Microsoft 365 の情報保護とコンプライアンスの機能

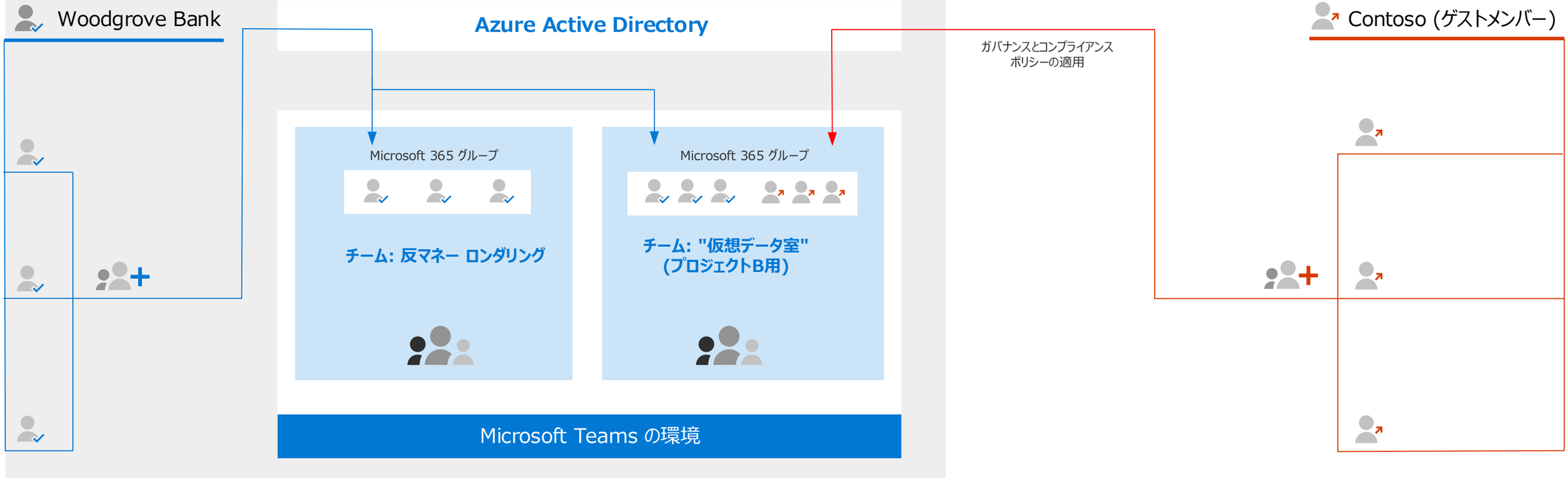
はじめに

Microsoft 365 には、幅広い情報保護機能とコンプライアンス機能が含まれています。Together with Microsoft (Microsoftと共に)の生産性向上ツールの機能は 組織の共同作業をリアルタイムで行うことができるように設計されており、同時に厳格に法的コンプライアンスフレームワークに準拠できるようになっています。

このイラストには、最も規制の厳しい業界、 財務関連のサービス業界のいずれかを使用して、共通の法的要件に対処するために、どのようにこれらの機能を使用したらよいかを示します。自由に これらのイラストを使用してください。

Microsoft 365 が、どのように金融サービス機関がセキュリティ とコンプライアンスの規制に準拠できるように役立つかについての詳細は、「米国銀行業界と 資本市場の主要なコンプライアンスとセキュリティに関する考慮事項」を参照してください。

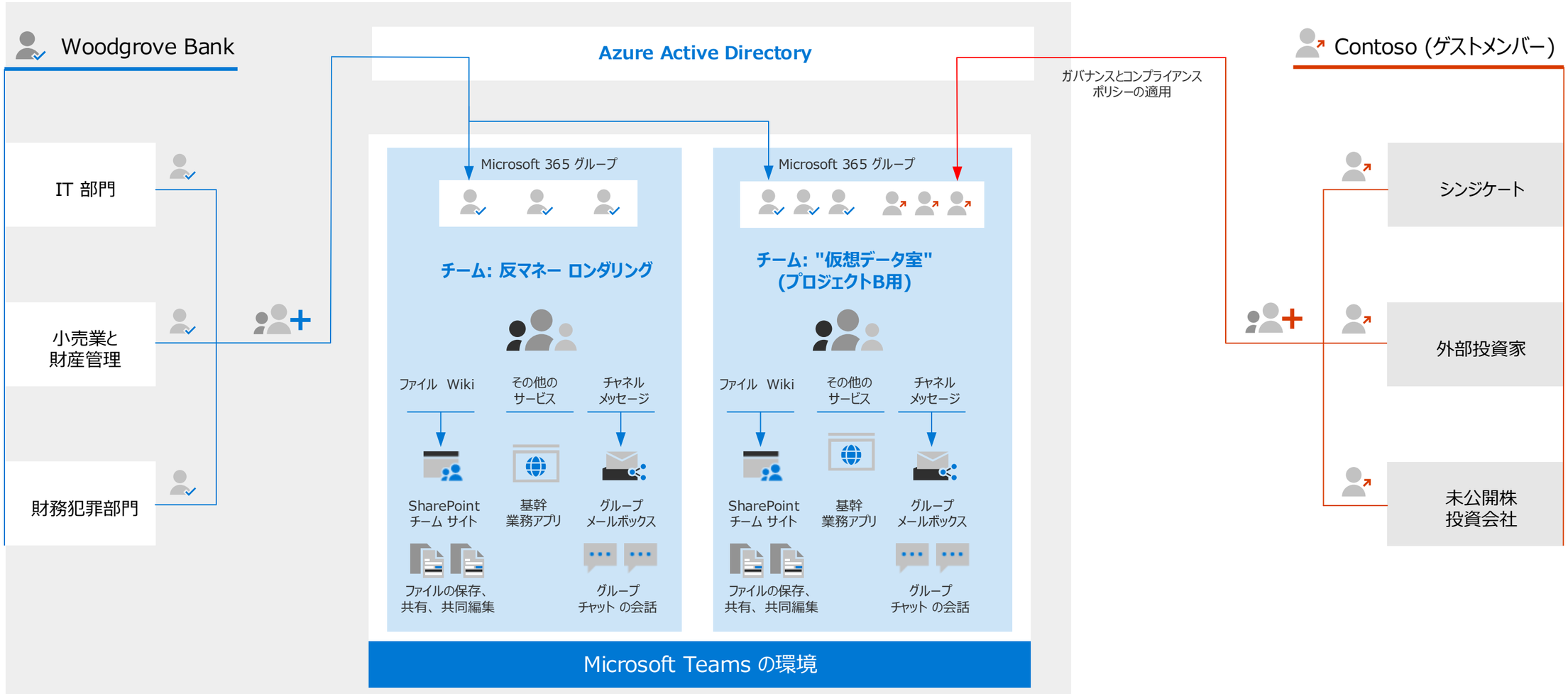
これらのイラストでは、Woodgrove Bank は、異なる 参加者を持つプロジェクトに対して 2 つのTeams 環境をホストします。各シナリオでは、各チームの Microsoft 365 グループが、メンバーシップにセキュリティ境界を、Azure Active Directory の多要素認証やその他の Microsoft Teams の条件付きアクセスポリシーを適用して 提供しています。



上位 Teams の論理アーキテクチャ

Teams を財務サービスに利用する場合の一般的なシナリオとしては、社内のプロジェクトまたは プログラムを実行している場合です。たとえば、多くの金融機関では、反マネー ロンダリグやコンプライアンスの対策を取っています。この図では、Woodgrove Bank が 2 つの Teams 環境のプロジェクトをホストしていますが、参加者は異なります。

この反マネー ロンダリングのプロジェクトには Woodgrove Bank 従業員のみが含まれます。プロジェクト B の "仮想データ室" のには、Contoso のゲストメンバーが含まれます。仮想データルームは、認証されたユーザーのみがアクセスできるデータを 共有するための安全な場所として機能します。また、Azure Active Directory は、ゲストの複数ファクター認証やその他の条件付きアクセス ポリシー を強制します。

