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

Ver 3.0 | 2022.3.1

JBS 日本ビジネスシステムズ株式会社

【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	2021/03/01	JBS	名称変更、章構成、文言修正 *アドバンスサービス見直し
3.0	2022/03/01	JBS	章構成、文言修正

【目次】

1. はじめに

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」という)が「マネージドセキュリティサービス Microsoft Defender for Office 365」のサービス(以下、「サービス」という)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。

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、当社が提供する Microsoft Defender for Office 365 を対象とした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 Office 365」(以下、「MDO」とする)

2.2. サービスの前提条件

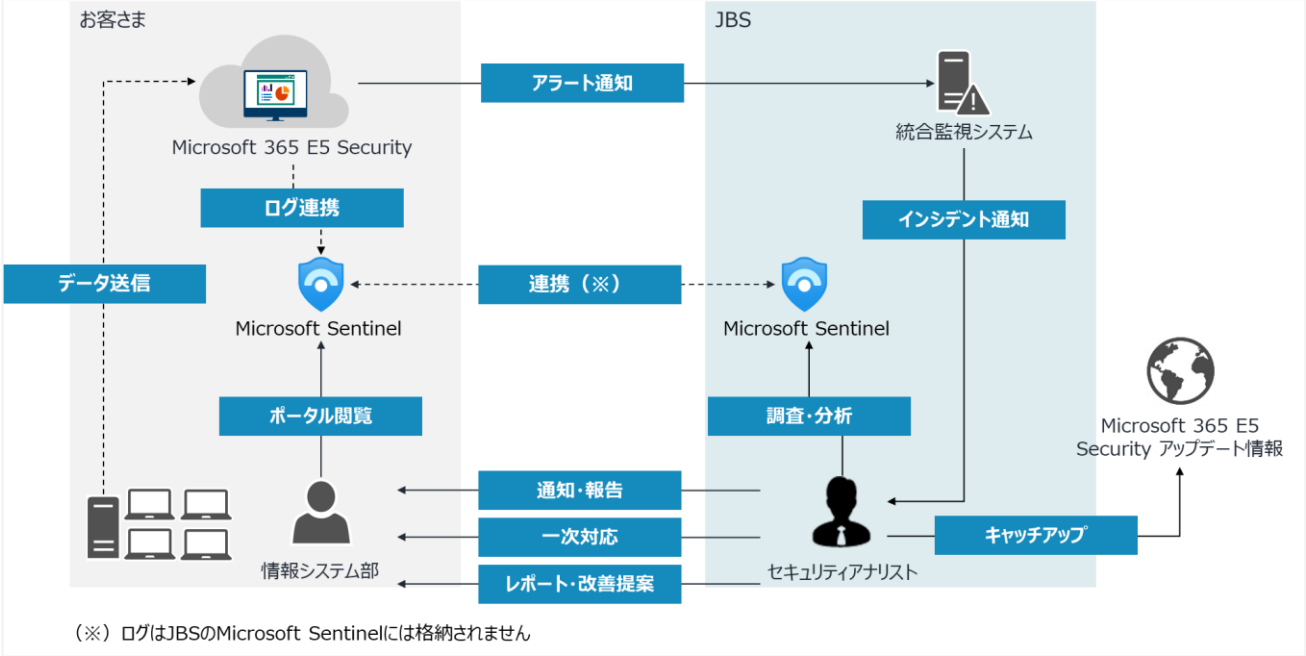
当社が本サービスをお客様へ提供するうえで、必要となる前提条件は下表の通りです。

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サービス利用人数分、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
インシデント管理	インシデントのやり取りは、インシデント管理システム（OpsRamp）にて対応となります。
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。
Microsoft Sentinel	脅威情報の分析・可視化のため、お客様環境の 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	当社環境からお客様環境の MDO 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様環境の Azure AD にゲストユーザとして登録していただきます。

条件	内容
	また、MDO 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様環境の MDO 管理画面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。

2.3. 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。



2.4. 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。

2.5. インシデント管理システム（OpsRamp）

当社はお客様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. サービス提供条件

3.1. サービス提供準備項目

本サービスを提供するにあたり、必要な準備項目は下表の通りです。

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。	お客様
MDO の導入	お客様環境に MDO を導入し、設定します。	お客様
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。	お客様
Exchange Online Protection の展開	Exchange Online Protection を展開します。	お客様
管理者アカウント登録（※1）	当社が指定するユーザをお客様環境の Azure AD にゲストユーザとして登録していただきます。 また、MDO 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。	お客様
グローバル IP アドレスの登録	当社からお客様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。	お客様
CSP 新規契約（※2）	Direct CSP Azure サービス（お客様の既存テナントに Azure サブスクリプションを追加）を新規に契約します	お客様・当社
Azure サブスクリプションへの権限委任（※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。	お客様・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	当社の仕組みで Microsoft Defender for Cloud Apps のアラート情報を取得するために、Azure AD のアプリ登録を実施します。	お客様
独自システムの構築	お客様環境の MDO からアラート情報を当社に定期的に取得するために、当社環境上に独自システムを構築します。	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

（※1）お客様環境のポリシー上、ゲストユーザへの権限付与が困難な場合は、お客様環境の 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）お客様でご契約中の Microsoft Sentinel を持っていない、または新規に Microsoft Sentinel を構築する場合に限ります

