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

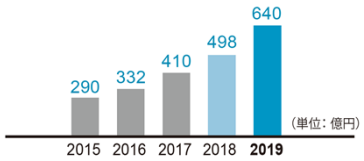
日本ビジネスシステムズ株式会社
事業企画本部 MS 統合サポートセンター
エキスパート
秋葉 俊明

会社概要

会社概要：日本ビジネスシステムズ株式会社

JBS

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

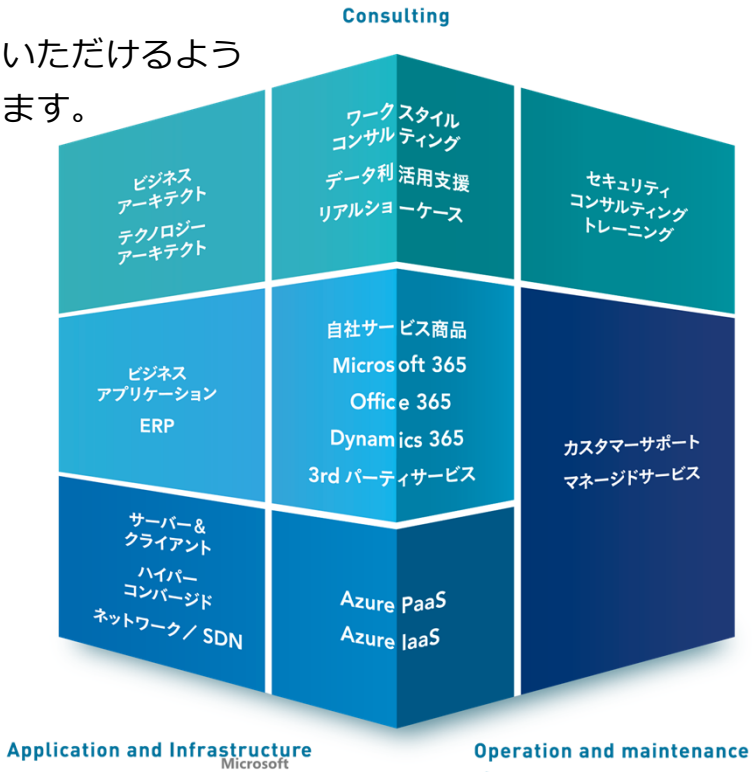
会社概要：OUR BUSINESS

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。

Microsoft Partner of the Year 2019 AWARD
Microsoft Partner of the Year 2018 AWARD
Microsoft Partner of the Year 2017 AWARD
Microsoft Partner of the Year 2016 AWARD
Microsoft Partner of the Year 2015 AWARD
Microsoft Partner of the Year 2014 AWARD
Microsoft Partner of the Year 2013 AWARD

Gold Microsoft Partner
Microsoft

Microsoft Partner
Microsoft
2018 Partner of the Year Winner
Japan Partner of the Year



