

法人向け



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 の適用は事実特定のうえ、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

© 2017 Microsoft. All rights reserved.

# 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<sup>※1</sup>、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 一般データ保護規則 (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<sup>※2</sup>



#### 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

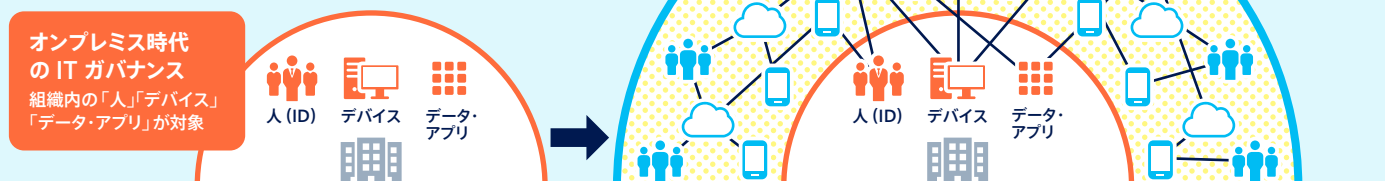


EU から個人データの処理に  
ついて委託を受けている組織



## 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

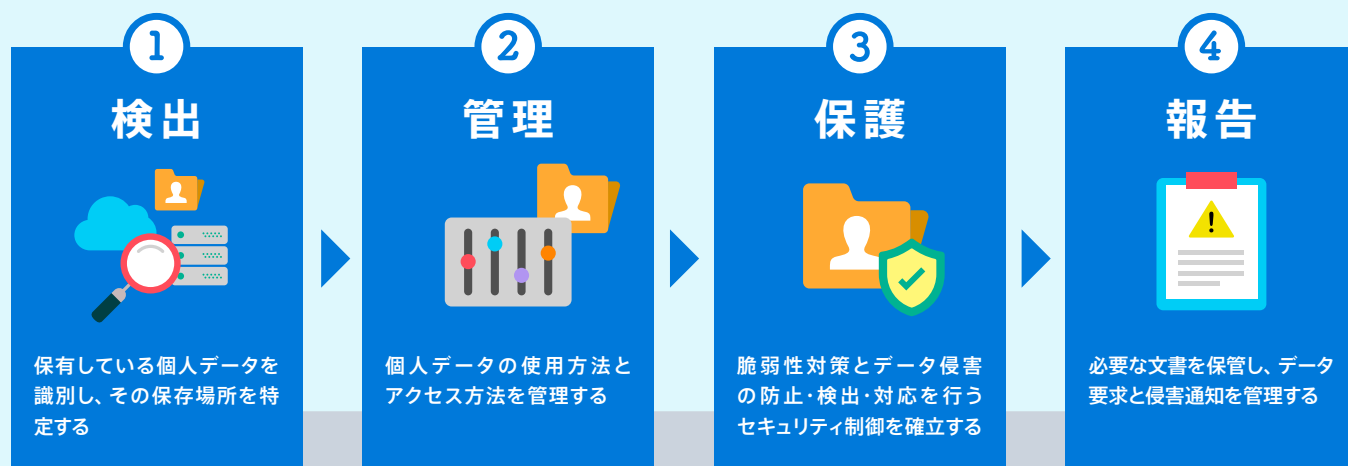
- GDPR に準拠したポリシーの実装
- コンプライアンスを証明するための監査証跡の提供

### 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

クラウド アプリの検出

組織が保有している  
個人データを把握する

Office 365 の電子情報開示

オンプレ (サーバー) にある  
個人データについて調査する

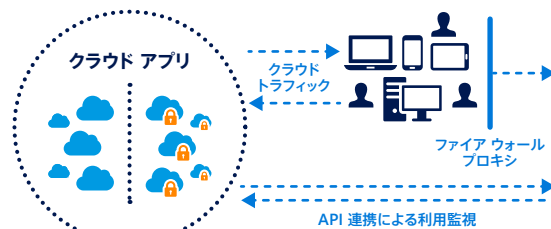
オンプレミス、クラウドのスキャン

## 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。



Cloud App Security

15,000 を超える使用中の  
クラウド アプリを検出  
(エージェント不要)

