

組織内部からの重要な情報の漏洩対策を実現する
包括的なデータ セキュリティ ソリューション

Microsoft Purview

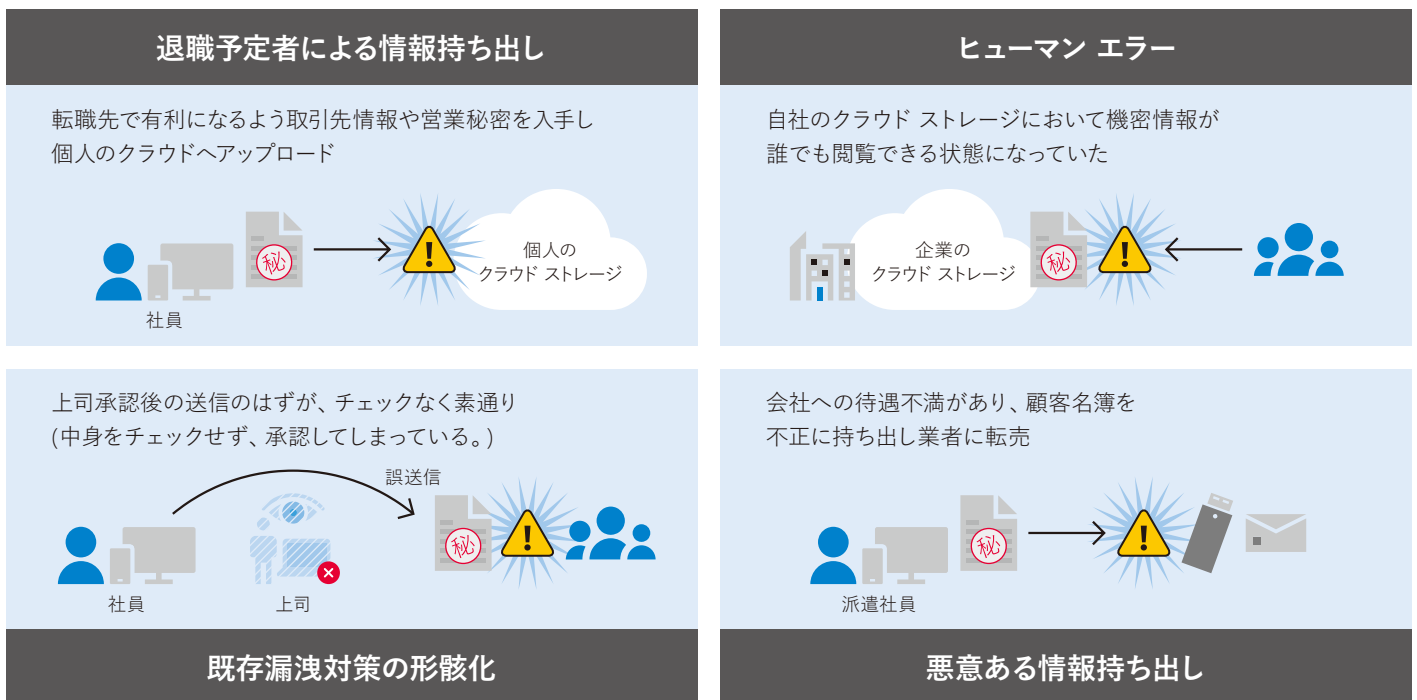
Microsoft Priva



雇用の流動化が進行している今、組織内部からの情報漏洩リスクが非常に高まっています

転職が一般的となり退職者による営業秘密の持ち出しや、ハイブリッドワークやコラボレーションツールの発展に伴い社内外とのコミュニケーションパスが多様化し、従来とは異なる経路からの情報漏洩リスクなどもあります。これまでの性善説に基づく対応から、時代に合わせた柔軟なデータセキュリティ対策への対応が求められています。

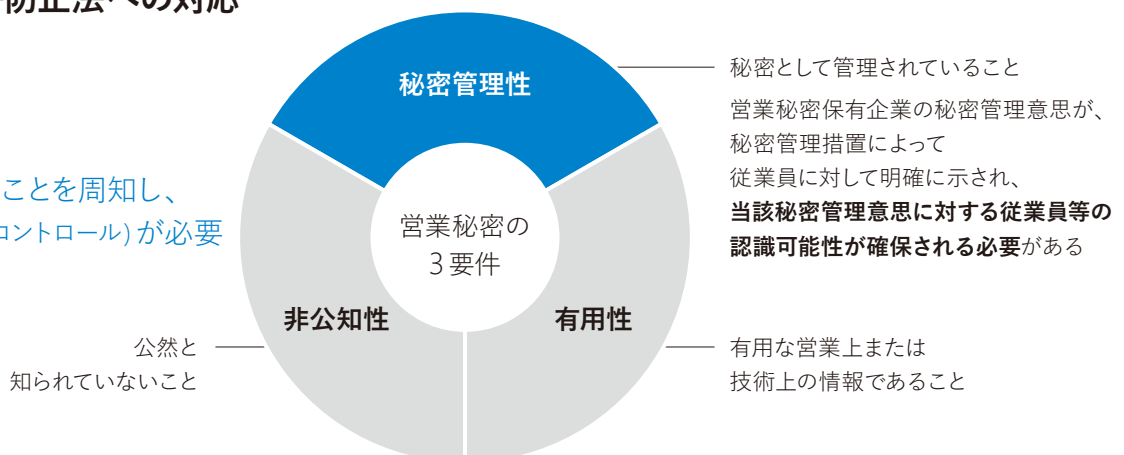
企業内部からの情報漏洩リスク



営業秘密に関連する検挙件数も年々増加傾向にあります。しかしながら、法令に従った運用を日々行っていないと、インシデントが発生した際に、きちんと対処できない可能性があります。たとえば、不正競争防止法で、営業秘密の持ち出しを刑事罰として罪を問うには、持ち出される情報が事前に以下の3要件を満たしておく必要があります。

不正競争防止法への対応

従業員に
社外秘であることを周知し、
適切な統制(コントロール)が必要



参考：経済産業省 営業秘密の保護・活用について
<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706tradesecc.pdf>

これからのデータ セキュリティ対応は 技術的な対策だけでなく総合的に行う時代

ハイブリッド ワーク環境が進み、監視の目が届きにくい今、時代に合った対策への転換が必要です。



参考: 経済産業省 秘密情報の保護ハンドブック

POINT 1 情報の棚卸/ 分類の重要性

効率的に機密情報を守るためには、守るべき情報を特定し、情報の管理担当者によって暗号化やアクセス制御など事前に保護を行っておくことが重要です。事前に保護しておくことで、闇雲に持ち出しの出口対策を行わなくても一定の効果が期待できます。また不要となった個人情報などは、所在を特定したうえで、一定期間で削除するなど、管理対象を日常的に削減しておくことも必要です。

