



Microsoft Security Forum 2020

B2: セキュリティ エコシステム時代のマネージド サービス パートナーの選び方

Microsoft 365 セキュリティと Azure Sentinel
を活用した最新事例の紹介

2020/3/12

JBS Japan Business Systems, Inc.

Agenda

■ 会社概要

- ・ 日本ビジネスシステムズ株式会社
- ・ OUR BUSINESS

■ 事例紹介

- ・ 東洋エンジニアリング株式会社 様 ①
- ・ 東洋エンジニアリング株式会社 様 ②
- ・ 全体構成
- ・ Sentinel 活用紹介 (頻発アラートの調査用ブック①)
- ・ Sentinel 活用紹介 (頻発アラートの調査用ブック②)
- ・ Sentinel 活用紹介 (ハンティングのアラート通知)

■ JBS ソリューション紹介

- ・ JBS マネージドセキュリティサービス
- ・ 今後の取り組み



日本ビジネスシステムズ株式会社
事業企画本部 MS 統合サポートセンター
エキスパート
秋葉 俊明

会社概要



会社概要：日本ビジネスシステムズ株式会社



売上高推移



640 億円

拠点数



国内

海外

6 拠点 / 5 拠点

社員数



2,250 人

MCP 取得 / 認定者数 (延べ)



1,163 人

社員研修講座数



168 講座

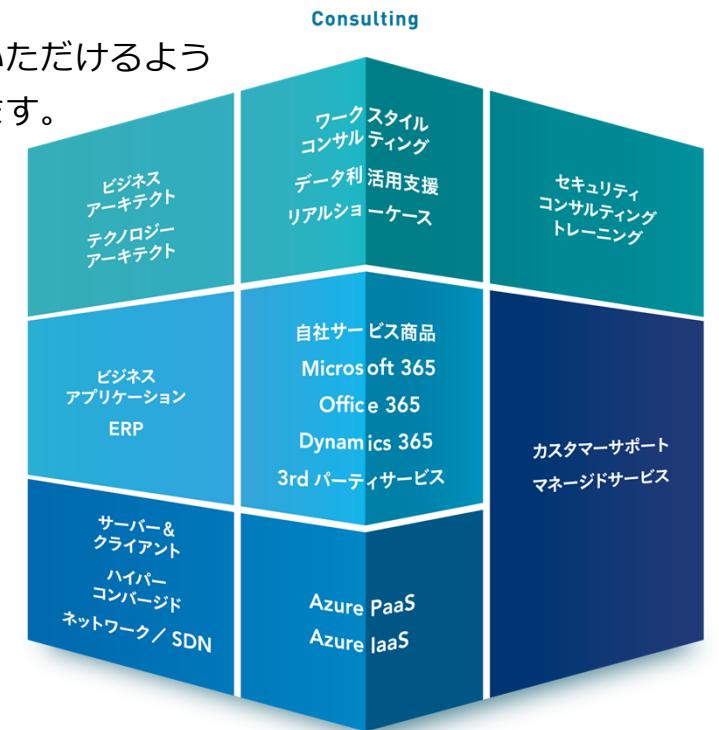
会社概要：OUR BUSINESS

JBS は、Licensing Solution Partner (LSP)、Cloud Service Provider (CSP)、FastTrack Partner および Microsoft Partner の立場で、マイクロソフトの各種ライセンス及びソリューションを導入・活用いただけけるよう販売・計画からサポートまで一連の導入支援サービスを提供しています。



Japan Business Systems, Inc.

Copyright © Japan Business Systems, Inc.



Application and Infrastructure

Microsoft

Microsoft

DIGITAL TRUST SECURITY

Alliance

Operation and maintenance

事例紹介



事例紹介：東洋エンジニアリング株式会社 様 ①



東洋エンジニアリング株式会社 様

業種：プラントエンジニアリング



選定製品

Microsoft 365 セキュリティ

(Office 365 Advanced Threat Protection、Microsoft Cloud App Security、Azure Information Protection)

+ **Azure Sentinel**

+ **JBS マネージドセキュリティサービス**

事例紹介：東洋エンジニアリング株式会社様 ②

1

背景

2

ソリューション

- ・標的型攻撃など、セキュリティ対策に危機感
- ・脅威可視化アセスメントによる現状分析
- ・Office 365 上のアクティビティに関するセキュリティ課題への対応