承認されていない  
クラウド アプリなど  
「シャドー IT」の検出も可能

## 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担とコストの削減に役立ちます。



テーマ

単なるキーワード検索ではなく、テーマを使うことで効率的に関連する情報を探し出すことができます。

予測符号

特定のテーマに対し情報の関連性をシステムに学習させることで、関連性のある情報のみを効率的に抽出することができます。

重複検出

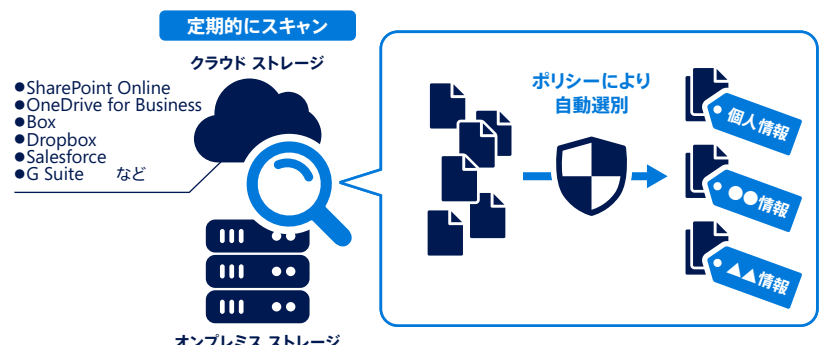
全く同じ、もしくは類似のドキュメントを検出し、レビューすべき情報を絞り込むことができます。メールスレッド等途中のスレッドにすべて含まれる場合、最後のスレッドの情報のみ抽出することができます。

## 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。

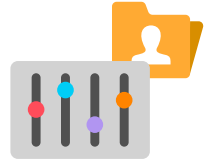




## 2 管理

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、ルール、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

