一般データ保護規則 (GDPR) への対応を開始する

Microsoft Cloud による GDPR 準拠の促進

Microsoft

2017 年 5 月版

目次

免責事項

このホワイト ペーパーは、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、このホワイト ペーパーは、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、このホワイト ペーパー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。このホワイト ペーパーは "現状有姿" で提供され、このホワイト ペーパー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。

このドキュメントは、Microsoft 製品の無体財産権に関する法的な権利をお客さま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、このホワイト ペーパーを複製して使用することができます。

2017 年 5 月公開
バージョン 1.1

はじめに

2018 年 5 月 25 日に、欧州でプライバシーに関する法律が発効となる予定ですが、これによって、プライバシーの権利、セキュリティ、コンプライアンスに関する世界的な新しい基準が設けられることになります。

この一般データ保護規則 (GDPR) は、基本的に個人のプライバシーの権利の保護と確立を目的としています。GDPR によって、データの送信、処理、保存を行う場所にかかわらず、個人の選択を尊重しながら、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厳格で世界的なプライバシー要件が確立されます。

マイクロソフトとお客様には、GDPR のプライバシーに関する目標を達成するために尽力することが求められます。マイクロソフトでは、プライバシーを基本的な権利ととらえており、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ると考えます。しかしながら、GDPR によって、世界中の組織に大きな変更が必要となることも認識しています。

GDPR に対する取り組みは困難だと思われるかもしれませんが、マイクロソフトがお手伝いいたします。

マイクロソフトの GDPR への取り組み

マイクロソフトのミッションは、世界のすべての個人と組織がより多くのことを達成できるようサポートすることであり、その中核となるのが信頼です。マイクロソフトは、信頼構築に対する原則に基づいたアプローチを取ることで、プライバシー、セキュリティ、透明性を確保できるよう配慮しています。マイクロソフトは、GDPR への準備を行う際にこれらの原則を適用しています。

マイクロソフトは、GDPR 準拠は共同責任であると理解しています。このような理由から、マイクロソフトは、2018 年 5 月 25 日の GDPR 適用開始時にはマイクロソフトのクラウド サービス全体で GDPR 準拠を完了できているよう全力を尽くしています。

また、複雑な規制への準拠における当社の経験を共有することで、皆様の組織が GDPR のプライバシー要件への対応に向けた最善の手順を決めるお手伝いをさせていただきます。マイクロソフトは、クラウドプロバイダーの中でもきわめて包括的なコンプライアンス/セキュリティのオファリングと巨大なパートナー エコシステムを用意し、現在および将来のお客様のプライバシーとセキュリティの取り組みを支援できる体制を整えています。

GDPR 準拠への取り組みにお客様と連携して当たることの一環として、お客様の準備に役立てていただくために、このホワイト ペーパーを作成しました。本書では、GDPR の概要と、GDPR への準備のためにマイクロソフトが取り組んでいる内容について説明します。また、お客様が GDPR 準拠への取り組みを開始するために、今すぐマイクロソフトと共に実行できる手順の例を共有します。

この重要な新しい法律に準拠して、その過程で個人のプライバシー保護を進めるうえでマイクロソフトがどのようにお客様を支援できるかについて、さらに最新情報を共有できることを楽しみにしています。その他のリソースと、特定の GDPR 要件を達成するためにマイクロソフトがどのようにお客様を支援できるかの詳細については、Microsoft Trust Center の GDPR のセクションを参照してください。

GDPR 概要

マイクロソフトがお客様の GDPR への準備を具体的にどのような方法で支援できるかの説明に入る前に、この規制と、お客様に対する影響について、最も基本的かつ重要な疑問を解決していきたいと思います。より詳しい概要については、ここを参照してください。

GDPR とは何ですか?

一般データ保護規則 (GDPR) は、欧州連合 (EU) 全体を対象にした新しいプライバシー規制です。GDPR は個人に対し、自分の個人データの管理の強化、データ使用の透明性の確保、データ保護のためのセキュリティと制御の義務化を要求するものです。

GDPR は私の組織に適用されますか?

GDPR は、一見した感じよりも広範に適用されます。この法律は、欧州連合 (EU) 圏内の個人に商品やサービスを提供したり、EU 加盟国の居住者に結び付けられたデータを収集/分析したりする企業、政府機関、非営利団体、およびその他の組織に新しい規則を課すもので、EU 内に設立された組織、EU 内で商品やサービスを提供する組織、または EU 加盟国の居住者の行動を監視する組織に適用されます。

他の管轄区域のプライバシー法とは異なり、GDPR はあらゆる規模および業種の組織に適用されます。EU は国際的にプライバシー問題に関するロール モデルと見なされることが多いため、GDPR の概念はいずれ世界の他の地域でも採用されると思われます。

GDPR はいつ発効しますか?

GDPR は 2018 年 5 月 25 日に発効します。1995 年から施行されている既存のデータ保護指令 (指令 95/46/EC) は GDPR に置き換わることになります。GDPR は実際には EU 内で 2016 年 4 月に制定されましたが、この規制に準拠するために一部の組織で必要になる大幅な変更を考慮に入れて、2 年間の移行期間が設定されました。

GDPR で重要な概念は何ですか?

GDPR は次の 6 つの原則を軸に構成されています。

- 個人データを処理および使用するうえでの透明性を義務化する。
- 個人データの処理を特定された正当な目的に限定する。
- 個人データの収集および保管を意図された目的に限定する。
- 個人による自分の個人データの修正および削除要求を可能にする。
- 個人を識別可能なデータの保管を、意図された目的のために必要な期間のみに限定する。
- セキュリティ上適切な方法を使用して個人データが保護されるよう徹底する。

これらの原則に関連する GDPR の要件の例にはどのようなものがありますか?

- GDPR の下では、個人は、組織が自分の個人データを処理しているかどうかを知り、その処理の目的を理解する権利があります。個人が持つ権利には、自分のデータを削除または修正してもらう権利、今後処理しないよう要求する権利、ダイレクト マーケティングに異議を唱える権利、および自分のデータの特定利用への同意を取り消す権利があります。データの携行性の権利は、自分のデータを別の場所に移動したり、その際に支援を受けたりする権利を個人に与えるものです。

- GDPR では、個人データをその機密度に従ってセキュリティで保護することが組織に求められます。データ侵害が発生した場合、データ管理者は、通常 72 時間以内に当局に通知する必要があります。さらに、侵害が、個人の権利および自由に高いリスクをもたらす結果となる可能性がある場合、組織は影響を受ける個人にも遅滞なく通知する必要があります。

- 個人データを処理するには法的根拠が必要です。個人データの処理についての同意は、"自由に申し出ることができ、明確で、情報に基づき、あいまいではない" 必要があります。GDPR で子供を保護するために、固有の同意要件があります。

- 組織は、データ保護影響評価を実施して、プロジェクトがプライバシーに及ぼす影響を予測し、必要に応じてリスク軽減策を採用する必要があります。処理活動、データ処理への同意、および GDPR 準拠の記録を維持する必要があります。

- GDPR 準拠は 1 回限りの活動ではなく、継続的なプロセスです。GDPR 準拠を怠った場合、多額の罰金が科せられる可能性があります。GDPR に確実に準拠するには、個人データの点で個人の利益を守るため、プライバシーを重視する文化を組織に取り入れることを推奨します。

GDPR のより詳しい概要を参照する場合、および仮名化、処理、管理者、処理業者、データ主体、個人データなどの用語の理解を深める場合は、Microsoft.com/GDPR にアクセスしてください。マイクロソフトは、お客様が GDPR の要件を満たし、個人のプライバシーの権利をさらにサポートできるよう全力で支援いたします。

GDPR への取り組みにおけるマイクロソフトとの連携

GDPR への準拠は、時間、ツール、プロセス、および専門知識が必要とされるビジネス全体の課題であり、お客様のプライバシーとデータの管理手法に大幅な変更が必要になる可能性があります。適切に設計されたクラウド サービス モデルで事業を運営し、効果的なデータ ガバナンス プログラムを導入していれば、GDPR 準拠への取り組みは、より円滑に進みます。GDPR への準拠を成功させる場合、マイクロソフトおよびその広範なパートナー エコシステムからサポートを得ることができます。