- ・将来的に Microsoft Office 製品で作られたデータもセキュリティ対象となる為、Office 製品との親和性を期待し Microsoft 365 セキュリティ製品を選定

3

導入効果

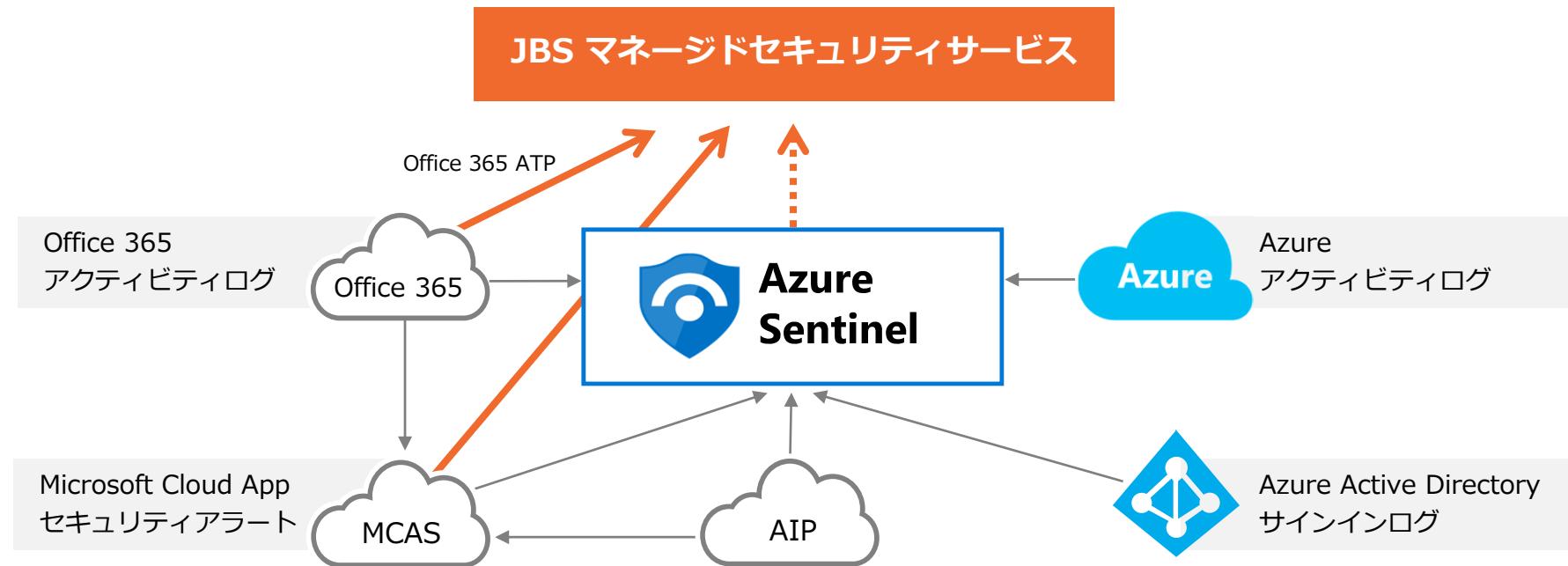
パートナー選定ポイント

- ・なりすまし、フィッシング等を可視化可能に
- ・不審な Office 365 アクティビティを捕捉可能に
- ・パスワードを使わずにファイルを暗号化
- ・社内に専門のセキュリティチームを配置しなくて良い

- ・Microsoft 365 セキュリティ製品を確実に導入できるベンダーとして選定
- ・運用も同時に提供できるベンダーが決定ポイント

事例紹介：全体構成

Microsoft 365 セキュリティ の導入と共に、マネージドセキュリティサービスをご採用、さらに Azure Sentinel との連携を図る。



事例紹介：Sentinel 活用紹介（頻発アラートの調査用ブック①）

指定期間内で、選択したアカウントのアラート・アクティビティを表示

SharePoint等で、短時間に1ユーザーが大量のファイルダウンロード

検索期間: 過去 28 日

•[tkensyo@ onmicrosoft.com] がトリガーしたMCASのその他アラート

TenantId	↑↓ TimeGenerated	↑↓ DisplayName	↑↓ AlertName	↑↓ AlertSeverity	↑↓ Description
aaaaaaaa-1337-4702-baef-baef00000000	2020/2/20 20:36:09	Logon from a risky IP address	Logon from a risky IP address	High	Activity policy 'Logon from a risky IP address'
aaaaaaaa-1337-4702-baef-baef00000000	2020/2/20 20:27:19	Logon from a risky IP address	Logon from a risky IP address	High	Activity policy 'Logon from a risky IP address'