Microsoft DIGITAL TRUST SECURITY Alliance

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

LAC × JBS

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

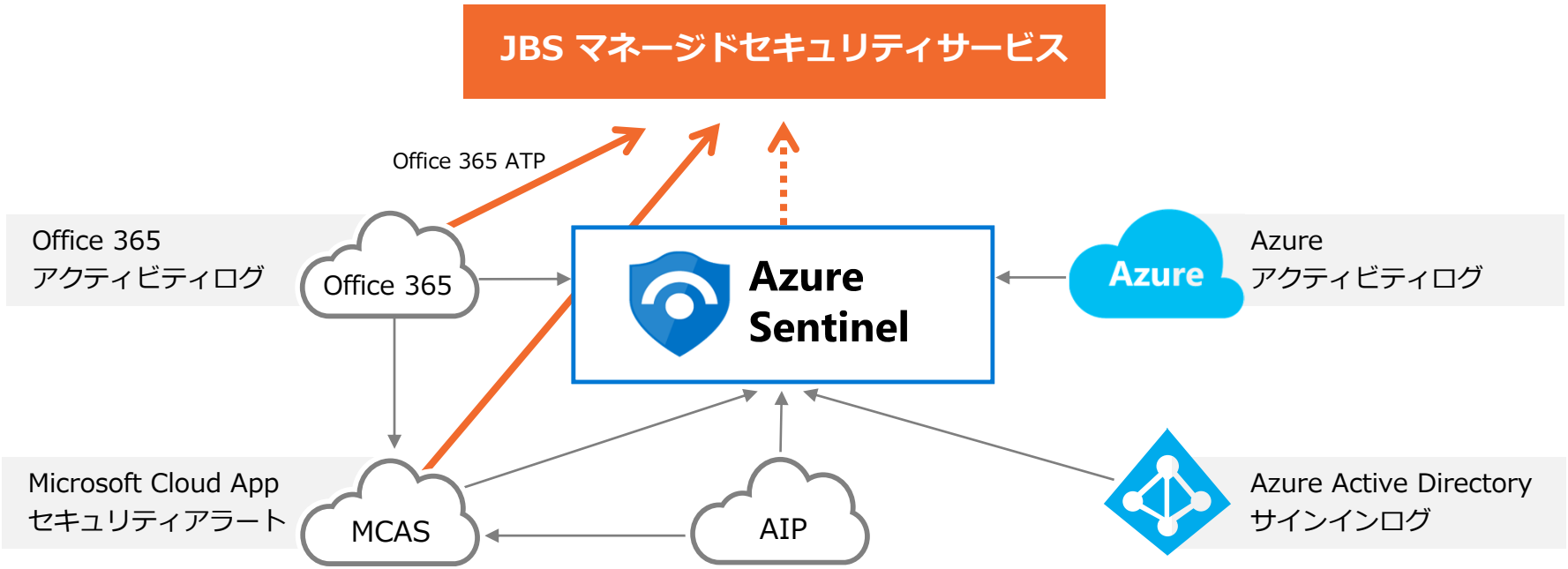
・なりすまし、フィッシング等を可視化可能に
・不審な Office 365 アクティビティを捕捉可能に
・パスワードを使わずにファイルを暗号化
・社内に専門のセキュリティチームを配置しなくて良い

