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

Ver 2.0 | 2021.3.23

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	2021/03/23	滝瀬	名称変更、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 Identity」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。
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 Identity を対象としたセキュリティ監視運用サービスです。

2.1. サービス提供対象商品

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 Identity」(以下、「MSDI」という)

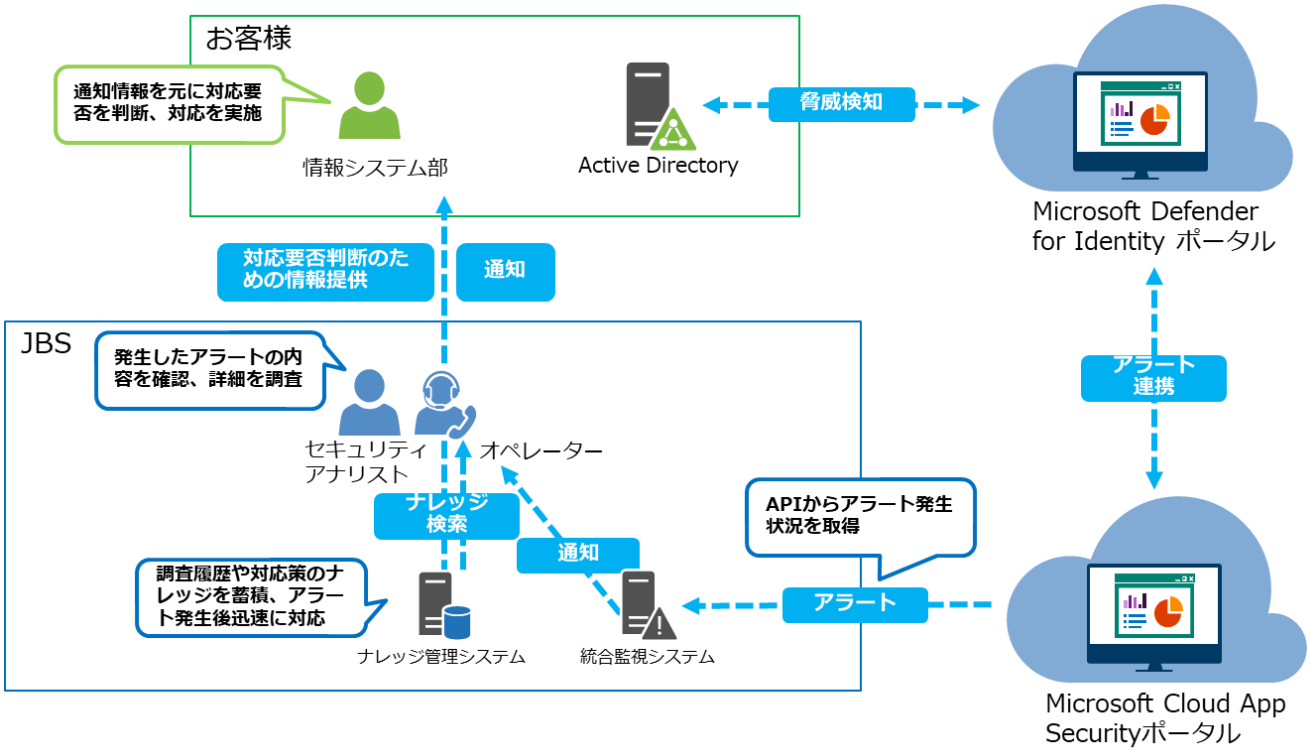
2.2. サービスの前提条件

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以下の通りです。

条件	内容
ライセンス	Enterprise Mobility + Security E5 または Microsoft 365 E5 の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。
監視するサービス	オンプレミス Active Directory を管理する MSDI のメッセージのみ監視するものとします。
管理者アカウント	当社からお客様環境の MSDI 管理画面にアクセスおよび、以下の操作が可能なユーザをご提供いただきます。 ・アラート確認 ・調査に必要な操作
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。
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 MSDI 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。
その他連携など	● 当社環境より、MSDI のアラート情報を定期的に取得する為に、お客様環境の Azure AD 上に、アプリケーションの登録が必要となります。 ● 当社環境より、MSDI のアラート情報を定期的に取得する為に、お客様環境の MSDI と Microsoft Cloud App Security が連携されている必要があります。

2.3. サービス提供イメージ図

サービス提供は以下のフローで実施されます。



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. 問い合わせ用ページ(OpsRamp)

当社はお客様に対し OpsRamp 上の問い合わせ用ページを用意し、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問い合わせ用ページ経由で行うものとします。

メニュー	機能
インシデント管理	インシデントの詳細や対応状況の管理
Q&A	よくあるご質問の提示

3. サービス提供要件

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、必要な準備項目は以下の通りです。

準備項目	内容	担当
ヒアリング	以下の項目を確認します。 ● 監視内容 ● 運用内容 ● 連絡先情報	お客様・当社
管理者アカウント登録	当社が利用する管理者アカウントを Azure AD 上に登録します。	お客様
Azure AD のアプリ登録	当社の仕組みで MSDI 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 MSDI 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