マイクロソフトには、信頼できるクラウド サービスを提供してきた長い歴史があります。マイクロソフトは、プライバシー、セキュリティ、コンプライアンス、および透明性に対する原則に基づいたアプローチを取ることで、ユーザーが信頼できるデジタル技術を安心して利用できるように配慮しています。マイクロソフトは、業界でもきわめて広範なコンプライアンス ポートフォリオを揃えています。クラウドのプライバシー標準である ISO/IEC 27018 など、主な標準規格を初めて採用したのもマイクロソフトです。マイクロソフトはそのプライバシー、セキュリティ、コンプライアンス、および透明性におけるマイクロソフトの経験豊富なリーダーシップにより、お客様とパートナーに貢献しています。

以下に、GDPR に準拠するための準備を行う際に、お客様がマイクロソフトにどのようなことを期待できるかについて説明します。

- **お客様のニーズに合うテクノロジ。**マイクロソフトの幅広いエンタープライズ クラウド サービス ポートフォリオを利用して、個人データの削除、訂正、転送、アクセス、処理に対する異議申し立てなど、さまざまな領域に対する GDPR の義務を果たすことができます。さらに、マイクロソフトのテクノロジを利用する際には、広範なグローバル パートナー エコシステムからエキスパートのサポートを得ることができます。
- **契約責任。**新しい GDPR 要件に従ったタイムリーなセキュリティ サポートと通知など、クラウド サービスの契約責任によってお客様を支援します。2017 年 3 月から、Microsoft クラウド サービスの顧客ライセンス契約には、GDPR の適用開始時に GDPR 準拠を確立できているようにするための契約が追加されています。
- **経験の共有。**マイクロソフトにおける GDPR 準拠への取り組みを共有することで、マイクロソフトの経験を、お客様の組織にとって最善の手順を決める際の参考となるように努めています。

GDPR への取り組みの開始

プラットフォームによる GDPR へのアプローチ

データの作成、保管、分析、および管理に使用するシステムは、個人所有デバイスやオンプレミス サーバー、クラウド サービス、さらにはモノのインターネットまで、さまざまな IT 環境に分散している可能性があります。つまり、お客様の IT 環境のほとんどが GDPR の要件の対象になる可能性があります。

GDPR の要件達成への最適な取り組み方は、全体的な視点と、プライバシーに関する規制および法律上の義務というコンテキスト内で要件を確認することです。たとえば、GDPR では、脆弱性とデータ侵害の防止、検出、および対応のためのセキュリティ制御が要求されますが、その多くは、ISO 27018 クラウド プライバシー標準など、他のデータ保護標準で期待される制御に似ています。

それぞれの標準と規制で必要な制御を個別に追跡するのではなく、それらの要件を満たす全般的な制御と能力を特定することがベスト プラクティスです。同様に、GDPR のような包括的な規制に照らして個々のテクノロジやソリューションを評価するのではなく、プラットフォーム的な視点 (Windows、Microsoft SQL Server、SharePoint、Exchange、Office 365、Azure、および Dynamics 365 を含む視点) でとらえることで、手順が明確になり、GDPR だけでなく他の重要な要件にも確実に準拠できるようになります。

次の 4 つの重要なステップに焦点を合わせて、GDPR 準拠への取り組みを開始することをお勧めします。

- **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します。
- **管理** — 個人データの使用方法とアクセス方法を管理します。
- **保護** — 脆弱性とデータ侵害の防止、検出、および対応を行うセキュリティ制御を確立します。
- **レポート** — データの要求に対応し、データ侵害をレポートして、必要なドキュメントを保管します。

これらの各ステップについて、そのステップの要件に対応するために使用できるマイクロソフトのさまざまなソリューションのツール、リソース、および機能の例の概要が示されています。このドキュメントは包括的な "手引書" ではありませんが、詳細を入手できるリンクが Microsoft.com/GDPR に記載されています。

どれほどたいへんな作業になるかを考えると、GDPR の施行が開始してからの準備では間に合いません。すぐにプライバシー保護とデータ管理の実施方法を見直す必要があります。

以降のセクションでは、GDPR の構成要素それぞれについて特定の要素の概要を説明します。また、マイクロソフトが現在販売している製品とサービスを使用して準備を開始する方法についても説明します。

今すぐアクションを開始

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

GDPR 準拠への最初のステップでは、GDPR がお客様の組織に適用されるかどうか評価し、適用される場合は、その範囲を評価します。この分析は、保有しているデータとその保存場所の特定から始めます。

GDPR は私のデータに適用されますか?

GDPR では、"個人データ" の収集、保存、使用、および共有が規制されます。GDPR では、個人データは、自然人として識別されたまたは識別可能な個人に関連するデータであると、きわめて広義に定義されています。

お客様の組織の顧客データベース、顧客が入力するフィードバック フォーム、電子メール コンテンツ、写真、CCTV 映像、ロイヤルティ プログラムの記録、人事データベース、またはその他の場所に存在するデータ、あるいは収集しようとしているデータが EU 加盟国の居住者に属するか関連している場合は、GDPR に準拠する必要があります。GDPR に準拠するために個人データを EU 圏内に保存する必要はありません。GDPR は、データが EU 加盟国の居住者に関連している場合は、EU 圏外で収集、処理、または保存されるデータにも適用されます。

データの一覧の構築

GDPR がお客様の組織に適用されるどうか、また適用される場合は課される義務は何かを理解するには、組織のデータの一覧を作成することが重要です。これにより、どれが個人データであるかを判断し、データの収集と保存が行われているシステムを特定できるほか、収集された理由、処理と共有の方法、および保持期間を把握することができます。

次に、マイクロソフトのクラウドおよびオンプレミスのオファリングが、GDPR 準拠の最初のステップを支援する具体的な例を紹介します。

Azure

Azure は、柔軟性の高いオープン クラウド プラットフォームであり、データ ソースを簡単に検出し、特定できるようにするサービスが含まれています。Microsoft Azure Data Catalog は、組織のデータ ソースの登録システムおよび検出システムとして機能する完全に管理されたクラウド サービスです。つまり、Azure Data Catalog は、データ ソースを検出、把握、および使用して、既存のデータからより多くの価値を得られるよう支援するものです。Azure Data Catalog にデータ ソースを登録すると、そのメタデータにインデックスが付けられるため、必要なデータの検索と検出が簡単になります。

Dynamics 365

Dynamics 365 は、Dynamics 365 のレポートおよび分析ダッシュボードから使用可能な、個人データを識別するためのいくつかの可視化および監査の機能を提供します。

- Dynamics 365 には、XML や SQL ベースのクエリを使用せずにレポートを簡単に作成できるレポート ウィザードが含まれています。
- Dynamics 365 のダッシュボードでは、ビジネス データの概要を表示できます。このデータは、組織全体で表示できる操作可能な情報です。
- Microsoft Power BI は、データの検出、分析、および可視化に使用できるセルフサービス ビジネス インテリジェンス (BI) です。これらの洞察は、同僚と共有したり共同作業で使用したりできます。

Enterprise Mobility + Security (EMS) E3 スイート

Enterprise Mobility + Security は ID ベースのセキュリティ テクノロジを特徴とし、組織が保有する個人データの検出、制御、および保護のほか、潜在的な盲点の発見や、データ侵害発生時の検出にも役立ちます。

Microsoft Cloud App Security は、クラウド アプリケーション内のデータの高度な可視性、包括的な制御、および保護の強化を提供する包括的なサービスです。可視性によって、組織のネットワーク内で使用されているクラウド アプリを把握し (すべてのデバイスから 1 万 3,000 を超えるアプリを識別できます)、リスク評価と継続的な分析を取得できます。

Microsoft Azure Information Protection は、どのような機密データがどこにあるのかを特定するのに役立ちます。特定の機密度でマーキングされているデータを照会することも、ファイルまたは電子メールの作成/変更時に機密データをインテリジェントに識別することもできます。識別されたデータは、企業が選択したポリシーに基づいて自動的に分類またはラベル付けすることができます。

