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

Ver 3.0 | 2021.3.1

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
2.0	2020/7/31	JBS	章構成、文言修正
3.0	2021/03/01	滝瀬	名称変更、章構成、文言修正 *アドバンスサービス見直し

【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 Azure Active Directory Identity Protection」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 Azure Active Directory Identity Protection 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・機能は以下とします。

Microsoft Corporation 製 「Azure Active Directory」（以下、「Azure AD」とする）製品の「Identity Protection」（以下、「IdP」とする）機能

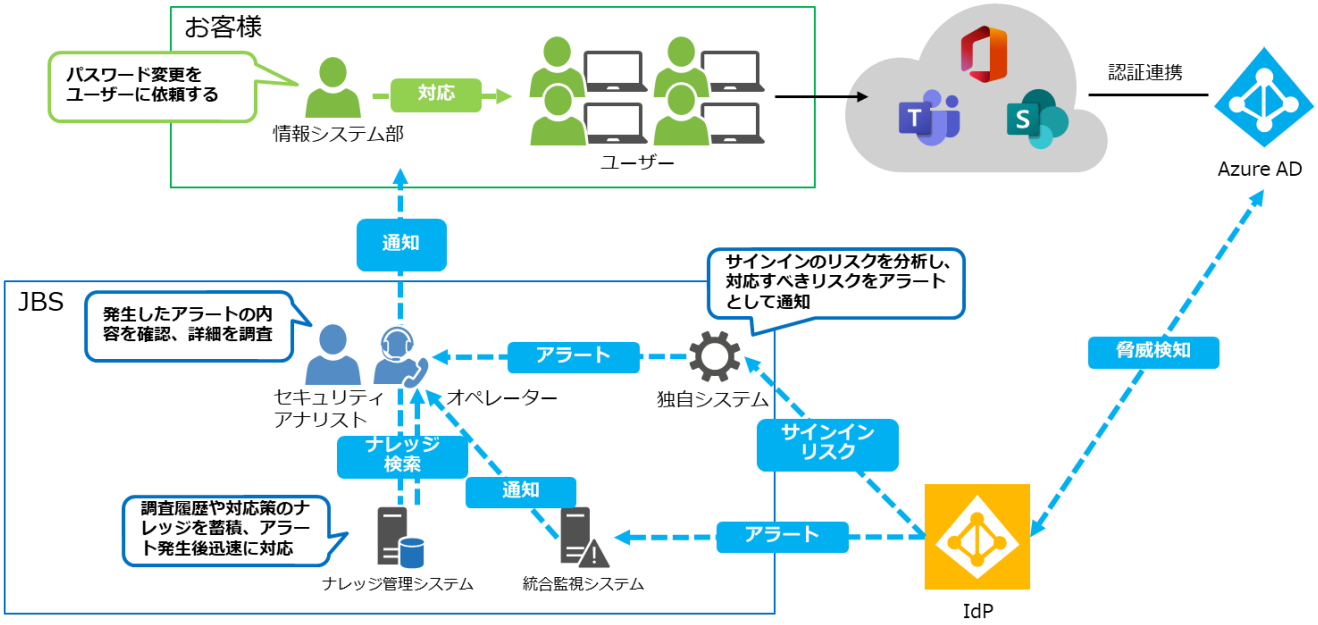
2.2. サービスの前提条件

当社が本サービスをお客様へ提供する上で、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	本サービスを対象とする Azure AD のユーザ人数分の IdP が含まれるライセンスの契約が必要となります。
管理者アカウント	当社からお客様環境の IdP 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 ・ユーザリスクの「ユーザに対するセキュリティ侵害を確認」の実行 ・調査に必要な操作
機能の有効化	・サービス利用ユーザに Azure Multi-Factor-Authentication (MFA) の設定が必要となります。 ・保護対象ユーザで SSPR (セルフパスワードリセット)機能が有効化されている必要があります。 ・Azure AD パスワードライトバックが有効化されている必要があります。 ・当社環境より、IdP から利用者のサインイン情報を定期的に取得する為に、お客様環境の Azure AD 上で、アプリケーションの登録が必要となります。
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。

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、必要な準備項目を以下に示します。

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 IdP のアラート・サインイン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
ユーザ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。	お客様
独自システムの構築	お客様環境の IdP からアラート・サインイン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、IdP の機能を利用し、IdP で検知されるアラートについて、サインインレベルおよび、サインイン状態に応じ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)

IdP 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、通知方法は危険度レベルによるものとします。

アラート通知の定義

サインイン危険度 レベル(IdP)	サインイン 状態	当社 危険度レベル	アラート項目	通知方法
High(高)	成功	High	・漏洩した資格情報 資格情報の漏洩など、危険な状態のユーザがサインインをした場合に検知される。 危険度が高く、早急な対応が必要。	即時通知 (メール)
	中断・失敗			
Medium(中)	成功	Normal	・匿名の IP アドレスからのサインイン	

サインイン危険度レベル(IdP)	サインイン状態	当社危険度レベル	アラート項目	通知方法
Medium(中)			・特殊な場所へのあり得ない移動 ・不審なアクティビティのある IP アドレスからのサインイン ・未知の場所からのサインイン 情報漏洩はしていないが、サインインの状態に危険が含まれていると判断された場合に検知される。 緊急ではないが、危険度は高いため、状態監視が必要。	
	中断・失敗	-		月次報告で通知
Information(低)	成功	–	・感染しているデバイスからのサインイン 既にマルウェアに感染している、ボットサーバーとの通信が頻繁に行われている等のデバイスからサインインした場合に検知される。 危険度は低いが、状態監視が必要。	
	中断・失敗	–		

通知内容

通知タイミング	項目	内容
初報	インシデント検知日時	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当社危険度レベル
	アラート件名	アラートの概要
	サインイン情報	ユーザ名、接続元 IP アドレスなどの情報
	パスワード変更要求	対象ユーザにパスワード変更が要求された旨

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。

支援内容

項目	内容
パスワード変更の要求	対象ユーザの危険度レベルを High(高)に変更し、IdP の機能により、パスワード変更を要求します。

インシデント対応支援通知内容

通知タイミング	項目	内容
月次報告	パスワード変更対象者	パスワード変更を要求されたユーザ
	パスワード変更実施の有無	対象ユーザがパスワード変更を実施したかの結果

4.1.4. 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、パスワード変更の対象者と実施結果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・当社年末年始休日を除く)

4.2.2. 報告会

本サービスの対象となる IdP 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。