



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

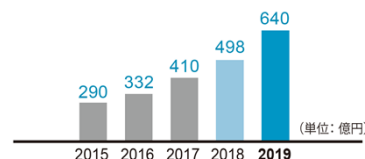
会社概要



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



6 拠点 / 5 拠点

社員数



2,250 人

MCP 取得 / 認定者数 (延べ)



1,163 人

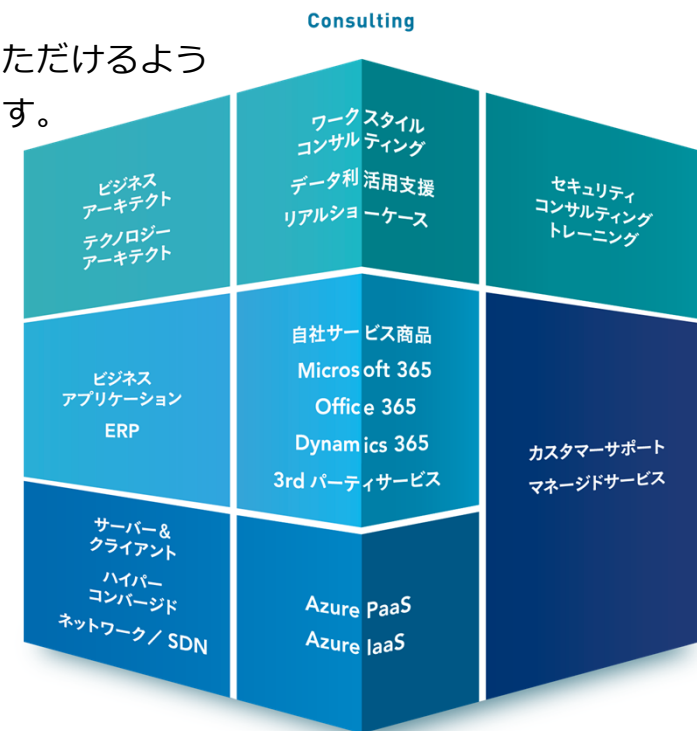
社員研修講座数



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。



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

- ・ 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

2

ソリューション

- ・ 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

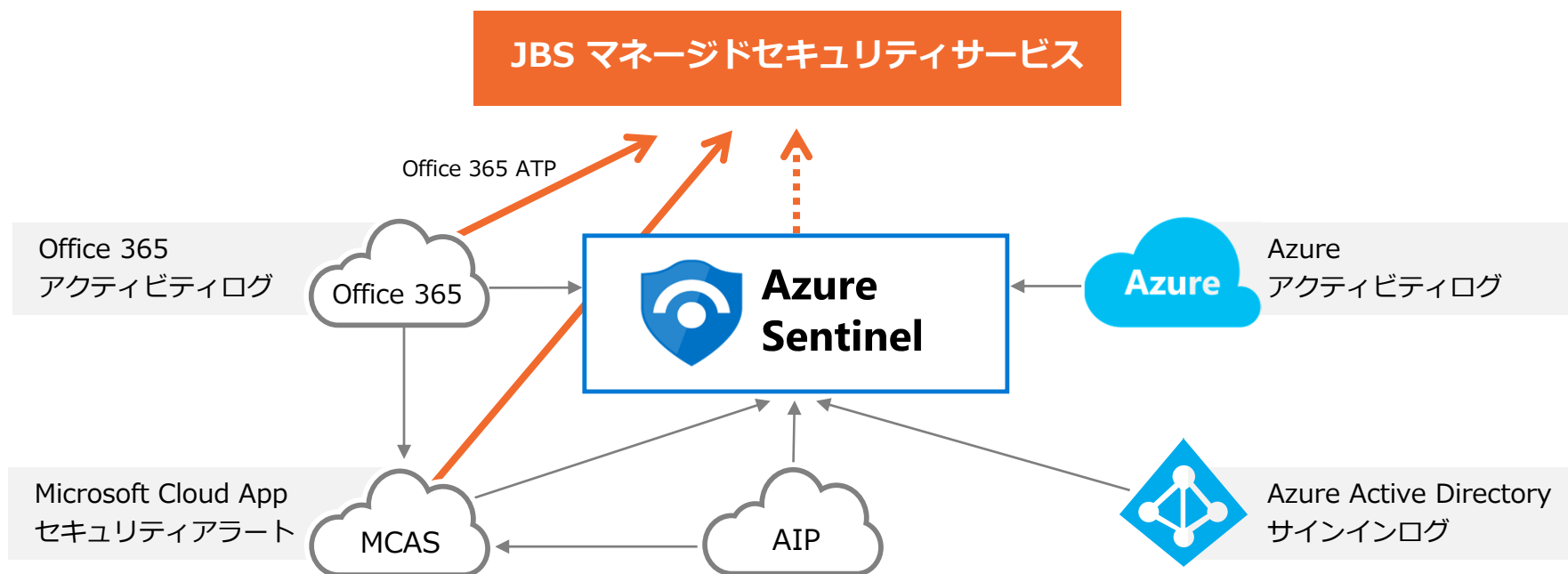
- ・ なりすまし、フィッシング等を可視化可能に
- ・ 不審な Office 365 アクティビティを捕捉可能に
- ・ パスワードを使わずにファイルを暗号化
- ・ 社内に専門のセキュリティチームを配置しなくて良い