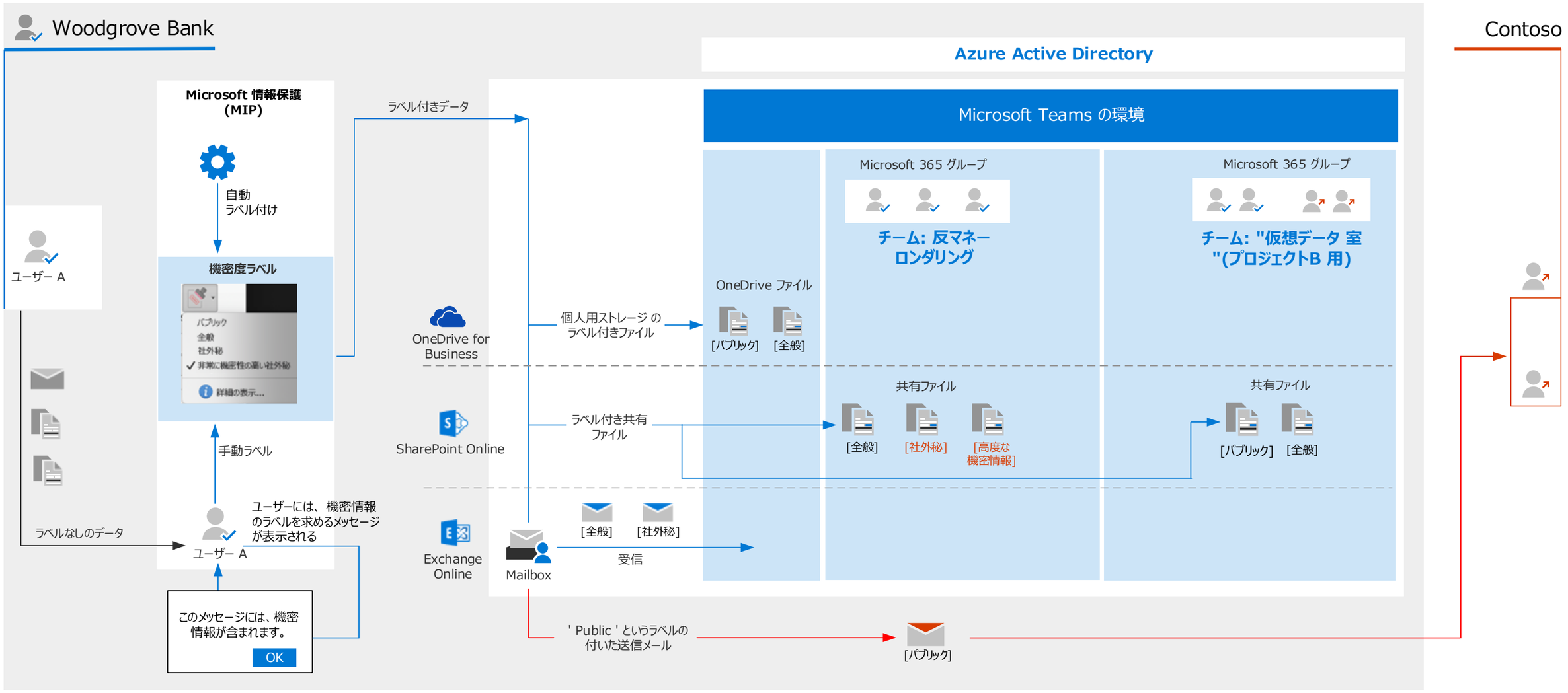


機密情報を特定し、データの損失を防ぐ

Microsoft 365 では、組織内の機密データを特定することができますが、それには 強力な以下の機能を組み合わせて行います。Microsoft Information Protection (MIP) や Office 365 Data Loss Prevention (DLP) も含まれます。 MIP を使用するとドキュメントや メールをインテリジェントに並べ替えることができますが、それには機密度ラベルを使用して賢く、手動で、または機械-学習で行います。

機密度ラベル

次のシナリオでは、機械 学習を通して、または手動で (次に、ユーザーのプロンプトと教育を通して表示される)機密性の高い情報をラベルで表示する方法を示しています。DLP では、これらのラベルをスキャンして、データ損失防止ポリシーを実施します。

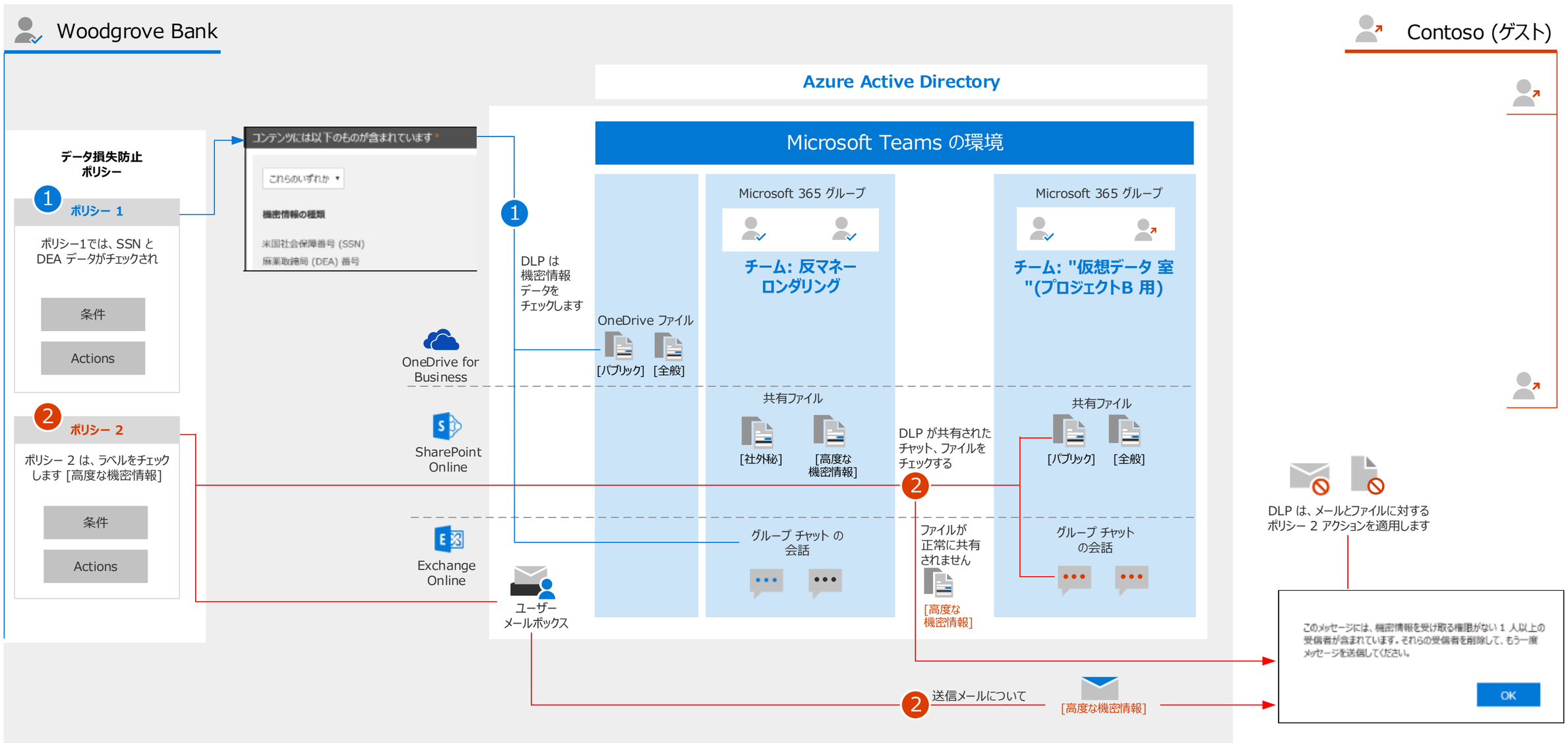


次ページに続く

データ損失防止

データに機密度ラベルが適用されると、DLP を使用して、ドキュメントや、メール、会話を見つけて機密度ラベルを検索することができます。このデータに適切なポリシーを適用し、監視し, 保護し、の機密情報の共有を防ぐことができます。またユーザーがワークフローを中断することなく、準拠している状態を維持できます。