データの自動ラベリング

不正アクセスを防ぐために  
ID の管理を強化する

ID の保護と管理

個人情報が含まれる  
データの管理を徹底する

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。

自動でラベル適用

ポリシーの設定により  
データの分類と保護を  
自動的に適用

ユーザーによる適用

作業中のメールや  
ファイルに対して  
機密度の分類を選択

機密区分に応じて暗号化や透かし文字などを自動で適用



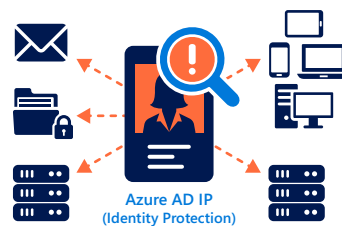
### ID の保護と管理

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。

ID に対する脅威の検出・保護

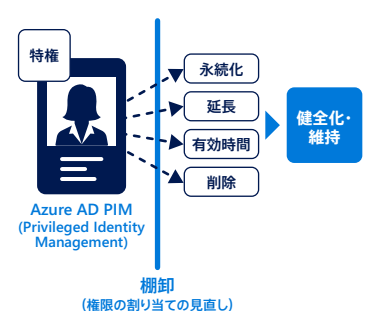


機械学習により  
脅威を検出

ID の侵害状況  
を可視化

ID を自動的に  
保護

特権 ID の管理・制御・監視



### 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。

データの  
自動分類



経過日数、種類、機密性など  
データの特性に基づいた  
自動分類

インテリジェントな  
ポリシー



機械学習により組織内  
にある特定の種類のデータ  
を検出、推奨する保持ポリ  
シーを提示

アクションの  
自動適用



設定したポリシーに基づ  
き、保持や削除のアクシ  
ョンを自動適用

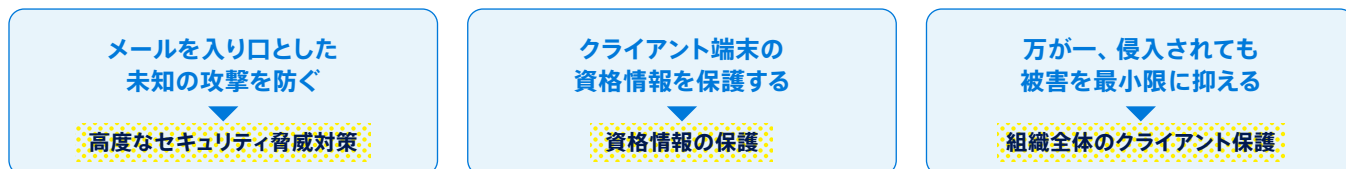
### 3 保護

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

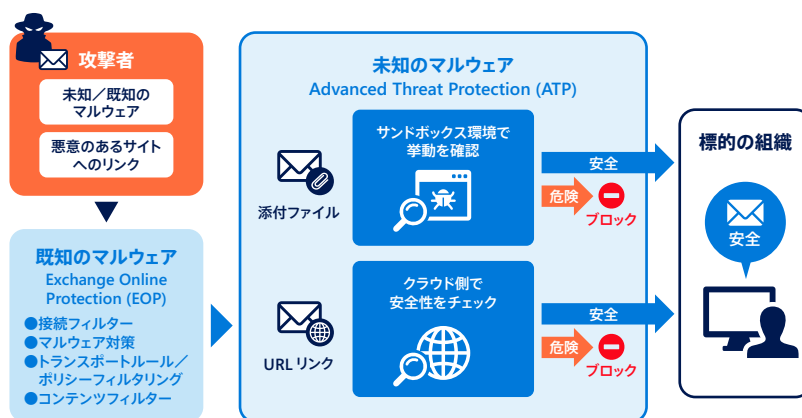


#### 高度なセキュリティ脅威対策

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。

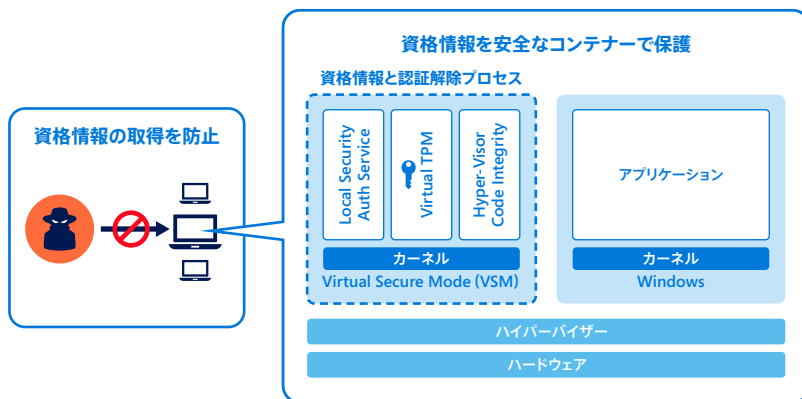


#### 資格情報の保護

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。

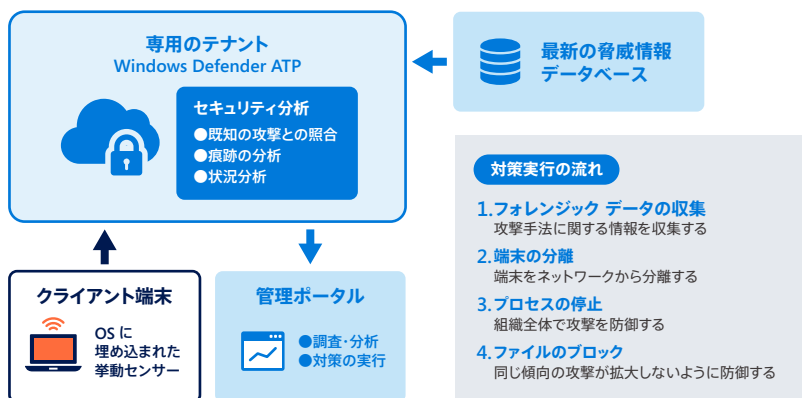


#### 組織全体のクライアント保護

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

監査ログ レポート

不正なサインインの  
発生状況を把握する

セキュリティ レポート

いつ・誰が・何をしたのか  
データの利用状況を追跡する

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



ファイルへの  
アクセス



ファイルの  
変更



ファイルの  
削除



メールボックスへの  
サインイン



メールボックスからの  
メッセージの削除