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

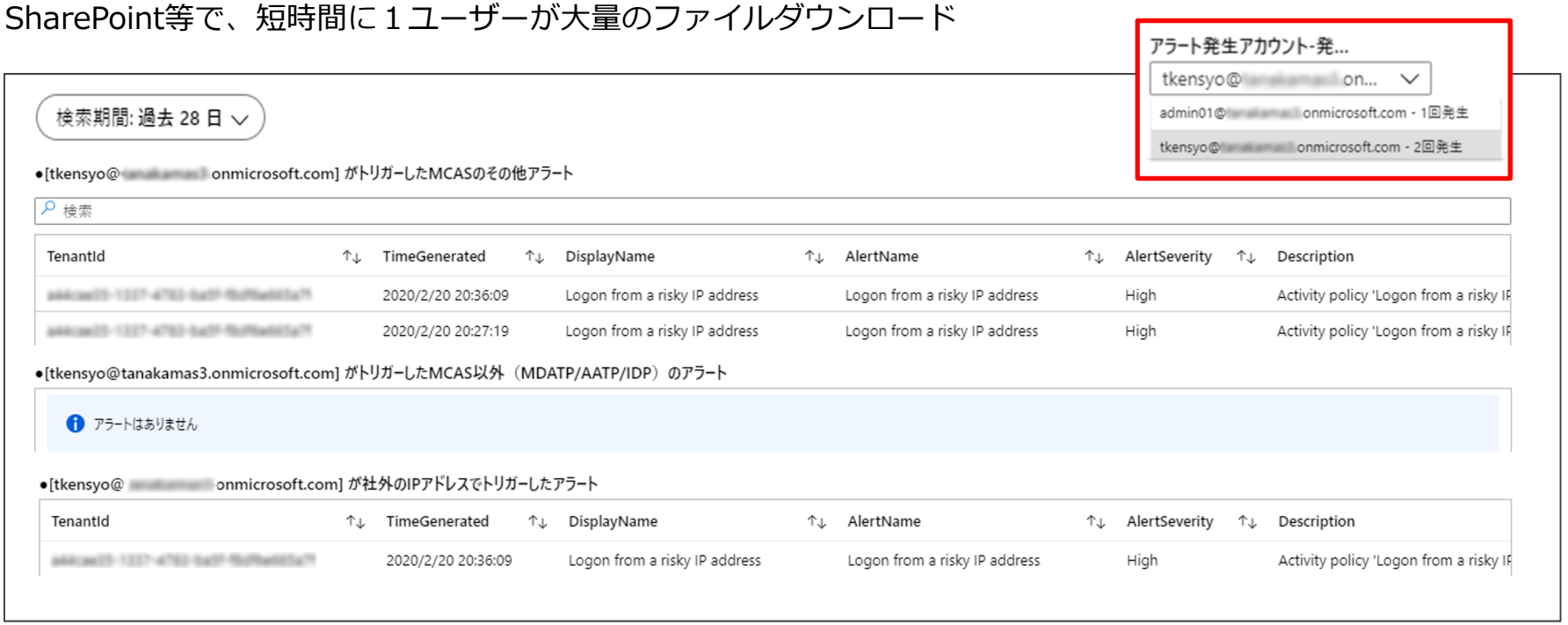
事例紹介：全体構成

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）

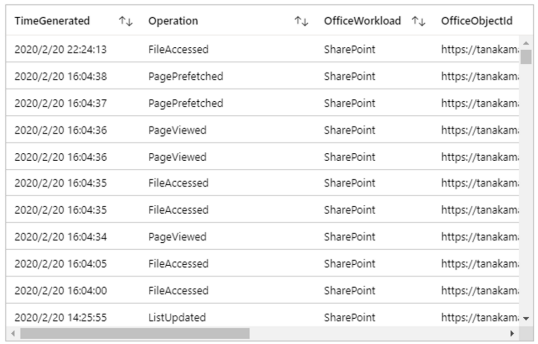
指定期間内で、選択したアカウントのアラート・アクティビティを表示
SharePoint等で、短時間に１ユーザーが大量のファイルダウンロード



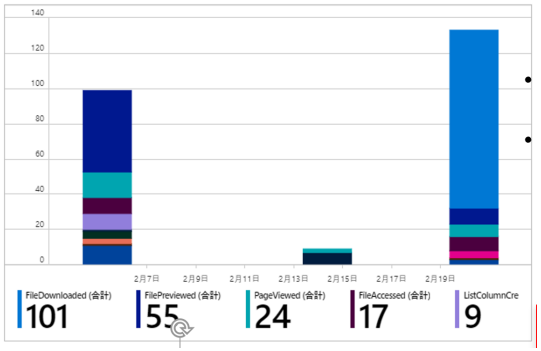
事例紹介：Sentinel 活用紹介（頻発アラートの調査用ブック②）

通常と異なる O365アクティビティを視覚的に判断

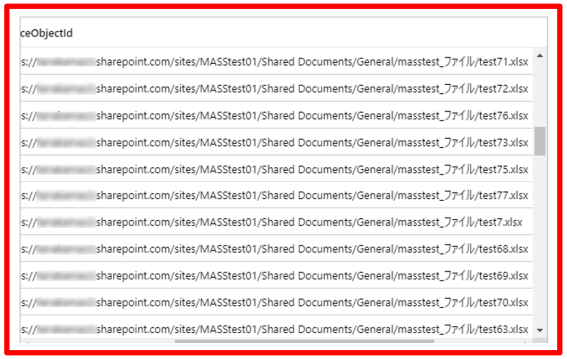
● Office 365 アクティビティー一覧・グラフ（日単位）



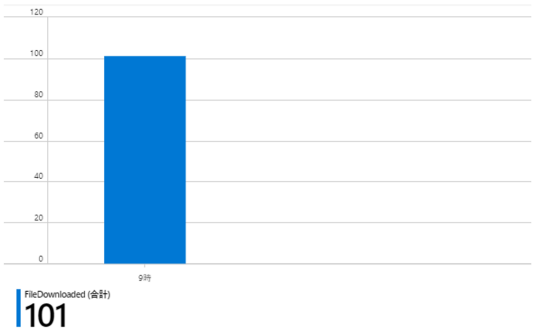
TimeGenerated	Operation	OfficeWorkload	OfficeObjectId
2020/2/20 22:24:13	FileAccessed	SharePoint	https://tanakam
2020/2/20 16:04:38	PagePrefetched	SharePoint	https://tanakam
2020/2/20 16:04:37	PagePrefetched	SharePoint	https://tanakam
2020/2/20 16:04:36	PageViewed	SharePoint	https://tanakam
2020/2/20 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ー一覧・グラフ（日単位）