パートナー選定ポイント

- ・ 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、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@tanakamas3.onmicrosoft.com] がトリガーしたMCASのその他アラート

検索

TenantId	↑↓	TimeGenerated	↑↓	DisplayName	↑↓	AlertName	↑↓	AlertSeverity	↑↓	Description
ad44ae25-1337-4783-ba3f-9b0fba035a79		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
ad44ae25-1337-4783-ba3f-9b0fba035a79		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

●[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@tanakamas3.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
ad44ae25-1337-4783-ba3f-9b0fba035a79		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

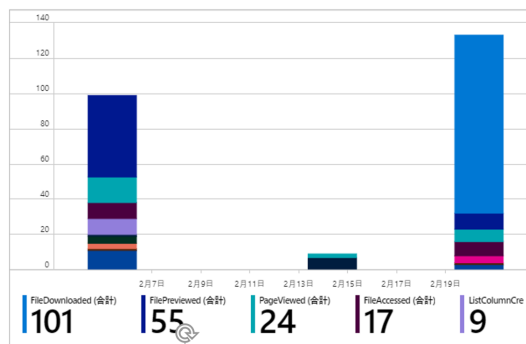
アラート発生アカウント-発...
tkensyo@tanakamas3.on... ▼
admin01@tanakamas3.onmicrosoft.com - 1回発生
tkensyo@tanakamas3.onmicrosoft.com - 2回発生

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 0365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）

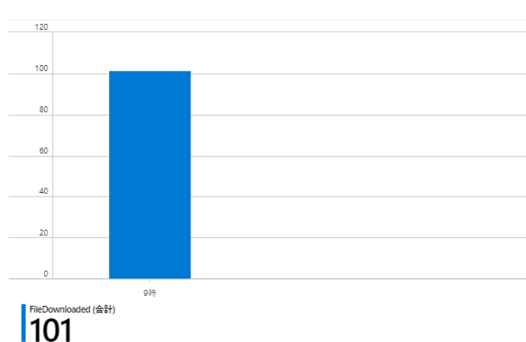
TimeGenerated	↑↓	Operation	↑↓	OfficeWorkload	↑↓	OfficeObjectid
2020/2/20 22:24:13		FileAccessed		SharePoint		https://tanakam...
2020/2/20 16:04:38		PagePrefetched		SharePoint		https://tanakam...
2020/2/20 16:04:37		PagePrefetched		SharePoint		https://tanakam...
2020/2/20 16:04:36		PageViewed		SharePoint		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...