POINT 2 モニタリング運用 の必要性

職種によっては秘密情報・個人情報の扱いも業務上必要となるため、一定のルールや IT による制御だけでは、生産性を維持しながら秘密情報の持ち出しや社内の不正行為を完全に止めることは困難です。疑わしい操作をすべて防止するのではなく、一定レベルの制御を行いながらユーザーを軸とした定量的なモニタリングも同時に実施して、リスクに対応することがバランスの取れた効率的な対策となります。リスクの高いユーザーに絞ってモニタリングし、度を越したケースに対して個別対処することで、善良な大半の社員への影響を最小化しつつ、重大インシデントに発展する前に未然に不正行為の端緒を掴むようになります。

POINT 3 社員の意識向上 につなげる

社会がデジタル化するに従って、機密情報や個人情報などのデータが金銭と同等以上に重要になってきています。刑事罰対象となる営業秘密の要件を満たすためにも、何が社外秘の情報であり、それらがどのように扱われるべきか、社内で周知されている必要があります。

ラベルによる情報区分の明示、違反する操作への警告、また不正が見つかった場合は懲罰対象となることなどが徹底されるような社内のエコ システムを作り上げることで、社員の意識向上を図り、不正が発生しにくい職場環境にしていくことが求められます。

Microsoft Purview で実現する 包括的なデータ セキュリティ

いかに早く社内の不正に気づき対処できるか。

ただログを収集するだけでなく、保護すべき情報を分類し、ログからリスクが高いユーザーを特定して詳細に調査することで、社内の情報資産を効率的に保護できます。

Microsoft 365 との親和性

Microsoft 365 のクラウド環境、Windows 10/11 や Microsoft 365 Apps にセンサーや機能が組み込まれているため、Microsoft 365 の展開が完了していれば、ポリシーを定義するだけで各種機密情報の分類・保護・保全・監視など一連の機能の利用が可能です。また展開やアップデートなどの個別の運用をすることなく、ニーズに応じて日々更新される新機能が順次利用可能となります。

Office ファイルを秘密度ラベルで暗号化保護しても、SharePoint Online / OneDrive for Business での全文検索や、Office for the web での表示・編集、Microsoft 365 Apps を含めた共同編集ができ、生産性への影響を最小化できます*。また管理者による eDiscovery 対応において、秘密度ラベルで暗号化保護を行った場合でもファイルの全文検索や調査が可能です*。

*これら機能の有効化には、トレードオフが伴う設定が必要となります。

新しいコミュニケーション ツールである Teams を含め Microsoft 365 のデータ セキュリティを強化し、社内外のコラボレーションがよりセキュアに行えるようになるので、Microsoft 365 の活用をさらに進められます。



Information Protection & Governance

機密情報保護への意識付け

- 自動もしくは手動で個人情報・機密情報の識別
- ユーザーに見える形で情報のラベル付け、保護、取り扱いに関する警告
- 分類に応じた情報のライフサイクル管理



Insider Risk Management

悪質なケースで個別調査

- ユーザー操作を定量的に監視し、機密情報・個人情報の取り扱いに関するリスク識別
- 社内外での不適切なコミュニケーションを検出
- 利益相反するユーザー間のコミュニケーションを制限



eDiscovery & Audit

訴訟に備え否認防止・証拠保存

- 効率的なコンテンツ検索と、機会学習ベースの検索結果の絞り込みおよび抽出
- 長期のログ保存と、インシデント時に重要となる追加ログの記録



Compliance Manager

コンプライアンス対応状況を各国規制に従って継続的に評価

対策不備を継続確認



機密情報を識別してデータを保護・統制

Information Protection & Governance では、マイナンバーやクレジットカード番号などの事前定義済みの機密情報、別途定義したキーワードや正規表現のパターン、氏名や住所などの固有名詞、データベースから取り込まれた顧客情報、画像（スクリーンショット等）に含まれるテキスト情報などを通じて、クラウドストレージ、ファイルサーバー、端末上で動作する Microsoft 365 Apps などで機密情報や個人情報を識別します。

識別された情報に応じて、秘密度ラベルにより、機微な情報であることを明示しながらファイルを暗号化し、社内ユーザーしか開けないようなアクセスコントロールや、印刷、コピー & ペーストなどの二次利用への制限を適用することができます。

管理外のクラウドストレージや、USB ディスクなどへのファイル書き込みを防止したり、そのような操作の際警告を出すことで、ユーザー自身へも自覚を促しながら機密情報の保護を一段高められます。印刷や USB ディスクなどへのファイル書き込みは制限しないものの、どのようなファイルが持ち出されたかを確認するためのファイルの現物をコピーし保全することもできます。また、不要となった機密情報や個人情報が残存しないように、クラウドに保存されたデータを一定期間保護したうえで期間経過後は削除することも可能です。

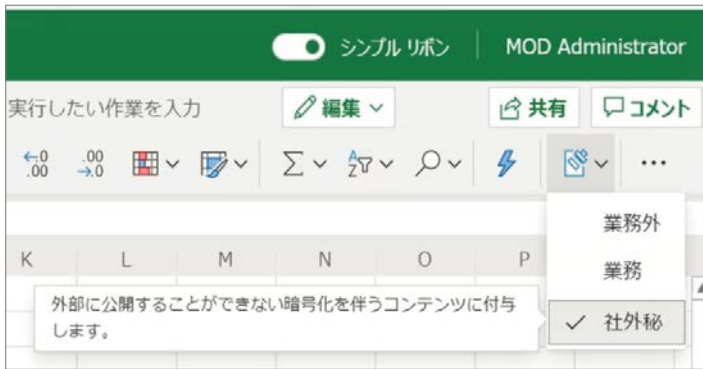


- ☑ Office ファイルや PDF ファイルの中身を分析して、識別された機密情報・個人情報に応じたファイルの保護や二次利用制限が可能
- ☑ 中身が直接確認できないファイル種別であっても、ファイルの拡張子に応じたポリシーを作成することで、管理外へのデータの共有やアップロードを監視・制御可能
- ☑ SharePoint Online のサイトや Microsoft 365 グループなどのデータの格納場所にも秘密度ラベルを設定することができ、ラベルに応じてゲスト招待の可否や多要素認証を必須としたり、管理された端末からのアクセスが必要などの条件設定が可能
- ☑ 保存場所に設定された秘密度ラベルより高い秘密度のラベルが設定されたファイルがアップロードされた際、サイト管理者とファイル投稿者にメールでアラートを送信することが可能
- ☑ SharePoint Online のライブラリにデフォルトの秘密度ラベルを設定し、ラベルが設定されていない Office ファイル等がアップロードされた際、自動で秘密度ラベルを適用することが可能

