法人向け

Microsoft

2018年5月25日より適用開始

GDPRが与える影響と準拠に向けた4つのステップ

免責事項

本冊子は、GDPR の説明であり、発行時点におけるマイクロソフトの解釈を表しています。マイクロソフトは、GDPR の意図と意味について、長い時間を費やしてじっくりと考えてきました。しかしながら、GDPR の適用は事実特定的であるうえ、GDPR のあらゆる側面と解釈が確定されているわけではありません。

そのため、本冊子は、情報の提供のみを目的としており、法律上の助言として、あるいはお客様およびお客様の組織が GDPR を適用する方法を決定するために利用することはできません。法的に資格のある専門家と協力し、GDPR がお客様の組織に具体的にどのように適用されるのか、また法令を遵守するための最善の方法は何かなど、GDPR について議論することをお勧めします。

明示、黙示または法律の規定にかかわらず、本冊子の情報についてマイクロソフトはいかなる責任も負わないものとします。本冊子は “現状有姿” で提供され、本冊子に記載されている情報や見解 (URL 等のインターネット Web サイトに関する情報を含む) は、将来予告なしに変更されることがあります。

本冊子は、Microsoft 製品の無体財産権に関する法的な権利をお客様に許諾するものではありません。内部的な参照目的に限り、本冊子を複製して使用することができます。

2017 年 11 月公開 バージョン 1.0

個人情報保護に関する世界的な新基準 ——

EU 一般データ保護規則（GDPR）とは

2018 年 5 月※1、EU（欧州連合）において個人情報保護に関する新しい法律「EU 一般データ保護規制（GDPR）」が施行されます。GDPR は個人のプライバシーの権利の保護と確立を目的としており、個人データを管理および保護する方法を制御するためのさまざまな要件を定めた法律です。
GDPR は個人のプライバシーの権利を明確にして確立するための重要な一歩であり、これにより、これからの時代に求められる厳格かつ世界的なプライバシー要件が確立されることになります。
GDPR は EU 圏内に所在する組織だけでなく、EU と取引のあるすべての組織が対象となるため、現在、日本を含む世界中の組織において GDPR 準拠に向けた取り組みが進められています。

※1　2018 年 5 月 25 日より適用開始となる予定です

GDPR の主要な要素

GDPR は 1995 年から運用されてきた「EU データ保護指令」に代わる新しい規則であり、個人のプライバシーの権利の強化やデータ保護の義務の厳格化などに関する要件が盛り込まれています。GDPR の主要な要素は次のとおりです。

個人のプライバシーの権利の強化

個人が持つ権利

- 自分の個人データへのアクセス、不正確さの修正、削除
- 自分の個人データの処理に対する異議申し立て

データ保護の義務の厳格化

データ保護の要件

- セキュリティ上適切な方法を使用した個人データの保護
- コンプライアンスの確保、データ処理に関する記録保持

プライバシー侵害時の報告の義務化

侵害通知の義務

- 個人データの侵害（情報漏えいなど）が発生した場合、侵害を認識してから 72 時間以内の管轄監督機関への通知

非準拠に対する巨額の制裁金※2

厳しい制裁措置

- 多額の制裁金を科すなど、非準拠に対する厳しい制裁措置
- 意図的であるか不注意であるかにかかわらず適用

※2　2000 万ユーロ（約 26 億円）または前会計年度の世界の年間売上高合計の 4％のいずれか高い方が適用されます。2017 年 10 月 17 日のレート 1 ユーロ 131.96 円で換算