ceObjectId
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test71.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test72.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test76.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test73.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test75.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test77.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test7.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test68.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test69.xlsx
s://[redacted]sharepoint.com/sites/MASStest01/Shared Documents/General/masstest_ファイル/test70.xlsx
s://[redacted]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
[redacted]	2020/3/9 9:35:59	2020/3/9 9:36:07	59	2020/3/9 9:35:59

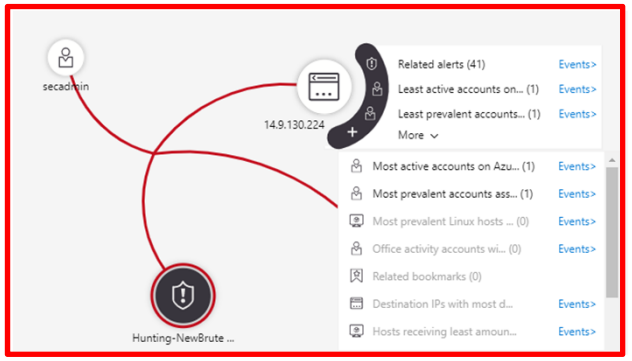
•SharePointFileOperation via devices with previously unseen user agents

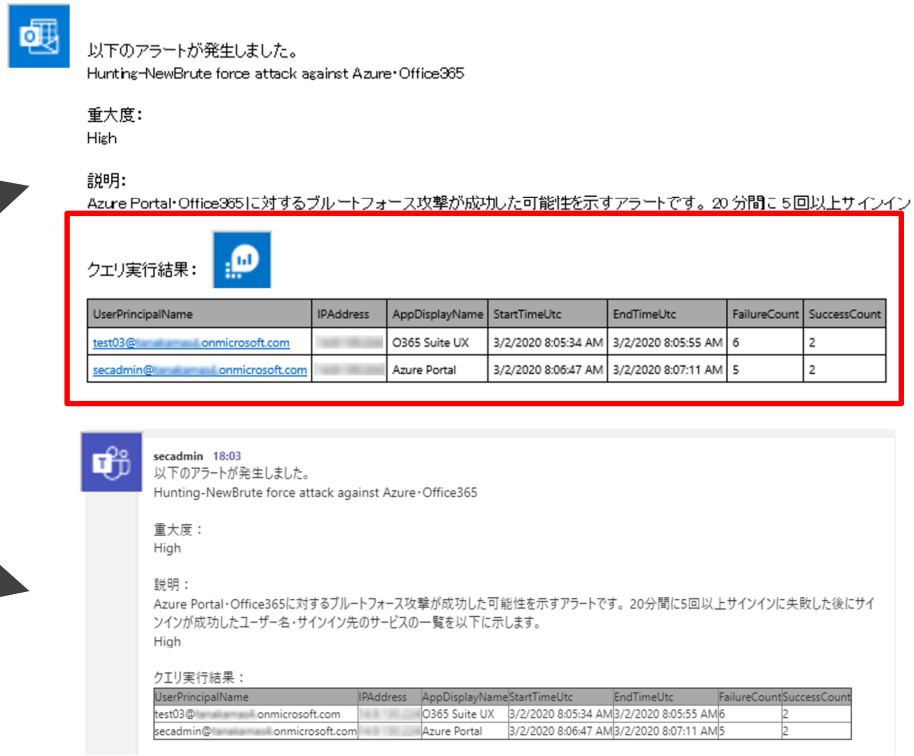
-アラート発生アカウントで直前14日間で使用されなかったユーザーエージェントによるSharePointファイル操作