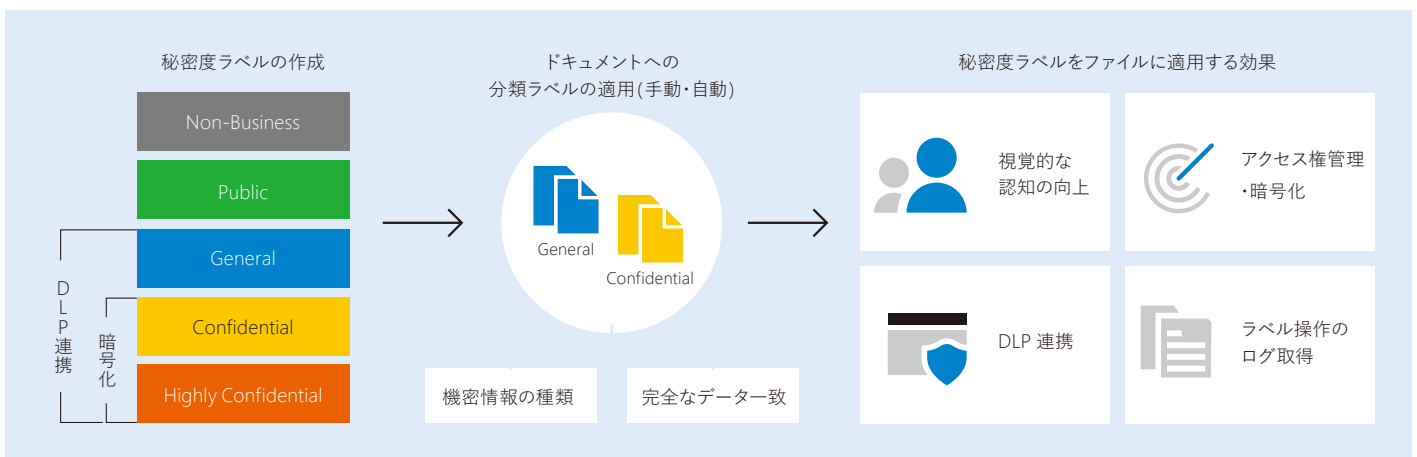


機密情報の分類と保護

自動・手動で付与できる秘密度ラベル

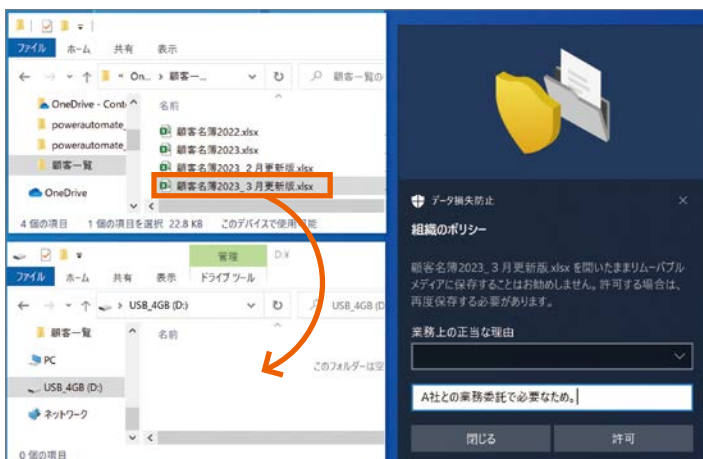


- 「営業秘密の秘密管理性」要件を満たす運用の実現
- 秘密度ラベルによって、社外のユーザーは開けないなどファイルの適切な保護レベルを簡単に選択可能
- ファイルを受け取ったユーザーも視覚的にファイルの秘密度を認識可能
- 秘密度ラベルやファイルに含まれる機密情報・個人情報に応じて、管理外のクラウドへのアップロードや、USB ディスクへの書き込みを防止もしくは警告可能
- 秘密度ラベルの付与・変更、保護されたファイルのアクセスなどの操作は、クラウド側でログ記録される



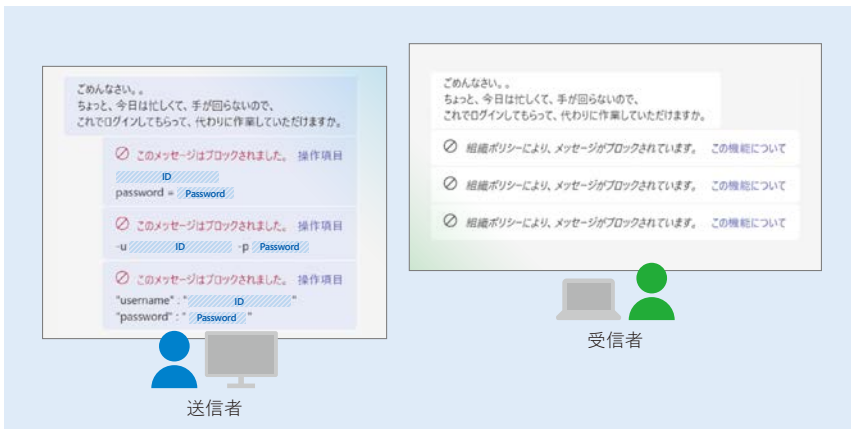
データ損失防止

機密情報の外部への流出を防止



デバイスからの情報漏洩を防止

- デバイス上での機密情報の流出につながる行為を監視及び制御 (クリップボードへのコピー、USB へのコピー、印刷など)
- ブラウザーを経由したクラウド サービスへの機密情報のアップロードを検知し、未然に流出を防止
- 一律での流出防止ポリシーではユーザーの生産性に影響があるため、理由を書かせることにより、外部共有を許可するような柔軟な設定も可能 (生産性向上とユーザーへの機密情報取り扱い教育を両立)



Teams からの情報漏洩を防止

- Teams を経由した外部とのコミュニケーションにおいて機密情報ファイルの流出を防止
- やり取りされるメッセージについても機密情報に該当するものについては、相手側では見えなくなる動作
- 事前定義された分類子を活用することで、社内に散在する資格情報 (パスワード、API Key など) の流出を検知および防止

適用範囲	ソリューション	役割
メール	Exchange Online DLP	メールによる外部への機密情報送信の保護
ファイル共有	SharePoint Online OneDrive for Business DLP	外部に共有された機密ファイルの保護
デバイス上の操作	Endpoint DLP	端末上での不正な操作の検出と制御
チャット・チャネル	Teams DLP	<ul style="list-style-type: none"> • チャット・チャネル内のメッセージの保護 • Teams に紐づく SharePoint サイトや OneDrive アカウント上で共有されるファイルの自動保護
ファイル サーバー	オンプレミス DLP	ファイル サーバー上に保存される機密情報に対するアクセスの保護
SaaS アプリ (Box, Salesforce など)	Microsoft Defender for Cloud Apps	機密情報を含むファイルの検知と保護

データのライフサイクル管理

ドキュメント要件に応じた保持、削除の実現

- SharePoint Online のサイト、Exchange Online のメールボックス、Microsoft 365 グループに対して、部署情報などのプロパティを条件として、ポリシー範囲を定義
- 特定のポリシー範囲に対して、コンテンツをどれくらいの期間保持し、いつ削除するか定めたアイテム保持ポリシーを展開可能
- 特定のポリシー範囲に対して、保持ラベルの自動適用や、利用可能な保持ラベルを設定することができ、コンテンツ単位にユーザーが保持ラベルを上書きして異なる保持期間を指定することも可能
- Microsoft Entra ID (旧 Azure Active Directory) で設定された管理単位を用いて、管理単位内のユーザーやチームに保持ポリシー・保持ラベルを展開することも可能
- クラウド添付ファイルの保持 (Teams で共有された時点のファイルの保持)