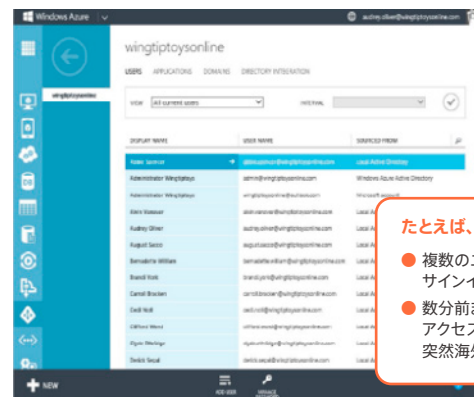
### セキュリティ レポート

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



たとえば、

- 複数のエラー発生後にサインインしている…
- 数分前まで東京からアクセスしていたのに突然海外からアクセス…

### 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

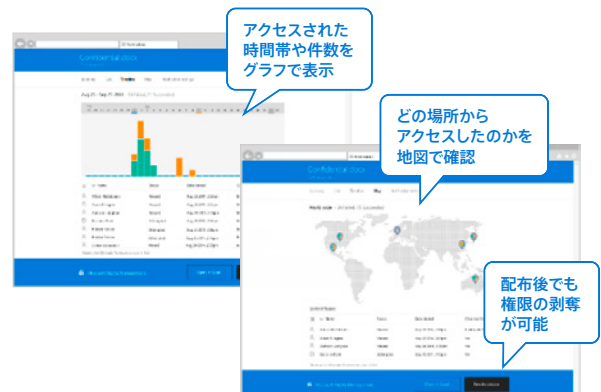
誰が

開いたか

拒否されたか

転送したか

などの  
追跡が可能



アクセスされた  
時間帯や件数を  
グラフで表示

どの場所から  
アクセスしたのかを  
地図で確認

配布後でも  
権限の剥奪  
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 対応支援

EU で 2018 年 5 月の施行が予定されているプライバシー法制 GDPR (一般データ保護規則) では、厳格な規制内容とともに違反企業に最大で連結売上高の 4%、または 2,000 万ユーロまでの制裁金を科す罰則規定が存在します。また EU 域外の会社を対象とした広域な適用範囲を特徴としています。KPMG では、グローバル企業が保有するプライバシーデータを、GDPR の要求事項を充足させながら安全に管理・運用する仕組みの構築を支援します。

### ■ KPMG が考える GDPR で対応すべき 5 つの領域

多岐にわたる領域への対応に対して、組織横断的な取組みを支援します。

領域	法令要件	主な対応内容
1. ガバナンス構築	責任体制の整備	CPO・DPO・代理人等の役割・責任の設定および任命
	国際移転の保護措置整備	SCC のテンプレート策定・締結
	データ保護方針の策定	プライバシーポリシー等の作成
	DPIA の実施	DPIA 実施体制の整備、実施記録の取得
	法令遵守の徹底	教育体制の整備、コンテンツの制作、教育実施、記録の取得
	法令遵守の証明	監査体制の整備、監査計画の立案、監査実施、記録の取得
2. インシデント報告	当局・データ主体等への報告	インシデント発生時のエスカレーションフロー、対応体制の整備
	個人データ侵害の記録	記録保管体制の整備、記録方法の整備、記録の取得
3. 取引先管理	適切な取引先の選定	取引先選定体制の整備、取引先選定基準の整備
	取引先との契約締結	契約確認体制の整備、標準契約書の作成、取引先アセスの実施
4. プロセス整備	適切な情報提供・同意取得	データ主体への情報の通知、同意取得の内容・方法の整備
	取扱いの記録保管	データマッピング実施、台帳整備手順の整備、台帳の整備
	個人データ取扱手順の整備	個人データ取扱規程・手順書等の作成
	データ主体の権利への対応	問い合わせ体制の整備、問い合わせ対応手順の整備
5. システム対応	リスクに応じた技術的措置	リスクに応じたシステム分類と技術的措置の整理、システム改修
	システム開発・保守態勢の整備	影響評価に基づいた要件定義等、開発・保守態勢の整備
	インシデント対応態勢の整備	インシデント 72 時間対応態勢の整備、モニタリング方法の整備