次の図は、いくつかの機密情報の種類 (ポリシー 1) に一致する DLP 強制ポリシーと、"高機密" (ポリシー 2) というラベルが付いたデータを示しています。ここでは、許可された受信者以外の ' 高機密 ' マークされたデータを共有することが 試みられている場合、DLP は、情報の共有をブロックしデータ損失を防ぎます。



データを管理し、保持のためのコンプライアンス要件を管理する

アイテム保持ポリシーと保持ラベル

Microsoft 365 は、記録管理要件をインテリジェントに実装するためのアイテム保持ポリシーと保持ラベルを定義する柔軟な機能を提供します。

構成する保持設定は、コンテンツを最小限の期間保持することを要求する業界規制への準拠、訴訟やセキュリティ違反の場合のリスクの軽減、効果的で機敏な方法での知識の共有に役立ちます。

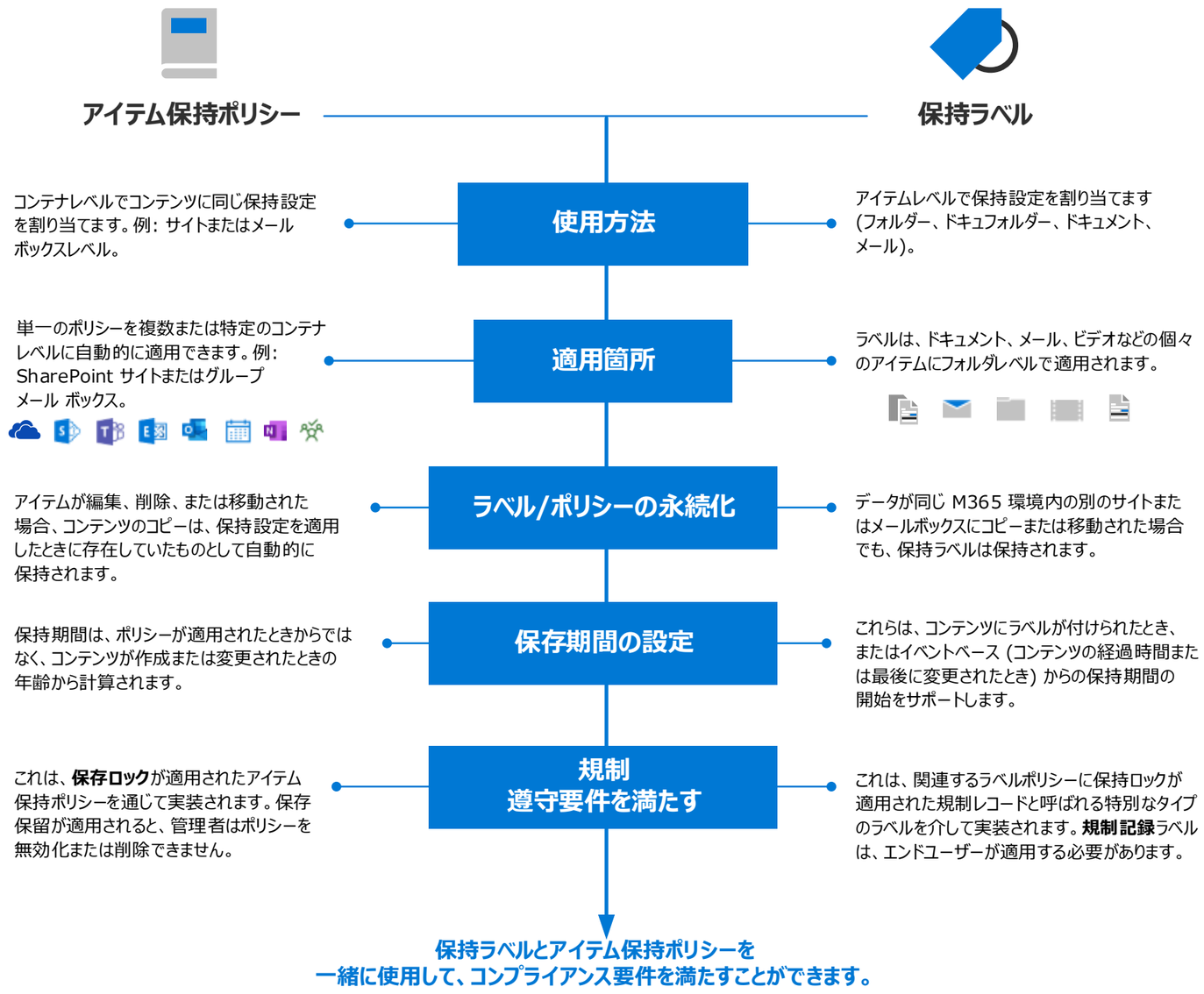
アイテム**保持ポリシー** と**保持ラベル**の両方を使用して、保持設定を割り当てることができます。

これらは両方とも、SEC Rule 17a-4(f) などの金融規制機関によって定義された規則に準拠するための特定の方法を備えています。この規則では、規制対象のエンティティは「記録を書き換え不可、消去不可の形式で排他的に保存する」必要があります。Microsoft 365 は、アイテム保持ポリシーまたはラベルポリシー (規制レコードラベルの場合) に保持ロックを適用することでこれを実現します。これにより、ポリシーをオフにしたり、制限を緩和したりすることができなくなります。アイテム保持ポリシーと規制記録のラベルについては、後の図 (トピック5/8) で触れています。

テナントでサポートされる保持ラベルの数に制限はありません。ただし、テナントでサポートされるポリシーの最大数は 10,000 であり、これらにはラベルを適用するポリシーが含まれます。