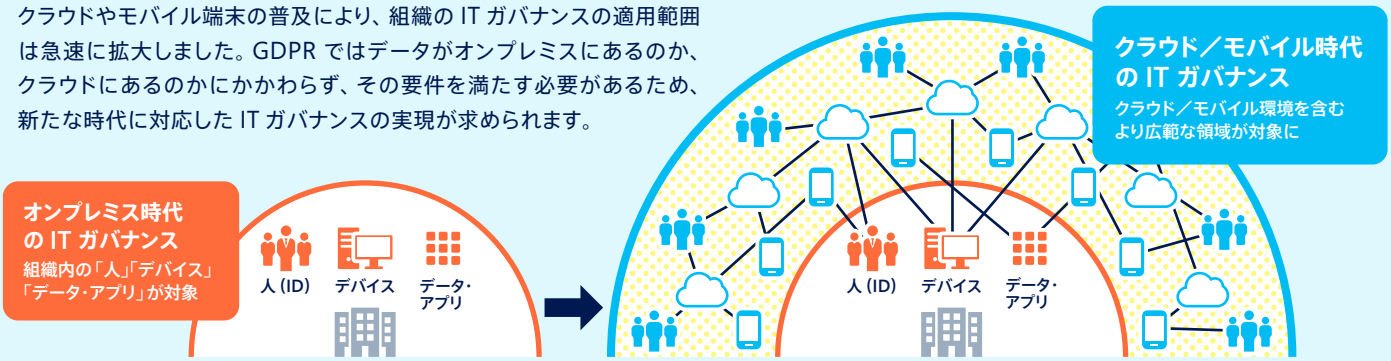
影響を受ける組織

たとえば以下のような場合は、日本の組織であっても規制の対象となります。日本国内で EU 居住者のデータを扱う組織に対しても適用されるため、GDPR が自分たちの組織に適用されるかどうか、また、適用される場合はその範囲を明らかにしておく必要があります。

- EU に拠点があり現地に従業員がいる組織
- EU 居住者に対して商品やサービスを提供している組織
- EU から個人データの処理について委託を受けている組織

クラウド／モバイル時代の IT ガバナンスへ

クラウドやモバイル端末の普及により、組織の IT ガバナンスの適用範囲は急速に拡大しました。GDPR ではデータがオンプレミスにあるのか、クラウドにあるのかにかかわらず、その要件を満たす必要があるため、新たな時代に対応した IT ガバナンスの実現が求められます。



GDPR のプライバシー要件への手立て

保存場所と使用方法に対する制御の強化

- GDPR に準拠した個人データの保存場所と使用方法の管理
- システムおよびプロセスの更新／構築

データ ガバナンス ツールの強化

- 透明性、記録保持、およびレポートに関する新しい要件への対応
- データ侵害の防止、リスクの評価

データ ポリシーの強化

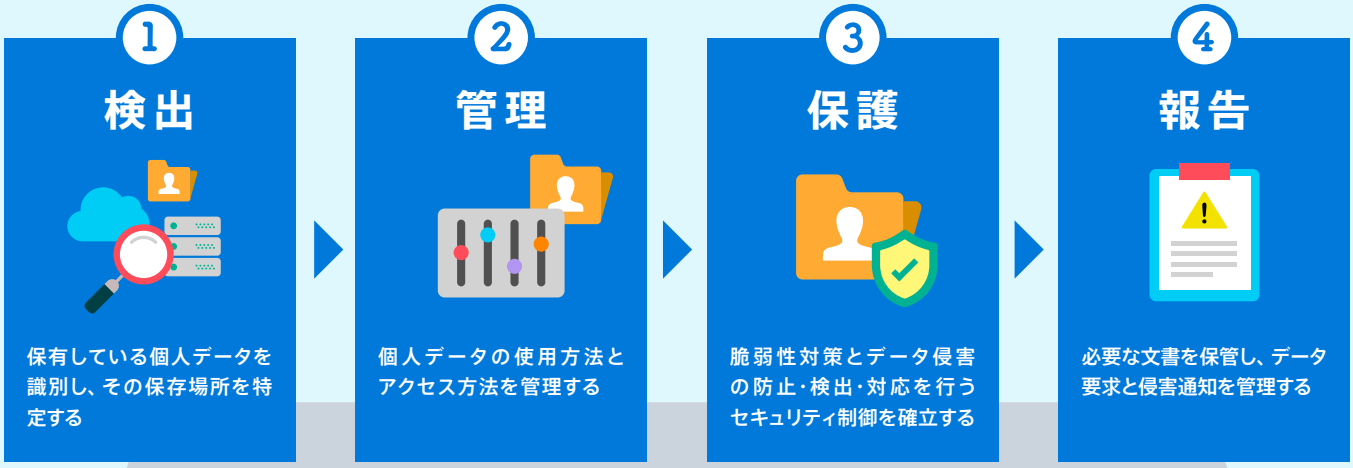
- GDPR に準拠したポリシーの実装
- コンプライアンスを証明するための監査証跡の提供