Office 365

特に個人データへのアクセスの特定または管理に役立つ Office 365 ソリューションがあります。

- Office および Office 365 のデータ損失防止 (DLP) では、財務情報、医療情報、個人を特定できる情報などの 80 種類を超える一般的な機密データを識別できます。
- Office 365 セキュリティ/コンプライアンス センターのコンテンツ検索では、メールボックス、パブリック フォルダー、Office 365 グループ、Microsoft Teams、SharePoint Online サイト、One Drive for Business の場所、および Skype for Business の会話を検索できます。
- Office 365 の電子情報開示の検索を使用して、SharePoint Online、OneDrive for Business、Skype for Business Online、および Exchange Online といった Office 365 の資産全体のコンテンツに含まれるテキストおよびメタデータを見つけ出すことができます。

- Office 365 Advanced eDiscovery は、機械学習テクノロジで機能強化されており、特定の情報カテゴリ (コンプライアンスの調査など) に関連するドキュメントを迅速に、また従来のキーワード検索や多量のドキュメントの手動でのレビューより正確に特定できます。Advanced eDiscovery では、機械学習を使用してシステムをトレーニングして、大規模なデータセットをインテリジェントに検索し、関連データに迅速に狙いを定めるようにします。これによってレビューの前にデータを縮小し、関連ドキュメントおよびデータの関係性を特定するコストと作業を大幅に軽減できます。
- アドバンスト データ ガバナンスでは、インテリジェンスと機械支援型洞察を使用して、組織にとって最も重要なデータの検索、分類、ポリシー設定を行い、それらのデータのライフサイクルを管理する措置を取ることができます。

SharePoint

SharePoint Search Service とアプリケーション内の検索機能を利用して、個人データを追跡できます。機密コンテンツを特定および検索するため、SharePoint Server 2016 は、Office 365 と同じデータ損失防止機能を備えています。

SQL Server および Azure SQL Database

SQL 言語を使用して、データベースのクエリ、およびこの要件を可能にするために役立つ可能性のあるツールやサービスのカスタマイズを実行できます。検索はクエリによって十分にサポートされていますが、完全なトレース ログは、アプリケーション レベルで実行する必要があります。スクリプト タスクでは、SQL Server Integration Services が提供する組み込みのタスクや変換では使用できない複雑なデータクエリなどのカスタム機能を実行するコードを使用できます。スクリプト タスクでは、複数のタスクや変換を使用するのではなく、1 つのスクリプトに複数の関数を組み合わせることもできます。この製品スイートには、データの洞察へのエンド ユーザー アクセスを提供する強力なビジネス インテリジェンス機能も含まれています。

Windows および Windows Server

Windows 内のデータを検索するには、Windows Search を利用して、ローカル コンピューターや、適切なアクセス許可を持っている接続デバイス上の個人データを追跡、特定できます。Windows Search の機能を強化して対象データを検索するには、[コントロール パネル] の [インデックスのオプション] を構成して Windows Search の機能をカスタマイズできます (たとえば、ファイルの内容のインデックスを作成できます)。

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 によって、データが関連している個人であるデータ主体は、自分の個人データが取り込まれ、使用される方法をより強固に制御できるようになります。たとえば、データ主体は、自分に関連しているデータを共有する、他のサービスに転送する、データ内の間違いを修正する、特定の場合に特定のデータの以降の処理を制限するなどの要求をお客様の組織に行うことができます。場合によっては、これらの要求に、決められた期限内で対処する必要があります。

データ ガバナンス

データ主体に対する義務を果たすために、お客様は組織が処理する個人データの種類、処理方法、および処理の目的を理解する必要があります。前述したデータの一覧作成は、この理解を得るための最初のステップです。データの一覧を作成したら、データ ガバナンス計画を作成して実装することが重要です。データ ガバナンス計画は、個人データのアクセス、管理、および使用に関するポリシー、ロール、および責務の定義に役立ち、データ処理方法が GDPR に準拠するよう支援します。たとえば、データ ガバナンス計画によって、組織は、データ主体からのデータの削除や転送の要求に効果的に対処できる自信を得ることができます。

Microsoft クラウド サービス

お客様のデータ ガバナンス戦略をサポートするため、Microsoft クラウド サービスは、マイクロソフトの Privacy-by-Design および Privacy-by-Default の手法を使用して開発されています。データを Azure、Office 365、または Dynamics 365 に預けても、お客様は単独の所有者のままです。つまり、サービスに保存したデータの権利、所有権、および利害はお客様が保持します。

Microsoft クラウド サービスでは、承認されていない人物による不適切なアクセスや使用から顧客データを保護するため、強力な措置を取っています。詳細については、Microsoft Trust Center を参照してください。これらの措置には、マイクロソフトの担当者と下請業者によるアクセスを制限すること、および行政機関による顧客データの要求に対応するための要件を慎重に定義することが含まれます。ただし、お客様は、どのような理由であれ、いつでもご自分の顧客データにアクセスできます。

さらに、法律で禁止されていない限り、行政機関からお客様のデータを求める要求があった場合、マイクロソフトは、その要請をお客様にリダイレクトして、お客様に直接要求が行われるようにします。行政機関はこれまでそのような要求を裁判所で公開することを禁止するよう図ってきましたが、マイクロソフトはそれに異議を申し立ててきた経緯があります。

Microsoft クラウド サービスが正しく管理されるよう徹底すると共に、当社のお客様に保証を提供するため、クラウド サービスは少なくとも年 1 回、HIPAA と HITECH、CSA Star Registry、および複数の ISO 標準を含む複数のグローバルなデータ プライバシー標準に照らして監査されています。これらのレポートは、https://servicetrust.microsoft.com/Documents/ComplianceReports でご覧いただけます。

こうした取り組み以外にも、マイクロソフトは、データがどのように管理されているか、および組織内のだれがどのデータにアクセスできるかを確認するために必要な制御を提供します。

Azure

Azure Active Directory は、クラウドでの ID およびアクセス管理ソリューションです。これは、ID を管理して、Azure、オンプレミス、およびその他のクラウドのリソース、データ、およびアプリケーションへのアクセスを制御します。Azure Active Directory Privileged Identity Management を使用すると、Azure リソースを管理するための一時的な Just-In-Time (JIT) 管理者権限をユーザーに割り当てることができます。

Azure ロールベースのアクセス制御 (RBAC) は、Azure リソースへのアクセスの管理に役立ちます。これにより、ユーザーに割り当てられているロールに基づいてアクセス権を付与できるので、ユーザーが自分の作業を実行するために必要なアクセス許可のみをユーザーに付与することが簡単になります。組織のビジネス モデルおよびリスク許容度に基づいて RBAC をカスタマイズできます。

Office 365

Office 365 ソリューションには、個人データの管理に役立つ機能が複数あります。

- Office 365 セキュリティ/コンプライアンス センターのデータ ガバナンス機能は、Exchange Online メールボックス、SharePoint Online サイト、および OneDrive for Business の場所にあるコンテンツをアーカイブおよび保持したり、データを Office 365 にインポートしたりする場合に役立ちます。
- Office 365 のアイテム保持機能は、必要なコンテンツを保持し、不要になったらコンテンツを削除することで、電子メールとドキュメントのライフサイクルの管理を支援します。
- アドバンスト データ ガバナンスでは、インテリジェンスと機械支援型洞察を使用して、組織にとって最も重要なデータの検索、分類、ポリシー設定を行い、それらのデータのライフサイクルを管理する措置を取ることができます。
- SharePoint Online の情報管理ポリシーでは、コンテンツの保持期間の制御、ユーザーによるコンテンツの操作内容の監査、およびドキュメントへのバーコードまたはラベルの追加を行うことができます。
- Exchange Online のジャーナリングは、受信および送信の電子メール通信を記録することにより、法律、規制、および組織のコンプライアンス要件に対処するのに役立ちます。