データ ライフサイクル管理



一定期間の**保持と削除**

情報がバナンス

必要なものだけを保持し、デジタル資産全体で不要なものを削除することで、リスクと責任範囲を低減



レコード管理

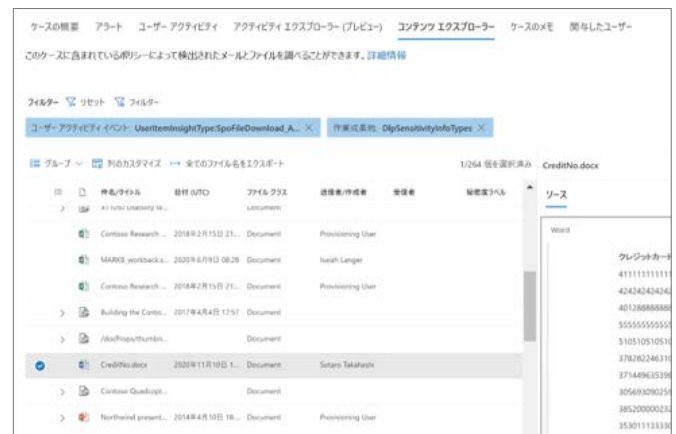
法律、ビジネス、または規制で求められる記録保持義務を満たすために定められた期間、変更や削除からコンテンツを保護



ファイル操作・コミュニケーションの監視でリスクを早期に察知

ユーザーを軸にクラウドおよび端末上でのファイル操作を監視

内部リスクの管理では、特定の閾値を超えた機密情報の疑わしい操作を行ったユーザー、退職予定のユーザー、別途指定したユーザーなどを対象に、一連の操作の中からリスクを判定し、ユーザー操作の妥当性をレビューできます。データ損失防止のポリシーでは、ある一つの操作を止めるか・止めないかといった制御のみですが、内部リスクの管理では、機密情報のダウンロードから端末上での流出行為に及び一連の操作の流れや普段との活動量の違い、ファイルの中身なども加味しながら、機密情報の持ち出しを中心としたユーザーのリスクを判定できます。



退職予定者等の情報持ち出し行動の検出

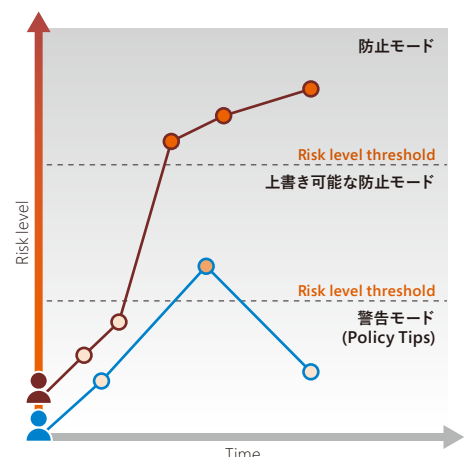
- 退職間際のユーザーや、指定したユーザー、アカウントが削除されたユーザーなどの条件に合致したユーザーの一連の挙動を分析
- 分析対象となったユーザーの疑わしいファイル操作を分析し、閾値に応じてアラートを生成
- アラートが発生した際には、必要に応じて匿名の状態のままレビューが可能
- アクティビティ エクスプローラーを通じて、ファイルの中の機密情報の検知有無と共に、Office 365 からのファイル ダウンロード、端末からのファイルのアップロードや印刷、USB ディスクへの書き込みなどのファイル操作を分析可能

ケース化して詳細に調査

- アラートの中身にに応じて、詳細な分析が必要となった場合、ケース化し、分析担当者をアサインすることで、複数の分析担当者間でのメモの共有や、Teams チャネル チャットでの会話が可能となる
- ケース化することで、Office 365 を起点としたファイルについては、コンテンツ エクスプローラーを通じて中身の参照も可能となる
- Power Automate を通じた通知やシステム連携などの自動化も実装可能

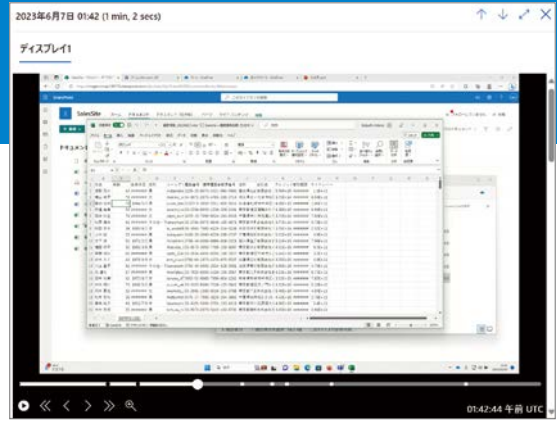
高リスクユーザーのみへの動的なポリシー適用

- 機械学習モデルによって定義および分析されたリスク レベルに基づいて、ユーザーに適切な DLP ポリシーを動的に適用
- 一律の DLP ポリシーを全ユーザーに適用するのではなく、リスクの高いユーザーにのみ DLP ポリシーが適用され、リスクの低いユーザーは生産性を維持
- ポリシー制御は常に調整されるため、ユーザーのリスク レベルが変更されると、新しいリスクレベルに合わせたポリシーが動的に適用



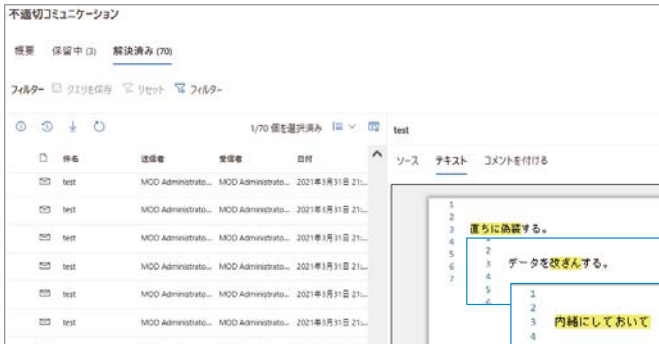
持ち出し行動を動画で記録

- リスクのあるアクティビティを行ったユーザーの実際の操作を動画として記録
- 動画による記録のため、セキュリティ チームにより深い分析情報を提供可能
- プライバシーに配慮し、動画取得には承認作業が必要
- 動画を格納する容量をアドオン ライセンスで別途購入が必要



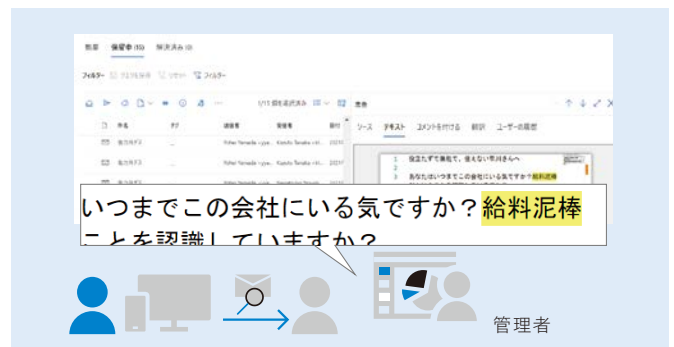
業務で利用しているツールでのコミュニケーションの監視

社内外とのメールやチャットなどから、不正やハラスメントが疑われる会話を早期に検知し、大事に至る前に個別聞き取りなどを通じて是正を図ることができます。



コミュニケーション リスクの検出

- キーワードの定義次第で、検査偽装、価格カルテル、汚職、不正会計、不適切営業、武器輸出など、さまざまな不正行為が疑われる会話を検知・分析可能
- 冒涇、ハラスメント、脅しの会話など機会学習ベースで検出できるカテゴリも順次追加
- OCR による画像読み取りにも対応
- 適切なコンプライアンス担当者により、検知したメールやチャットをレビューすることで、社内の不正の芽を早期に発見し、是正可能



利益相反するユーザー部門間のコミュニケーションを事後査閲

- 金融機関などにおいてインサイダー取引を防止するため、担当企業の内部情報を知る部門と取引や営業を行う部門など、利益相反する特定の部門間のメールやチャットを検出しレビューすることも可能

不正への勧誘やハラスメントを会話の中から検出

- 内部不正への勧誘・共謀に関わる会話を察知
- ハラスメント等職場に不適切な言動を監視可能



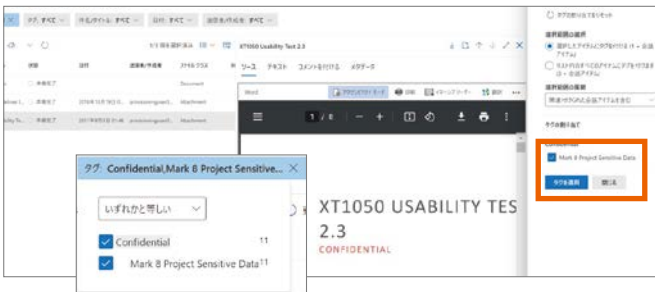
データ コネクタを通じて 3rd Party アプリのデータを取り込み分析することも可能

- マイクロソフトが提供するコネクタを通じて、Bloomberg、IceChat、Slack などを対象に、データを Exchange Online のメールボックスに取り込むことで、これらのアプリでのコミュニケーション内容を保持し、監視し、また電子情報開示機能で必要に応じ検索し、エクスポートすることが可能
- Veritas 社、TeleMessage 社、17a-4 LLC 社、CellTrust 社などが提供するコネクタを利用することで、Cisco Jabber、Cisco Webex Teams、Zoom、WeChat、WhatsApp、ServiceNow などのアプリにおいても、同様にデータを取り込むことで、コミュニケーション内容の保持、監視、電子情報開示対応が可能



Office 365 およびデータ コネクタにより 取り込まれたメール・チャット・ファイルなどの データをスマートに抽出し、レビュー、エクスポート

社内不正が疑われる場合には、過去に遡って当事者のメールやチャット、ファイル共有などを対象とした社内調査が必要となります。電子情報開示 (Premium) では、通常のコンテンツ検索や電子情報開示ではできなかった、Teams にも対応した効率的なコンテンツの抽出とレビューができるよう拡張されています。



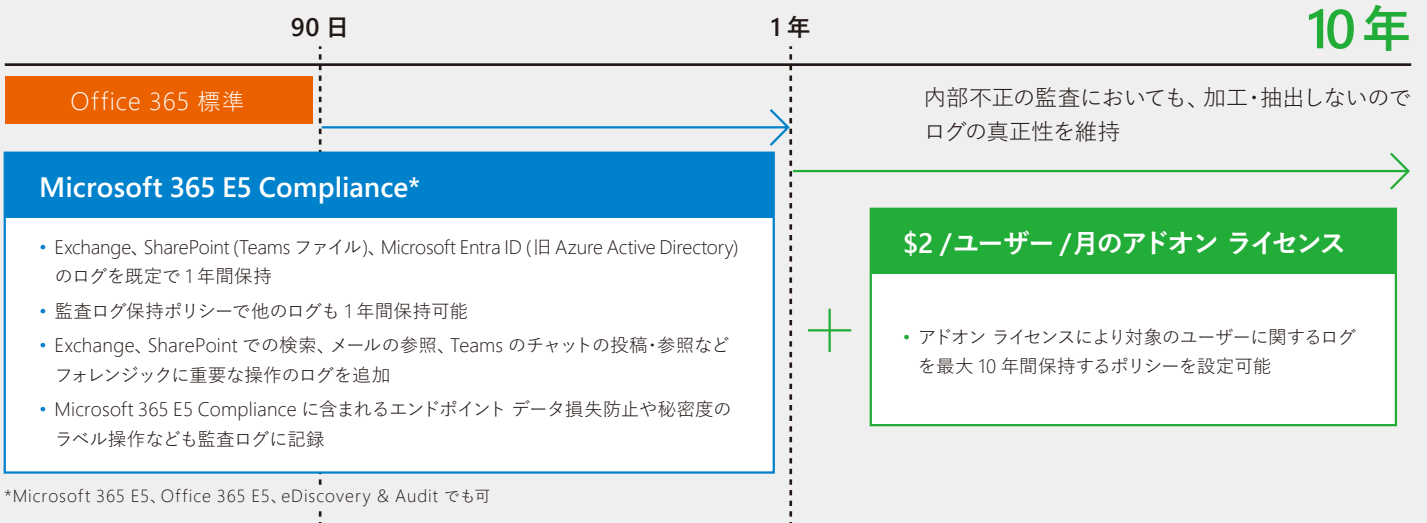
Web UI から複数人でレビューし、情報の絞り込みが可能

- 検索キーワードや、当事者の指定などにより、該当するコンテンツを専用の Web UI を通じて、複数人でレビュー・タグ付けしながら精査可能
- 削除や改ざんからコンテンツを保護しながら、関連するものだけに絞り込んでエクスポートすることも可能

検索でヒットしたアイテムだけでなく、スレッド全体や、リンクされた添付ファイルもレビュー可能

- 検索でヒットしたアイテムだけではなく、Teams チャットのスレッド全体や、メールや Teams に添付されたファイルも対象に抽出・分析が可能

Microsoft 365 E5 Compliance のライセンスでログ保管を 1 年間に延長可能



監査 (Premium) では、エンドポイント データ損失防止で監視している端末上の機密情報の操作ログを含め Office 365 のログ保管期間を標準の 90 日から 1 年間に延長できるだけではなく、SharePoint Online や Exchange Online での検索キーワードや、Teams の会議開催・会議参加など、追加のログも記録が可能です。さらにアドオンの追加により最大 10 年間のログ保管にも対応しています。



各国レギュレーションへの準拠をサポート

コンプライアンス マネージャーを活用することで、各国レギュレーションに応じたテンプレートをベースにセキュリティ・コンプライアンスの対策を採点し、対策漏れを軽減するだけでなく、各国レギュレーションへの準拠をサポートします。

標準組み込み

- **Data Protection Baseline**

対応ライセンス

- Microsoft 365 F1/F3
- Microsoft 365 E1/E3
- Microsoft 365 Business
- Office 365 F3/E1/E3

プレミアム テンプレート

3つまで
利用可能

- **GDPR**
- **NIST 800-53**
- **ISO 27001**
- **プライバシー マーク - JIS Q 15001 : 2017**
- **ISO 27017:2015**
- **ISO/IEC 27018 etc.**