•[tkensyo@tanakamas3.onmicrosoft.com] がトリガーしたMCAS以外 (MDATP/AATP/IDP) のアラート

アラートはありません

•[tkensyo@ onmicrosoft.com] が社外のIPアドレスでトリガーしたアラート

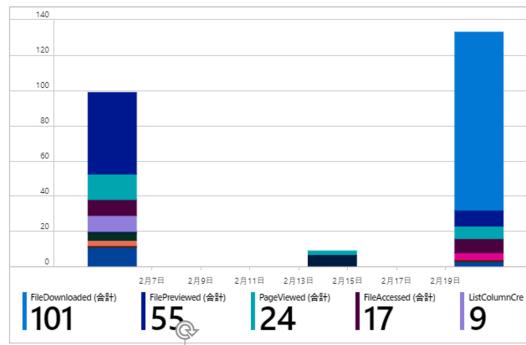
TenantId	↑↓ TimeGenerated	↑↓ DisplayName	↑↓ AlertName	↑↓ AlertSeverity	↑↓ Description
aaaaaaaa-1337-4702-baef-baef00000000	2020/2/20 20:36:09	Logon from a risky IP address	Logon from a risky IP address	High	Activity policy 'Logon from a risky IP address'

事例紹介 : Sentinel 活用紹介 (頻発アラートの調査用ブック②)

通常と異なる O365アクティビティを視覚的に判断

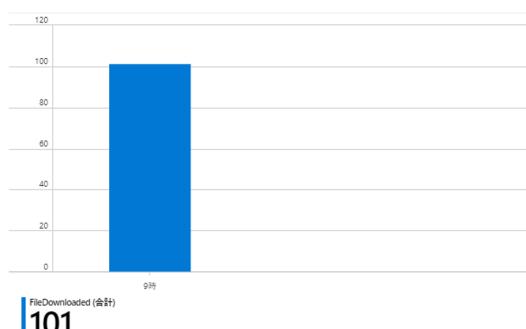
● Office 365 アクティビティ一覧・グラフ (日単位)

TimeGenerated	Operation	OfficeWorkload	OfficeObjectId
2020/2/20 22:24:13	FileAccessed	SharePoint	https://tanakam...
2020/2/20 16:04:38	PagePrefetched	SharePoint	https://tanakam...
2020/2/20 16:04:37	PagePrefetched	SharePoint	https://tanakam...
2020/2/20 16:04:36	PageViewed	SharePoint	https://tanakam...
2020/2/20 16:04:36	PageViewed	SharePoint	https://tanakam...
2020/2/20 16:04:35	FileAccessed	SharePoint	https://tanakam...
2020/2/20 16:04:35	FileAccessed	SharePoint	https://tanakam...
2020/2/20 16:04:34	PageViewed	SharePoint	https://tanakam...
2020/2/20 16:04:05	FileAccessed	SharePoint	https://tanakam...
2020/2/20 16:04:00	FileAccessed	SharePoint	https://tanakam...
2020/2/20 14:25:55	ListUpdated	SharePoint	https://tanakam...



● Office 365 ダウンロードアクティビティ一覧・グラフ (日単位)

ceObjectId
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test1.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test2.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test76.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test73.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test75.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test77.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test7.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test68.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test69.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test70.xlsx
s://sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test63.xlsx



- アラート時にダウンロードされたファイル一覧
- 普段使われない IP アドレス・デバイス操作をハンティング

● ハンティングクエリ

• SharePointFileOperation via previously unseen IPs

-アラート発生アカウントで直前14日間で使用されなかったIPアドレスによるSharePointファイル操作の検出

ClientIP	StartTimeUtc	EndTimeUtc	recentCount	timestamp
10.0.0.100	2020/3/9 9:35:59	2020/3/9 9:36:07	59	2020/3/9 9:35:59