（※3）お客様環境のポリシー上、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

3.2. 担当者情報の登録

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。当社はお客様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。

電話連絡の場合は、優先度の高い方からご連絡します。
メールでのご連絡は、ご登録いただいたすべての通知先に同報で送付するものとします。

4. サービス内容

本サービスのサービス項目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。

4.1. サービスプラン

4.1.1. シングルプラン

シングルプランは、当社が提供するマネージドセキュリティサービスシリーズの 5 つのうち、1 つをご契約していただくお客様向けのプランとなります。

4.1.2. マルチプラン

マルチプランは、当社が提供するマネージドセキュリティサービスシリーズの 5 つのうち、複数をご契約していただくお客様向けのプランとなります。

4.2. 標準サービス

4.2.1. サービス提供時間

4.2.1.1. シングルプラン

シングルプランの標準サービス提供時間は下表の通りです。

サービス項目	サービス内容	対応時間
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	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	月次レポート・改善提案、ポータル提供	
ログを活用した脅威分析	Security Alert ログ、Office Activity ログの分析	

4.2.1.2. マルチプラン

マルチプランの標準サービス提供時間は下表の通りです。

サービス項目	サービス内容	対応時間
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	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	月次レポート・改善提案、ポータル提供	
ログを活用した脅威分析	Security Alert ログ、Office Activity ログ、Azure AD Sign-in ログ、Azure AD Audit ログの分析	

4.2.2. セキュリティ監視サービス

4.2.2.1. アラート監視

検知される（監視する）アラートについては、お客様と監視対象ポリシーを決定し、「セキュリティ監視仕様書」の「4. サービスごとの監視基準」に記載されたポリシーに関連するものとします。

なお、「2.2 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が監視対象となります。

4.2.2.2. アラート通知

アラート検知時に下表の通知レベル・判断基準に従い、インシデント管理システム（OpsRamp）からメールにて通知するものとします。

通知レベル	判断基準
即時通知	組織に対して大きな影響があり、早急な対応が必要となるアラート ＜通知アラート　例＞ ・潜在的に悪意のある URL のクリックが検出された ・電子情報開示検索の開始またはエクスポート ・メッセージが遅延しています ・配信後に検出されたマルウェア活動 ・ユーザが電子メールの送信を制限されている ・疑わしい電子メール送信パターンが検出された ・電子メールの異常な増加はフィッシングとして報告された
月次報告にて通知	即時性はないが、組織的に検討する必要があると想定されるアラート ＜通知アラート　例＞

通知レベル	判断基準
	・転送/リダイレクトルールの作成 ・マルウェアの活動が検出され、ブロックされた

アラート通知の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レベル
アラート件名	アラートの件名

4.2.3. インシデント対応支援サービス

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、MDO 機能を利用して下表の対応を実施します。

対応	内容
インシデント調査	インシデントの原因・経緯・結果等を MDO 機能の範囲で調査・報告します。
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様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。
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）が実施される。

インシデント調査の結果はインシデント管理システムにて、お客様の担当者に報告いたします。
報告内容は下表の通りとなります。

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、本サービスがお客様に推奨する対応事項

4.2.4. 再発防止・対策支援

4.2.4.1. 月次レポート・改善提案

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、お客様に提供いたします。
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
- お客様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

4.2.4.2. ポータル提供

お客様環境の Azure AD と紐づいた Microsoft Sentinel に、組織内のアラートの発生状況等を表示するポータル機能を提供いたします。
お客様はポータルに変更を加えることはできませんが、ポータルには基本的にいつでもアクセス・閲覧が可能です。

4.2.5. ログを活用した脅威分析

4.2.5.1. シングルプラン

インシデント発生時に Microsoft Sentinel に格納されているログの分析による脅威の調査を行います。
Microsoft Sentinel に格納するログは下表の通りとなります。

ログの種類	内容
Microsoft Defender for Office 365 の Security Alert	Microsoft Defender for Office 365 が検知したアラート情報
Office 365 Activity	Office 365 上でのアクティビティ情報

4.2.5.2. マルチプラン

インシデント発生時に Microsoft Sentinel に格納されているログの分析による脅威の調査を行います。

また、Microsoft Sentinel に格納されているログを相関的に分析し、製品だけでは検知できない潜在的な脅威を検知します。

Microsoft Sentinel に格納するログは下表の通りとなります。

ログの種類	内容
Microsoft Defender for Office 365 の Security Alert	Microsoft Defender for Office 365 が検知したアラート情報
Office 365 Activity	Office 365 上でのアクティビティ情報
Azure Active Directory ・ SigninLog ・ AuditLog	Azure Active Directory に記録されているサインインと監査に関する情報

4.3. オプションサービス

標準サービスをご契約中のみ、オプションサービスをご契約いただくことができます。標準サービスを解約すると、オプションサービスも解約となります。

4.3.1. サービス提供時間

オプションサービスの提供時間は以下の通りとします。

提供時間：月～金 9:00-17:30　（土日祝日・当社指定の休日を除く）

4.3.2. 月次報告会

当社は本サービスの対象となる Microsoft Defender for Office 365 が検知したアラートについて、当社のアナリストが月次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