対応ライセンス

- Microsoft 365 E5
- Microsoft 365 E5 Compliance
- Office 365 E5



マイクロソフト側運用については採点済みで、各種セキュリティ・コンプライアンス機能の活用に応じて、お客様対応部分も自動で採点

各国のさまざまなレギュレーションのテンプレートを用意

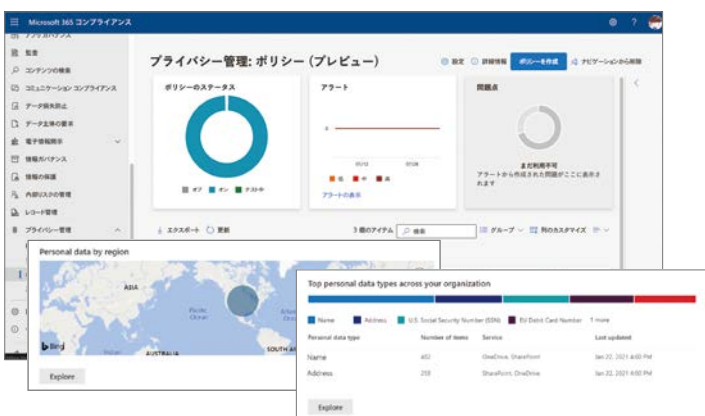
- 対応ライセンスがあれば、700 を超えるプレミアム テンプレートから 3 つまで利用可能 (4 つ目以降は、追加のアドオン ライセンスが必要)

- データセンター運用部分は既定で採点済み
- 機能の活用に応じた自動採点も実施



Microsoft 365 に統合されたプライバシー管理ソリューション

Microsoft Priva は、先回りでプライバシーのリスクを特定し、それに対する防御を支援するプライバシー管理ソリューションです。組織に存在する個人情報の検索や視覚化、エンド ユーザーからのデータ主体権利の要求に対応する機能を提供します。



- 個人データの状況、好ましくないデータの転送、データの過度な公開、溜め込みから生じるプライバシーのリスクの傾向など、組織のプライバシー態勢を可視化
- 重大なプライバシー リスクを先回りで防ぐためのカスタマイズ可能なビルトイン ポリシーを用意
- プライバシー リスクを軽減するための自動修復アクションを Microsoft Outlook や Microsoft Teams などのアプリ内に表示し、従業員の行動変容を推進
- プライバシー関連の規制に係るデータの可視化、管理、追跡、主体の権利要求などに対する運用負担やコスト軽減を実現

インサイダーリスクも想定したセキュリティの実現へ。 Microsoft 365 E5 Compliance を活用して 成りすまし攻撃者と内部リスクへの備えを強固に。

NTTコミュニケーションズ株式会社（以下、NTTコミュニケーションズ）では従来より、情報セキュリティおよびサイバーセキュリティに注力し、外部からの攻撃者への備えを常に更新してきました。そして今、NTTコミュニケーションズでは、近年発生するインシデントの傾向からサイバー攻撃だけではなく内部不正に対する対策も重要性が増していることから、情報資産の保護や監視についても取り組みを開始。リモートワークの環境下でも内部に侵入してしまった攻撃者や内部リスクをいち早く特定できるように、Microsoft 365 E5 Compliance を活用して社内の情報セキュリティを透明化。さらに、インシデントが生じてから過去のログを見直すのではなく、異常がないか監視することで重大なインシデントが生じる前に対処することを実現、社員に余計な負担をかけることなく、安心して重要情報を取り扱うことができる進化した OA 環境を整えることで、「働きやすさ」と「安心・安全」の両立を実現しています。

未曾有の「不正アクセス」の教訓から、 サイバー攻撃と内部リスク対策を実施。

NTTコミュニケーションズを始め、世界中の企業・団体が情報セキュリティおよびサイバーセキュリティの対策を練り、さまざまな施策を実施してきましたが、サイバー攻撃による情報漏洩などの事例は後を絶ちません。IT 技術は進化に伴って防御方法が変わる度に、悪意ある攻撃者たちは手法を変えて、企業・団体の活動を脅かしてきました。また、近年ではサイバー攻撃ではなく故意・過失を含めた関係者による情報資産漏洩問題も浮き彫りになっています。

そして今、NTTコミュニケーションズでは近年発生しているインシデントの傾向から、セキュリティ対策の方針を新たにしています。それが内部に侵入し、成りすまし攻撃を行うサイバー攻撃と内部リスクへの対応を目的としたゼロトラスト セキュリティの考え方に基づくコンプライアンスの強化です。

同社 情報セキュリティ部 セキュリティマネジメント室 室長である高口 正孝 氏は、次のように説明します。

「これまではセキュリティ リスクとして、外部からの不正アクセスや、標的型メールによる攻撃などを想定し、境界型防御の社内のセキュリティ環境を整備し、ユーザーの啓発も行ってきました。しかし、『転職した社員が、元の勤務先から機密情報を持ち出していた事件』のニュースなどに触れたことが、考え方を変えるきっかけになりました。そしてもう1つ、非常に大きなきっかけとなったのが、2020年5月に公表した当社で発生したインシデントです。このインシデントに際して私たちが得た教訓の1つが、内部に侵入し、成りすましていた攻撃者をいち早く特定することがいかに重要かということでした」

ID やパスワードを盗み、既存の社内ユーザーに成りすました攻撃者が、誰になりすまし、今どこにアクセスして、どのデータをコピーして持ち出したのか、あるいは改ざんを行ったのかということ迅速に把握するには、従来の外部からの攻撃者を排除する「境界型防御型のセキュリティ」だけでは対策が不十分だったのです。そこで、成りすました攻撃者や内部犯行を排除するためにコンプライアンス機能の強化が不可欠だと判断した同社では、2020年度からより効果的なソリューションを求めて検討を開始しました。

検討の結果、いくつものツールの導入や仕組みの整備などを推進。もともとデジタル改革推進部が導入を予定していた Microsoft 365 E5 Compliance を、時期を同じくしてセキュリティ強化にも活用することが決定しました。

※ Microsoft 365 Compliance は、Microsoft 365 Purview にブランド名が変更されております。

クリック1つで重要データの保護を徹底。

NTTコミュニケーションズでは、2020年8月に Microsoft 365 E5 Compliance を含むスイート製品である Microsoft 365 E5 の採用を決めると、2021年度の始まりとなる4月から段階的にさまざまなセキュリティ ソリューションを展開。中でも特筆すべきポイントが、Azure Information Protection (AIP) と、Microsoft 365 E5 Compliance に含まれる Insider Risk Management (IRM) などを活用した「内部リスクの透明化」です。

NTTコミュニケーションズでは従来から、社内のドキュメントに情報管理区分を設定し、厳格なルールに沿って運用・管理してきました。しかし、今までは「手動」による管理であり、ユーザーの判断に頼っていた側面があることは否めなかったと、高口氏は言います。「従来、機密性レベルを最高ランクの『SA』から『D』までの5段階



NTTコミュニケーションズ株式会社
情報セキュリティ部
セキュリティマネジメント室 室長
高口 正孝 氏



NTTコミュニケーションズ株式会社
情報セキュリティ部
セキュリティマネジメント室 担当課長
早川 宏 氏



NTTコミュニケーションズ株式会社
デジタル改革推進部
情報システム部門 担当部長
豊嶋 剛司 氏



NTTコミュニケーションズ株式会社
デジタル改革推進部
情報システム部門 担当課長
井上 秀治 氏

に設定し、書面にも表示して運用管理してきました。しかし基本的には人の手によって管理されていたので、セキュリティ上の穴がなかったかと言えば、心許ない部分もありました」