これら2つの方法の大きな違いは、対面図に示されています。

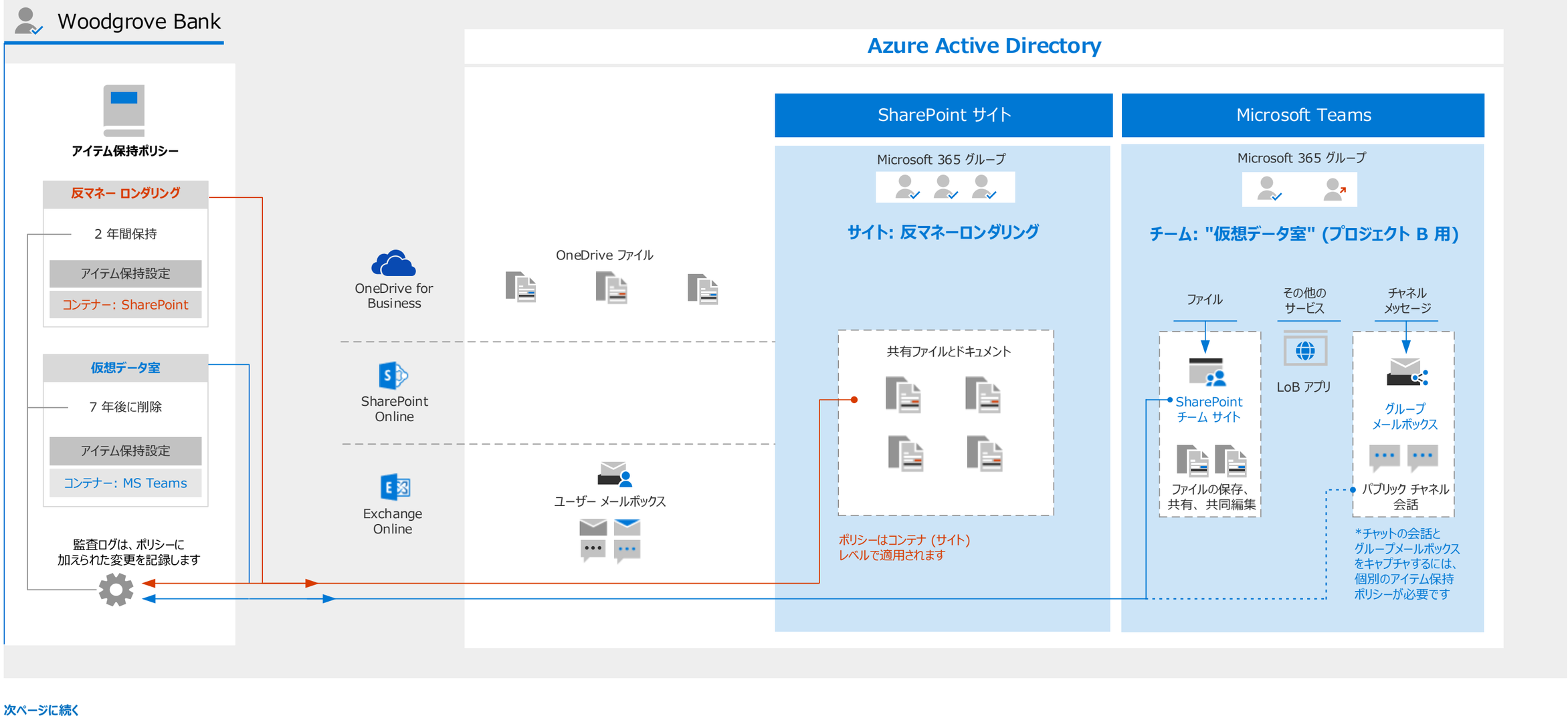
次ページに続く



アイテム保持ポリシーの適用

アイテム保持ポリシーを使用すると、サイトまたはメールボックスレベルでコンテナごとにコンテンツに同じ保持設定を割り当てることにより、コンテンツをプロアクティブに保持、削除、または保持してから削除することができます。 アイテム保持ポリシーは複数のコンテナーをサポートできますが、単一のアイテム保持ポリシーにサポートされているすべてのコンテナー (Teams、SharePointなど) を含めることはできません。 アイテム保持ポリシーを構成するときに、次を選択できます

コンテンツを無期限に、または特定の日数、月数、または年数の間保持するため。 保持期間は、アイテム保持ポリシーが適用されたときからではなく、コンテンツの経過時間 (コンテンツが作成または変更されたときから) から計算されます。次の図は、M365 環境のさまざまなコンテナ内のデータに適用されているアイテム保持ポリシーを示しています。

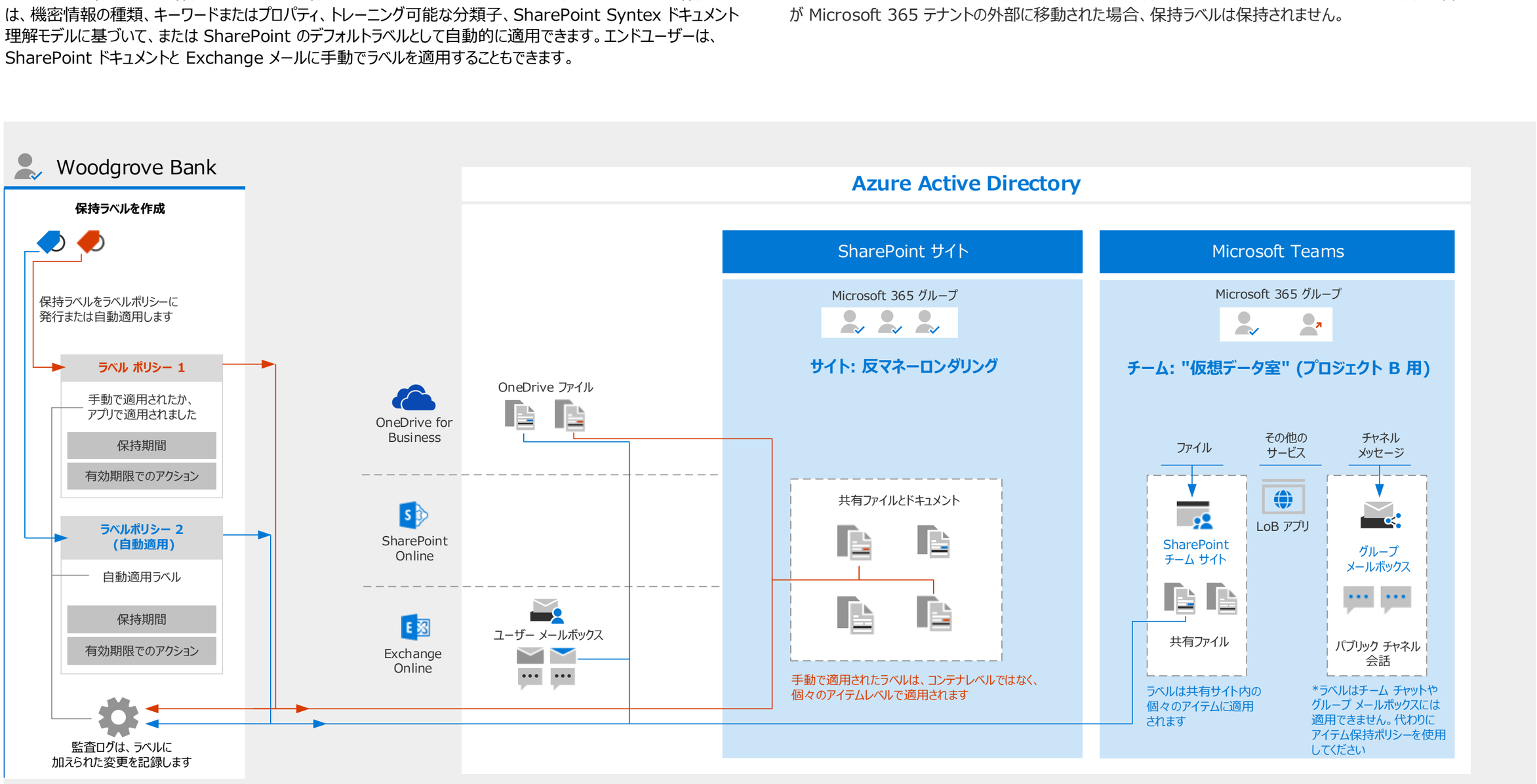


次ページに続く

保持ラベル アプリケーション

保持ラベルは、アイテムレベル (ドキュメント、電子メール、またはフォルダー) でデータを保持および削除するのに役立ちます。ラベルを作成したら、保持ラベルポリシーを作成して、これらのラベルを適用できる場所を指定します。保持ラベルは、機密情報の種類、キーワードまたはプロパティ、トレーニング可能な分類子、SharePoint Syntex ドキュメント理解モデルに基づいて、または SharePoint のデフォルトラベルとして自動的に適用できます。エンドユーザーは、SharePoint ドキュメントと Exchange メールに手動でラベルを適用することもできます。