クラウド／モバイル時代の IT ガバナンスの実現

- シャドー IT を含むアプリの管理、モバイル端末などデバイスの統合管理
- セキュリティ インサイトに基づく ID の高度な保護、データの自動分類など

GDPR 準拠に向けた 4 つのステップ

GDPR に準拠するためには、個人データを扱う専用のレポジトリやアプリケーションにおいて適切な安全対策を講じるとともに、それらレポジトリやアプリケーションから派生する二次データを含めて、IT 環境全体で個人データを厳密に取り扱うようにする必要があります。
マイクロソフトでは、GDPR 準拠のために「検出」「管理」「保護」「報告」という 4 つのステップをご提案しています。
Microsoft 365 Enterprise E5 は、この 4 つのステップで役立つソリューションをご提供し、お客様の GDPR 準拠を支援いたします。



Microsoft 365 Enterprise E5

Office 365 Enterprise E5

クラウド / モバイル時代に求められるデータの保護と IT ガバナンスの実現

Enterprise Mobility + Security E5 (EMS)

Azure Active Directory を基盤とした個人データの使用方法とアクセス方法の管理

Windows 10 Enterprise E5

標的になりやすいクライアント環境を保護する進化したセキュリティ機能

1 検出

保有している個人データを識別し、その保存場所を特定する

最初のステップでは、GDPR が自分たちの組織に適用されるかどうか、また、適用される場合はその範囲を明らかにします。そのために重要になるのが、組織のデータ一覧です。まずは、組織が保有している個人データを識別し、その保存場所を特定することから始めましょう。

GDPR 要件への手立て

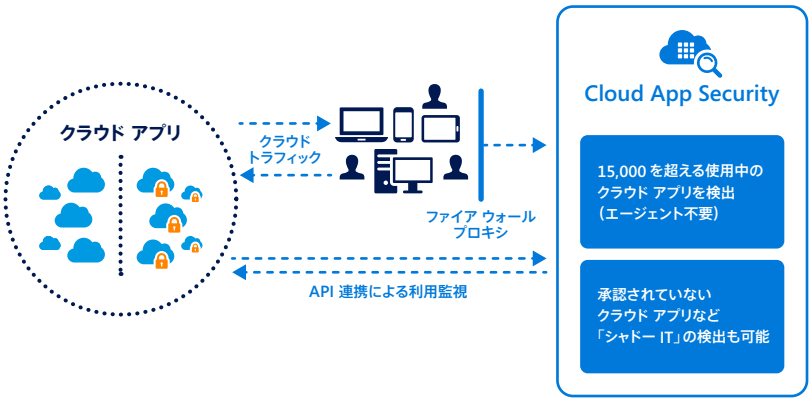
組織内で使用されている クラウド アプリを可視化する	組織が保有している 個人データを把握する	オンプレ (サーバー) にある 個人データについて調査する
▼	▼	▼
クラウド アプリの検出	Office 365 の電子情報開示	オンプレミス、クラウドのスキャン

クラウド アプリの検出

EMS　Cloud App Security

シャドー IT を含むクラウド アプリを可視化

80％以上の従業員が未承認のクラウド アプリを使用していると言われています。Cloud App Security は 15,000 を超えるクラウド アプリを識別し、ネットワーク内で使用されているクラウド アプリの可視化とリスクの評価、継続的な分析を支援します。