- 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ディング

● 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_7741/1/test71.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test72.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test76.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test73.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test75.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test77.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test7.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test68.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test69.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test70.xlsx
s:// sharepoint.com/sites/MASSTest01/Shared Documents/General/masstest_7741/1/test63.xlsx
```



● 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	↑↓
192.168.1.100		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	↑↓
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）

Hunting-NewBrute force attack against Azu...
インシデント ID: 71

高 重大度
新規 状態
未割り当て 所有者

説明
Azure Portal・Office365に対するブルートフォース攻撃が成功した可能性を示すアラートです。
20分間に5回以上サインインに失敗した後にサインインが成功したユーザー名・サインイン先のサービスの一覧を以下に示します。

secadmin
14.9.130.224
Hunting-NewBrute ...

Related alerts (41)
Least active accounts on... (1)
Least prevalent accounts... (1)
More

Most active accounts on Azu... (1)
Most prevalent accounts ass... (1)
Most prevalent Linux hosts ... (0)
Office activity accounts wi... (0)
Related bookmarks (0)
Destination IPs with most d...
Hosts receiving least amoun...



以下のアラートが発生しました。
Hunting-NewBrute force attack against Azure・Office365

重大度：
High

説明：
Azure Portal・Office365に対するブルートフォース攻撃が成功した可能性を示すアラートです。20分間に5回以上サインイン

クエリ実行結果:

UserPrincipalName	IPAddress	AppDisplayName	StartTimeUtc	EndTimeUtc	FailureCount	SuccessCount
test03@...onmicrosoft.com		O365 Suite UX	3/2/2020 8:05:34 AM	3/2/2020 8:05:55 AM	6	2
secadmin@...onmicrosoft.com		Azure Portal	3/2/2020 8:06:47 AM	3/2/2020 8:07:11 AM	5	2

secadmin 18:03
以下のアラートが発生しました。
Hunting-NewBrute force attack against Azure・Office365

重大度：
High

説明：
Azure Portal・Office365に対するブルートフォース攻撃が成功した可能性を示すアラートです。20分間に5回以上サインインに失敗した後にサインインが成功したユーザー名・サインイン先のサービスの一覧を以下に示します。

クエリ実行結果:

UserPrincipalName	IPAddress	AppDisplayName	StartTimeUtc	EndTimeUtc	FailureCount	SuccessCount
test03@...onmicrosoft.com		O365 Suite UX	3/2/2020 8:05:34 AM	3/2/2020 8:05:55 AM	6	2
secadmin@...onmicrosoft.com		Azure Portal	3/2/2020 8:06:47 AM	3/2/2020 8:07:11 AM	5	2

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・対応を実現！ 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 クラウド 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、お客様自身のセキュリティ強化と被害の低減をサポートします。

サービス概要

Microsoft Defender ATP は、Windows 10 クラウド PC から多種多量の情報収集を行い、その情報から潜在的脅威を探ります。
JBS では、セキュリティイベントを監視・分析し、お客様のセキュリティ強化を支援します。

	Windows 10 Enterprise	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 (クラウドアプリケーションサービスの可視化と制御) Azure Advanced Threat Protection (Azure への ID 攻撃検知)	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの保護)

Microsoft Defender Advanced Threat Protection (以下、Microsoft Defender ATP) とは、Windows 10 クラウド 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 は、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、お客様の自身のセキュリティ強化と被害の低減をサポートします。

