Microsoft 365 導入サービス

業務効率向上・働き方改革に役立つオールインワンクラウドサービス
Microsoft 365 の導入サービスをご提供します

◆ Microsoft 365 のクラウドサービス

■ Microsoft 365 のクラウドサービスを活用することにより“ いつでも ”、“ どこでも ”、“ 安全な方法で ” 業務を行え、「 業務効率の向上 」、「 働き方改革 」に役立ちます。
■ 従業員のコミュニケーションやチームワークを支援する安全性の高いワークススペースが提供されます。
■ クラウドへデータを蓄積することによりインテリジェントな分析、業務の効率化への活用を図ります。

■ Microsoft 365 には、Microsoft 365 Enterprise と Microsoft 365 Business が含まれます。

● Microsoft 365 Enterprise :
大企業など大規模な組織向けに設計されており、以下のサービスがパッケージ化された安全かつインテリジェントな統合ソリューションです。従業員が創造力を発揮し、安全かつ確実に連携できるようにします。
✔ Office 365 Enterprise
✔ EMS（Enterprise Mobility + Security）
✔ Windows 10 Enterprise
さらにMicrosoft 365 Enterprise は、以下の2つのプランが提供されます。
・Microsoft 365 Enterprise E3
・Microsoft 365 Enterprise E5

● Microsoft 365 Business :
最大 300 人のユーザーを持つ中小企業向けに設計されており、以下のサービスがパッケージ化、統合されています。従業員の能力を強化し、ビジネスを保護し、IT管理を簡素化するサービスを提供します。
✔ Office 365 Premium
✔ EMS（Enterprise Mobility + Security）
✔ Windows 10 Pro

◆ エクシオグループの Microsoft 365 導入サービス

■ Microsoft 365 の導入にあたって設計、設定などの環境構築をします。
■ またお客様のご要望により既存データのクラウド移行や Microsoft 365 利用環境のソリューションの開発をします。

※ Microsoft 、マイクロソフト、Windows、Office 365 は米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
※ その他の社名・商品名は、各社の商標または登録商標です。

特　長

Microsoft 365 のクラウドサービス

創造力を最大限に発揮
- インテリジェントなアプリで優れたコンテンツを作成。
- インク、音声、タッチ機能で自然に作業。
- 情報を新しい方法で視覚化。
- どのデバイスでもつながる。

チームワークを強化
- メールと予定表を Exchange で。
- 人、コンテンツ、アプリにつながるための SharePoint 。
- 音声、ビデオ、チャットをSkype とMicrosoft Teams で。
- 組織を横断して人のネットワークを作るYammer 。
- Office 365 Business / ProPlus で共同編集。

統合によるシンプルな管理
- 展開、管理、サービスの TCO を最小化。
- PC 、Mac 、iOS 、Android のプラットフォームを幅広くサポート。
- 全社員を包括的に管理。

インテリジェント セキュリティー
- ID（Identity : 認証情報）とアクセスの管理。
- 情報の保護。
- 脅威の防止。
- セキュリティー管理。
- GDPR 準拠を促進。

※ TCO（Total Cost of Ownership）: 総所有コスト。
※ GDPR（The General Data Protection Regulation）: EU 一般データ保護規則。EU（欧州連合）内のすべての個人のデータ保護およびプライバシーに関するEU 法の規制。EU 域外への個人データの輸出も規制対象。

Microsoft 365 のセキュリティー

ID & アクセス管理

■ パスワード攻撃に対する保護 : パスワードをより強力な 2 要素認証に置き換えて強化するなど、執拗な脅威から認証情報を保護します。
- Windows Hello（生体認証（顔認識または指紋）を使用します。迅速かつ安全にログインできます。）
- Multi-Factor Authentication（多要素認証。Exchange Online メールボックスや OneDrive for Business ファイルを含むクラウドサービスへのパスワードのみのアクセスを防ぎます。）
- Intune device configuration（紛失または盗難にあったデバイスへのログインはポリシーの設定でパスワードや PIN（Personal Identification Number : 暗証番号）の入力を要求し、複数回のログインエラー時は企業データを消去します。）

■ アクセス管理 : 侵害された ID（Identity : 認証情報）が悪用されないよう未然に防止します。
- Azure Active Directory Conditional Access（特定の条件に基づいてアプリへのアクセスを制御します。適切な人々が特定の条件下でリソースにアクセスできる一方で、他の状況下ではアクセスをブロックできるように制御します。）
- Credential Guard（攻撃者が Pass－the－Hash または Pass－the－Ticket 攻撃を通じて組織内の他のリソースにアクセスするのを防ぎます。）

■ ID に関連した脅威の検出と対処 : 企業ユーザーがクラウドアプリケーションをより安全に使用できるよう管理します。
- Cloud App Security（アクセス、データ共有、またデータ保護のきめ細かい制御とポリシー設定を使用して安全なクラウド環境を整備します。ネットワーク内のすべてのクラウドアプリケーションの危険性の高い使用状況およびセキュリティー上の問題を特定するとともにユーザーの異常な行動を検出し、脅威を防止します。）

情報の保護

■ クラウドアプリケーションのセキュリティー管理 : オンプレミスアプリケーションのセキュリティーも確保します。
- Microsoft Cloud App Security（オンプレミスアプリケーションに対して条件付きアクセス制御を適用し、リアルタイムでユーザー動作の監視・制御ができ、機密文書の不正なダウンロードをブロックできます（管理されていないデバイスや企業ネットワーク外からアプリケーションにアクセスしての機密文書のダウンロードをブロック。）