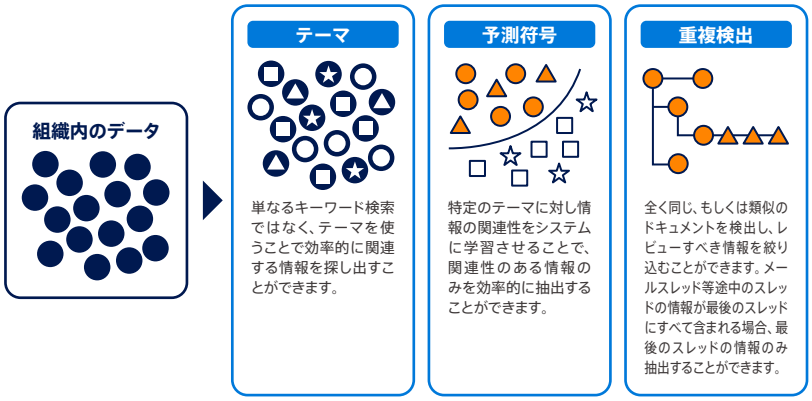


Office 365 の電子情報開示

Office 365　Office 365 Advanced eDiscovery

個人データの調査･分析をサポート

Office 365 Advanced eDiscovery は機械学習により指定したトピックに関連するデータを効率的に抽出する手助けとなる機能です。膨大なデータから関連する情報を見つけ出し、調査、分析を行うための作業負荷とコストの削減に役立ちます。

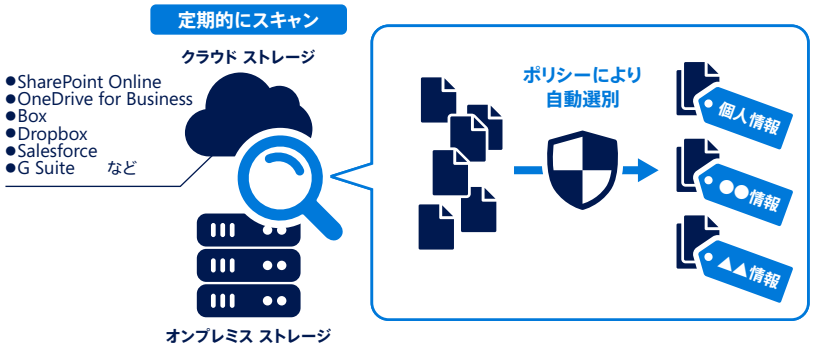


オンプレミス、クラウドのスキャン

EMS　Azure Information Protection (AIP) P2 / Cloud App Security

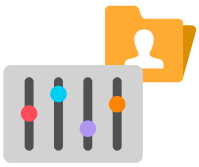
ストレージ内の個人データを検出し自動で保護

AIP には、Office ファイルを分析し自動で保護する機能があります。ファイルサーバーなどを定期的にスキャンして、組織が定めたルールに基づいて個人データを検出･ラベル付けして、暗号化により保護することも可能です。Cloud App Security と連携することで、クラウド ストレージに対しても個人データの検出および保護 (予定) が可能となります。



② 管理　個人データの使用方法とアクセス方法を管理する

GDPR では個人の権利が強化されます。個人データの訂正や削除など、個人データの使用や管理に関する要求に対し、適切に対応しなければなりません。組織は、こうした GDPR の要件を踏まえて、個人データの使用方法や管理に関するポリシー、ロール、責務などを定義し、実装する必要があります。



GDPR 要件への手立て

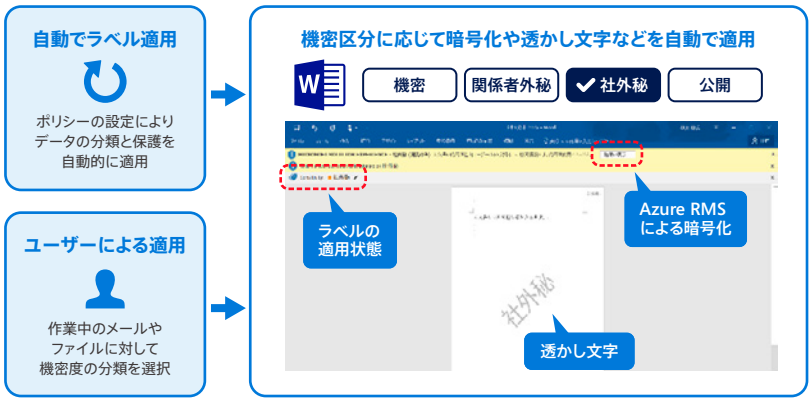
セキュリティ ポリシーの適用漏れを防ぐ	不正アクセスを防ぐために ID の管理を強化する	個人情報が含まれるデータの管理を徹底する
▼	▼	▼
データの自動ラベリング	ID の保護と管理	データのライフサイクル管理