そこでNTTコミュニケーションズでは、人の手による運用に生まれる「穴」が発生しないように、AIPを導入してドキュメントの保護を自動化。併せて機密性レベルのルールを見直し、機密性レベルの呼称も「3」を最高レベルとして、お客様などの社外ともやり取りが行える「0」までの4段階を再設定。機密性レベル「1」以上に設定されたドキュメントにおいては閲覧者の限定や、閲覧履歴の確認、配布後の閲覧停止までコントロールできる環境が整っています。

高口氏は、AIPの導入によって実現したこの環境を「社員にとっても働きやすい環境」だと話します。

「社内で作成するドキュメントはもとより、お客様から提供されたドキュメントまで、Office製品のツールバーから機密レベルを選んでクリックするだけで、機密性レベルに応じて『暗号化』が自動的に設定されるようになっており、開示範囲もカスタム設定できるようになっています。これまでの手動管理とは大きな違いです」

社内のモニタリングに活用。

IRMは、組織内の不審なアクティビティを検出、調査、および操作できるようにすることで、内部リスクを最小限に抑えるのに役立つコンプライアンスソリューションです。必要に応じて、組織内で識別および検出するリスクの種類を定義することで「機密データの流出」を含めた広範な内部リスクを特定し、調査および対処することに役立ちます。

同社では主に外部からの「なりすまし侵入者」に備えることを主眼としていますが、「不審な振る舞いを検出できる仕組みの運用には、セキュリティに関する社内の理解を高めることが必要だった」と情報セキュリティ部セキュリティマネジメント室担当課長早川氏は説明します。

「まず、グループ内のセキュリティ意識を向上させる目的で、2020年の夏頃から各組織、各グループ会社へのキャラバンを行ないました。このキャラバンでは情報漏洩などの内部リスクに関する過去のヒヤリハット事例なども交えて、原因と対策の説明、ゼロトラストセキュリティについて認識するように努めました。AIPやIRMなどのサービス導入時に際しては、利用マニュアルも作成し、ヘルプデスクも新設しました」

さらに、日常的なセキュリティ研修なども充実させていると早川氏は続けます。

「年に1回、オンラインで全社セキュリティ研修を実施しているほか、新しく入社される方にもセキュリティ研修を受講してもらっています。そのほか、組織、各グループ会社を含めた『セキュリティ委員会』を設置して定期的に会議を行い、ハンドブックやマニュアルの作成など継続的な啓発活動を進めています。また年末には『セキュリティ週間』というイベントも行っています」

ビジネスの成長のために、終わりなきセキュリティとコンプライアンスの追求を。

NTTコミュニケーションズでは、こうしてゼロトラストセキュリティの確立に向けてシステム活用と、セキュリティ教育を進めていますが、Microsoft 365 E5の活用は「まだ始まったばかり」だとデジタル改革推進部情報システム部門担当課長井上秀治氏は言います。

「Microsoft 365 E5という包括的なパッケージの中で各機能の親和性も高いため、AIPやIRMの展開も短期間に終わらせることができました。こうしたスピード感を得られることは、大きなメリットだと思います。実際にE5 Complianceを導入してから半年で、一定の成果も上がりました。しかし、Microsoft 365 E5は非常に多機能ですので、すべて展開して使いこなすにはまだ時間がかかるでしょう。IRMも、広範な内部リスクに備えた機能を備えていることもあり、ユーザーのアクティビティに対して、どこをチェックするように設定すれば私たちの求める、適切なアラートや監査ログが得られるのか試行錯誤しています。今でも一定の効果を感じていますが、今後も運用状況をフォローしながら範囲の拡大も検討し、より良い成果が得られるよう進めていきたいと思います」

デジタル改革推進部情報システム部門担当部長豊嶋剛司氏は「セキュリティに終わりはない」と前置きした上で、次のように話します。「セキュリティと利便性は、相反する関係にあります。テクノロジーが進化する中、ITの利便性が後退することはありません。テクノロジーが進化すれば、それに伴ってセキュリティ対策も絶えず変化していきます。当社もこれから先、セキュリティへの取り組みを継続していきますが、OA環境自体は、今よりも利便性が高く、生産性の優れたものになるでしょう。NTTコミュニケーションズやNTTグループ内へ、Microsoft 365 E5や、セキュアなFAT端末である『セキュアドPC』の活用によるノウハウの蓄積により、お客様へゼロトラストセキュリティを提示できる、当社ならではの新しいセキュリティソリューションを確立したいと考えています。その実現のためにも、マイクロソフトの高いソフトウェア開発力で、高度なソリューションが提供され続けることを期待しています」


最後に、高口氏は言います。

「世の中が急激にクラウドに移行し、SaaSやPaaSなどマイクロソフトはもとより、星の数ほどのサプライヤーがサービスを展開している中、当社としてもそれらを活用しつつ、いかに高度なセキュリティを保ち続けていくかということが、大きな課題になっていると実感しています。セキュリティインシデントは、今や企業の命運を左右するほどの一大事です。そのようなリスクを遠ざけ、安心してビジネスを展開するためには、ゼロトラストセキュリティを確立することが不可欠だと思っています。その一助として、マイクロソフトには新しいサービスの提供だけでなく、グローバルで先進的な事例やセキュリティのトレンドなどに関する情報を提供してくれることを期待しています」

●本お客様事例は、インターネット上でご覧いただけます。
<https://customers.microsoft.com/ja-jp/>

Microsoft Purview 機能一覧

 <h2>Information Protection & Governance</h2> <p>機密情報保護への意識付け</p> <ul style="list-style-type: none"> 自動もしくは手動で個人情報・機密情報の識別 ユーザーに見える形で情報のラベル付け、保護、取り扱いに関する警告 分類に応じた情報のライフサイクル管理 	 <h2>Insider Risk Management</h2> <p>悪質なケースで個別調査</p> <ul style="list-style-type: none"> ユーザー操作を定量的に監視し、機密情報・個人情報の取り扱いに関するリスク識別 社内外での不適切なコミュニケーションを検出 利益相反するユーザー間のコミュニケーションを制限 	 <h2>eDiscovery & Audit</h2> <p>訴訟に備え否認防止・証拠保存</p> <ul style="list-style-type: none"> 効率的なコンテンツ検索と、機会学習ベースの検索結果の絞り込みおよび抽出 長期のログ保存と、インシデント時に重要となる追加ログの記録
--	---	--

 <h2>Compliance Manager</h2>	コンプライアンス対応状況を各国規制に従って継続的に評価	対策不備を継続確認
---	-----------------------------	-----------

ライセンス	機能	概要	
Microsoft 365 E5 Compliance	トレーニング可能な分類器	マシン ラーニングで類似するドキュメントや表現をマッチング	
	完全なデータ一致	型ではなく顧客データベース等の実データの値を元にマッチング	
	Office 365 での自動ラベル付け	SharePoint Online / OneDrive for Business に保存されたファイルや Office Online での自動分類	
	エンドポイント データ損失防止	端末上での機密情報の漏洩を監視・防止	
	オンプレミス スキャナー / DLP	AIP スキャナーの拡張で、ファイル サーバーや SharePoint Server に保護すべきファイルが見つければラベルを適用もしくは権限を変更	
	データ ライフサイクル管理	削除からの保護と一定期間での削除	
	カスタマー キー	テナントの暗号化キーをお客様が所持	
	高度なメッセージ暗号化	外部へ送信する暗号化メールのブランディングのカスタマイズと取り消し	
	Teams でのデータ損失防止	Teams チャット内で機密情報を検出し送信を防止	
	二重キー暗号化	お客様側で個別に管理するサーバーも使ってファイルを暗号化	
	Insider Risk Management	内部リスクの管理	ユーザーを軸に機密情報の漏洩が疑われる一連の操作を分析し、レビュー
		コミュニケーション コンプライアンス	不適切な単語の利用や不正が疑われるコミュニケーションを監査
		情報バリア	特定組織のメンバーが Teams・SharePoint で情報を発信できる先を制限
		カスタマー ロックボックス	マイクロソフト運用担当者が生データにアクセスする際、お客様承認を必須に
		特権アクセス管理	特権の利用を制限し統制
eDiscovery & Audit	監査 (Premium)	最大1年間の監査ログの保持と追加の操作記録	
	電子情報開示 (Premium)	Teams コンテンツにも対応し、検索で抽出したデータを複数の監査担当者でレビュー	
Compliance Manager	コンプライアンス マネージャー	GDPR、NIST 800-53、ISO 27001 やカスタムでの対策の評価・アセスメント	
関連サービス	監査ログ延長	10年間ログ保管延長	
	Compliance Manager	プレミアム テンプレート	
	Priva	プライバシー リスク管理	Microsoft 365 のコンテンツの中から個人情報の所在やリスクを可視化する単独製品
		主体の権利要求	個人情報の主体からの要求に応じて保持している個人情報を特定し、レビューし、レポートする機能
	データ コネクタ	各社製のコネクタ (Microsoft, Veritas, TeleMessage, 17a-4 LLC, CellTrust)	電子情報開示、保持、監視等 Microsoft Purview 機能を 3rd Party アプリに適用するために、3rd Party アプリに応じてデータをメールボックスに取り込むための各種コネクタ
	Azure 従量課金	データ マップ	IaaS / PaaS 上の各種データを定期的にスキャンしデータの所在を明確化
データ カタログ		IaaS / PaaS 上の各種データを各種機密情報定義に従って分類し一覧	
データ資産の分析情報		IaaS / PaaS 上の各種データの検出・分類状況を視覚化	

よくあるお問い合わせ



Q: 社内では端末の操作を事細かくログを取る製品を導入しています。情報持ち出し対策として十分でしょうか?

A: 十分ではありません。過去の情報持ち出しのインシデントの反省から、会社としての説明責任を果たすためにあらゆるログを集めておくという運用も考えられます。ただし、それだけでは情報持ち出しを防ぐ方法としては、効率的ではありません。ログを収集したとしても、それらの中からタイムリーに不正を見つけるようにしなければ、今起こっている不正は防げません。また、闇雲に大量のログを集めていると、日常的な監視は困難となります。「経済産業省 秘密情報の保護ハンドブック」にあるように、社外秘の情報であることを明示し、それらに対する不正な操作は防止または警告してユーザーの意識向上を図ると共に、効率的な監視ツールを用いて社内での不正に対する視認性を高め、不正の芽をユーザー単位で見つけてタイムリーに対処することが重要となります。

Q: ファイルを事前にすべて暗号化しておこうと思いますが、有効なセキュリティ対策でしょうか?

A: 必ずしも有効なセキュリティ対策ではありません。Microsoft 365 環境下では、秘密度ラベルによりファイルを暗号化していても、全文検索やブラウザーでの表示・編集、共同編集、eDiscovery 対応など、生産性への影響を最小化することが可能です。ただし、現場でのデータの再利用性の制限、外部への共有、システム間連携、暗号化解除の運用、今後の M&A 等によるシステム・環境の移行などを考えると、闇雲にすべてのファイルを暗号化した場合、日々の管理工数増大による生産性への影響やシステム環境が移行しづらくなるというデメリットの方が大きくなることもあります。重要なのは、ファイルをすべて暗号化することではなく、ユーザーを教育して正しい情報の分類と扱いを理解してもらい、適切な保護手段を都度判断して適用してもらうことです。また、全社員が最初から情報を分類し保護する必要があるわけではなく、個人情報や機密情報を管理する主に広報、人事、経営企画、経理、開発などの担当者が、適切な情報保護手段を用いてこれらの情報を管理・流通させることがまずは大切です。

Q: 社内の監視は、どこまで許されるのでしょうか?

A: 厳密には、社内のプライバシー ポリシーや就業規則等で説明されていることが望ましいですが、正しい業務遂行を管理監督し不正が行われていないことを一定程度保証するため、会社支給の端末やクラウド環境上での社員の就業時間中の行動や会話を監視することは、職場環境に対する善管注意義務の範囲内と考えられます。ただし欧州では、Web アクセスのログなどを通じて個人の通院履歴や病歴など機微な個人情報に該当するような情報を収集すると、一段と高いルールでログを管理する必要性が発生するため、事前に注意喚起を行い、収集されたデータの用途などを限定しておくことも重要です。またドイツなど労働組合の合意が必要となるようなケースでは、これら収集したデータは全社的なコンプライアンス担当者により不正の有無の確認のみに限定して利用し、上司が日常的に見て職務怠慢かどうかといったパフォーマンスの評価に使わないように留意することも必要です。

Q: コミュニケーションの監視で、さまざまな不正を防ぐことができるのでしょうか?

A: 複数の社員の共謀による犯行や、権限が集中していて誰にも監視されていない状況下での単独犯行など、不正が進行している状態においては、コミュニケーションの監視だけでは不正を見つけることも防ぐこともできません。限定的な社員による進行した不正については、職能の分割や定期的な人事異動等により防ぐ必要があります。一方で会社の責任としては、今後発生しうる組織ぐるみで行われる不正についての検知や対策、再発防止についても検討する必要があるため、この場合は不正の前段階で行われる不正への勧誘や意識合わせなどのコミュニケーションの監視で検知し、早期対処することが可能です。

Microsoft Purview についてはこちら
<https://aka.ms/mspurview-jp>



Microsoft Priva についてはこちら
<https://aka.ms/mspriva-jp>



お問い合わせは弊社営業またはパートナーまで

本資料は情報提供のみを目的としており、2023年7月時点での情報を基に作成したものです。状況等の変化により、内容は変更される場合があります。マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。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/> ■マイクロソフト 購入相談窓口 0120-167-400 (9:00~17:30 土日祝日、弊社指定休業日を除きます) ※電話番号のおかけ間違いにご注意ください。ご購入に関するお問い合わせは、マイクロソフト認定パートナーへ。■マイクロソフト認定パートナー <http://www.microsoft.com/ja-jp/partner/>