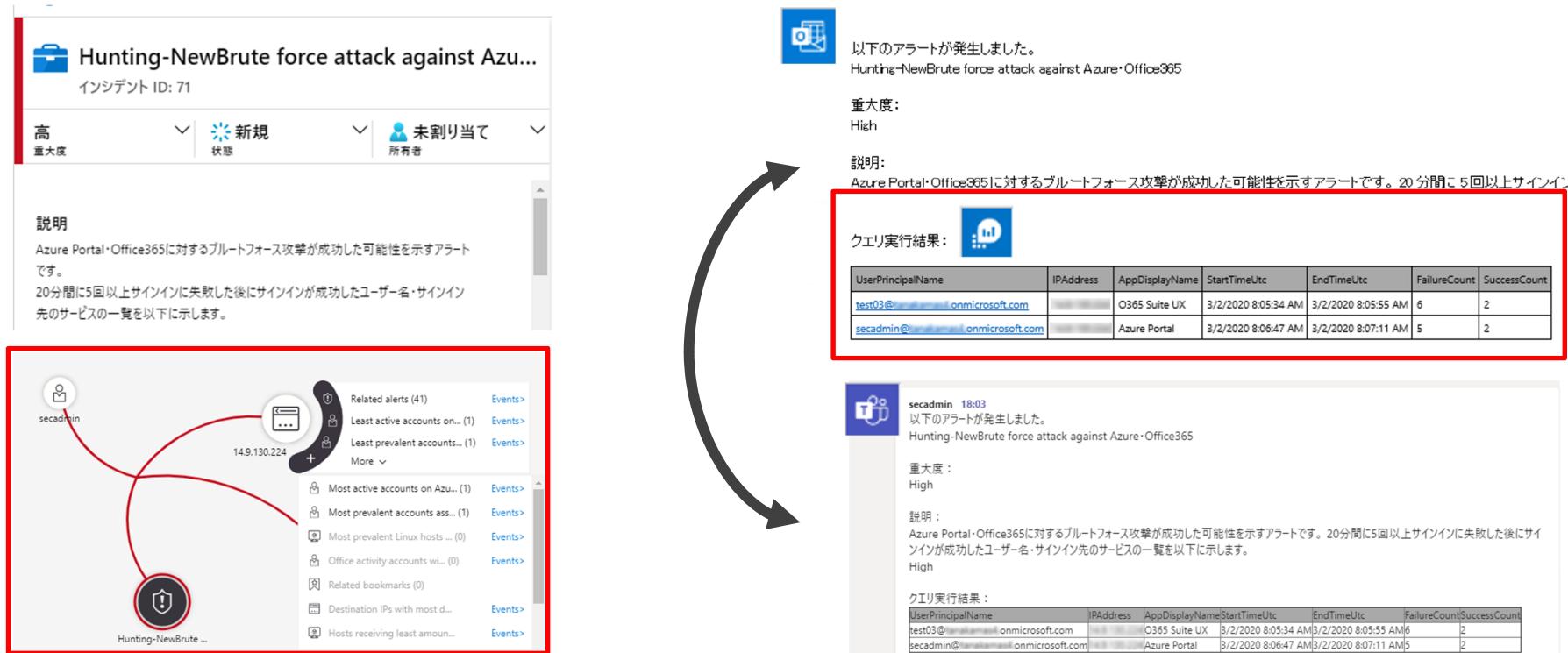
• SharePointFileOperation via devices with previously unseen user agents

-アラート発生アカウントで直前14日間で使用されなかったユーザーエージェントによるSharePointファイル操作

UserAgent	RecordType	StartTimeUtc	EndTimeUtc
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/...	SharePointFileOperation	2020/3/9 9:34:51	

事例紹介：Sentinel 活用紹介（ハンティングのアラート通知）

Sentinel ならではの高度な検出（例：ブルートフォース攻撃）



JBS ソリューション紹介



JBS ソリューション紹介：JBS マネージドセキュリティサービス

JBS マネージドセキュリティサービス for Microsoft 365 シリーズ

リアルタイムにインシデント検知・脅威分析・対処を実現！E5 ライセンスを活用！

マネージドセキュリティサービス for Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection は、Windows 10 クライアント PC のセキュリティ強化を実現します。JBS がお客様に代わり本製品の運用を行い、お客様負担のセキュリティ強化と改善の促進をサポートします。

サービス概要

Microsoft Defender ATP は各 Windows 10 クライアント PC から多種多様の情報収集を行い、その情報から潜在的脅威を探ります。JBS では、E5 ライセンスイベントを監視・分析し、お客様のセキュリティ強化を支援します。

Windows 10 Enterprise	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Enterprise Mobility + Security	Office 365 Enterprise
Microsoft 365 E5	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Azure Active Directory Identity Protection (ID 保護・特権管理)*	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの監視)