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、利用の制御および監視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助けるサポートを提供します。

	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 (クラウドアプリケーションサービスの可視化と制御) Azure Advanced Threat Protection (Azure への ID 攻撃検知)	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの保護)

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リスクを軽減し、可視化を強化して被害を軽減できる製品です。
クラウド上の重要なデータを保護し、シャドー IT の発見・リスクの軽減・ポリシーの適用・アクティビティの調査・脅威の検出を行うことで、組織内の重要なデータを保護し、継続しながらクラウドへの安全な移行をサポートします。

※ Azure Active Directory Identity Protection は、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、組織内のユーザーやコンピュータ、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す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。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、侵害された ID、および悪意のあるアクティビティの検出、検知、調査支援をサポートします。悪意のあるコンソール操作から導入の悪意のある攻撃者まで、JBS がワンストップで提供します。

	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 (クラウドアプリケーションサービスの可視化と制御) Azure Advanced Threat Protection (Azure への ID 攻撃検知)	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの保護)

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、オンプレミスの Active Directory システムを利用して、組織を対象とする高度な監視、検出された ID、および悪意のあるインサイダーによるアクションの検出を行います。

※ Azure Active Directory Identity Protection は、Azure Active Directory Premium P2 に含まれる機能です。

リアルタイムに ID への侵害を検知！ 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、攻撃の入口である 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、お客様の自身のセキュリティ強化と被害の低減をサポートします。

サービス概要

Azure Active Directory Identity Protection は、ひと月に 4500 個以上の認証を確認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、ID の不正なログインやパスワードの漏洩を検出・検知し、企業に Azure AD 上の危険な ID を通知し、ID を安全に運用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 (クラウドアプリケーションサービスの可視化と制御) Azure Advanced Threat Protection (Azure への ID 攻撃検知)	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの保護)

Azure Active Directory Identity Protection (以下、IDP) とは、マイクロソフトの脅威インテリジェンスと AI を利用してユーザーのサインインリスクを分析し、最先端の ID 対策を実現する製品です。攻撃者によるなりすまし、侵入をリアルタイムで防ぐことが可能になり、重要なリソースへのアクセスを防止します。

※ Azure Active Directory Identity Protection は、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、多種多様な標的型メールの脅威情報をもとに、Exchange Online を守る高度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、安全なクラウド利用を助けるサポートを提供します。

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 を守る高度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、安全なクラウド利用を助けるサポートを提供します。

	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 (クラウドアプリケーションサービスの可視化と制御) Azure Advanced Threat Protection (Azure への ID 攻撃検知)	Office 365 Advanced Threat Protection Plan 2 (メールフィルタリング、リンクの保護)

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、悪意のあるデータベースに基づき脅威は日々進化しています。未知のマルウェアやフィッシング攻撃から組織を保護します。送受信されるメールに添付されたファイルやハイパーリンクの検出、なりすましユーザーにより送られるメールの検出が可能です。

※ Azure Active Directory Identity Protection は、Azure Active Directory Premium P2 に含まれる機能です。

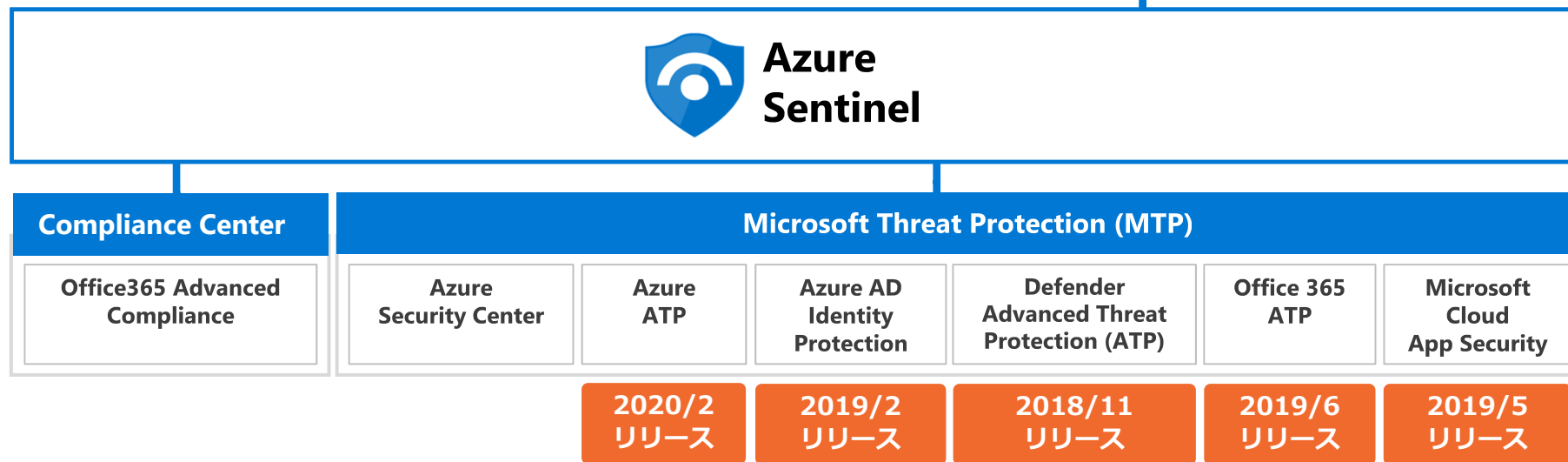
JBS ソリューション紹介：今後の取り組み

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

now
ServiceNow



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