### ■ 優先対応領域の明確化

KPMG では、3 つの方針で優先対応領域を明確化し、迅速かつ確実な GDPR 対応を支援します。

#### 【方針 1】リスク分析に基づく優先対応

プライバシーデータはその内容や件数によってリスクが異なります。**GDPR 対策は、リスクに応じて優先順位を定めて行います。**

情報システムの優先順位

- α XXX システム
- β XXX システム
- γ XXX システム

委託先の優先順位

- 1 XXX 委託先
- 2 XXX 委託先
- 3 XXX 委託先

#### 【方針 2】システム対策の優先対応

システム改修には相応の期間を要するため、「システム対策の強化」についてはワークストリームを分け、**要対応事項を早期に決定**します。

GDPR で求められるシステム要件

- 個人データの仮名化および暗号化
- データの機密性、完全性、可用性を確保し、システム復旧を確実にする機能
- 事故や障害が発生した際も、速やかに復旧し個人データにアクセスできる機能
- セキュリティを確実にするため技術的および組織的対策を定期的に点検および評価するプロセス

UK やアイルランドの監督機関 (ICO、DPO 等) のガイドライン等をベースに要件を早期に決定

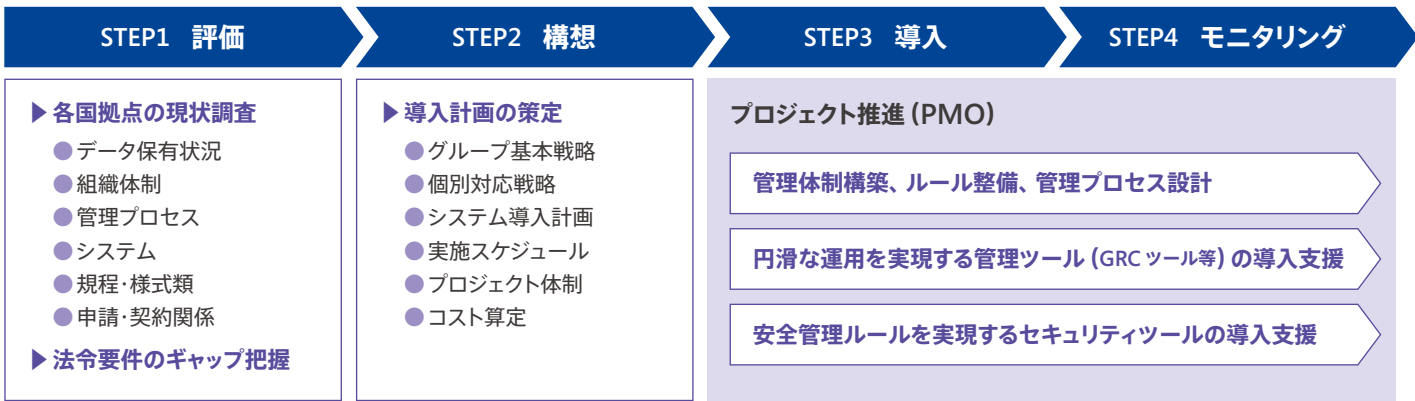
#### 【方針 3】厳罰事項への優先対応

GDPR の罰則金設定は、違反事項により 2 種類の上限が定められています。**より厳しい罰則金が適用される事項を最優先で対応**します。

罰則金	違反事項
売上高 4%、または 2,000 万ユーロのいずれか高い方	<ul style="list-style-type: none"> <li>● 個人データ処理に係る違反</li> <li>● 処理の合法性に係る違反</li> <li>● 同意取得の条件に係る違反</li> <li>● 特別データの処理に係る違反</li> <li>● データ主体の権利に係る違反</li> <li>● EU 域外への移転に係る違反</li> <li>● 当局からの命令に係る違反</li> </ul>
売上高 2%、または 1,000 万ユーロのいずれか高い方	<ul style="list-style-type: none"> <li>● 未成年データに係る違反</li> <li>● DPO の任命に係る違反</li> <li>● 処理者の義務に係る違反</li> <li>● セキュリティ対策に係る違反</li> <li>● 当局等への通知に係る違反</li> <li>● プライバシーリスク影響評価に係る違反</li> </ul>