データの自動ラベリング

EMS　Azure Information Protection (AIP) P2

機密区分に応じてデータを分類・保護

Office クライアントでのファイル作成時や変更時にデータを自動的に分類し、保護 (暗号化、認証、使用権) または視覚的なマーキング (透かし文字など) を適用します。分類と保護は、保存場所や共有相手にかかわらず、永続的にデータに適用されます。

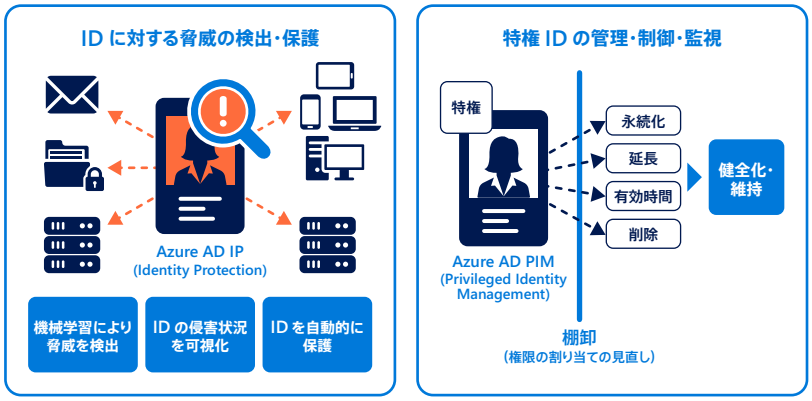


ID の保護と管理

EMS　Azure Active Directory Premium P2

ユーザー ID の統合管理を実現

Azure AD はユーザー ID の統合管理を実現するソリューションです。その機能のひとつである「Azure AD IP」はリスクに晒されている ID を割り出し、自動的に保護します。一方、「Azure AD PIM」は増え続ける特権 ID を可視化し、権限の割り当ての健全化を支援します。

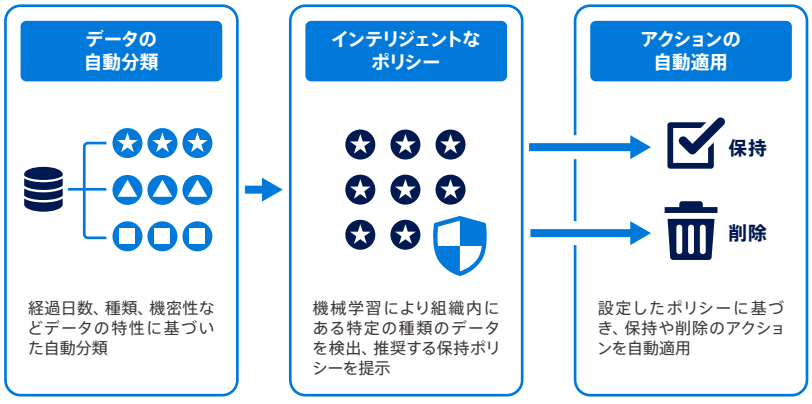


データのライフサイクル管理

Office 365　Advanced Data Governance

分類ポリシー設定、アクションを自動化

機械学習を活用し、Office 365 に保存されているデータのライフサイクル管理を支援します。データの自動分類やデータに基づいた推奨ポリシーの提案、ポリシーに基づいて保持／削除のアクションを自動適用することができます。



③ 保護

脆弱性対策とデータ侵害の防止・検出・対応を行う
セキュリティ制御を確立する

GDPR では、個人データを扱う専用のレポジトリやアプリケーションにおいて適切な安全対策を講じることを求めています。しかし、レポジトリやアプリケーションで安全対策を施していたとしても、PC や ID が乗っ取られてしまうと、個人データが盗まれる可能性があります。こうした脅威には多層の防御策で対処し、PC や ID への攻撃を早期に検知することが重要です。