3.2. 担当者情報の登録

お客様は、インシデントの発生を検知した場合の担当者の連絡先を当社にご提供いただきます。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　連絡基準」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. 標準サービス

4.1.1. サービス提供時間

標準サービスの提供時間は以下の通りとします。

対応時間	サービス項目
24 時間 365 日	セキュリティ監視
9:00～17:30 (祝祭日・当社年末年始休日を除く)	一次対応支援

4.1.2. セキュリティ監視サービス

当社は、MSDI の機能を利用し、MSDI で検知されるアラートについて、インシデント登録後、以下の方法で通知を行います。

- 監視システム(OpsRamp)による自動メール通知
- お客様担当者へメール通知(必要に応じて電話)

MSDI で検知するアラートの危険度レベルを以下の基準で判断し、通知方法はすべてメールにて行います。

アラート通知の定義

危険度レベル	アラート項目	通知方法
High(高)	・SMB を介したデータ流出 ・データ保護 API マスター キーの悪意のある要求 ・DCShadow 攻撃の可能性 (ドメイン コントローラーの昇格) ・DCShadow 攻撃の可能性 (ドメイン コントローラーのレプリケーション要求) ・DCSync 攻撃の可能性 (ディレクトリ サービスのレプリケーション) ・ゴールデン チケット使用の可能性 (偽造認証データ) ・ゴールデン チケット使用の可能性 (存在しないアカウント) ・ゴールデン チケット使用の可能性 (チケットの異常)	即時通知 (メール)

危険度レベル	アラート項目	通知方法
	・ゴールデン チケット使用の可能性 (時間の異常) ・システムアラート	
Medium(中)	・アカウント列挙攻撃による偵察 ・ハニートークン アクティビティ ・ネットワーク マッピングの偵察 (DNS) ・リモート コード実行の試行 ・DNS 上のリモート コード実行 ・セキュリティ プリンシパルによる偵察 (LDAP) ・ブルートフォース攻撃の可能性 (SMB・LDAP) ・ゴールデン チケット使用の可能性 (暗号化のダウングレード) ・over-pass-the-hash 攻撃の可能性 (暗号化のダウングレード) ・overpass-the-hash 攻撃の可能性 (Kerberos) ・スケルトン キー攻撃の可能性 (暗号化のダウングレード) ・Metasploit ハッキング フレームワークの使用の可能性 ・WannaCry ランサムウェア攻撃の可能性 ・DNS を介した疑わしい通信 ・機密性の高いグループへの疑わしい追加 ・悪意のあるサービスの作成 ・疑わしい VPN 接続 ・ユーザとグループ メンバーシップの偵察 (SAMR) ・ユーザと IP アドレスの偵察 (SMB)	
Information(低)	・その他	

通知内容

通知タイミング	項目	内容
初報	インシデント判定日時	当社にてインシデントが発生したと判断した日時
	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
	危険度	当該インシデントの危険度レベル
	アラート件名	アラートの概要

4.1.3. インシデント対応支援サービス

インシデント発生時に、当社が緊急で処理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象製品の機能を利用し、一次対応を実施します。

インシデント対応支援

種類	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 MSDI 機能の範囲で調査・報告します。

インシデント調査報告の通知内容

通知タイミング	項目	内容
一次報告 （調査結果報告）	インシデント内容	当該インシデントの内容
	調査結果内容	アラートの詳細情報
	対応推奨事項	対応の観点でお客様にて実施を推奨する事項
	関連検知情報	当該インシデントに関連する情報がある場合のみ記載

4.1.4. ポリシー設定支援（定期）

当社はお客様より依頼された内容や、お客様環境での監視結果を考慮したポリシー設定のアドバイスおよび改善提案を行います。ポリシー設定支援（定期）では、月 1 回、1 ポリシーまでの設定変更を実施します。複数件の対応が必要な場合は、アドバンスドサービスでの対応となります。

4.1.5. レポーティングサービス

レポーティングサービスでは、監視結果総評、検知アラート、インシデント発生状況、各種ログをグラフ化した情報を月次報告書としてご提供します。原則、レポート対象期間は月末締めとし、翌月 10 営業日までを目安に作成します。

4.2. 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。

4.2.1. 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 (祝祭日・弊社年末年始休日を除く)

4.2.2. 報告会

当社は本サービスの対象となる MSDI で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。
※遠地の場合はお客様当社協議の上、リモート対応で報告会を行います。現地訪問を伴う場合は、旅費・交通費を実費請求いたします。

4.2.3. アドバンスドサービス

アドバンスドサービスは、都度見積もりとさせていただきます。

- ポリシー設定支援

当社はお客様より依頼された内容や、お客様の監視結果を考慮したポリシー設定のアドバイスおよび改善提案を行います。その利用料金は本契約の委託料と別に都度請求となります。