データ分類

データの分類は、あらゆるデータ ガバナンス計画における重要な部分です。組織全体に適用される分類スキームの採用は、データ主体の要求に対応する際に特に有用です。このような分類スキームによって、個人データに関する要求をより迅速に特定して処理できるからです。

現在、マイクロソフトはガイダンスとツールを提供して、データ分類の複雑性に対処するのを支援しています。

Azure

Data Classification のホワイトペーパーは、Azure のデータ分類についての具体的なガイダンスを提供し、データ分類の手法、処理、用語、および実装の背後にある原則を段階的に説明しています。このドキュメントには、その他にも大量の情報とリンクが含まれています。

Dynamics 365

「Dynamics 365 (online) のセキュリティおよび準拠計画ガイド」には、ディレクトリ同期やシングルサインオンなどのエンタープライズ ディレクトリ統合サービスを含む環境での Dynamics 365 (オンライン) の展開計画に関連する主要なコンプライアンスおよびセキュリティの考慮事項を理解するための包括的なガイダンスが載っています。これには、データのプライバシーおよび機密性のポリシー、データ分類、および影響に関する情報も含まれています。

Enterprise Mobility + Security (EMS)

Azure Information Protection は、作成時や変更時のデータの分類やラベル付けに役立ちます。さらに、機密データに保護 (暗号化、認証、および使用権) または視覚的なマーキングを適用することもできます。分類ラベルと保護は永続的でデータに付随するため、保存場所や共有相手にかかわらず、常にデータが識別可能で、保護されるようになります。

Office および Office 365

- Office および Office 365 のデータ損失防止 (DLP) では、財務情報、医療情報、個人を特定できる情報などの 80 種類を超える一般的な機密データを識別できます。さらに、機密情報を識別したときに実行する操作を組織で構成して、機密情報を保護し、機密情報が誤って公開されるのを防ぐこともできます。
- アドバンスト データ ガバナンスでは、インテリジェンスと機械支援型洞察を使用して、組織にとって最も重要なデータの検索、分類、ポリシー設定を行い、それらのデータのライフサイクルを管理する措置を取ることができます。自動分析およびポリシー推奨事項に基づいてデータを分類した後、データを適切な場所に保存するか、必要に応じて消去する措置を適用します。インプレースデータ ソースおよびサードパーティのデータ ソースを Office 365 に取り込んで、メッセージの種類で分類することができます。メッセージの種類による分類を使用すると、さまざまなデータソースの検索、並べ替え、およびエクスポートが可能になり、電子情報開示のレビューの実行プロセスが簡素化されます。

Windows および Windows Server

Windows Server 2012 R2 の Microsoft Data Classification Toolkit には、組織の IT 担当者、監査担当者、会計士、弁護士、およびその他のコンプライアンス担当者が実行するコンプライアンス関連のアクティビティの支援に使用できるサンプルの検索式とルールが用意されています。

保護: 脆弱性とデータ侵害の防止、検出、および対応を行うセキュリティ制御を確立する

各組織は情報のセキュリティの重要性に対する理解を深めつつありますが、GDPR がその水準をさらに引き上げています。GDPR では、組織が適切な技術的および組織的な対策を講じて、個人データの損失や未承認のアクセスまたは開示を防ぐことが求められます。

データの保護

データのセキュリティは、複雑な領域です。識別および考慮すべきリスクの種類はたくさんあります。物理的な侵入や許可されていない従業員から意図しない損失やハッカーまでさまざまです。リスク管理計画の作成、およびパスワード保護、監査ログ、暗号化などのリスク軽減措置の実行が、コンプライアンスの確保につながります。

マイクロソフトのクラウドは、特にリスクの把握とリスクからの防御を支援するよう構築されており、オンプレミスのコンピューティング環境より多くの点において安全です。たとえば、マイクロソフトのデータセンターは、国際的に認められているセキュリティ標準の認定を受けており、24 時間体制の物理的監視で保護され、厳格なアクセス制御機能があります。

クラウド インフラストラクチャをセキュリティで保護するしくみは、包括的なセキュリティ ソリューションの一部に過ぎず、クラウドかオンプレミスかにかかわらず、マイクロソフトのすべての製品に、データのセキュリティによる保護を支援するセキュリティ機能があります。

Azure

Azure の以下のサービスとツールは、クラウド環境で個人データを保護するのに役立ちます。

- Azure Security Center では、Azure リソースのセキュリティを可視化および制御できます。また、リソースを継続的に監視し、セキュリティに関する推奨事項をお知らせします。企業のセキュリティ要件、使用するアプリケーションの種類、およびデータの機密度に基づいて、Azure サブスクリプションとリソース グループのポリシーを定義できます。さらに、ポリシーに基づくセキュリティに関する推奨事項を使用して、サービスの所有者が必要な制御を実装するプロセスをガイドします。たとえば、マルウェア対策やリソースのディスク暗号化を有効にするプロセスなどです。Security Center は、マイクロソフトおよびパートナーのセキュリティ サービスとアプライアンスを迅速にデプロイして、クラウド環境の保護を強化するのにも役立ちます。
- Azure のデータ暗号化は、保存データおよび転送中のデータをセキュリティで保護します。たとえば、データを Azure Storage に書き込む際に、Storage Service Encryption を使用して自動的にデータを暗号化できます。さらに、Azure Disk Encryption を使用して、Windows 仮想マシンと Linux 仮想マシンが使用するオペレーティング システムとデータ ディスクを暗号化することもできます。データはアプリケーションと Azure 間での転送中にも保護され、常にきわめて高いセキュリティが保たれます。

- Azure Key Vault を使用すると、データを保護するための暗号化キー、証明書、およびパスワードを保護できます。Key Vault では、ハードウェア セキュリティ モジュール (HSM) が使用されます。Key Vault は、キーの制御を保持することによって、データの制御が保持されるよう設計されており、マイクロソフトがお客様のキーを表示したり抽出したりすることはできません。Azure ログによって、保存されているキーの使用を監視および監査できます。また、ログを Azure HDInsight やセキュリティ情報/イベント管理 (SIEM) システムにインポートして、さらなる分析と脅威の検出に利用することもできます。
- Azure Cloud Services および Virtual Machines 向け Microsoft マルウェア対策は、ウイルス、スパイウェア、およびデータの窃盗を狙ったその他の悪意のあるソフトウェアの特定と保護に役立つ無料のリアルタイム保護機能で、既知の悪意のあるソフトウェアや望ましくないソフトウェアが Azure システムへのインストールまたは実行を試みた場合に警告する構成可能なアラートを備えています。

Dynamics 365

Dynamics 365 のセキュリティ概念を使用して、Dynamics 365 組織のデータの整合性とプライバシーを保護できます。ビジネス ユニット、ロールベース セキュリティ、レコードベース セキュリティ、およびフィールドベース セキュリティを組み合わせて、Dynamics 365 組織内でユーザーに付与する全体的な情報アクセスを定義できます。

- Dynamics 365 のロールベース セキュリティでは、指定されたユーザーが実行できるタスクを制限する一連の特権をまとめることができます。これは特に、組織内でユーザーのロールが変わる場合に重要な機能です。
- Dynamics 365 のレコードベース セキュリティでは、特定のレコードへのアクセスを制限できます。
- Dynamics 365 のフィールドレベル セキュリティでは、個人を特定できる情報など、影響の大きい特定のフィールドへのアクセスを制限できます。

Enterprise Mobility + Security (EMS)

大半のデータ侵害で、攻撃者は脆弱な資格情報、既定の資格情報、または盗んだ資格情報を利用して企業ネットワークに侵入しています。マイクロソフトのセキュリティ アプローチは、リスクベースの条件付きアクセスによるフロント ドアでの ID 保護から始まります。

- Enterprise Mobility + Security の Azure Active Directory (Azure AD) を使用すると、特権のある ID と特権のない ID を含め、組織の ID を管理および保護することによって、アクセス レベルで組織を保護できます。Azure AD は、数千のアプリにアクセスできる保護された 1 つの共通 ID を提供します。Azure AD Premium には、デバイスの正常性、ユーザーの所在地、ID、およびサインイン リスクに基づくアクセス制御である多要素認証 (MFA) のほか、包括的なセキュリティ レポート、監査、およびアラートの機能があります。Azure AD Privileged Identity Management (PIM) は、セキュリティ ウィザード、レビュー、およびアラートを通じて、特権