GDPR 要件への手立て

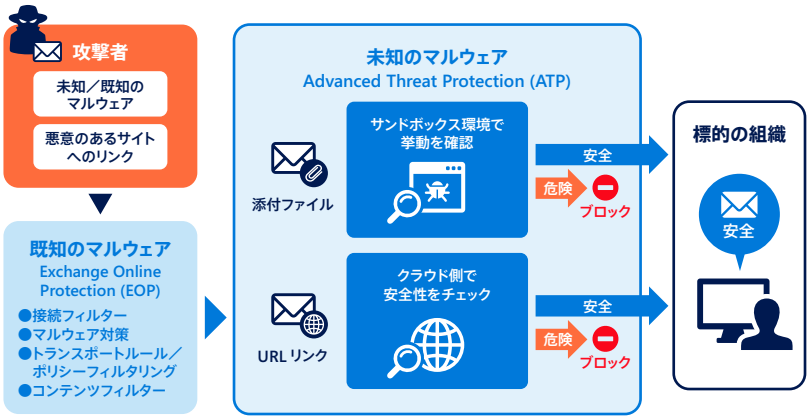
メールを入り口とした未知の攻撃を防ぐ	クライアント端末の資格情報を保護する	万が一、侵入されても被害を最小限に抑える
▼	▼	▼
高度なセキュリティ脅威対策	資格情報の保護	組織全体のクライアント保護

高度なセキュリティ脅威対策

Office 365　Advanced Threat Protection (ATP)

未知のマルウェアからも組織を保護

Office 365 ATP は添付ファイルや URL を利用した攻撃に対してリアルタイムの防御機能を提供します。既知のマルウェアは EOP でブロックし、未知のマルウェアを ATP でブロックします。

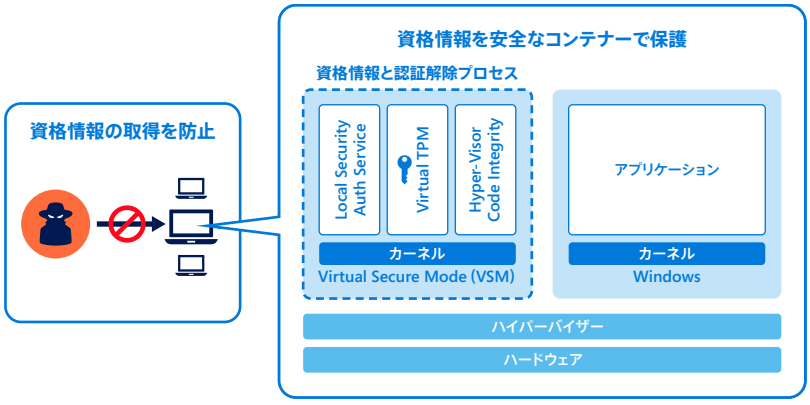


資格情報の保護

Windows 10　Credential Guard

パスワード ハッシュの取得を防止

ユーザーの資格情報をセキュリティで保護された領域に隔離。OS の実行領域とは異なる場所に保管することで、資格情報を不正に取得する “pass-the-hash” などの攻撃から保護します。

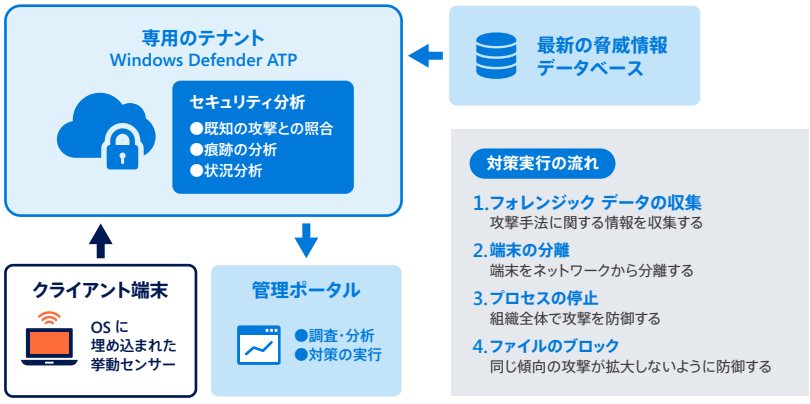


組織全体のクライアント保護

Windows 10　Windows Defender ATP

脅威の検出から調査、分析、対処までを実現

クライアント端末の挙動センサーから収集した情報をもとに、マイクロソフトの脅威データベースを活用して調査、分析を行います。ネットワークを標的とした高度な攻撃をいち早く検出し必要な対策を講じることで、被害の拡大を防ぎます。



④ 報告

必要な文書を保管し、データ要求と侵害通知を管理する

GDPR では、「個人データの侵害が発生した場合、管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから 72 時間以内に個人データの侵害を管轄監督機関に通知しなければならない」という記述があります。準拠するためには、監査ツールなどを活用し、個人データのあらゆる処理の追跡と記録が行える環境を整備しておく必要があります。