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）

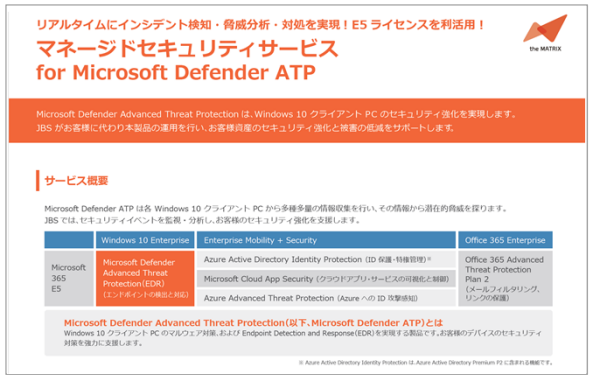




JBS ソリューション紹介

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

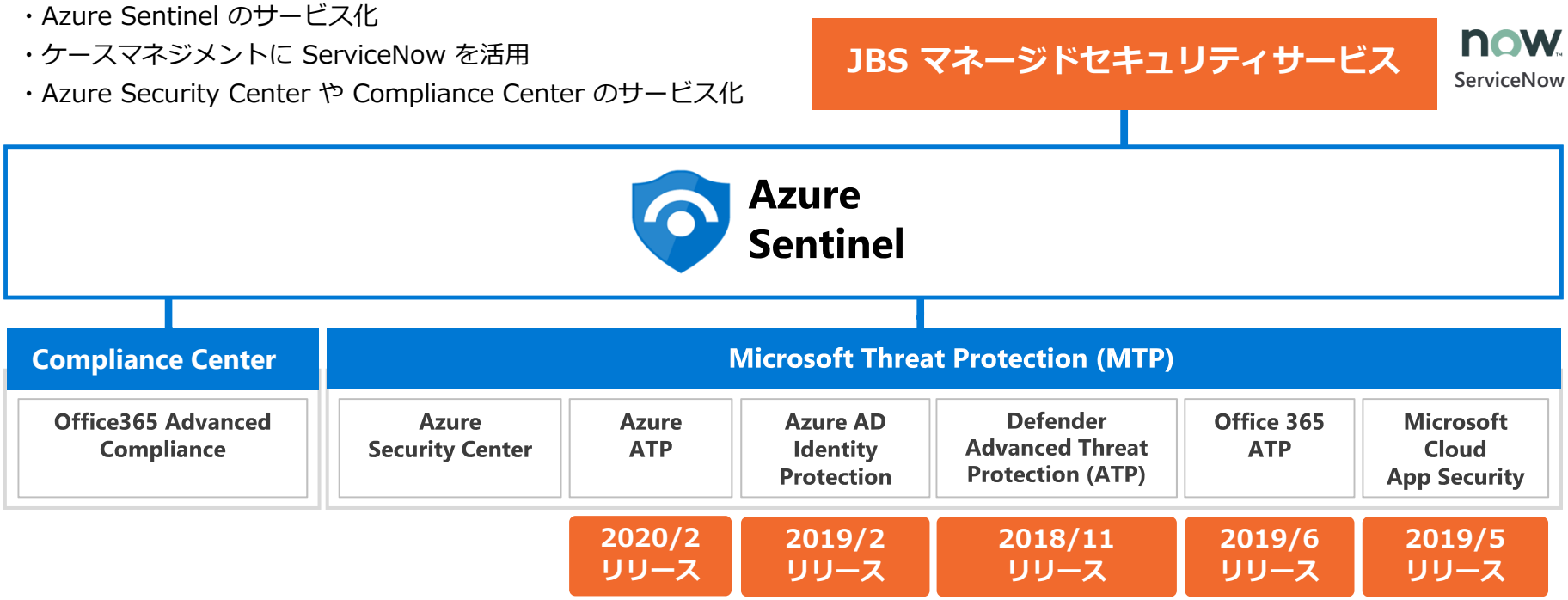
JBS マネージドセキュリティサービス for Microsoft 365 シリーズ



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



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

JBS

Customer First

お客様とともに