■ データ漏えい防止 : 情報の保存場所や共有先に関係なく、情報へのアクセスを制御します。
- Office 365 Data Loss Protection（Office 365 環境内のファイルを機密性に応じてラベル付け分類し、ラベルに応じたポリシーでデータ損失を防ぎます。）
- Azure Information Protection + Azure Rights Management（主にOffice 365 環境外のファイルを機密性に応じてラベル付け分類し、機密データを暗号化（Azure Rights Management）し、使用権を定義します。情報の保存場所や共有先に関係なく、情報へのアクセスを制御できます。）
- Microsoft Intune（モバイルデバイス管理に条件付きアクセス制御を適用し、管理されていないデバイスへのファイルのダウンロードをブロックします）
- Windows Information Protection + BitLocker（BitLocker はWindows 10 デバイスのディスク全体を暗号化し、デバイスの紛失や盗難時のデータ漏えいを防ぎます。Windows Information Protection は Windows 10 デバイス 内で企業データと個人データを分離し、企業データを偶発的なデータ漏えいから保護します。例えば企業データを個人データエリアや USB メモリーにコピーできないようブロックします。）

脅威の防止

■ セキュリティー リスクの評価・分析・予防 : セキュリティー評価・分析をして、セキュリティーリスクを把握でき、ポリシーおよび改善計画の策定に役立てることができます。
- Office 365 Threat Intelligence（脅威インテリジェンスデータの膨大なデータベースを活用して、攻撃の挙動や不審な動作に対応するパターンを見つけます。）

■ シャドー IT（私物のパソコン、スマートホン、タブレットなど管理されていないデバイスの使用）の可視化 : リスクの高いクラウドアプリケーションを検出し、管理します。
- Microsoft Cloud App Security（アクセス頻度が極めて低い場所からのアクセス、また管理外デバイスや危険な IP アドレスからのアクセスなど、環境内のすべての SaaS（Software as a Service）アプリケーションの異常な動作を検出して警告します。）

■ 電子メールを介した未知の脅威からの保護 : 未知のマルウェアやフィシング攻撃に対する防御に役立つゼロデイ保護を提供します。
- Office 365 Advanced Threat Protection（機械学習モデルや高度ななりすまし検出アルゴリズムを利用して受信メッセージをチェックし、未知のマルウェア、ウィルス、ランサムウェア、フィッシング攻撃などを検出、設定されたポリシーに則って組織を保護します。）

■ 不審な動作の検出 : 機械学習などを利用して、不審な動作を特定します。
- Microsoft Advanced Threat Analytics（複数のデータソースからネットワーク内のログやイベントなどの情報を収集して、ユーザーと環境内の他のエンティティーの動作を学習、分析し、不審な動作（悪意のある攻撃、異常な動作、セキュリティーの問題とリスク）を検出します。）

■ 高度な脅威の検出と対処 : 人工知能、機械学習、およびその他の手段を使用して、攻撃を軽減し、リスクの高い動作を特定し、被害を受ける前に迅速に攻撃を阻止します。
- Microsoft Defender Advanced Threat Protection（Windows 10 デバイスの OS に組み込んだ動作センサーで収集したセンサーデータを分離されたクラウドインスタンス（仮想コンピュータ）へ送り、機械学習、動作分析を利用して、ネットワーク上の高度なゼロデイ攻撃やデータ侵害を検出、調査し、被害を受ける前に迅速に攻撃を阻止します。）

詳　細

エクシオグループの Microsoft 365 導入サービス

Microsoft 365 導入サービス

基本作業	データ移行	開発
● Microsoft 365 の導入計画・設計・設定・拠点展開などの環境構築をします。	● お客様のご要望により、既存で利用していたメールやファイルなどのリソースを最適な方法でクラウドへ移行します。	● お客様のご要望に合わせて Microsoft 365 利用環境に合わせたソリューションの開発をします。

■ Microsoft の推奨する FastTrack のフレームワークによるサービスをご提供いたします。
■ 全国一元的に導入サービスをご提供いたします。

※ FastTrack : FastTrack は、Office 365 や Enterprise Mobility Suite といったマイクロソフト クラウド サービスにお客様がスムーズかつ確実に移行できるようにする成功支援サービスです。

Microsoft 365 導入サービス　オプション

◆ Active Directory 連携サービス
AD 同期やAD FSによるクラウド環境との認証システムの構築をします。

◆ Microsoft 365 専用ネットワーク
既存のネットワークに影響を与えないようにMicrosoft 365 専用のネットワーク構築をします。

◆ Microsoft 365 利用デバイス提供サービス
ユーザーが利用するタブレット端末 Surface Pro や会議用の大画面デバイス Surface Hubなどのデバイスをご提供いたします。

※ AD（Active Directory）同期 : オンプレミスのドメインコントローラーとクラウド上のドメインコントローラーとの間で定期的にデータベースの内容を同一にする処理。
※ AD FS（Active Directory Federation Services）: オンプレミスとクラウド環境など異なるドメインに配置されたシステムやアプリケーションへのシングルサインオンアクセスをユーザーに提供するサービス。
※ シングルサインオン（Single Sign－On）: 1 回のサインオン（ユーザー認証）で複数のコンピューターやアプリケーション、サービスなどにアクセスし利用できるようにすること。