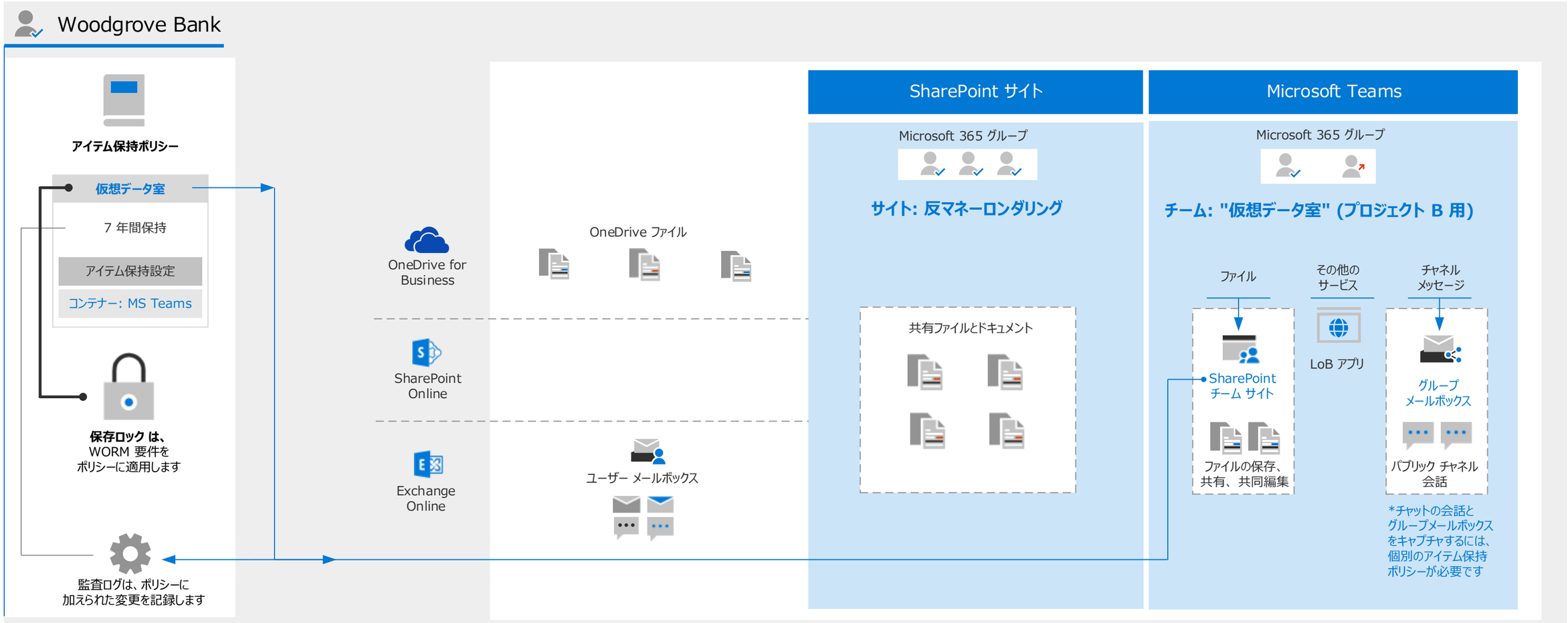
保持ラベルを使用して、アイテムをレコードまたは規制レコードとしてマークすることもできます。これが発生し、コンテンツが Microsoft 365 に残っている場合、ラベルは、規制要件を満たすのに役立つコンテンツにさらに制限を課します。データが Microsoft 365 テナントの外部に移動された場合、保持ラベルは保持されません。



データを管理し、保持のためのコンプライアンス要件を管理する

アイテム保持ポリシーと保持ロック

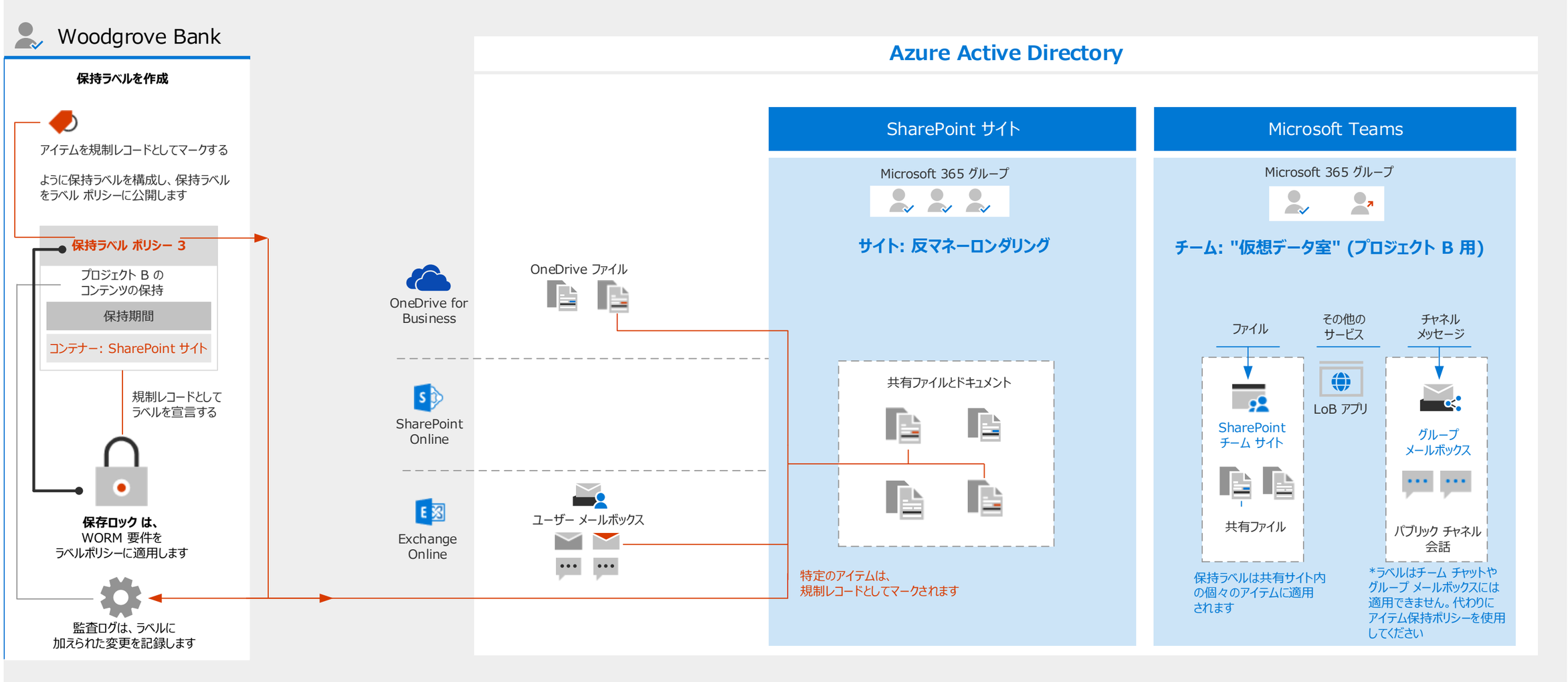
いくつかの金融規制では、電子データを消去不可能な形式で保存する必要があります (WORM：Write-Once-Read-Many)。アイテム保持ポリシーがロックされている場合：オフにすることはできません。コンテナは追加できますが削除できません。ポリシーに準拠したコンテンツは、保持期間中に管理者が変更または削除することはできません。保持ロックは、これらに準拠するのに役立ちますアイテム保持ポリシーのロックをオンにした後、それをオフにしたり、制限を緩和したりできないようにすることによる金融規制です。 要約すると、ロックされたアイテム保持ポリシーは増やすことも延長することもできますが、減らすこともオフにすることもできません。 以下に、WORM 要件を満たす必要があるデータに適用された保存ロックを示します。



次ページに続く

保持ラベルと規制レコード

保持ラベルは、ドキュメントが削除された場合にデータを保持するための規制レコードとして構成できます。 規制レコード レーベルがラベル ポリシーに公開された後、17a-4 に完全に準拠するには、そのポリシーを保持ロックでロックする必要があります。コンテンツに適用された後は、グローバル管理者でさえ、誰もラベルを削除できません。さらに、規制記録用に構成された保持ラベルには、次の管理者制限があります。(1) 保持期間を短くすることはできません、拡張のみ、(2) これらのラベルは保持ラベルポリシーを使用して適用する必要があります。(3) これらのラベルを保持ラベルポリシーに追加/保存した後は、これらのラベルを場所から削除することはできず、新しい場所を追加するだけです。 規制記録をコンテンツに自動的に適用することはできません。 以下に、WORM 要件を満たす必要のあるデータに適用される規制記録を示します。

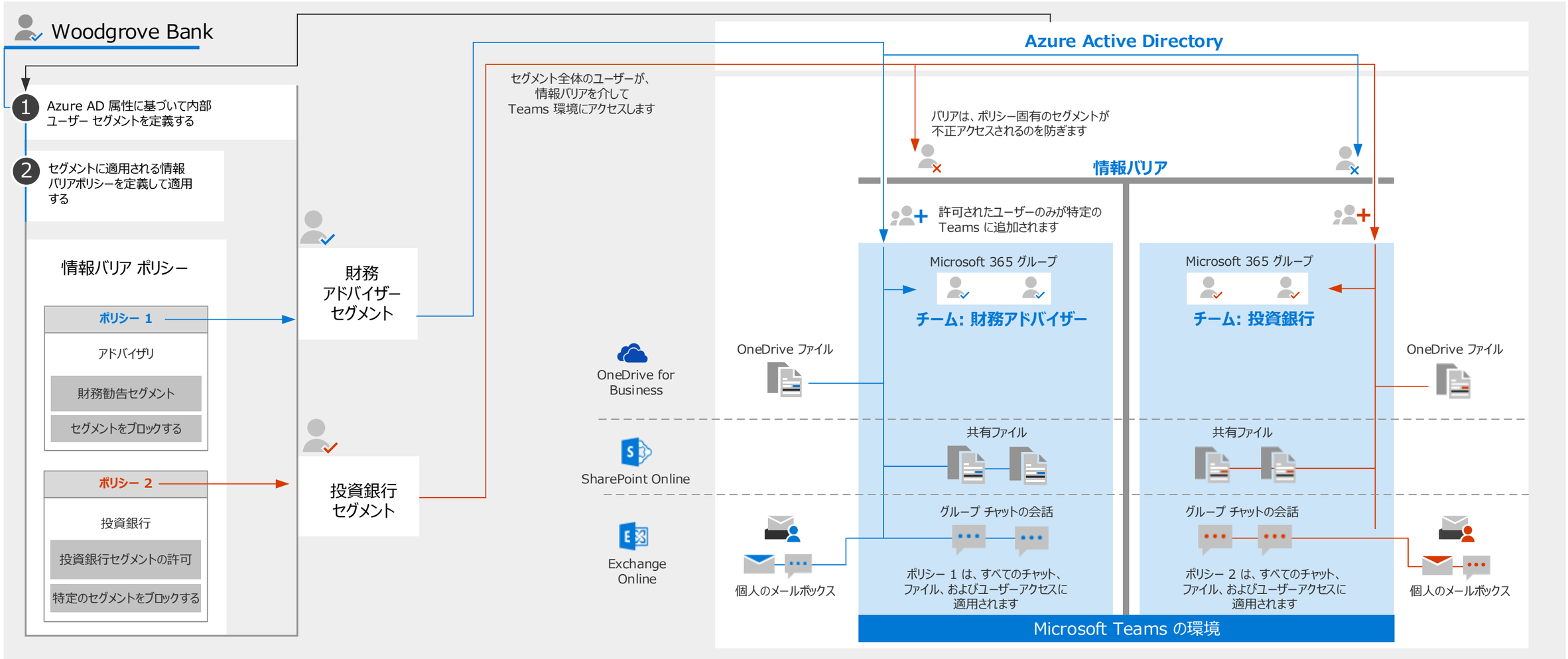


情報バリアにより、倫理的境界を確立する

金融機関は、特定の従業員の役割が情報を交換したり、他の役割と協力したりすることを禁止する規制の対象となる可能性があります。**FINRAは規則2241 (b)(2)(G) 、2242(b)(2)(D)、(b)(2)(H)(ii)および (b)(2)(H)(iii)** 銀行サービス、販売、または取引における役割の間にポリシーと情報バリアを設ける必要があります-アナリストとの情報交換を防ぎます。

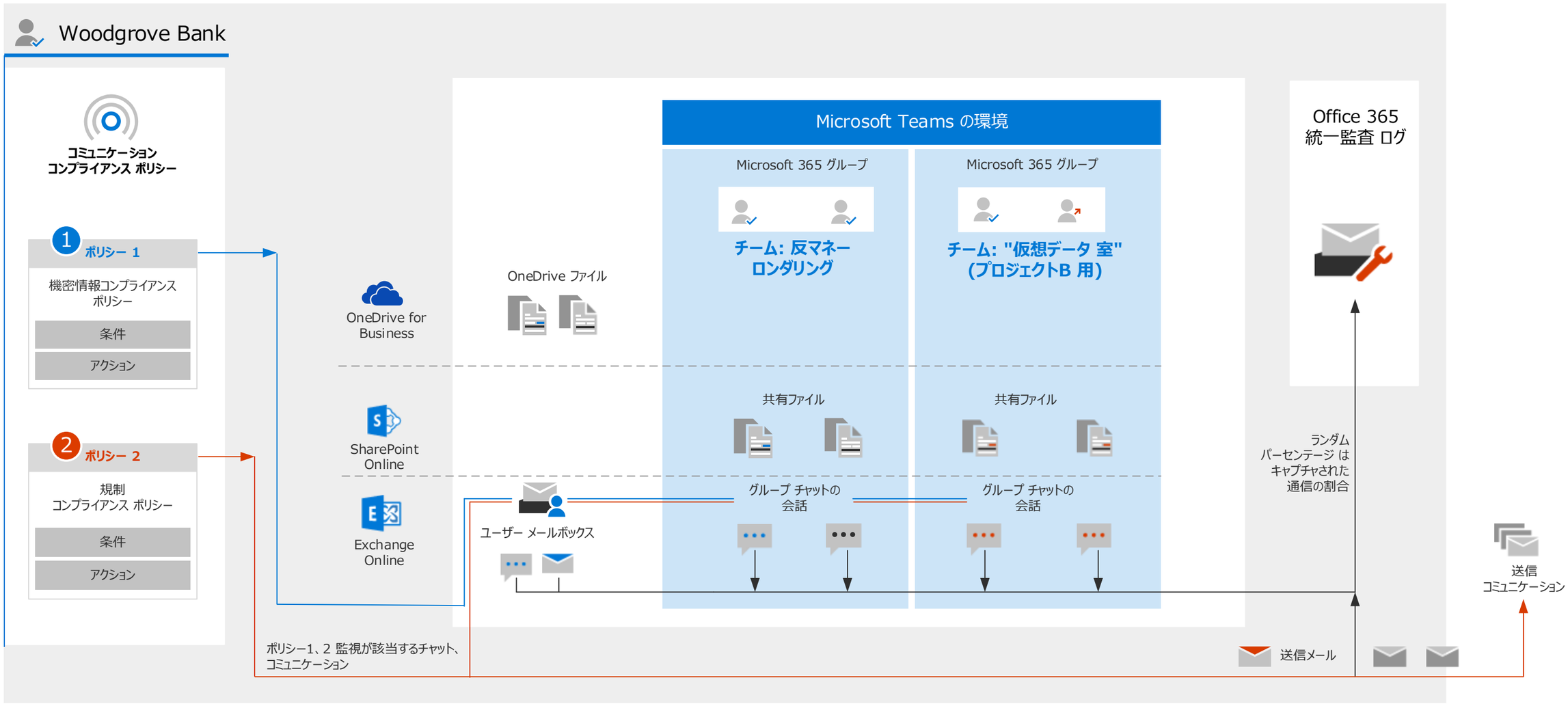
情報バリアにより、Office 365 環境内の倫理的な壁が可能になり、Teams 内のユーザーグループ間のすべての通信を定義するポリシーが可能になります。

以下の例は、ファイナンシャルアドバイザーとインベストメントバンカーのセグメント間に情報バリアを作成するポリシーの実施を示しています。セグメントは、Azure Active Directory を介して定義されます。



通信のコンプライアンス: 監督制御を実装する

FINRA は、財務組織内での監督機能を確立し、従業員の活動が、該当する証券関連の法律に準拠できるように手助けします。例えば **FINRA Rule 3110 (監督) および FINRA Rule 3120 (監督制御システム)**です。Microsoft 365　を使用すると、組織は事前にポリシーを構成して、監視とレビューのために通信をキャプチャできます。承認された監督。次の図に、従業員の通信に適用される2つのポリシーを示します。他の情報保護機能と同様に、これらのポリシーの条件は 機密情報の種類 (ポリシー1 など) に基づきます。通信のランダムな割合は、 通信コンプライアンスメールボックスで以降のレビューのためにログに記録されます。

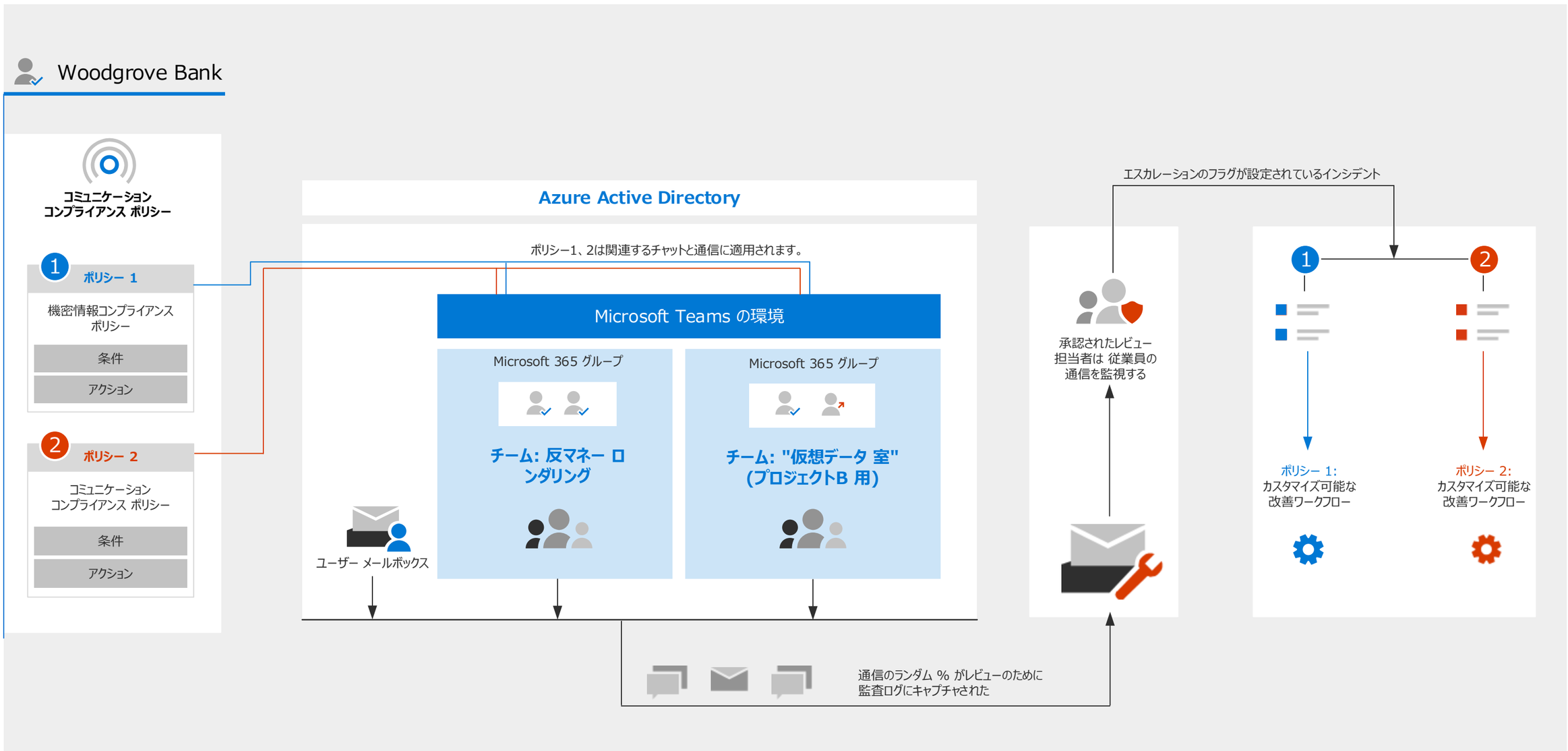


次ページに続く

柔軟な修復ワークフロー

コミュニケーションのコンプライアンス ポリシーにより、コミュニケーション チャネルに送信されるメッセージをスキャンして、コンプライアンスの問題を迅速に確認して改善することができます。機能が組み込まれた、改善されたワークフローを使用すると、組織のポリシーの一致を使用して、(監査ログのレビューによって監視される) メッセージを特定し、対処することができます。レビュー担当者は、ダッシュボードで、フラグ付きのものをレビューしますポリシー違反が生じている可能性がある通信とフラグが設定されたアイテムを解決済みとしてマークします。

次の図は 特定のログに記録された通信が インシデントを引き起こしたシナリオを表示していますが、確認が必要なインシデントでした。レビュー担当者は、組み込みの柔軟な改善ワークフローを使用して、これらのインシデントを調査します。



データ流出とインサイダー リスクから保護する

インサイダー リスクの管理

どこにいてもアクセスできるオンライン共同作業ツールを利用できるようにすることにより、本質的に、データ流出のリスクが組織にもたらされます。Microsoft 365 のインサイダー リスク管理を使用すると、ファイルのコピーなど、ユーザーの Windows 10 デスクトップからのシグナルを関連付けることができます。

USB ドライブにファイルをコピー、あるいは個人のメールアカウントにメールを送信する、また、確認、分離などの HR イベントおよびオンラインサービス、Office 365 メール、SharePoint Online、Microsoft Teams、OneDrive for Businessなどからの活動も含むデータ流出のパターンを特定します。

シグナル → 機械学習 → リスク管理

デバイス
Microsoft Defender ATP
- プリント
- コピーする
- セキュリティ シグナル
- など

Microsoft 365
データ損失防止
共有
ダウンロード
など。

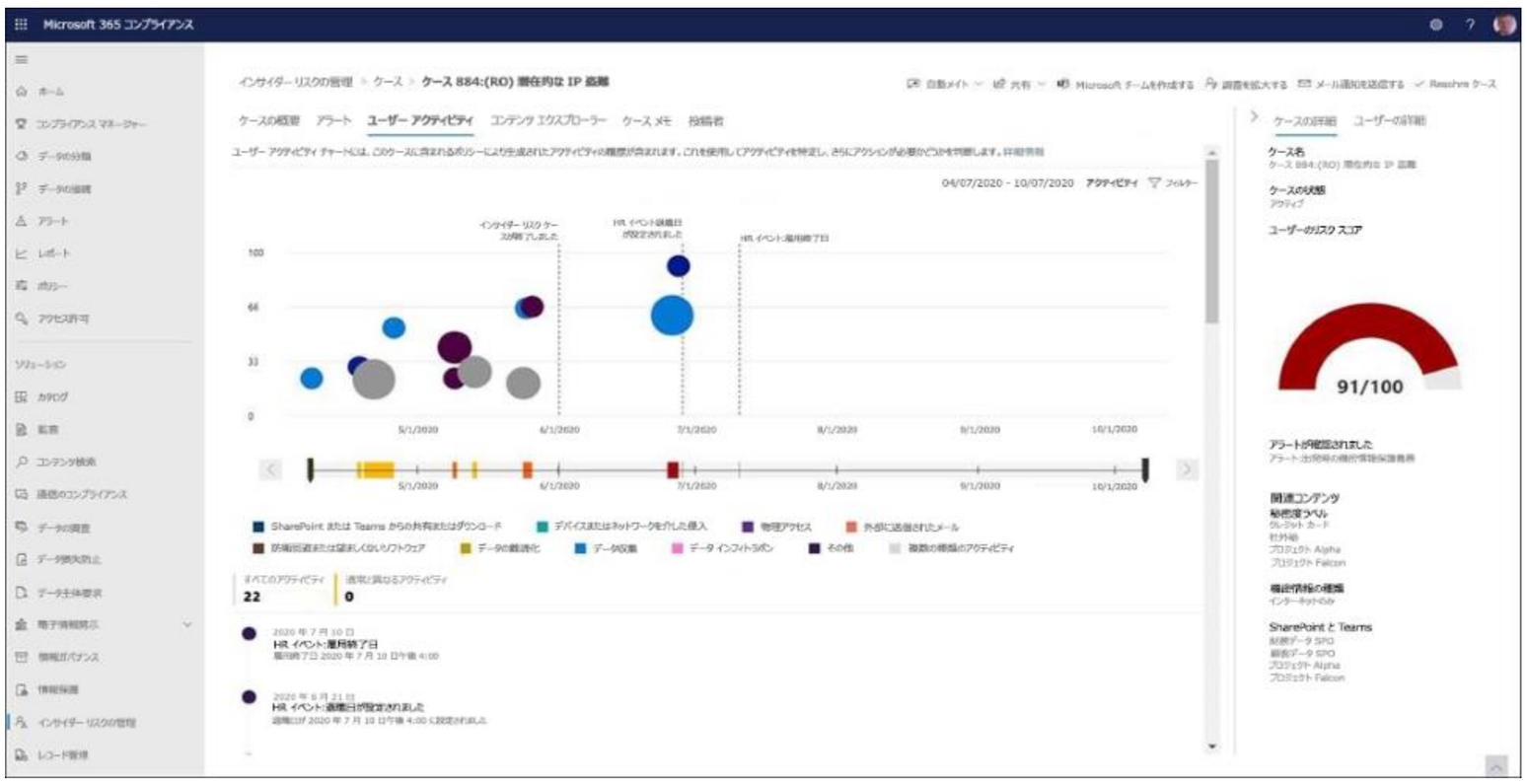
人事関連のイベント
出発時
退職
など。

Microsoft 情報保護
不快感を与える言語
カスタム研修可能な ML 分類子
など.

その他のデータ ソース

時間の経過に伴うインジケーターについての考察

警告
ケース
調査
アクション



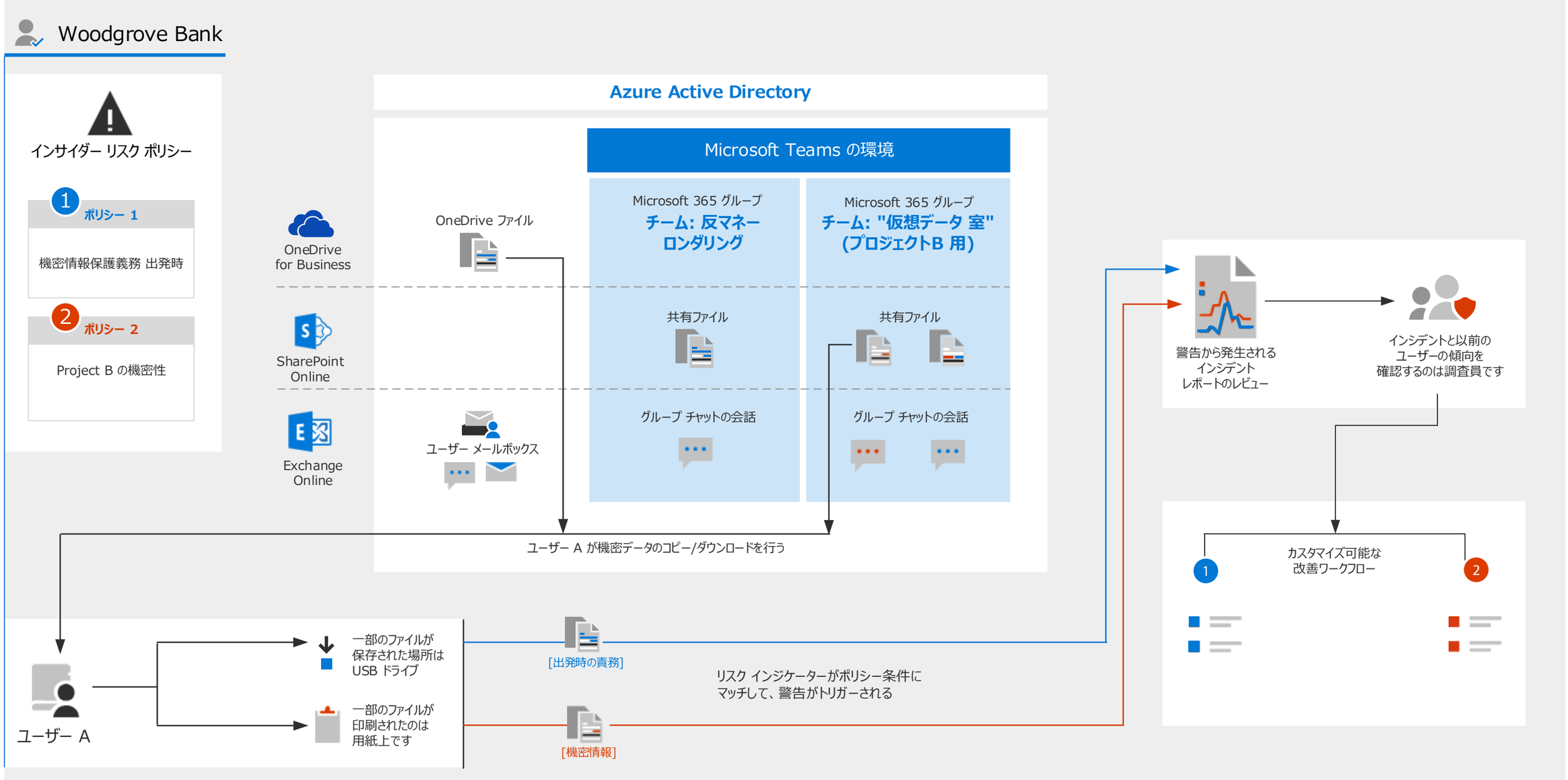
インサイダー リスク管理機能のビデオ チュートリアルについては、「aka.ms/insiderriskguide」。

次ページに続く

インサイダー リスク管理ワークフロー

インサイダー リスク管理ワークフローを使用すると、組織の内部のリスクを特定して調査し、対処することができます。優先ポリシー テンプレート、Microsoft 365 サービス全体での全般的活動シグナリングおよびケース管理ツールを使用すると 、実用的な 分析結果を使用して、リスクのある動作をすばやく識別し、対処することができます。

次の図は、特定のユーザーのアクティビティがポリシー条件をトリガーするシナリオを示しています。これらの自動的に発生される通知が生成され [確認が必要な状態] が付与されます。レビュー担当者は、状況に応じて、これらの警告をすばやく特定して、レビューして、トリアージすることができます。



サードパーティ アプリケーション データの取り込み

管理者はMicrosoft 365でデータ コネクタを使用してサードパーティ データをMicrosoft365組織のメールボックスにインポートしたり、アーカイブしたり ことができます。主な利点の1つは非Microsoft データが関連する規制や基準に準拠していることを確認するためにさまざまなコンプライアンス ソリューションをそれをインポートした後に適用できることです。

次の図はのデータ コネクタによって M 365 のユーザー プロフィールに関連付けられているメールボックスにのデータ コネクタによって取り込まれている Bloomberg チャットの例を示しています。

保持ポリシーをユーザーのメール ボックスに**適用し**、保持期間が終了した後サードパーティのデータ （およびその他のメール ボックスのコンテンツ） を保持してから削除できます。また**保持ラベルを使用して**サードパーティ データの保存期間が終了したときに廃棄レビューをトリガーすることもできます。

このサードパーティデータのインポートとアーカイブを使用して**通信コンプライアンスを確保し内部リスク、を最小限に抑え、必要な規制に準拠するように保持設定を適用できます。**

詳細については、[サード- パーティーのデータをアーカイブするを参照してください。]