DELL Technologies

Microsoft 365のセキュリティ対策は万全ですか？

Microsoft 365 セキュリティアセスメントサービス

“組織のセキュリティをより強靭に“

Microsoft 365の利用率が高いことを背景に、Microsoft365ユーザーを狙った侵入等の不正アクセス被害が非常に多く発生しています。
お客様のセキュリティ対策は万全でしょうか？デル・テクノロジーズではMicrosoft 365をご利用のお客様向けに、より強靭なセキュリティ環境を構築するため、現状の潜在的リスクを特定し、その対策方法並びに対策実現までの計画策定を支援するサービスをご提供しています。
先ずは何から始めるべきか、その答えが「Microsoft 365セキュリティアセスメントサービス」にあります。

Microsoft 365をご利用中のお客様に最適なサービス

現在このような課題をお持ちではありませんか？

- どこからセキュリティ対策をすればよいか分からない
- Microsoft 365のセキュリティリスクを可視化したい
- 優先度の高いセキュリティ対象領域を絞りたい
- Microsoft365のセキュリティ製品の活用方法が分からない

これらの課題に対する最適解として、当社専門コンサルタントによる約4週間のアセスメントにより以下の成果物をご提供します。
（詳細は裏面をご覧ください）

ご提供するレポート（成果物）

現状ヒアリング 分析結果まとめ	アセスメント結果	実施計画 兼 ロードマップ

デル・テクノロジーズが提供するセキュリティ関連サービス

本サービスはNIST*サイバーセキュリティフレームワークで定義されるコアの5つの機能の内、「特定」にフォーカスをしたサービスです。網羅的に課題を抽出した後に、課題の絞り込みをすることで、効果的・効率的な「防御」につなげます。
デル・テクノロジーズでは、このそれぞれの機能に対応するサービスをご提供しております。詳しくは当社のお客様担当営業までお問い合わせください。

NISTサイバーセキュリティフレームワーク

特定 IDENTIFY	防御 DETECT	検知 RESPOND	対応 RECOVER	復旧 PROTECT

*NIST: National Institute of Standards and Technology「米国国立標準技術研究所」

Microsoft 365セキュリティアセスメントサービスの概要

現状を評価・スコア化

- Microsoft 365ご利用状況のヒアリングおよび整理
- Microsoft 365以外のセキュリティ製品利用状況のヒアリング
- セキュリティ状態を、アセスメントおよび現状の可視化