GDPR 要件への手立て

ユーザーや管理者の操作情報を詳しく調査する	不正なサインインの発生状況を把握する	いつ・誰が・何をしたのか データの利用状況を追跡する
監査ログ レポート	セキュリティ レポート	ファイル利用のトラッキング

監査ログ レポート

Office 365　Office 365 の監査ログ

ユーザーおよび管理者の操作情報を記録

Office 365 の監査機能を使用して、組織内のユーザーと管理者が何を行ったかを確認できます。メール、グループ、ドキュメント、アクセス許可、ディレクトリ サービスなどに関連するアクティビティを検索することが可能です。該当するユーザーや期間を指定して検索し、結果を CSV 形式でエクスポートすることもできます。

監査ログの検索

該当するユーザーや
アクティビティ、期間を
指定してログを検索

セキュリティ レポート

EMS　Azure Active Directory Premium P1 / Cloud App Security

疑わしいアクティビティを検出

Azure AD にはアプリの利用状況や不正なサインインの発生状況などを把握できる詳細なセキュリティ レポートが用意されています。また Cloud App Security は、普段とは異なる場所からの管理者操作、メールの転送設定、外部への機密情報の共有など疑わしいアクティビティを検出することができます。

アプリの利用状況や
不正なサインインの
発生状況などを把握
することが可能に

ファイル利用のトラッキング

EMS　Azure Information Protection (AIP) P1

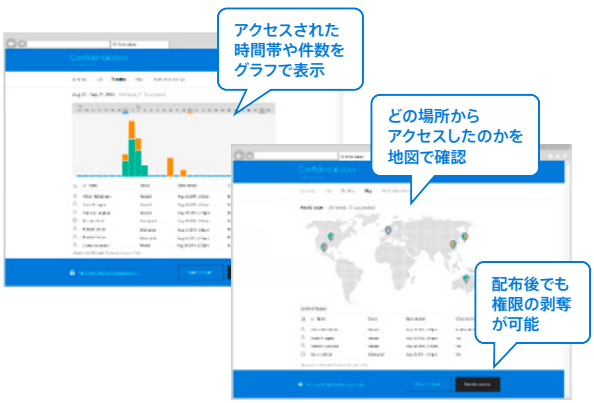
追跡から権限の剥奪までをサポート

事前に分類・保護されたファイルについては、そのファイルにアクセスしたユーザーや時間、場所など、利用状況を追跡して把握できます。また、ファイル自体が暗号化されているため、正規ユーザー以外はデータが読み取れません。外部ユーザーなど範囲を限定して共有した場合でも権限を後から無効化できます。なお ID が盗まれた場合は、ID の無効化やパスワードのリセットで対処できます。

付与されている
アクセス コントロールに
基づいて

- いつ
- 誰が
- 開いたか
- 拒否されたか
- 転送したか

などの
追跡が可能



クラウド／モバイル時代の IT ガバナンスを実現する

Microsoft 365 Enterprise E5

Microsoft 365 Enterprise E5 は、以下の 3 つの「E5」をまとめて利用することができるお得なライセンス プランです。
GDPR 準拠に向けた組織の取り組みを支援し、クラウド／モバイル時代に対応した IT ガバナンスを実現します。

Office 365 Enterprise E5
クラウド／モバイル時代に求められる
データの保護と IT ガバナンスの実現

Enterprise Mobility + Security E5 (EMS)
Azure Active Directory を基盤とした
個人データの使用方法とアクセス方法の管理

Windows 10 Enterprise E5
標的になりやすいクライアント環境を
保護する進化したセキュリティ機能

① 検出	② 管理	③ 保護	④ 報告

Security & Compliance Center
Office 365 に保存されたデータの保護、権限付与などが行えるポータル サイトの提供

データ損失防止
クライアント エンド ポイントをカバーする統合ポリシー

Advanced Data Governance
自動分析と推奨ポリシーに基づいたデータの分類、保存／削除

Azure Information Protection
組織内の機密情報の自動検出、ラベル付け、保護による不当なアクセスの防止

Azure Active Directory (Identity Protection および Privileged Identity Management を含む)
権限のあるユーザーと権限がないユーザーの検出、リソース、アプリケーション、データへのアクセスコントロール。アクセス権の剥奪による情報保護