ID とそれらの ID によるリソースへのアクセスを検出、制限、監視する際に役立ちます。これにより、期間限定で "Just In Time" & "Just Enough" administration (必要なときに必要なだけの管理) アクセスを提供するなどのシナリオが有効になります。

Enterprise Mobility + Security は、オンプレミスおよびクラウドでのユーザー、デバイス、およびデータのアクティビティを詳細に可視化し、強力な制御と適用によってデータの保護を支援します。

- Azure Information Protection は、データに対する制御をデータのライフサイクル全体に拡張するのに役立ちます。その範囲は、オンプレミスおよびクラウド サービスでデータが作成されるところから始まり、保管、社内外での共有、ファイルの配布の監視へと続き、最終的には予期しないアクティビティへの対応にまで及びます。
- Cloud App Security は、お客様の従業員が利用しているサービスとしてのソフトウェア (SaaS) とクラウド アプリに対する詳細な可視性と強力なデータ制御機能を提供します。そのため、お客様は完全なコンテキストを得て、きめ細かいポリシーでデータを制御できるようになります。
- Microsoft Intune は、クラウドからのモバイル デバイス、モバイル アプリケーション、および PC の管理機能を提供します。Intune を使用すると、企業データの強固なセキュリティを確保しながら、従業員がほぼどこからでも、ほぼあらゆるデバイスで会社のアプリケーション、データ、およびリソースにアクセスできるようにすることが可能です。

Office および Office 365

Office 365 プラットフォームでは、アプリケーションの開発から物理的なデータセンター、エンド ユーザー アクセスまで、あらゆるレベルにセキュリティが取り入れられています。Office 365 アプリケーションには、データ保護のプロセスを簡素化する組み込みのセキュリティ機能と、お客様固有のビジネス ニーズにとって意味のある方法でセキュリティを構成、管理、および統合できる柔軟性の両方が含まれています。Office 365 のコンプライアンス フレームワークには、進化する業界標準に合わせて Office 365 を最新に保つことができる制御が 1,000 個以上あります。これには 50 以上の証明書と構成証明が含まれます。

セキュリティ制御の多くは既定で利用可能です。たとえば、SharePoint と OneDrive for Business はどちらも、転送中のデータと保存データに対して暗号化を使用します。さらに、デジタル証明書を構成してデプロイすることで個人データを難読化したり、Office のアクセス制御を使用して個人データへのアクセスを付与および制限したりできます。

Office 365 は、データを保護し、データ侵害が発生したタイミングを特定するのに役立つ機能をほかにも備えています。

- Secure Score は、お客様のセキュリティ体制、および生産性とセキュリティを両立しながらリスクを軽減するために利用可能な機能に関する洞察を提供します。
- Exchange Online 向けの Advanced Threat Protection (ATP) を使用すると、新しい高度なマルウェア攻撃から電子メールをリアルタイムで保護できます。また、悪意のある添付文書や、電子メールからリンクされる悪意のある Web サイトにユーザーがアクセスしないよう阻止するポリシーを作成することもできます。Exchange Online 向けの ATP には、未知のマルウェアやウイ

ルスに対する保護、悪意のある URL に対するクリック時の保護、および機能が充実したレポートおよび URL トレース機能が含まれています。

- Information Rights Management (IRM) は、お客様とそのユーザーが、承認されていない人物による機密情報の印刷、転送、保存、編集、またはコピーを防止するのに役立ちます。SharePoint Online で IRM を使用すると、リストやライブラリからダウンロードされたファイルに対してユーザーが実行できる操作を制限できます。たとえば、ファイルのコピーの印刷や、ファイルからのテキストのコピーなどを制限できます。Exchange Online で IRM を使用すると、電子メールメッセージや添付ファイル内の機密情報が電子メール、オンライン、およびオフラインで漏えいするのを防止できます。
- Office 365 のモバイル デバイス管理 (MDM) では、ユーザーの登録済み iPhone、iPad、Android デバイス、および Windows スマートフォンをセキュリティで保護して管理するのに役立つポリシーとルールを設定できます。たとえば、デバイスをリモートでワイプしたり、詳細なデバイス レポートを表示したりできます。Office 365 では、追加のセキュリティを提供するために多要素認証も使用されます。

SQL Server および Azure SQL Database

SQL Server と Azure SQL Database は、デバイス アクセスと承認を複数のレベルで管理するための制御を備えています。

- Azure SQL Database のファイアウォールは、承認された接続のみにアクセスを制限することによって、Azure SQL Database サーバー内にある個々のデータベースへのアクセスを制限します。サーバー レベルおよびデータベース レベルでファイアウォール規則を作成して、接続を承認する IP 範囲を指定できます。
- SQL Server 認証は、有効な資格情報を持つ、許可されているユーザーのみがデータベース サーバーにアクセスできるようにするのに役立ちます。SQL Server は、Windows 認証と SQL Server ログインの両方をサポートします。Windows 認証は統合セキュリティを提供し、認証プロセスが完全に暗号化された、より安全なオプションとしてお勧めします。Azure SQL Database は Azure Active Directory 認証をサポートします。これはシングル サインオン機能を提供し、管理対象ドメインと統合ドメインでサポートされます。
- SQL Server の承認により、最小特権の原則に従ってアクセス許可を管理できます。SQL Server と SQL Database はロールベース セキュリティを使用しており、ロール メンバーシップとオブジェクトレベルのアクセス許可の管理により、データのアクセス許可をきめ細かく制御できます。
- 動的データ マスク (DDM) は、特権のないユーザーやアプリケーションがデータにアクセスした場合にデータをマスクすることによって機密データの開示を制限するために使用できる組み込みの機能です。クエリ結果内の指定したデータ フィールドがその場でマスクされますが、データベース内のデータは変更されません。DDM は構成が簡単で、アプリケーションの変更は必要ありません。Azure SQL Database のユーザーに対して、動的データ マスクによって潜在的な機密データを自動的に検出して、適用すべき適切なマスクを提案できます。
- 行レベルのセキュリティ (RLS) は、SQL Server と SQL Database のお客様がデータ行アクセ

スに制限を実装できるようにする追加の組み込みの機能です。RLS を使用すると、データベーステーブルの行に対する詳細なアクセスを有効にして、どのユーザーがどのデータにアクセスできるかをより細かく制御できます。アクセス制限ロジックはデータベース層に存在するため、この機能により、アプリケーション セキュリティの設計と実装が大きく簡素化されます。

SQL Server と SQL Database は、データを保護し、データ侵害が発生したタイミングを特定する一連の強力な組み込み機能を備えています。

- Transparent Data Encryption は、データベース、関連するバックアップ、およびトランザクション ログ ファイルを物理記憶域層で暗号化することにより、保存データを保護します。この暗号化は、アプリケーションに透過的であり、ハードウェア アクセラレータを使用して、パフォーマンスを向上させます。
- トランスポート層セキュリティ (TLS) は、SQL Database 接続上で転送中のデータの保護を提供します。
- Always Encrypted は、SQL Server および SQL Database で機密性の高いデータを保護する業界で初めての機能です。Always Encrypted を使用すると、クライアントでは、クライアント アプリケーション内の機密データを暗号化して、データベース エンジンに暗号化キーを決して公開しないことが可能になります。データの暗号化と暗号化解除は、Always Encrypted 対応クライアント ドライバーで透過的に実行されるため、このメカニズムは、アプリケーションに透過的です。
- SQL Database の監査と SQL Server Audit は、データベース イベントを追跡して監査ログに書き込みます。監査により、データベースの継続的なアクティビティを把握できることに加え、過去のアクティビティを分析、調査して、潜在的な脅威や不正使用の疑いがある行動、およびセキュリティ違反を特定することもできます。
- SQL Database の脅威検出は、データベースに対する潜在的なセキュリティ上の脅威を示す異常なデータベース アクティビティを検出します。脅威検出は、一連の高度なアルゴリズムを使用して、アプリケーションの動作を継続的に学習してプロファイルを作成し、異常または疑わしいアクティビティを検出すると直ちに通知します。脅威検出は、GDPR のデータ侵害の通知要件を達成するのに役立ちます。

Windows および Windows Server

Windows 10 と Windows Server 2016 には、業界最先端の暗号化テクノロジとマルウェア対策テクノロジ、およびパスワードからより安全な認証形態への移行を可能にする ID とアクセス ソリューションが含まれています。

- Windows Hello は、パスワードに代わる便利なエンタープライズ レベルの機能で、自然の方法 (生体認証) または使い慣れた方法 (PIN) を使用して、ID を検証します。追加の周辺機器を必要とすることなく、スマートカードのセキュリティ上の利点を利用できます。
- Windows Defender ウイルス対策は、すぐに使用できる堅牢なマルウェア対策ソリューションで、保護された状態を維持するのに役立ちます。Windows Defender ウイルス対策は、新たなマルウェアをすばやく検出して、マルウェアから保護できます。また、ユーザー環境のいずれかの部分で脅威が初めて確認された場合に、直ちにデバイスを保護するのに役立ちます。
- Device Guard は、デバイスやサーバーをロック ダウンして、マルウェアの新しい変種、未知の変種、および持続的標的型攻撃から保護できます。ウイルス対策プログラムのような、最新の脅威を検出するために絶えず更新を必要とする検出ベースのソリューションとは異なり、Device Guard はデバイスをロック ダウンして、選択した承認されているアプリケーションのみを実行できるようにします。これはマルウェアに対抗するうえで非常に効果的な方法です。
- Credential Guard は、Windows オペレーティング システム全体が侵害された場合でも、シングル サインオン トークンなどのデバイス上のシークレットをアクセスから分離します。このソリューションは、基本的に、"pass-the-hash" などの防御が難しい攻撃の使用を阻止します。
- Windows 10 と Windows Server 2016 の BitLocker ドライブ暗号化は、エンタープライズ レベルの暗号化を提供し、デバイスの紛失時や盗難時にデバイスを保護するのに役立ちます。BitLocker は、コンピューターのディスクとフラッシュ ドライブを完全に暗号化して、承認されていないユーザーがデータにアクセスするのを防止します。
- Windows Information Protection は、BitLocker の処理が完了した時点から機能し始めます。BitLocker がデバイスのディスク全体を保護するのに対し、Windows Information Protection は、承認されていないユーザーとアプリケーションがマシン上で実行されないようにしてデータを保護します。さらに、ビジネスからビジネス以外のドキュメントまたは Web 上の場所へデータが漏えいするのを防止するのにも役立ちます。
- シールドされた仮想マシンでは、BitLocker を使用して、ディスクと Hyper-V 上で実行される仮想マシン (VM) を暗号化し、侵害された管理者または悪意のある管理者が、保護された VM の内容を攻撃するのを防ぐことができます。
- Just Enough Administration および Just in Time Administration により、管理者は、通常のジョブと操作を実行しながら、管理者が実行できる機能と時間の範囲を制限できます。特権付きの資格情報が侵害されても、被害範囲が大幅に限定されます。この手法では、プロジェクトでの作業時間中に必要なアクセス レベルのみが管理者に提供されます。

データ侵害の検出と対応

GDPR では、データ侵害の発生時に組織は規制当局への迅速な通知が求められます。場合によっては、組織は、影響が及ぶデータ主体にも通知する必要があります。この要件を満たすために、組織は、システム侵入の監視と検出の機能を利用できます。

一部またはすべての対応責任を負うインシデントのため、マイクロソフトは詳細なセキュリティ インシデント対応管理プロセスを設けています。たとえば、Azure や Office 365 向けのプロセスの概要を参照できます。

さらに、ホワイト ペーパー『Shared Responsibilities in Cloud Computing』では、共同責任モデルの下でマイクロソフトがどのようにお客様と協力して作業に当たっているかの概要を説明しています。

潜在的な侵害を検出したら、次の 4 ステップのプロセスを推奨します。これは、マイクロソフトが独自のインシデント対応プログラムで使用しているものです。

- イベントの影響と重大度を評価する。証拠によっては、評価がさらにサイバーセキュリティ/データ保護対応チームへとエスカレーションされる場合も、されない場合もあります。
- 技術的調査またはフォレンジクス調査を実施して、リスクの封じ込め、軽減、および回避の戦略を特定する。個人データが不正な個人または承認されていない個人に開示された可能性があるとサイバーセキュリティ/データ保護チームが確信した場合、GDPR で要求されている通知プロセスが並行して開始されます。
- 問題を軽減するための復旧計画を作成する。影響を受けたシステムの隔離など、危機の封じ込めステップを診断と並行して直ちに実行する必要があります。直近のリスクが終わった後に実施する長期的な軽減策を計画できます。
- ポリシー、手順、およびプロセスを変更してイベントの再発を防止することを目的として、インシデントの詳細を記述した事後分析を作成する。この段階は、侵害に関する事実、その影響、および実施した是正措置を記録することを求めた GDPR 第 31 条に沿ったものです。

Azure

システム内の個人データの保護、およびコンプライアンスのレポートとレビューは、GDPR の重要な要件です。GDPR のこれらの義務を達成するには、Azure の以下のサービスとツールが役立ちます。

- Azure の統合サービスを使用すると、より迅速かつ簡単にセキュリティ体制全体を把握し、クラウド環境に対する脅威を検出、調査できます。Azure Security Center は、先進的なセキュリティ分析を採用しています。画期的なビッグ データおよび機械学習テクノロジを使用してクラウド ファブリック全体のイベントを評価することで、手動アプローチでは識別不可能な脅威を検出し、攻撃の進化を予測します。これらのセキュリティ分析には以下が含まれます。
    - 統合脅威インテリジェンス。マイクロソフトの製品とサービス、Microsoft Digital Crimes Unit (DCU)、Microsoft Security Response Center (MSRC)、および外部フィードからのグローバルな脅威インテリジェンスを使用して、既知の敵対者を探します。

- 行動分析。既知のパターンを適用して悪意のある行動を検出します。
- 異常検出。統計的プロファイリングを使用して履歴ベースラインを作成します。潜在的攻撃ベクトルに従って設定されたベースラインからの逸脱があった場合、アラートを生成します。

さらに、Security Center は、関連するイベントや影響を受けるリソースなど、攻撃キャンペーンについての洞察を得ることができる、優先順位付きのセキュリティ アラートも提供します。

- Azure Log Analytics は、構成可能なセキュリティ監査およびログ オプションを備えており、クラウド内またはオンプレミス環境のリソースによって生成されたデータの収集と分析に役立ちます。Azure Log Analytics は、統合検索機能とカスタム ダッシュボードを使用してリアルタイムの洞察を提供し、物理的な場所に関係なく、すべてのワークロードとサーバーの数百万件のレコードを迅速に分析できます。これは、セキュリティ イベントに対する迅速な対応と徹底調査の促進に役立ちます。

Dynamics 365

マイクロソフトは、セキュリティ、パフォーマンス、および可用性の保証と新機能の提供のため、Dynamics 365 (オンライン) を定期的に維持および更新しています。場合によっては、サービス インシデントにも対応します。こうした活動それぞれについて、組織の Dynamics 365 管理者に電子メール通知が送られます。サービス インシデントの際には、Dynamics 365 (オンライン) の顧客サービス担当者から電話や、電子メールでのフォローアップがある場合もあります。マイクロソフトの Dynamics 365 のポリシーおよびコミュニケーションの詳細については、TechNet を参照してください。

Enterprise Mobility + Security (EMS)

マイクロソフトの包括的な脅威インテリジェンスでは、最先端の行動分析と異常検出テクノロジを使用して、オンプレミスおよびクラウド上の両方で疑わしいアクティビティを発見し、脅威を指摘します。それには、ご使用のシステムの既知の悪意のある攻撃 (Pass the Hash、Pass the Ticket など) やセキュリティの脆弱性が含まれます。また、強力なサポートによって、検出した攻撃に対して即座にアクションを取り、回復を効率化できます。マイクロソフトの脅威インテリジェンスは、クラウドの大量のデータセットと機械学習から得られたインテリジェント セキュリティ グラフを使用して強化されます。

- Microsoft Advanced Threat Analytics (ATA) はオンプレミス製品です。この製品は、エンティティ (ユーザー、デバイス、およびリソース) の通常の動作と異常な動作を自動的に分析、学習、識別することで、IT セキュリティの専門職が高度な標的型攻撃から組織を保護するために役立ちます。ATA は、オンプレミスの Active Directory、SIEM システム、および Windows イベントログの情報と、機械学習を使用して、疑わしいユーザーやエンティティの行動 (デバイスおよびリソース) を検出することで、オンプレミスの持続的標的型攻撃 (APT) を発見します。さらに、既知の悪意のある攻撃 (Pass the Hash など) も検出します。最後に、ユーザーが重要な事象に迅速に集中できるよう、明確で適切な攻撃情報をシンプルな攻撃タイムラインで提供します。

- Cloud App Security は、マイクロソフトの脅威インテリジェンスや調査によって強化されるクラウド アプリケーション向けの脅威防御機能を備えています。リスクの高い利用法とセキュリティ インシデントを識別し、異常なユーザー動作を検出し、脅威を回避できます。Cloud App Security の高度な機械学習ヒューリスティックは、各ユーザーが各 SaaS アプリケーションと対話する方法を学習し、動作分析によって各トランザクションのリスクを評価します。これには、2 か国からの同時ログイン、テラバイト単位のデータの突然のダウンロード、またはブルート フォース攻撃の可能性を示す複数回のログインの失敗が含まれます。
- Azure Active Directory (Azure AD) Premium は、クラウドで ID レベルの脅威検出機能を提供します。Azure AD は、セキュリティ レポートと監視によって、アプリケーションの使用状況を監視し、高度な脅威からお客様のビジネスを保護します。アクセスおよび使用状況レポートによって、組織のディレクトリの整合性とセキュリティが可視化されます。さらに、通知、分析、および修復のための推奨事項を提供して ID を保護します。

Office および Office 365

Office 365 には、データを保護し、データの侵害が発生したタイミングの特定と対応に役立つ複数の機能があります。

- Threat Intelligence を使用すると、Office 365 で高度な脅威の検出および阻止をプロアクティブに実行できます。マイクロソフトの世界的展開、インテリジェント セキュリティ グラフ、およびサイバー脅威ハンターからの入力などにより用意される脅威に対する深い洞察を使用すると、アラート、動的ポリシー、およびセキュリティ ソリューションを迅速かつ効果的に有効にできます。
- Advanced Security Management では、リスクの高い使用状況や異常な使用状況を特定して、潜在的な侵害に関するアラートを生成できます。その他に、アクティビティ ポリシーを設定して、リスクの高い操作と疑わしいアクティビティを追跡し、それらに対応することもできます。また、生産性アプリを発見することもできます。これにより、組織のログ ファイルの情報を使用して、Office 365 とその他のクラウド アプリにおけるユーザーのアプリ使用状況を把握して対策を取ることができます。
- Exchange Online 向けの Advanced Threat Protection を使用すると、新しい高度なマルウェア攻撃から電子メールをリアルタイムで保護できます。また、悪意のある添付文書や、電子メールからリンクされる悪意のある Web サイトにユーザーがアクセスしないよう阻止するポリシーを作成することもできます。

SQL Server および Azure SQL Database

SQL Server と SQL Database は、データ侵害が発生したタイミングを特定する一連の強力な組み込み機能を備えています。

- SQL Database の監査と SQL Server Audit は、データベース イベントを追跡して監査ログに書き込みます。監査により、データベースの継続的なアクティビティを把握できることに加え、過去のアクティビティを分析、調査して、潜在的な脅威や不正使用の疑いがある行動、およびセキュリティ違反を特定することもできます。

- SQL Database の脅威検出は、データベースに対する潜在的なセキュリティ上の脅威を示す異常なデータベース アクティビティを検出します。脅威検出は、一連の高度なアルゴリズムを使用して、アプリケーションの動作を継続的に学習してプロファイルを作成し、異常または疑わしいアクティビティを検出すると直ちに通知します。脅威検出は、GDPR のデータ侵害の通知要件を達成するのに役立ちます。

Windows および Windows Server

Windows Defender Advanced Threat Protection (ATP) により、セキュリティ運用チームは、ネットワーク上のデータ侵害の検出、調査、封じ込め、および対応を行うことができます。Windows Defender ATP では、最大 6 か月分の履歴データを使用して、すべてのエンドポイントでの高度な侵害の検出、調査、および対応の機能を実現できます。これらの機能は、エンドポイントがオフラインの場合、ネットワーク ドメインの外部にある場合、再イメージ化されている場合、および既に存在しない場合でも有効です。GDPR では、データ侵害の検出、調査、およびレポートについて明確な手順が設定されています。Windows Defender ATP は、この重要な要件の達成に役立ちます。

レポート: データの要求に対応し、データ侵害をレポートして、必要なドキュメントを保管する

GDPR によって、透明性、アカウンタビリティ、記録保持における新しい標準が設定されます。個人データの扱い方に関してだけでなく、個人データの処理と使用を定義する文書の積極的な保守方法に関しても、透明性を強化する必要があります。

記録保持

個人データを処理する組織は、処理の目的、処理対象の個人データのカテゴリ、データを共有する第三者の ID、第三国が個人データを受け取るかどうか (とその国名) およびその転送の法的根拠、組織的および技術的なセキュリティ対策、さまざまなデータセットに適用されるデータ保持期間に関する記録を保持する必要があります。これを実施する 1 つの方法が、監査ツールの使用です。監査ツールを使用すると、収集、使用、共有などの処理内容にかかわらず、データのあらゆる処理の追跡と記録が可能になります。

Microsoft クラウド サービスは、この標準を満足するのに役立つ組み込みの監査サービスを提供しています。

Azure、Office 365、および Dynamics 365

Service Trust Portal では、レポートや構成証明を含め、Azure、Office 365、および Dynamics 365 のコンプライアンス、セキュリティ、プライバシー、および信頼のさまざまなオファリングに関する包括的な情報を入手できます。サードパーティの独立した監査レポートおよび GRC (ガバナンス、リスク管理、およびコンプライアンス) 評価レポートは、お客様の組織にとって重要であるグローバル標準にマイクロソフトのクラウド サービスがどう準拠しているかの最新状況の把握に役立ちます。信頼性関連ドキュメントは、マイクロソフトのクラウド サービスがお客様のデータをどのように保護し、お客様がクラウドサービスのデータのセキュリティおよびコンプライアンスをどのように管理できるかについての理解を促します。

Azure

セキュリティ関連イベントの監査とログ、および関連するアラートは、効果的なデータ保護戦略の重要な構成要素です。

Azure ログおよび監査機能を使用すると、以下のことが可能になります。

- Azure 仮想マシン ギャラリーから作成した仮想マシンおよび Azure に展開されているアプリケーションの監査証跡を作成できます。
- Azure のサービスとしてのインフラストラクチャ (IaaS) およびサービスとしてのプラットフォーム (PaaS) からセキュリティ イベントを収集することにより、大規模なデータ セットの一元化された分析を実行できます。そのうえで、Azure HDInsight を使用して、これらのイベントを集約および分析して、監視に使用するためにオンプレミスの SIEM システムにエクスポートできます。

- システム アクセスなどの管理操作の Azure ログを利用することによって、アクセスおよび使用状況のレポートを監視して、承認されていない変更や、意図しない変更が加えられたときに監査証跡を作成できます。Azure Active Directory テナントの監査ログを取得して、アクセスおよび使用状況のレポートを確認できます。
- Windows セキュリティ イベント ログおよびその他のセキュリティ固有のログを収集するよう構成可能な Azure Diagnostics を使用することによって、セキュリティ アラートをオンプレミスの SIEM システムにエクスポートできます。
- セキュリティの監視、レポート、およびアラート用のサードパーティ製ツールを Azure Marketplace から取得できます。

Microsoft Azure Monitor を使用すると、組織は、一元化されたダッシュボードからすべてのデータ監視タスクを簡単に表示および管理できます。詳細なパフォーマンスおよび使用状況の最新のデータ、各 API 呼び出しを追跡するアクティビティ ログ、および Azure リソースでのトレースに関する問題の対処に役立つ診断ログを表示できます。また、アラートを設定して、措置を自動化することもできます。Azure Monitor では、既存のツールが統合されるので、Azure Monitor と既に使い慣れている分析ツールとを組み合わせることによって、エンドツーエンドの充実した監視と分析を実行できるようになります。

Office および Office 365

- Office 365 セキュリティ/コンプライアンス センターでのサービス アシュアランスでは、マイクロソフトのコンプライアンス レポートおよび監査対象の管理方法の透明性ステータスの詳細と共に、以下のようなリスク評価の実施に関する深い洞察を入手できます。
    - Office 365 に保存されている顧客データに対するマイクロソフトのセキュリティ上の取り組み。
    - Office 365 に関する独立サードパーティ監査レポート。
    - ISO 27001、ISO 27018、医療保険の携行性と責任に関する法律 (HIPAA) などの、さまざまな業界にわたる標準、法律、および規定にお客様が準拠できるように支援するセキュリティ、プライバシー、およびコンプライアンスの管理の実装とテストの詳細。
- Office 365 監査ログでは、Office 365 のワークロード全体にわたって、ユーザーおよび管理者のアクティビティの監視と追跡を実行できます。これは、セキュリティおよびコンプライアンスに関する問題の早期検出および調査に役立ちます。Office 365 の [監査ログの検索] ページを使用して、組織内のユーザーおよび管理者のアクティビティの記録を開始します。Office 365 で監査ログの準備が整ったら、OneDrive や SharePoint Online へのアップロード、ユーザー パスワードのリセットなどの広範なアクティビティを監査ログで検索できます。管理者が加えた変更の追跡、およびメールボックスにそのメールボックスの所有者以外のだれかがアクセスしたときの追跡を実行するよう Exchange Online を設定できます。
- Customer Lockbox では、ヘルプ セッションでマイクロソフトのサポート エンジニアによるお客様のデータへのアクセスを許可するかどうかを制御する権限がお客様に与えられます。エンジニアが問題のトラブルシューティングを行って、問題を修正するためにお客様のデータにアクセスする必要がある場合、Customer Lockbox を使用してそのアクセス要求を承認または拒否できます。

アクセス要求を承認すると、エンジニアはデータにアクセスできます。各要求には有効期限があり、問題が解決されると、その要求は閉じられ、アクセス権は失効します。

Enterprise Mobility + Security (EMS)

Azure Information Protection には、機密データがどのように配布されているかを分析する機能豊富なログおよびレポートが用意されています。ドキュメント追跡により、ユーザーと管理者は、共有データに対するアクティビティを監視したり、不測のイベントが生じた場合にアクセスを取り消したりできます。Azure Information Protection には、ファイル共有、SharePoint のサイトとライブラリ、オンラインのリポジトリ、およびデスクトップまたはノート PC のドライブに存在する非構造化データの分析機能も用意されています。ファイルにアクセスできると共に、各ファイルのコンテンツをスキャンして、特定のクラスの個人データがファイル内に存在するかどうかを判別できます。そのうえで、存在するデータの種類に基づいて、各ファイルを分類して、ラベルを付けることができます。さらに、スキャンしたファイル、照合した分類ポリシー、および適用したラベルに関する情報が含まれる、このプロセスのレポートを生成できます。

Windows および Windows Server

Windows イベント ログは充実したイベント ログ機能を備えており、管理者は、オペレーティング システム、アプリケーション、およびユーザー アクティビティに関してログに記録された情報を参照できます。このログ システムは、ファイルへのアクセス、アプリケーションの使用状況、ポリシーの変更など、ユーザーとアプリケーションの詳細な操作を監査するように構成できます。Windows イベント ログでは、管理者は、クライアントとサーバーから中央の場所へイベントを転送して、レポートや監査を行うこともできます。

クラウド サービスのレポート ツールとドキュメント

個人データを扱うその他のデータベースやシステムと同様に、組織は、クラウド サービスの使用についても適切に記録し、十分に把握する必要があります。たとえば、組織のためにサービス プロバイダーが保持している個人データ、これらのサービスを管理する契約関係、およびサービス関係終了時のデータの取り扱いを理解する必要があります。

マイクロソフトは、Microsoft Cloud 内のお客様のアカウントに関するシンプルで明確なレポート ツールと併せて、マイクロソフトのクラウド サービス、そのしくみ、およびマイクロソフトとお客様との契約関係に関する詳しいドキュメントを維持することによって、この情報の管理を支援します。

データ主体への通知

GDPR では、データ保護要件が変更され、個人の権利と自由にリスクをもたらす結果となる個人データ侵

害の通知に関して、データ処理業者およびデータ管理者に対して、より厳格な義務が採用されます。新しい規定の下に、第 17 条、第 31 条、および第 32 条で規定されているとおり、データ処理業者は、このような個人データ侵害に気が付いたら、遅滞なくデータ管理者に通知しなければなりません。

侵害の認知後、データ管理者は 72 時間以内に関連するデータ保護機関に通知しなければなりません。侵害が、個人の権利および自由に高いリスクをもたらす結果となる可能性がある場合、データ管理者は影響を受ける個人にも遅滞なく通知する必要があります。つまり、企業におけるロールでデータ処理業者をデータ管理者として使用している場合は、起こりうる侵害通知に関して、契約に一連の明確な想定事項を組み込んでおく必要があります。

一部またはすべての対応責任を負うインシデントのため、マイクロソフトは詳細なセキュリティ インシデント対応管理プロセスを設けています。たとえば、Azure、Office 365、Dynamics 365 向けのプロセスの概要を参照できます。さらに契約書でも、マイクロソフトの GDPR への取り組みを記載しています。

Azure、Dynamics 365、Enterprise Mobility + Security、Office 365、Windows 10 など、マイクロソフトの製品とサービスは、セキュリティ上の脅威と侵害を検出して評価し、GDPR の侵害通知義務を達成するのに今すぐ役立つ解決策を備えています。

データ主体からの要求の処理

GDPR の中で最も重要な要素は、第 2 節「Information and Access to Data (情報およびデータへのアクセス)」、第 3 節「Rectification and Erasure (訂正と消去)」、および第 4 節「Right to Object and Automated Individual Decision Making (異議を唱える権利および個人に対する自動化された意思決定)」の条項で規定されている "データ主体" の権利です。

これらの義務は、お客様がデータ管理者の場合、その IT 環境と運用に影響し、お客様がデータ処理業者の場合、使用しているサービス プロバイダーの IT 環境と運用に影響する場合があります。

適切なデータ ガバナンスは、プライバシーに関する法律の重要な要素であり、データ保護およびプライバシーに関する大半の法令で推奨されています。GDPR におけるガバナンスの重要な要素の 1 つは、特定の状況におけるデータ保護責任者 (DPO) の確立であり、第 35 条、第 36 条、および第 37 条にその概要が規定されています。DPO は、個人データの保護に関係するすべての問題に関与する必要があります。

GDPR のガバナンスで 2 番目に重要な要素は、DPO の指示の下で、データ保護コンプライアンス レビューを完了してデータ保護影響評価 (DPIA) を生成することです。第 33a 条はそれらの要件を具体的に規定しており、それによると、データ管理者は DPIA の完了後 2 年以内にコンプライアンス レビューを実施して、個人データの処理が DPIA に準拠して実行されていることを実証する必要があります。

Microsoft Trust Center では、マイクロソフトがお客様の取り組みをいかに支援できるかに関する情報を提供しており、GDPR に対するマイクロソフトの考え方と取り組みについて特別なセクションを設けています。