必要な対策の洗い出し・優先度付け

- Microsoft 365、その他セキュリティ製品のご利用状況を踏まえた改善項目の優先順位付け
- 各改善項目の優先順位のご説明と合意形成

改善実施計画策定

- 優先度“高”の改善項目の導入案の作成※1
- お客様のビジョン・方針を加味したセキュリティ対策実現までのロードマップのご提示

セキュリティアセスメントサービス 実施例

ワークショップ実施例

1週目
▲WS#1
- 環境ヒアリング
- セキュアスコア結果Export

2週目
▲WS#2
- 現環境とセキュアスコア結果を踏まえたディスカッション
- 課題事項のヒアリング

3週目
▲WS#3
- 改善が必要な項目の優先順位の決定・合意

4週目
▲WS#4
- 改善実施計画ActionPlanのご報告および合意形成

データ、ヒアリング結果の分析
分析結果のまとめ*

課題の優先順位、検討項目の精査*

実施計画策定・資料化*

*弊社、専門コンサルタントによる作業

アウトプットイメージ

ツールより出力された結果レポートを弊社コンサルタントがレビューをし、課題を精査します。

ランク	おすすめの操作	顧客A Status	優先度	スコアへの影響	獲得したポイント	状態
1	Create Safe Links policies for email messages	To address	低	0.99%	0/9	要対処
19	セキュリティで保護されたアクセスのためにすべてのユーザーが多要素認証を完了できることを確認する	To address	高	0.99%	0.86/9	要対処
20	従来の認証を禁止するポリシーを有効にする	To address	高	0.88%	0/8	要対処
21	パスワードを無期限にする	Completed	—	0.88%	0/8	要対処
22	Turn on Safe Attachments in block mode	To address	中	0.88%	0/8	要対処
40	サインインのリスク ポリシーを有効にする	To address	中	0.77%	0/7	要対処
41	ユーザーのリスク ポリシーを有効にする	To address	中	0.77%	0/7	要対処
42	管理ロールに対して MFA を要求する	To address	高	1.10%	3.33/10	要対処
44	Turn on the common attachments filter setting for anti-malware policies	To address	低	0.55%	0/5	要対処
66	Do not allow Exchange Online calendar details to be shared with external users	To address	高	0.55%	0/5	要対処
67	管理対象外のアプリケーションにユーザーの承認を許可しない	To address	低	0.44%	0/4	要対処
68	Create an OAuth app policy to notify you about new OAuth applications	To address	中	0.44%	0/4	要対処
75	カスタマー ロックボックス機能を有効にする	To address	低	0.11%	0/1	要対処
76	Deploy a log collector to discover shadow IT activity	To address	中	0.11%	0/1	要対処
112	Create zero-hour auto purge policies for malware	Completed	—	0.66%	6/6	完了
115	ハイブリッドの場合にパスワード ハッシュの同期を有効にする	Completed	—	0.55%	5/5	完了
116	Turn on Microsoft Defender for Office 365 in SharePoint, OneDrive, and Microsoft Teams	Completed	—	0.55%	5/5	完了
117	Turn on Safe Documents for Office Clients	Completed	—	0.55%	5/5	完了
131	Create an app discovery policy to identify new and trending cloud apps in your org	To address	中	0.33%	3/3	完了
132	Create zero-hour auto purge policies for phishing messages	Completed	—	0.33%	3/3	完了
133	Create a custom activity policy to get alerts about suspicious usage patterns	To address	中	0.22%	2/2	完了
134	Ensure that there are no sender domains allowed for Anti-spam policies	To address	低	0.22%	2/2	完了
136	セルフサービスによるパスワードのリセットを有効にする	Completed	—	0.11%	1/1	完了
137	全体管理者を複数設定する	Completed	—	0.11%	1/1	完了
138	制限付き管理ロールを使用する	Completed	—	0.11%	1/1	完了
139	TLS 1.0/1.1 と 3DES への依存を排除する	To address	低	0.11%	1/1	完了
143	Create zero-hour auto purge policies for spam messages	Completed	—	0.11%	1/1	完了

課題内容を詳細化し、必要なアクションを以下のように整理します。

管理者ロールに対してMFAを要求する：

制限付き管理ロールを使用する：

パスワードを無期限にする：

管理対象外のアプリケーションに対するユーザーの承認を許可しない：

詳細

統合されたサードパーティ製アプリのアクセス許可を規制して、サービスのセキュリティを強化します。堅牢なセキュリティ管理策をサポートする、必要なアプリのみにアクセスを許可します。サードパーティ製アプリケーションは Microsoft によって作成されていないため、テナントからのデータの流出など、悪意のある目的に使用される可能性があります。攻撃者は、セキュリティ侵害を受けたアカウントを利用せずに、これらの統合されたアプリを通じてサービスへのアクセスを維持し続けることができます。

対処方法

組織のユーザーがサードパーティのアプリに Office 365 情報へのアクセスを許可しないようにし、管理者による今後の同意操作を要求するには、[Azure Active Directory 管理センター]、[エンタープライズ アプリケーション]、[ユーザー設定]、[エンタープライズ アプリケーション] の順に移動します。「ユーザーはアプリが自身の代わりに会社のデータにアクセスすることを許可できます」トグルを [いいえ] に設定します。

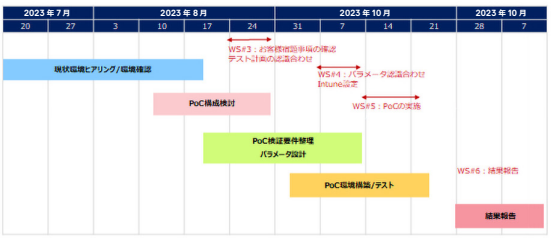
実装に向けたステップの明確化およびロードマップ例

お客様のセキュリティ状態、課題、要件、緊急性などを加味し対応すべきポイントの優先度付けをします。

製品	総数	状態		優先度			
		完了	要対処	高	中	低	対象外
Azure Active Directory	11	4	7	2	3	1	1
Defender for Endpoint	110	50	60	5	20	20	15
Defender for Office	9	6	3	0	0	1	0
Exchange Online	3	1	2	1	1	0	0
Microsoft Defender for Cloud Apps	4	2	2	0	0	0	2
Microsoft Teams	6	3	3	2	1	0	0

優先度に加え、製品間の依存や関係性を加味してセキュリティ強化実現のためのロードマップをご提供します。

今後のスケジュール案



セキュリティアセスメントサービス　ご提供内容及び価格

期間	約4週間	**ご提供するレポート（成果物）**	● 現状ヒアリング分析結果まとめ ● アセスメント結果 ● 実施計画兼ロードマップ
ワークショップ	4回（1回あたり2時間程度）	**ご提供価格**	80万円（税抜価格）
現状調査	ツールによるデータ収集		

■サービスの前提条件

※1 実施計画の策定はお客様と協議したうえで優先度が"高"となったものから最大5項目を対象に詳細化します。実装のための設計や導入作業のご依頼は別途お見積りとなります。

デル・テクノロジーズ株式会社
〒100-8159 東京都千代田区大手町一丁目2番1号 Otemachi Oneタワー 17階