

5.4.2. ダッシュボード提供

お客さま環境の Azure AD と紐づいた Microsoft Sentinel の「ブック」機能を利用し、組織内のアラートの発生状況等を表示するダッシュボードを提供します。
お客さまはポータルに変更を加えることはできませんが、ダッシュボードには基本的にいつでもアクセス・閲覧が可能です。

ダッシュボードに表示される項目は下表の通りです。

項目	内容	情報更新タイミング
OpsRamp インシデント情報	インシデント管理システム「OpsRamp」にて管理しているインシデントの数、オープン中のインシデントへのリンク	随時
アラート情報	対象製品のアラート数	随時
分析情報（MDE）	MDE アラートログを分析した情報	随時
分析情報（MDO）	Microsoft 365 Defender から取得可能な MDO に関連するログを集計・分析した情報	毎週日曜日
分析情報（MDA）	Office 365 アクテビティログを分析した情報	随時
分析情報（MDI）	Microsoft 365 Defender から取得可能な MDI に関連するログを集計・分析した情報	毎週日曜日
分析情報（IdP）	IdP アラートログ、AAD サインインログを分析した情報	随時

5.5. ログ分析

本サービスのメニュー「ログ分析」の内容を本項に示します。
本メニューは、Microsoft Sentinel に格納された下表のログを用いて「アクティビティの監視・通知」と「脅威分析・通知」を行います。

ログカテゴリ	対象製品	ログの内容
サインイン・監査イベント	Azure Active Directory	・Azure AD のサインインイベント ・ユーザやグループの管理操作など、監査対象となるイベント
メールイベント	Microsoft Defender for Office 365	・メール添付ファイルに関する情報 ・メールアイテム毎の詳細情報 ・メールボックス到達後の動作情報 ・メールに含まれた URL に関する情報

5.5.1. アクティビティの監視・通知

設定変更などの管理者が把握することが望ましいアクティビティを監視するために当社が作成したルールを用いて「5.5. ログ分析」に示した対象のログを監視し、一定期間内に記録されたアクティビティのリストを定期的に通知します。

5.5.2. 脅威分析・通知

「5.5. ログ分析」に示した対象のログから、脅威に繋がる異常なアクティビティがないかを分析し、脅威が発見された場合にお客さまに通知します。
脅威分析のため、お客さま環境の Azure AD と紐づいた Microsoft Sentinel 内に「分析ルール」を作成、有効化します。

5.6. 月次報告会

本サービス利用申込時に実施有無を選択いただくオプションメニューです。
本サービスの対象となる製品が検知したアラートについて、当社のアナリストが月次アドバイザリレポートの内容を基にオンサイトもしくは、リモート会議にて月次報告会を実施します。

※1 回あたり最大 2 時間を想定しています。
※遠地へのオンサイトの場合は、旅費・交通費を実費請求いたします。

6. 契約

本サービスの契約に関する諸事項を記載します。

6.1. 利用期間

本サービスの利用期間は、利用開始日からの 1 年間です。
利用契約の終了日の 45 日前までに、当社またはお客さまから相手方に対して利用契約を更新しない旨を通知しなかった場合は、本サービスの利用契約は更に当該利用契約と同一の期間かつ同条件で更新されるものとし、以後も同様とします。

6.2. 最短利用期間

本サービスの最短利用期間は 1 年間です。

6.3. 契約変更

以下の変更が発生する場合、当社に変更連絡をしていただく必要があります。
変更がある旨をご連絡いただき、当社指定の変更申込書をご記入の上送付ください。

- お客さま情報（企業情報・責任者・副担当者）の変更
- ご利用ユーザ数・台数の変更
- 対象製品の変更（追加・削除）

なお、本契約変更に伴い増額・減額される利用料金は、契約変更の成立した日の属する月の翌月から発生し、日割り計算はされないものとします。

6.4. 解約

本サービスの解約をご希望の場合は、利用終了予定日の 45 日以上前に、解約申込書によって当社に通知ください。なお、解約に伴い、サービス利用のために施した各設定の解除作業が必要となります。当社及びお客さまは、設定解除作業に必要な協力を行うものとします。
設定解除作業の主な内容を下表に記します。

項目	内容	担当
Azure AD アカウントの削除	当社からのアクセス用に貸与・招待いただいた Azure AD アカウントを削除・無効化します。	お客さま
OpsRamp アカウントの削除	お客さま宛に発行した OpsRamp アカウントを削除します。	当社
Azure AD アプリの削除	API 利用のために発行いただいた Azure AD アプリを削除します。	お客さま
JBS 内アラート監視システムの無効化	お客さま環境のアラートを監視し OpsRamp へ連携するシステムを停止します。	当社
分析ルールの無効化	Microsoft Sentinel に設定した分析ルールを無効化します。	当社
ブックの削除	Microsoft Sentinel に作成したブック（ダッシュボード）を削除します。	当社
Azure Lighthouse の解除	Microsoft Sentinel 閲覧・操作のための権限委任設定を解除します。	お客さま

6.5. サービス仕様変更

本サービスの仕様変更に関わる事項は、別紙「JBS サービス基本規約」の「第 18 条（サービス変更）」に記載の内容に従事します。
JBS サービス基本規約は下記 URL を参照ください。
https://www.jbs.co.jp/termsandconditions

6.6. サービスの提供中断

本サービスの提供中断に関わる事項は、別紙「JBS サービス基本規約」の「第 17 条（サービスの提供中断）」に記載の内容に従事します。
JBS サービス基本規約は下記 URL を参照ください。
https://www.jbs.co.jp/termsandconditions

7. サービス範囲外の作業

以下に該当する作業は、本契約に基づくサービスの範囲外となります。

- 対象製品の死活監視・正常性監視
- 本サービス内で提供するもの以外のドキュメント更新作業