コンテンツ検索
メールボックス、共有フォルダ、Office 365 Groups、Microsoft Teams、SharePoint Online、OneDrive for Business、Skype for Business を対象とした検索

Data Governance
Exchange Online、SharePoint Online、OneDrive for Business に保存されたコンテンツのアーカイブと保存、および Office 365 組織へのデータのインポート

Advanced Threat Protection
安全な添付ファイルおよび安全なリンク機能を活用した未知のマルウェアからのユーザーの保護

監査ログ
組織内のユーザーや管理者のアクティビティの記録と検索

eDiscovery
アクセス権の管理、関連する情報の保持、検索結果のエクスポート

メールフロールール
特定の条件での組織内のメールの検索･対処

Secure Score
組織のセキュリティ対応状況のスコア化およびセキュリティ強化のための推奨機能の提案

Service Assurance
マイクロソフトコンプライアンス レポートおよび監査状況レポートに基づいたリスク アセスメントの実施のための情報提供

Advanced eDiscovery
機械学習を活用したインテリジェントなシステムによる関連する文書やデータの特定

Exchange Online ジャーナリング
送受信メールの記録 (法律、規制、コンプライアンスの要件への対処)

Cloud App Security
組織内のセキュリティ状況の可視化およびポリシーによるセキュリティ制御 (ユーザー アカウントの停止やアクセス権の剥奪)

Customer Lockbox
トラブルシューティングの際のマイクロソフト サポートエンジニアによるお客様データへのアクセス制御

Cloud App Security
組織内のセキュリティ状況の可視化およびポリシーによるセキュリティ制御 (ユーザー アカウントの停止やアクセス権の剥奪)

情報管理ポリシー
SharePoint Online 上でのコンテンツの保持期間の制御、コンテンツを使用しているユーザーの監査、文書へのバーコード／ラベル付け

Microsoft Intune
モバイルデバイス、モバイル アプリケーション、PC が管理できるクラウド ベースの管理基盤の提供。セキュリティを維持しながら、さまざまなデバイスから会社のアプリケーション、データ、リソースにアクセスする環境の提供

Windows イベントログ
管理者が OS、アプリ、ユーザーアクティビティを把握できる詳細なログ機能

Windows Search
Windows Search 機能を強化するためのインデックス オプションの構成によるローカルマシン上の個人情報の特定と追跡

Windows 10 Enterprise
Windows Hello、Credential Guard、Device Guard、Defender ATP、BitLocker、Windows Information Protection といったセキュリティ機能による OS の保護

マイクロソフト クラウドサービスは、GDPR への準拠を契約に明記しています。
Online Services Terms (https://www.microsoft.com/ja-jp/licensing/product-licensing/products.aspx)

GDPR 準拠に向けた対応については
下記パートナーまでご相談ください。

EY アドバイザリー・アンド・コンサルティング株式会社
https://www.eyadvisory.co.jp/

EY の弁護士、IT 等の専門家が GDPR へのグローバルな支援を
ワンストップでご提供いたします。

✉ お問い合わせ先 AS-Markets@jp.ey.com（または Web のお問い合わせフォームより）

KPMG コンサルティング株式会社
kpmg.com/jp/cyber

152 ヵ国のグローバルネットワークにより、
個人データ保護法制への対応をご支援します。

✉ お問い合わせ先 cybersecurity@jp.kpmg.com

PwC コンサルティング合同会社
https://www.pwc.com/jp/ja.html

PwC Global Network で培った GDPR のナレッジおよび
メソドロジーを活用した対応策のご支援を提供します。

✉ お問い合わせ先 pwckk.microsoft.team@jp.pwc.com

（掲載順：五十音順）

Microsoft 365 に関する最新情報は
https://www.microsoft.com/ja-JP/Microsoft-365 をご覧ください。

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■インターネットホームページ　http://www.microsoft.com/ja-jp/
■日本マイクロソフト株式会社　0120-166-400　営業時間：月曜日～金曜日 9:00 ～ 17:30（祝日除く）

電話のおかけ間違いにご注意ください。

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー