

Microsoft  
**Security Forum 2020**



A-3

クラウドからエンドポイントまで  
企業に内在するリスクを管理する  
～Microsoft Compliance ソリューションのご紹介～

日本マイクロソフト株式会社  
クラウド&ソリューション事業本部 モダンワークプレイス統括本部 CISSP  
山本 明広



# Microsoft 365 が提供するセキュリティとコンプライアンス

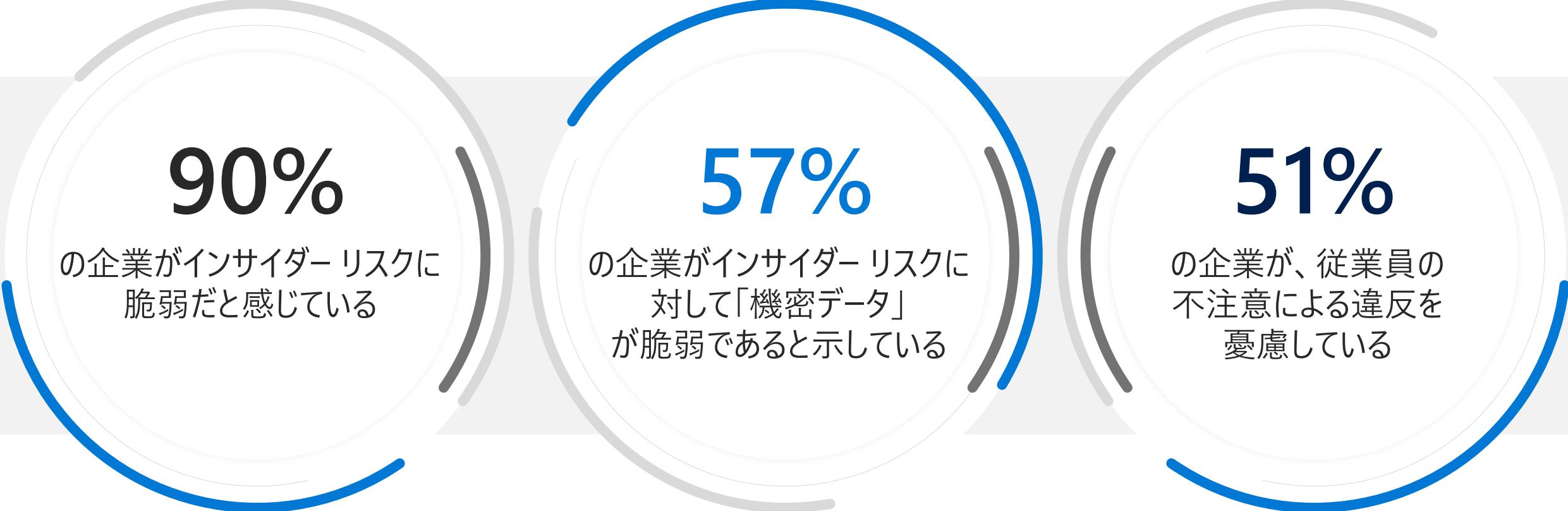
## 外部リスク対策



## 内部リスク対策



# 外部攻撃だけではなく内部犯行への対策も重要



90%

の企業がインサイダー リスクに  
脆弱だと感じている

57%

の企業がインサイダー リスクに  
対して「機密データ」  
が脆弱であると示している

51%

の企業が、従業員の  
不注意による違反を  
憂慮している

# IPA プレス発表「情報セキュリティ 10 大脅威 2020」と実被害の動向

順位	「組織」の 10 大脅威
1	標的型攻撃による被害
2	<b>内部不正による情報漏洩</b>
3	ビジネスメール詐欺による被害
4	サプライチェーンの弱点を悪用した攻撃の高まり
5	ランサムウェアによる被害
6	予期せぬIT基盤の障害に伴う業務停止
7	<b>不注意による情報漏洩(規則は遵守)</b>
8	インターネットサービスからの個人情報の窃取
9	IoT 機器の不正利用
10	サービス妨害攻撃によるサービスの停止

## 関連する実被害・ニュース

2019/12

### 廃棄情報機器の不正販売

個人情報が含まれたHDDを廃棄担当会社の社員が不正に持ち出してオークションで販売

2019/11

### 元従業員による顧客情報の不正持出

12万人分の顧客情報が従業員によって、持ち出されなりすましに悪用

# コンプライアンス および リスクマネジメント ソリューション



## Information Protection & Governance

データのライフサイクルを通じて  
データを保護し、統治します



## Insider Risk Management

重要な内部者リスクを特定し、  
対策を講じます



## eDiscovery and Audit

関連データの迅速な調査と  
対応を可能とします



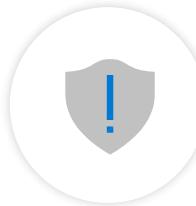
## Compliance Management | コンプライアンスの簡素化とリスクの低減

# コンプライアンス および リスクマネジメント ソリューション



## Information Protection & Governance

データのライフサイクルを通じて  
データを保護し、統治します



## Insider Risk Management

重要な内部者リスクを特定し、  
対策を講じます



## eDiscovery and Audit

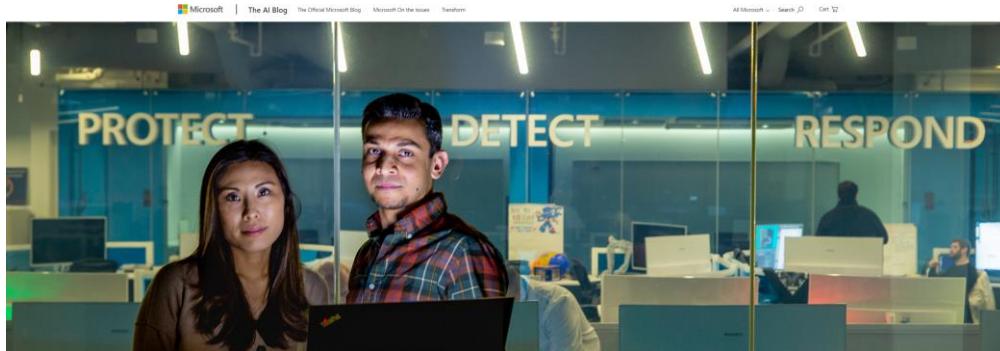
関連データの迅速な調査と  
対応を可能とします



## Compliance Management | コンプライアンスの簡素化とリスクの低減

# インサイダーリスクマネジメント

機械学習を使用して“**Microsoft 社内**”のデータ漏洩とインサイダーリスクを阻止する  
15万人の従業員の情報ガバナンスを管理



How Microsoft 365's new solution uses machine learning to stop data leaks and insider attacks



Bret Arsenault,  
Microsoft corporate vice president  
Chief Information Security Officer.

## マイクロソフトコンプライアンスソリューションの強み

### 1. マイクロソフトの従業員15万人の環境下で活用中

コーポレートバイスプレジデント兼最高情報セキュリティ責任者であるBret Arsenault の依頼により、各国のプライバシーに配慮されセキュリティチーム、Microsoft 365のエンジニア、人事、マイクロソフト内の専門家と連携し作成された。社内ソリューションの一部としてインサイダーリスク機械学習アルゴリズムを最初に開発し、世界中の150,000人の従業員によって既に生成されたデータから潜在的なインサイダーリスクをより適切に検出しました。

既存のツールの監査ログを使用する異常検出は、従業員にとって生産性を下げない方法でセキュリティを提供できるようにした。

### 2. 機械学習と Microsoft Graph を活用し 従業員に対して利便性を阻害しないソリューションを提供

機械学習アルゴリズムを使用して、SharePointサイトから数百の機密ファイルをダウンロードしたり、USBデバイスにファイルをコピーしたり、セキュリティソフトウェアを無効にしたり、社外の機密ファイルをメールで送信したりする、異常で潜在的に危険な動作のパターンを探します。Microsoft Graphやその他のサービスを活用して、Windows、Azure、および SharePoint、OneDrive、Teams、OutlookなどのOffice製品全体で異常な信号を探します。

Microsoft  
**Security Forum 2020**



# Video Insider Risk Management





インサイダーのリスクと行動規範に対する  
ポリシー違反を特定する2つのソリューション



Insider Risk Management

Communication Compliance

Microsoft  
**Security Forum 2020**

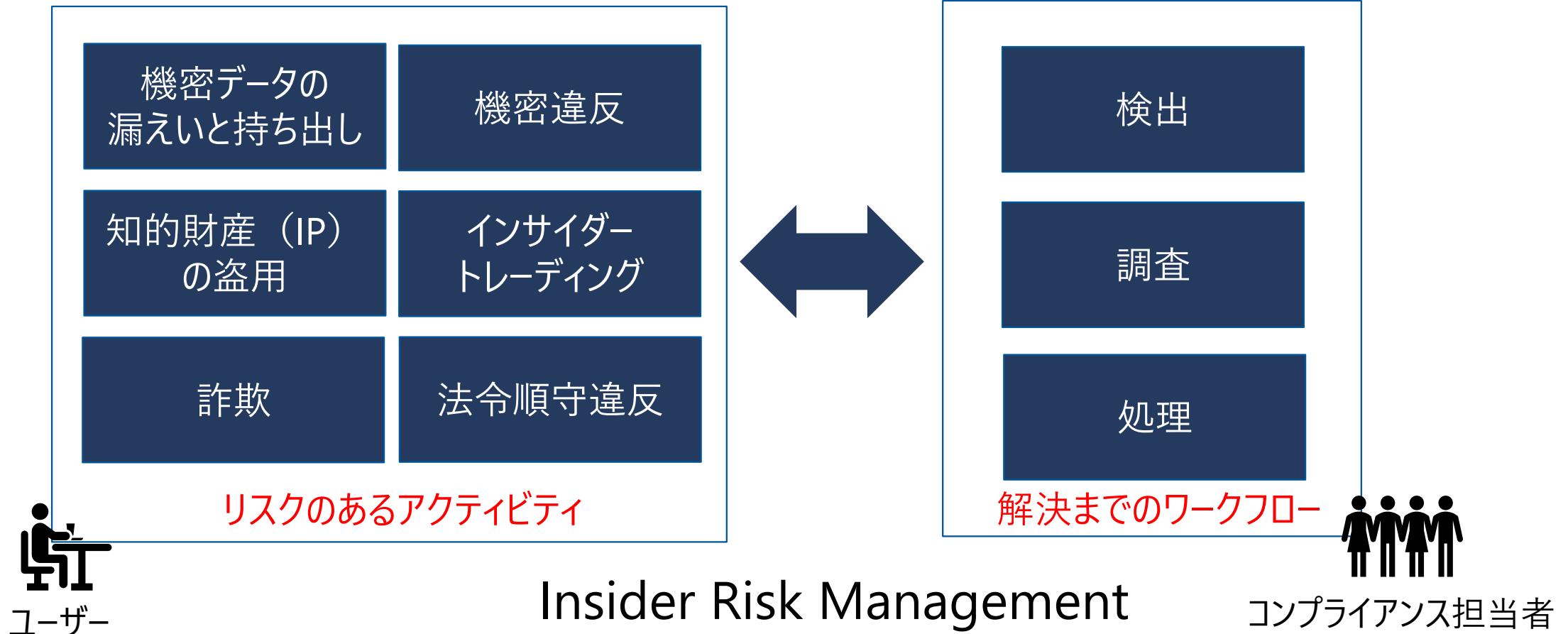


# Insider Risk Management 内部リスクの管理

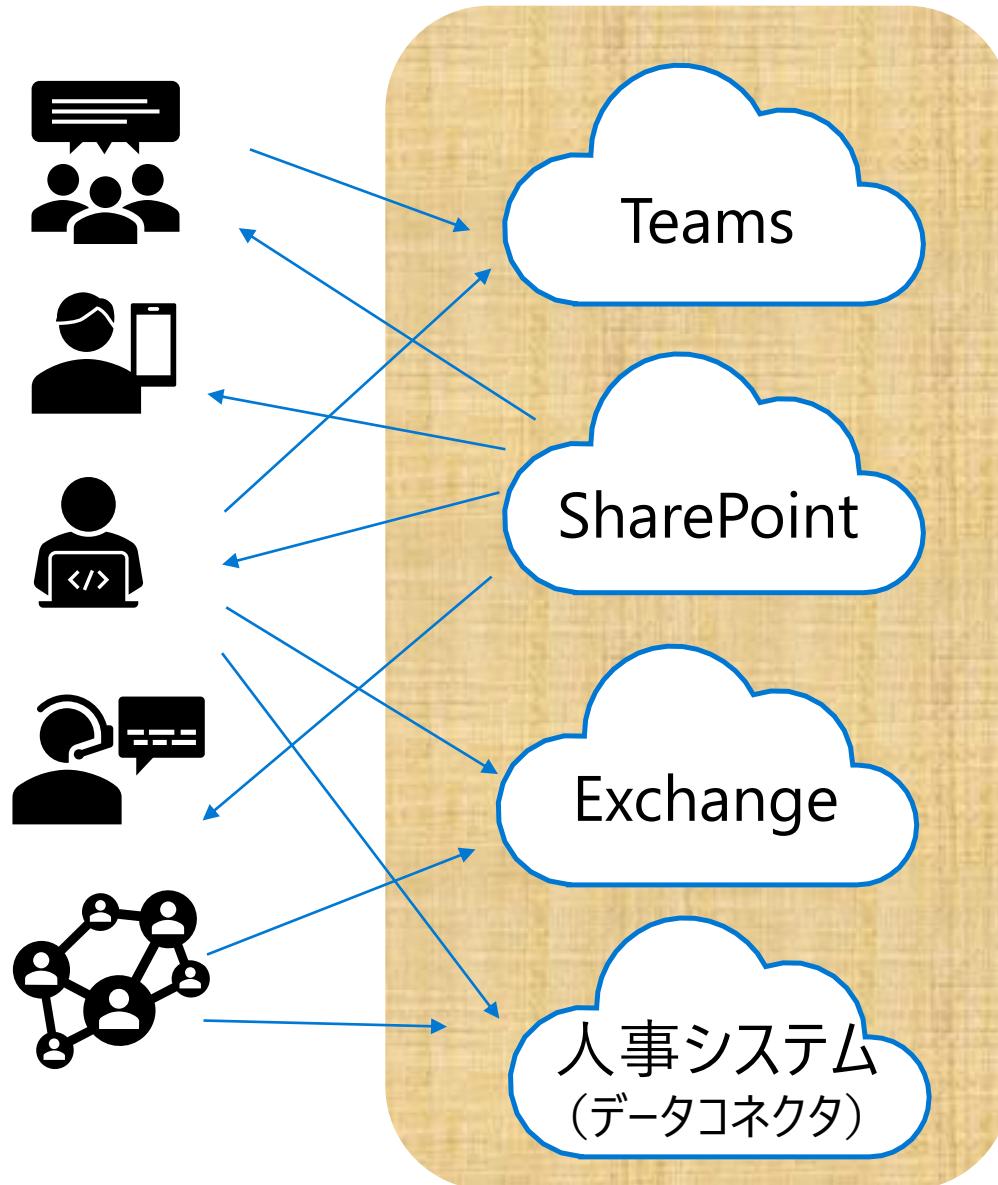


# Insider Risk Management とは

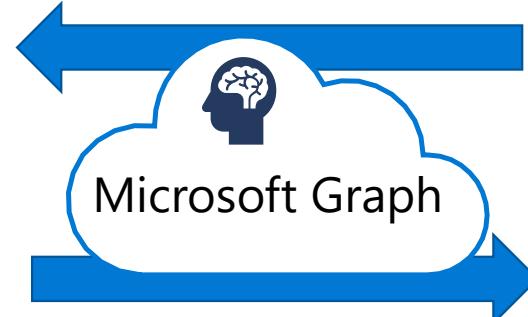
- ・ 社内のリスクを検知・分析し対処を実施するまでの一連のワークフローを提供



# リスクアクティビティの検出と対処



ユーザー活動の分析



インサイダーリスクの検出



コンプライアンス担当者

# インサイダー・リスクの検出

- 事前に定義されたプレイブックに従いリスクを検出

## 規定で用意されているプレイブック

退職する従業員による  
データの盗難

## 検出可能なアクティビティ

退職日付近に機微性の高いファイルをサイトからダウンロードしポータブルデバイスへコピーや印刷して持ち出す等の行為

機密情報の意図的または  
意図しない漏えい

機微性の高いファイルの外部ユーザーへの共有やポータブルデバイスへのコピー、組織外へのメールの送信等の行為

企業ポリシーに違反する言動

不適切または不快な言葉を含む電子メールメッセージの送信行為

# リスク指標とトリアージ

- リスク指標を機械学習により分析し、トリアージを実施

## 指標

内部リスクのポリシー テンプレートでは、検出および調査するリスク アクティビティの種類を定め、実行したときにアラートをトリガーする指標に基づいています。ポリシー テンプレートに含まれる指標

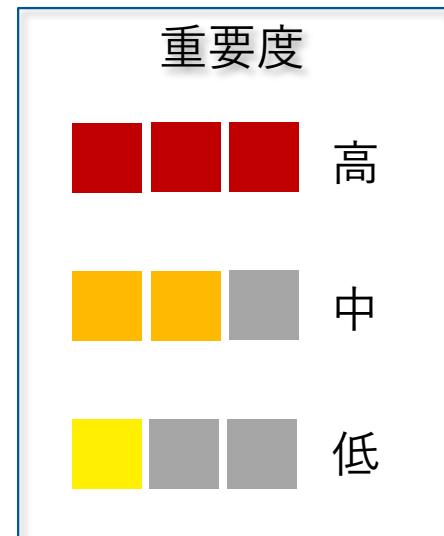
- すべて選択
- SharePoint Online からのファイルの共有
- SharePoint Online からのフォルダーの共有
- SharePoint Online サイトの共有
- SharePoint Online からのコンテンツのダウンロード
- 組織外へのメール送信
- 機密ファイルの USB へのコピー (近日公開の機能)
- 機密ファイルのクラウドへのコピー (近日公開の機能)
- 機密ドキュメントの印刷 (近日公開の機能)
- メールでの不快な言葉の使用
- 過去のポリシー違反
- 異常なアクティビティの評価



- アクティビティの種類
- アクティビティの発生回数や頻度
- ユーザーリスクアクティビティの履歴
- アクティビティの深刻さを高める可能性があるアクティビティ



連アクティビティ



トリアージの  
自動化

# 重要度の高いコンテンツの重みづけ

- 関連するコンテンツが配置されている場所、機密情報の種類、および適用される機密ラベルに基づいて、より高いリスクスコアを検出されたアクティビティに割り当てることが可能

SharePoint  
サイト

機密情報の種類

秘密度ラベル

- 顧客情報サイト
- 開発製品サイト
- 人事情報サイト など

- クレジットカード番号
- パスポート番号
- 特定のプロジェクト名 など

- 社外秘
- 極秘
- 機密 など

# ユーザーのプライバシー保護

- ユーザー名はランダムに仮名で表示されるためプライバシーの保護と公平な監査を実施可能

**プライバシー**

Microsoft では、あなたとユーザーにとってプライバシーがいかに重要かを認識するため、ユーザーについて、実際の名前を表示するか、匿名化された名前を使用して Identity がどのように扱われるかを確認する方法を実装しています。

**匿名化されたユーザー名を表示する**  
すべての内部リスクの管理機能 (ポリシー、アラート、ケースなど) で匿名化されたユーザー名が表示されます。

**匿名化されたユーザー名を表示しない**  
内部リスク ポリシーと一致するアクティビティを実行したすべてのユーザーが、実際のユーザー名で表示されます。

**既定ではユーザー名は仮名で表示される**



The screenshot shows the Microsoft Identity Protection dashboard. At the top, it displays 'Alerts to review' with 2 Medium and 1 Low severity alerts. Below this, 'Policy matches' are listed: 'Confidentiality obligation during departure' (Medium), 'Project Osiris Confidentiality' (Medium), and 'Anti-harrasment policy' (Low). On the right, a table shows detected users with their names (Anony85KF-34..., AnonyO4J5-34..., AnonyF3FD-34...) and the time they were detected (6 months ago, 2 years ago, 2 years ago). A large orange callout box on the right side of the dashboard states '既定ではユーザー名は仮名で表示される' (By default, user names are displayed as pseudonyms).

※必要な場合の時のみ匿名化を解除可能

# ユーザー アクティビティの調査

- アラートで検知したユーザーのアクティビティを相関分析、更に人事情報と関連付けた一連の操作を時系列で表示

## Insider risk management

Overview   Alerts   Cases   Policies   **Users**   Notice templates

The users here performed activities that matched one or more of your inside user's license changes, the scope of policies might change for that user. [Learn more](#)

↓ Export   Add user to a policy

Users	Risk level	Active alert
AnonyIS8-978	High	0
AnonyDB4-I35	Low	0
Anony85KF-34DF	Low	0

### History of recent user activity

	All activities	Anomalous activities
	4	0

October 22, 2019 6:00 AM  
**HR event: Resignation date set**  
Resignation date set for: November 2, 2019 6:00 AM

October 21, 2019 5:17 AM  
**Files printed**  
Risk score: 65  
10 files were copied to USB devices  
6 files contain sensitive info including: ABA Routing Number  
4 files have labels including: Internal Only

October 21, 2019 1:46 AM  
**Files copied to USB device**  
Risk score: 92  
113 files were copied to USB devices  
47 files contain sensitive info including: ABA Routing Number  
54 files have labels including: Internal Only

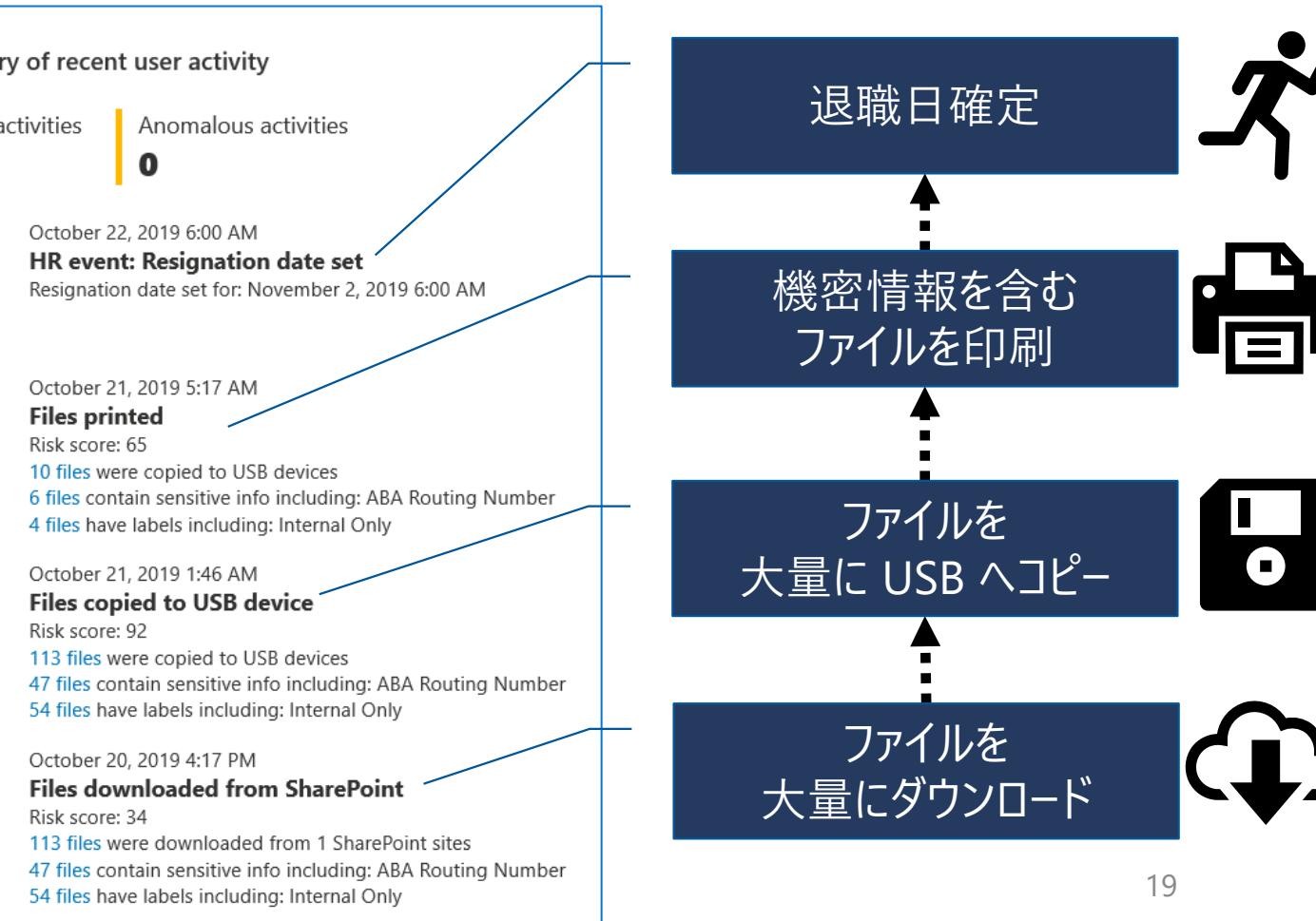
October 20, 2019 4:17 PM  
**Files downloaded from SharePoint**  
Risk score: 34  
113 files were downloaded from 1 SharePoint sites  
47 files contain sensitive info including: ABA Routing Number  
54 files have labels including: Internal Only

退職日確定

機密情報を含む  
ファイルを印刷

ファイルを  
大量に USB ヘコピー

ファイルを  
大量にダウンロード



# リスクアクティビティへの対処 ケースの管理

- 本格的な調査開始のためのケースを作成し、関係者のアサインおよび追加情報の調査とエスカレーションを実施

**Alert: Confidentiality obligation during departure**

Overview User activity User profile

History of recent user activity

All activities 4 Anomalous activities 0

October 22, 2019 6:00 AM  
**HR event: Resignation date set**  
Resignation date set for: November 2, 2019 6:00 AM

October 21, 2019 5:17 AM  
**Files printed**  
Risk score: 65  
10 files were copied to USB devices  
6 files contain sensitive info including: ABA Routing Number  
4 files have labels including: Internal Only

October 21, 2019 1:46 AM  
**Files copied to USB device**  
Risk score: 92  
113 files were copied to USB devices  
47 files contain sensitive info including: ABA Routing Number  
54 files have labels including: Internal Only

Case details User details

**Case name**  
Case 884: (RO) Potential IP theft

**Case status**  
Active

**User's risk score**

91 / 100

IP 盗難の可能性がある  
ケースとして登録

Confirm alert to an existing case Dismiss alert

ケースを作成し  
本格的な調査を開始

アナリスト、調査官の  
アサイン



本人および上司への確認



法務部門等を巻き込んだ  
更なるエスカレーション



# リスクアクティビティへの対処 関連するコンテンツの調査

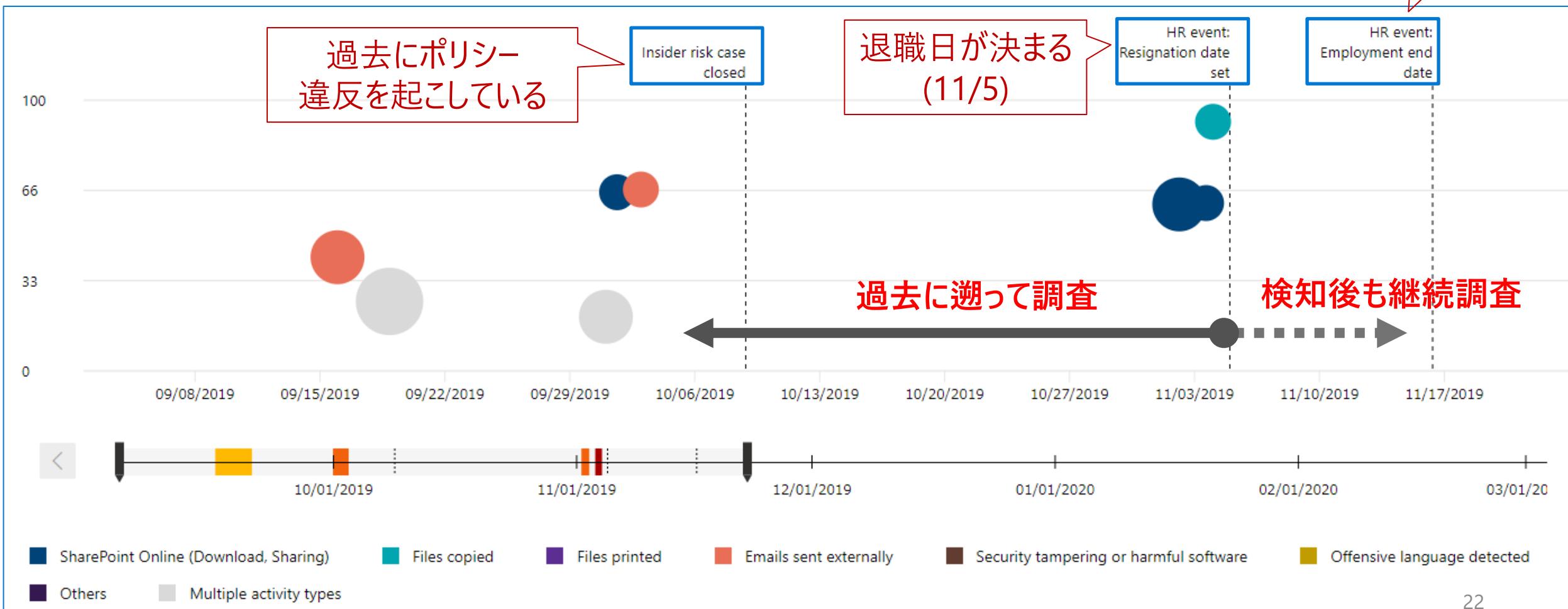
- ・ コンテンツ エクスプローラーを利用し持ち出されたファイルの内容を確認

## リスクアクティビティへの対処

# ユーザー活動の追跡

- 過去にユーザーが行った活動も併せてタイムラインで表示

退職日  
(11/16)



Microsoft  
**Security Forum 2020**



# Demo

Insider Risk Management  
リスクアクティビティへの対処



Microsoft  
**Security Forum 2020**



Communication Compliance  
コミュニケーションコンプライアンス



# コミュニケーション コンプライアンス

コミュニケーションのリスクを  
迅速に識別し修復



## 企業ポリシー

モラルなどの企業基準を遵守



## リスク管理

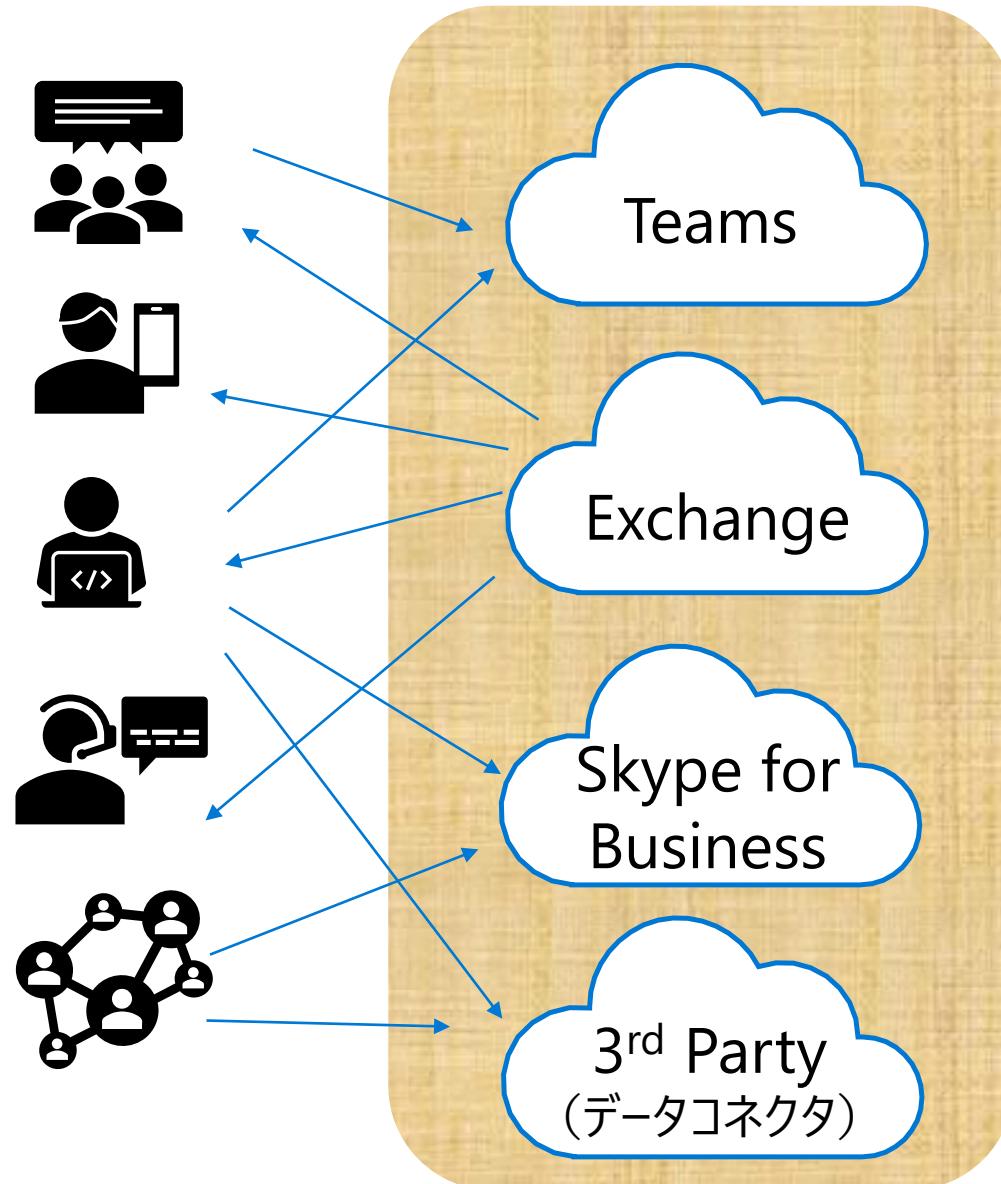
法的リスクと企業のリスクの特定と管理



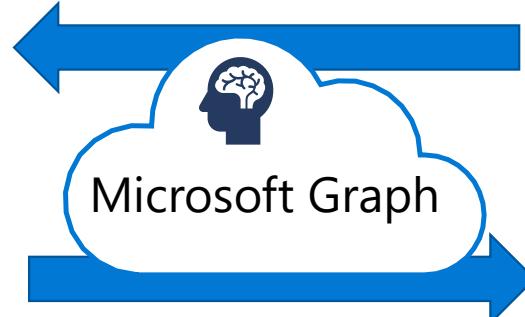
## 規制の順守

規制コンプライアンス標準の監視

# コミュニケーションリスクの検出と対処を提供



通信チャネルのスキャン



コミュニケーションリスクの検出

Communication Compliance

アラート	トリアージ
調査	対処



コンプライアンス担当者

# コミュニケーションリスクの検出

## 規定で用意されているプレイブック

## 検出可能なアクティビティ

### 不快な言葉の監視

組み込みの分類辞書を利用し、不適切または不快感を与える可能性があるコンテンツを自動的に検出

### 機密情報の監視

定義された機密情報の種類またはキーワードを含む通信をスキャンして、重要なデータの不適切な共有を防止

### 規制のコンプライアンスの監視

不適切または不快な言葉を含む電子メールメッセージの送信行為

### カスタムポリシー

組織内の監督に対して確認する特定の通信チャネル、個々の検出条件（キーワードなど）、および監査を実施するコンテンツの量を調整

# 監査対象となるサービスと通信の種類

サービス	通信の種類
Microsoft Teams	<ul style="list-style-type: none"><li>チャネル内のメッセージ</li><li>個々のチャット</li><li>添付ファイル</li></ul>
Exchange Online	<ul style="list-style-type: none"><li>メール本文</li><li>添付ファイル</li></ul>
Skype for Business Online	<ul style="list-style-type: none"><li>チャット</li><li>添付ファイル</li></ul>
3 <sup>rd</sup> Party のソース※ Instant Bloomberg, Facebook, LinkedIn, Twitter, カスタムデータコネクタ	<ul style="list-style-type: none"><li>チャット</li><li>メッセージ</li></ul>

# アクティビティの調査

- アラートを基に実際のメッセージを確認し対処を実施

コミュニケーション コンプライアンス > ポリシー > **Offensive or threatening language**

検知されたキーワードを強調表示

メッセージに対するコメントやマークを追記

履歴から過去に違反があったかどうかを確認

本人への通知やエスカレーション等を実施

概要 保留中 (20) 解決済み (1)

フィルター クエリを保存 フィルター

Things I need to say

ソースビュー テキストビュー 注釈ビュー ユーザーの履歴 (0)

From: Irvin Sayers <IrvinS@M365x533288.OnMicrosoft.com> on behalf of Irvin Sayers  
Sent on: Wednesday, February 26, 2020 8:53:27 AM  
To: Isaiah Langer <IsaiahL@M365x533288.OnMicrosoft.com>  
Subject: Things I need to say

you pathetic and dumb  
how r u jerk [REDACTED] e ?  
You're a moron, go back to your country  
I don't like you == I will hurt you

通知  
エスカレーション  
ケースの作成  
誤検知  
準重複 (3)  
完全な重複 (3)  
メッセージの詳細を表示

1 個のアイテムが選択されています。合計 20 個のアイテムがあります。

解決 タグ付け

Microsoft  
**Security Forum 2020**



# Demo

Communication Compliance  
コミュニケーションリスクへの対処



# コンプライアンス および リスクマネジメント ソリューション



## Information Protection & Governance

データのライフサイクルを通じて  
データを保護し、統治します



## Insider Risk Management

重要な内部者リスクを特定し、  
対策を講じます



## eDiscovery and Audit

関連データの迅速な調査と  
対応を可能とします



## Compliance Management | コンプライアンスの簡素化とリスクの低減

Microsoft  
**Security Forum 2020**



# Information Protection & Governance

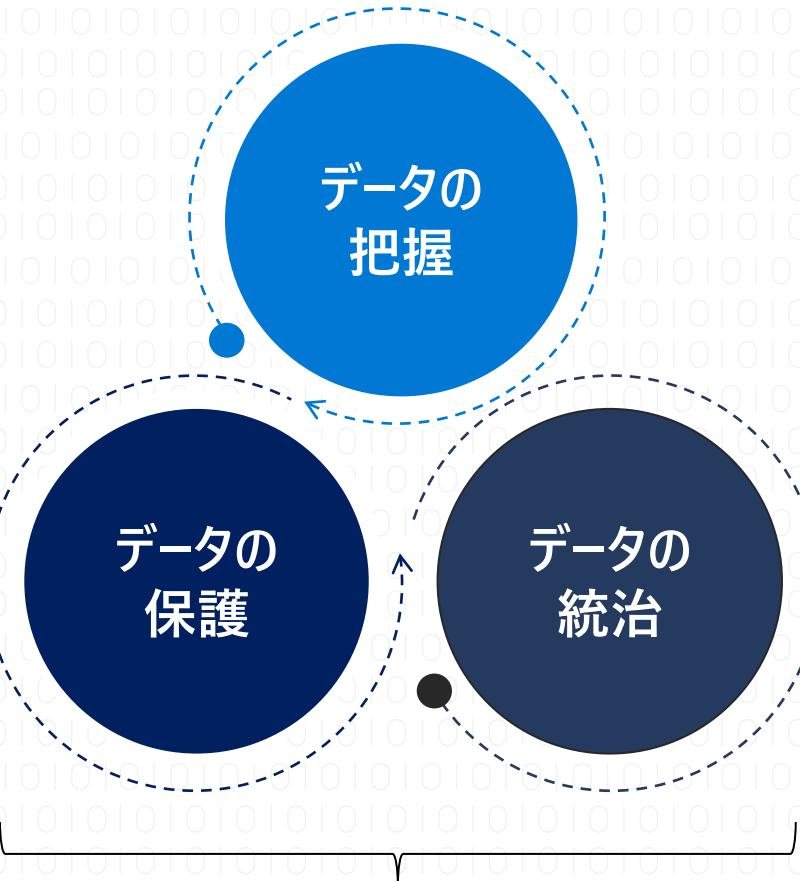


# Information Protection & Governance

データがどこに存在しようとも  
保護し統治します

暗号化、ビジュアル  
マーキング、DLP を含む  
保護アクションを適用

データ全体を理解し、ハイブリッド環境で  
重要なデータを特定



インテリジェントなプラットフォームを搭載  
自動データ分類、ポリシー管理、分析  
API への統一されたアプローチ

# データ分類の概要 (ダッシュボード)

組織全体の機密データおよびビジネスクリティカルデータの把握



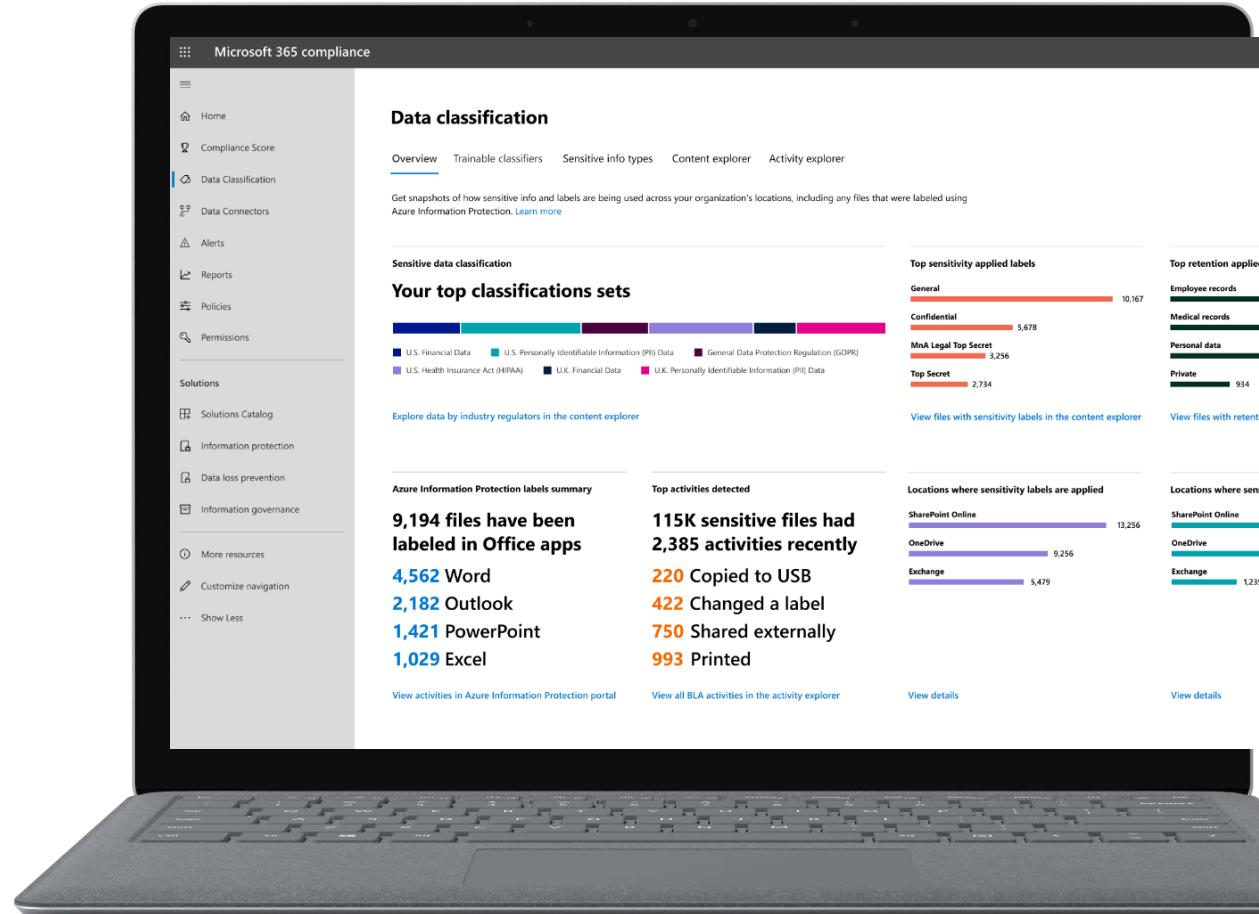
機密情報およびビジネスクリティカル情報の数と場所の可視化



機密情報に関する危険な行動を監視して DLP ポリシーを通知

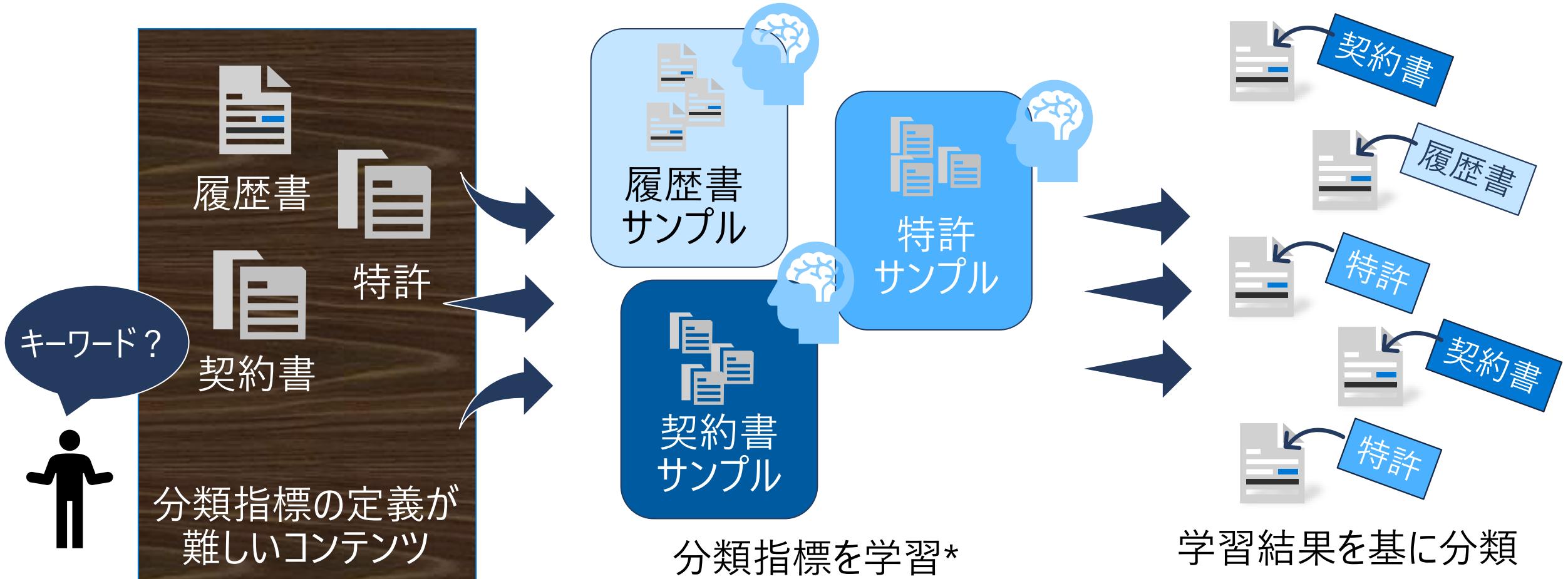


テナント全体でのラベル使用率をレポートし保護ポリシーとガバナンスポリシーを改善



# 学習可能な分類指標（プレビュー）

- 手動または自動のパターン一致方式のどちらかによって簡単に識別できないコンテンツに特に適用

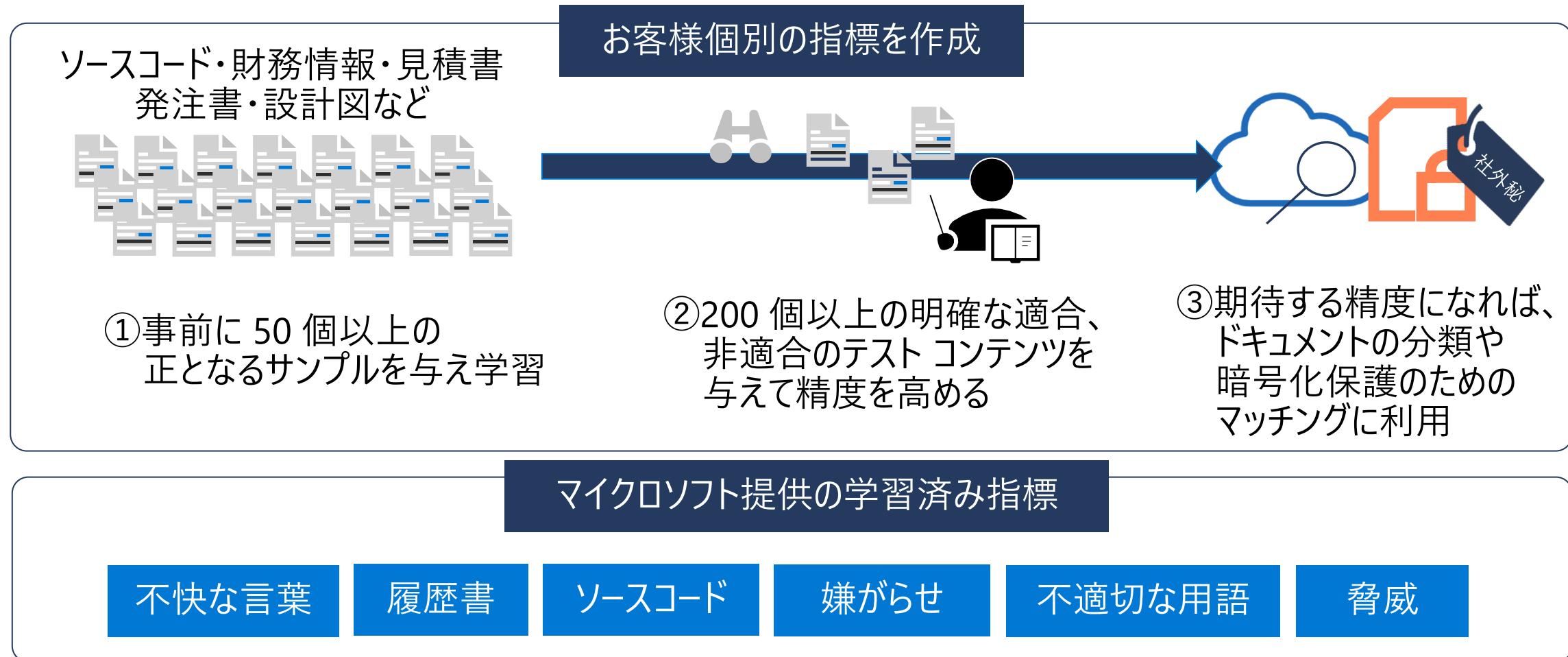


学習結果を基に分類

\* 現状は非暗号化の英語の文書のみ

# 2つの分類指標が設定可能(プレビュー)

- お客様個別の指標およびマイクロソフトによる学習済みの分類指標を利用可能



# コンプライアンス および リスクマネジメント ソリューション



## Information Protection & Governance

データのライフサイクルを通じて  
データを保護し、統治します



## Insider Risk Management

重要な内部者リスクを特定し、  
対策を講じます



## eDiscovery and Audit

関連データの迅速な調査と  
対応を可能とします



## Compliance Management | コンプライアンスの簡素化とリスクの低減

Microsoft  
**Security Forum 2020**



# eDiscovery and Audit



# Advanced Audit

- 迅速かつ効果的なフォレンジックおよびコンプライアンス調査を強化



監査ログの保管  
最大1年間保存

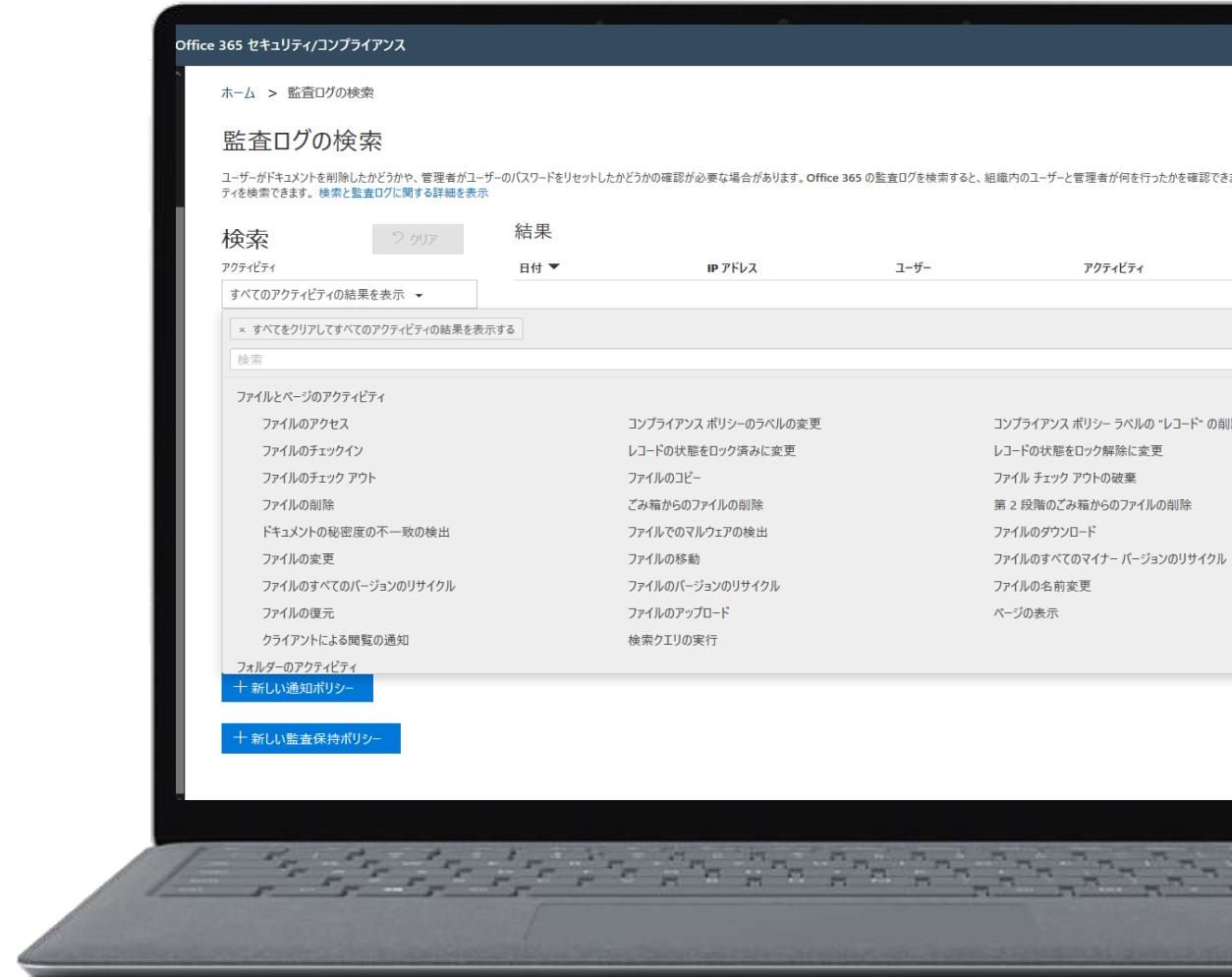


データへのアクセスの高速化  
毎分2,000リクエストでの検索  
E5 のお客様は他の組織の2倍の帯域  
での検索効率化



重要なイベントの監査

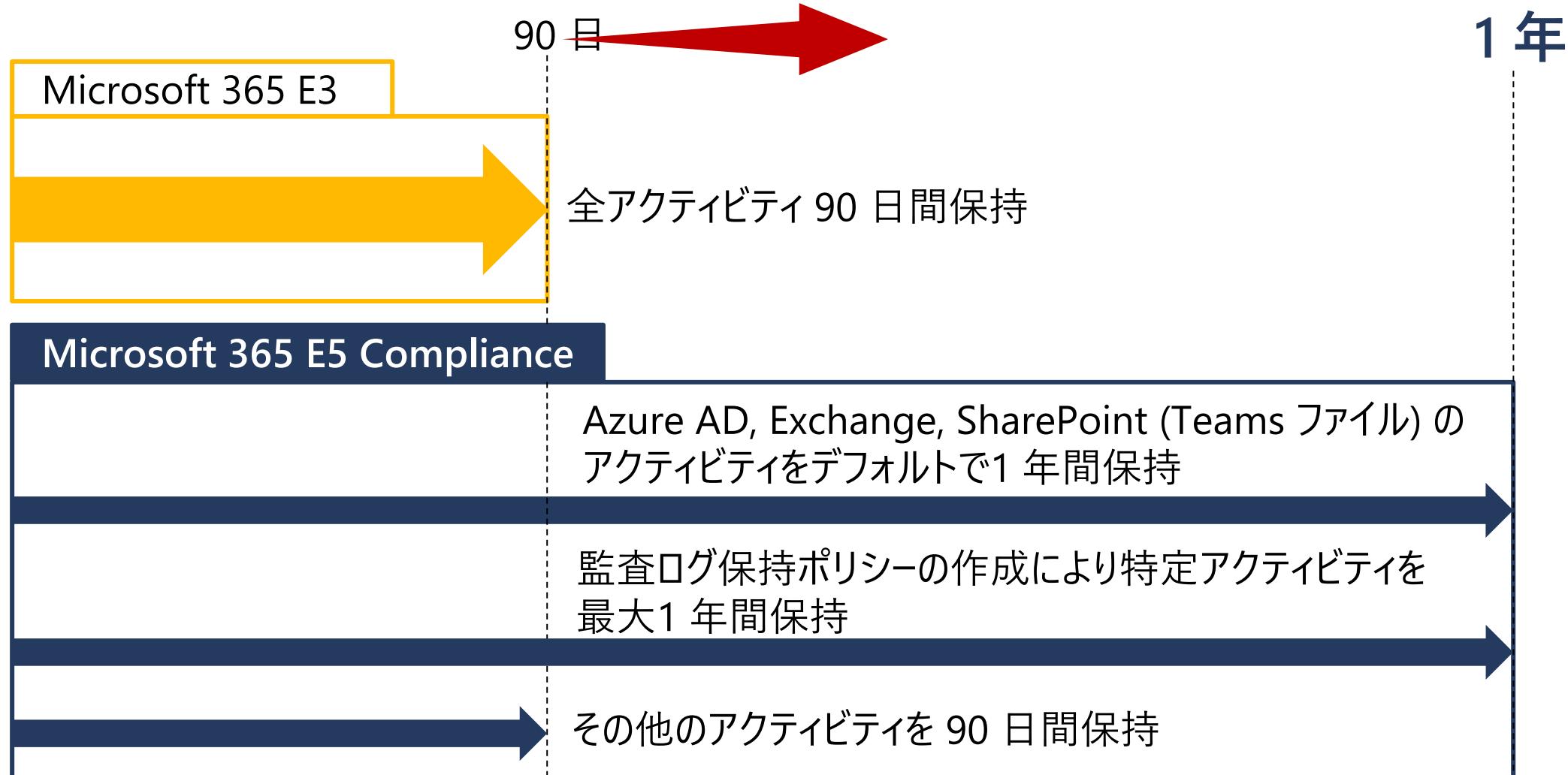
例：MailItemsAccessed  
(Exchange メールボックス監査の強化)



## Advanced Audit

# Microsoft 365 のアクティビティログを最大 1 年間保持

- 保持要件に対して柔軟に保持期間を個別設定



# コンプライアンス および リスクマネジメントソリューション

インテリジェントなコンプライアンス管理とリスク管理のソリューションを提供

## Microsoft 365 Compliance Center - [compliance.microsoft.com](https://compliance.microsoft.com)



### Information

### Protection & Governance

データのライフサイクルを通じて  
データを保護し、統治します



### Insider Risk Management

重要な内部者リスクを特定し、  
対策を講じます



### eDiscovery and Audit

関連データの迅速な調査と  
対応を可能とします



### Compliance Management | コンプライアンスの簡素化とリスクの低減

# コンプライアンス および リスクマネジメント ソリューション機能一覧

ソリューション	機能	効果
Information Protection Governance	Cloud DLP (MCAS + new value) ★	機密情報の大量ダウンロードなどの検知・ブロック
	Communications DLP (Teams chat)	Teams上でのクレジット番号などの機密情報などの共有禁止
	Rules-based auto classification	機密情報の自動ラベリング
	Machine Learning-based auto classification★	AIによる自動ラベリング作成・適応
	Information Governance advanced features (incl. Records Management★)	機密情報の削除・管理 (Office 365などのレコード機能)
	Customer Key	お客様による暗号化キー管理
	Advanced Message Encryption	Office 365 のメールの暗号化
Insider Risk Management	Insider Risk Management★	内部不正検知
	Communication Compliance★	パワハラ・セクハラなどの言葉のコミュニケーションを検知
	Information Barriers	Teams上でのコミュニケーションブロック
	Customer Lockbox	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にお客様の承認を必須に
	Privileged Access Management	Office 365 での特権アクセス管理
eDiscovery & Audit	Advanced Audit★	監査ログ1年管理
	Advanced eDiscovery	ML活用し機密情報データの分析と関連性の高いドキュメントの抽出

★ Includes new value



© 2020 Microsoft Corporation. All rights reserved.

本情報の内容(添付文書、リンク先などを含む)は、Microsoft Security Forum 2020 開催日(2020年3月12日)時点のものであり、予告なく変更される場合があります。  
本コンテンツの著作権、および本コンテンツ中で表示される商標権、団体名、ロゴ、製品、サービスなどは、各権利保有者に帰属します。