## ■ GDPR 対応支援サービスの対応ステップ

KPMG は、グローバルのプライバシーデータ管理態勢を構築するにあたり、グループ企業全社、全拠点を対象に、既存のプロセスの評価から制度設計・導入・モニタリングまでのサービスをワンストップで提供します。



## ■ KPMG の強み

<p><b>多岐にわたる実施事項と関係者を取りまとめ、全体コーディネート最適化を支援</b></p> <p>KPMG では Global Privacy Advisory Service を立ち上げており、1,700 名以上のサイバーセキュリティプロフェッショナルが連携してサービスを適用できる体制を整えています。類似プロジェクトの経験も豊富に有しており、企業における多岐にわたる実施事項等を取りまとめ、最適な全体コーディネートの実現を支援します。</p>	<p><b>業務実態を把握しながら現実的なルールの設定・導入を調整</b></p> <p>KPMG では、各国においてプライバシーデータ管理態勢の構築支援や関連法制へのコンプライアンス支援サービスを提供しています。特に企業の各部門との調整を行いながらの管理レベルの設定や取扱いルールの策定等において、経験・ノウハウが豊富であり、業務実態を把握しつつ現実的なルールの設定や導入の実現を支援します。</p>	<p><b>言語の壁を越えた着実なコミュニケーション</b></p> <p>KPMG では、世界 154 カ国のメンバーファームに約 200,000 名の精鋭スタッフを擁し、うち主要 36 カ国 75 都市に日本人および日本語対応可能なプロフェッショナルを有しており、適宜連携することにより、プロジェクトの遂行を支援します。</p>
--	---	--

## ■ 支援実績例

製造・販売	EU 一般データ保護規則への移行に伴う管理態勢見直し支援
家電	PIA 実施プロセス・ルール等の整備支援 (EU 一般データ保護規則の DPIA 対応含む)
製薬	企業グループにおける国際データ移転スキームの整備支援 (EU 一般データ保護規則、SCC 締結等の国際移転規制対応含む)
食品	EU 一般データ保護規則への移行に伴う管理態勢見直し支援
広告代理店	プライバシーデータ管理態勢構築支援 (EU 一般データ保護規則対応含む)
金融	EU 一般データ保護規則への移行に伴う管理態勢見直し支援
総合商社	企業グループにおける情報管理態勢見直し支援 (EU 一般データ保護規則対応含む)
インターネットサービス	IT およびセキュリティ部門に係る EU 一般データ保護規則対応支援
旅行代理店	EU 一般データ保護規則への移行に伴う管理態勢見直し支援



### KPMG コンサルティング株式会社 サイバーセキュリティアドバイザー

〒100-0004 東京都千代田区大手町 1-9-5 大手町フィナンシャルシティ サウスタワー  
TEL: 03-3548-5111

✉ [cybersecurity@jp.kpmg.com](mailto:cybersecurity@jp.kpmg.com)

🌐 [www.kpmg.com/jp/gdpr](http://www.kpmg.com/jp/gdpr)

本ページで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくは KPMG コンサルティング株式会社までお問い合わせください。  
ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2018 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ( "KPMG International" ), a Swiss entity. All rights reserved.  
The KPMG name and logo are registered trademarks or trademarks of KPMG International.

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。

※記載されている会社および、製品名は、各社の商標または登録商標です。  
※記載されている情報は、2018 年 2 月現在のものです。  
※製品の仕様は、予告なく変更する場合があります。あらかじめご了承ください。

マイクロソフト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。



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