Microsoft Defender Advanced Threat Protection(以下、Microsoft Defender ATP)とは
Windows 10 クライアント PC のマルウェア対策、および Endpoint Detection and Response(EDR)を実現する製品です。お客様のデバイスのセキュリティ対策を強力に支援します。

※ Azure Active Directory Identity Protection (ID 保護)、Azure Active Directory Premium P2 に含まれる機能です。

シャドー IT を見える化 & クラウド利用に統制を！E5 ライセンスを活用！

マネージドセキュリティサービス for Microsoft Cloud App Security

Microsoft Cloud App Security は、社内に危険なクラウド利用がないかを監視・制御するサービスです。JBS がお客様の代わりに本製品の運用を行い、お客様負担のセキュリティ強化と改善の促進をサポートします。

サービス概要

Microsoft Cloud App Security は、クラウドサービスの利用状況を可視化しながら、利用の制御および統制を行う包括的なソリューションです。JBS のセキュリティ専門家が監視と分析を行い、安全なクラウド利用を実現するための技術的・組織的サポートします。

Windows 10 Enterprise	Enterprise Mobility + Security	Office 365 Enterprise
Microsoft 365 E5	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Azure Active Directory Identity Protection (ID 保護・特権管理)※ Microsoft Cloud App Security (クラウドアプリサービスの可視化と統制) Office 365 Advanced Threat Protection (Azure への ID 対策機能)

Microsoft Cloud App Security (以下、Cloud App Security)とは
クラウドアプリケーションが提供するエンド-to-endの監視・可視化と、制御を統合できる製品です。クラウド上の重要なデータを監視し、シャドー IT の発見・リスクの低減・ポリシーの適用・クラウドの調査・脅威の防止を行うことで組織のセキュリティを強化・経営リスクがクラウドへの対応をサポートします。

※ Azure Active Directory Identity Protection (ID 保護)、Azure Active Directory Premium P2 に含まれる機能です。

組織内の ID を守れ！Active Directory 内の ID・資格情報セキュリティ対策

マネージドセキュリティサービス for Azure Advanced Threat Protection

Azure Advanced Threat Protection は、組織内のユーザー・コンピュータ・リソースなどの資格情報に対する不正なアクティビティや、悪意のある攻撃者による攻撃を検知・分析し、組織内の管理者が適切な対応を迅速にとることが可能になります。

サービス概要

Azure Advanced Threat Protection は、Active Directory 内のユーザー ID と資格情報を保護する為、ユーザーのアクティビティを学習し、悪意のあるアクティビティを監視します。JBS のセキュリティ専門家が監視と分析を行い、侵された ID、および悪意のあるアクティビティの識別、検出、調査をサポートします。お客様のコラボレーション・クラウド導入後の運用管理まで、JBS がフルサポートで提供します。

Windows 10 Enterprise	Enterprise Mobility + Security	Office 365 Enterprise
Microsoft 365 E5	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Azure Active Directory Identity Protection (ID 保護・特権管理)※ Microsoft Cloud App Security (クラウドアプリサービスの可視化と統制) Office 365 Advanced Threat Protection (Azure への ID 対策機能)

Azure Advanced Threat Protection (以下、Azure ATP)とは
Azure Advanced Threat Protection (ATP) はクラウドベースのセキュリティソリューションであり、インプレミスの Active Directory シルクロールを利用し、組織と対応する認証プロセス、使用された ID、および悪意のあるセキュリティ攻撃に対するアクションを実行します。

※ Azure Active Directory Identity Protection (ID 保護)、Azure Active Directory Premium P2 に含まれる機能です。

リアルタイムに ID への侵入を検知！Microsoft 365 E5 ライセンスを活用！

マネージドセキュリティサービス for Azure Active Directory Identity Protection

Azure Active Directory Identity Protection は、攻撃の糸口である ID に対してセキュリティ強化を実現します。JBS がお客様に代わり本製品の運用を行い、お客様負担のセキュリティ強化と改善の促進をサポートします。

サービス概要

Azure Active Directory Identity Protection は、ひと月に 4500 個以上の認証を処理することができるマイクロソフトが提供する最先端の ID 保護サービスです。本サービスは、IDP の導入・構成・インテグレーションから導入後の運用までをワンストップで提供し、専門家が Azure AD 上の組織 ID を効率よく、セキュリティに運用管理するためのサポートを行います。

Windows 10 Enterprise	Enterprise Mobility + Security	Office 365 Enterprise
Microsoft 365 E5	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Azure Active Directory Identity Protection (ID 保護・特権管理)* Microsoft Cloud App Security (クラウドアプリサービスの可視化と統制) Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの監視)

Azure Active Directory Identity Protection (以下、IDP)とは
マイクロソフトのクラウドベースの ID 管理サービスで、ID の作成・変更・削除・パスワードの変更などの操作を実行する製品です。攻撃者は、より簡単に組織のクラウドシステムへのアクセスを図るため、重要なデータへのアクセスを許せません。

※ Azure Active Directory Identity Protection (ID 保護)、Azure Active Directory Premium P2 に含まれる機能です。

標的型攻撃を入口で防げ！毎秒進化するクラウド型メールセキュリティ

マネージドセキュリティサービス for Office 365 Advanced Threat Protection

Office 365 Advanced Threat Protection (Office 365 ATP) は、多種多様な標的型攻撃メールに広く多くの対応可能なセキュリティ製品です。JBS がお客様に代わり本製品の運用を行い、お客様負担のセキュリティ強化と改善の促進をサポートします。

サービス概要

Office 365 Advanced Threat Protection は、リアルタイムに更新されるクラウドベースの脅威情報をもとに、Exchange Online を守る高品質なメールフィルタリングサービスです。JBS のセキュリティ専門家が監視と分析を行い、安全なクラウドを利用を約束する特徴的なサポートします。

Windows 10 Enterprise	Enterprise Mobility + Security	Office 365 Enterprise
Microsoft 365 E5	Microsoft Defender Advanced Threat Protection (EDR) (エンドポイントの検出と対応)	Azure Active Directory Identity Protection (ID 保護・特権管理)* Microsoft Cloud App Security (クラウドアプリサービスの可視化と統制) Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの監視)

Office 365 Advanced Threat Protection (以下、Office 365 ATP)とは
クラウドベースのメールフィルタリングサービスです。世界中の脅威情報を収集し、最高水準のセキュリティベースに基づき脅威なし(ゼロ)保護を提供することで、実効的な防御を実現します。送信されたメールが付与されたファイルハッシュ(暗号化)と照合され、なりすましユーザーにより送信されたメールが検出できます。

※ Azure Active Directory Identity Protection (ID 保護)、Azure Active Directory Premium P2 に含まれる機能です。

JBS ソリューション紹介：今後の取り組み

Microsoft 365 E5 Security 向けのインシデントレスポンスサービスを提供中

今後も **Modern SOC** を目指してサービスを拡充・刷新して行きます

- Azure Sentinel のサービス化
- ケースマネジメントに ServiceNow を活用
- Azure Security Center や Compliance Center のサービス化

JBS マネージドセキュリティサービス



Azure
Sentinel

Compliance Center

Office365 Advanced
Compliance

Azure
Security Center

Azure
ATP

Microsoft Threat Protection (MTP)

Azure AD
Identity
Protection

Defender
Advanced Threat
Protection (ATP)

Office 365
ATP

Microsoft
Cloud
App Security

2020/2
リリース

2019/2
リリース

2018/11
リリース

2019/6
リリース

2019/5
リリース

是非、アンケートをお願いします！

ご清聴ありがとうございました。

皆さまにより良い情報をご提供したいと思っております。ぜひともアンケートにご協力をお願いします。

(※ 1、2分で回答できます。)

アンケートURLはこちらから



オンデマンドウェビナーもやってます！

JBSのホームページでセキュリティウェビナーを開催しております。

「サイバー攻撃の近況」「なにを信頼（Trust）するか？」「脅威可視化PoCとは」

を各10分前後で視聴可能です。

<https://pages.jbs.co.jp/webinarList.html>



セキュリティウェビナーシリーズ
サイバー攻撃の近況

進化しつづけるサイバー攻撃。2020年の最新
情報についてご説明します。

▶ 視聴する



セキュリティウェビナーシリーズ
なにを「信頼（Trust）」するか？

Microsoft が提唱する新しいセキュリティモデル
とは？4つのポイントを解説します。

▶ 視聴する



セキュリティウェビナーシリーズ
脅威可視化PoCとは

組織に潜む脅威を見える化するワークショップの
詳細についてご紹介します。

▶ 視聴する



Customer First

お客様とともに