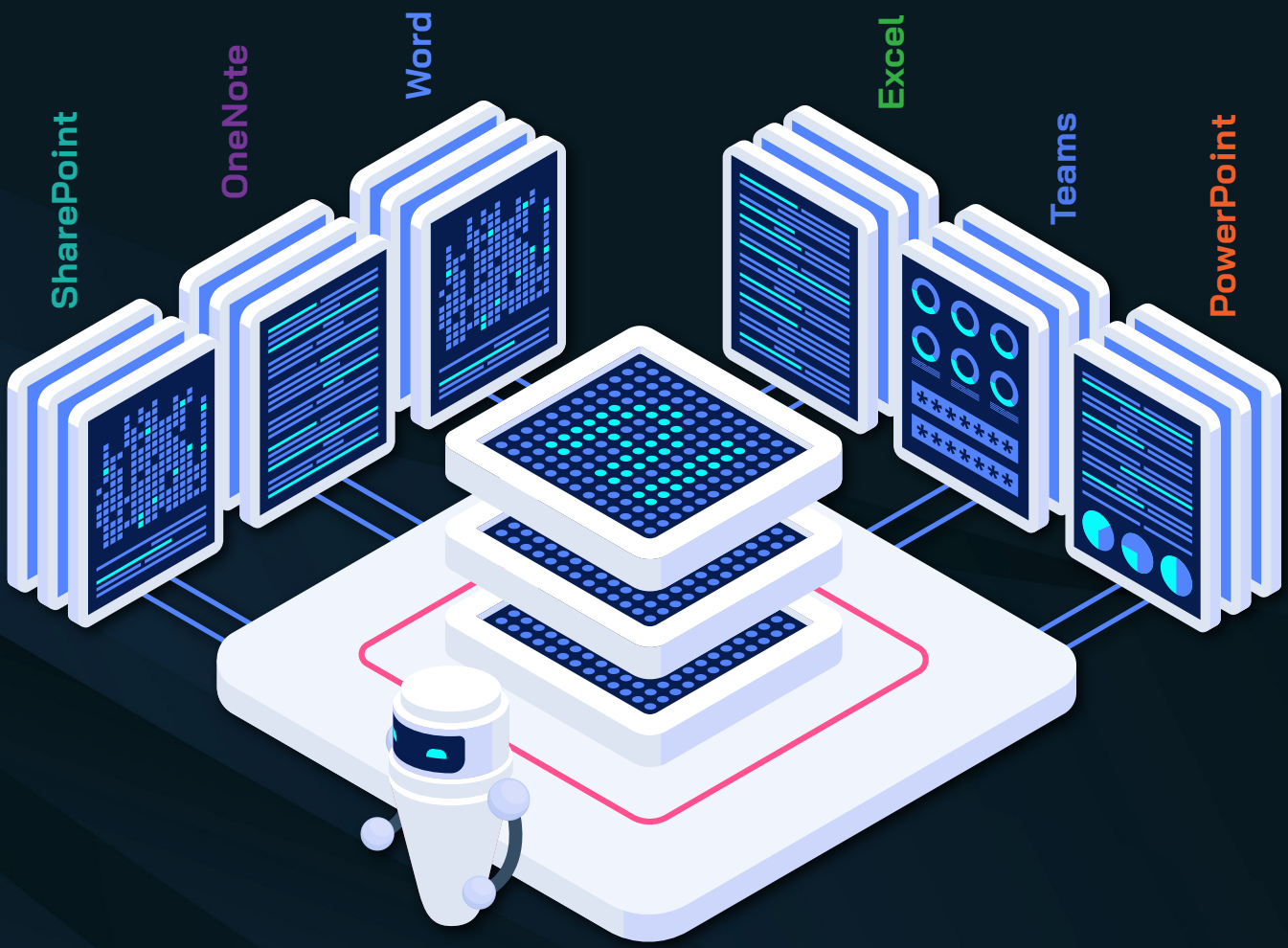
Microsoft Copilotを安全に導入・活用するために



HORNETSECURITY
BY proofpoint.

Microsoft Copilotを安全に導入・活用するために

Microsoft 365の権限を管理し、データ漏えいを防ぐ

Microsoft　Copilotは、従業員の日々の業務を大幅にかつ高速に補助してくれる利便性の高いツールです。このAIアシスタントは、プレゼンテーションのデザイン、要約の作成、メールの下書きなどをこなすことが可能です。そのためCopilotは、ユーザーが閲覧可能なMicrosoft　365のSharePointやOneDrive上のファイルやメールにアクセスし、パーソナライズされた結果を提供します。一見、業務を楽にする画期的な方法に思えますが、機密データが意図しない相手の手に渡ってしまう可能性という大きなリスクも潜んでいます。これは、CISOや管理者にとっては悪夢とも言える事態です。

本ホワイトペーパーでは、Copilot利用に伴うリスクを紹介し、ガバナンスの喪失を防ぎコンプライアンスを確保するための、効果的な権限管理の実現方法について解説します。

Copilotの検索によるOneDriveやSharePointからのデータ漏えいリスク

Copilotは、さまざまな面で業務を楽にすることが可能です。例えば、ユーザーが入力する「プロンプト」と呼ばれるコマンドを使って、情報の要約や編集、創造的な加工が可能です。

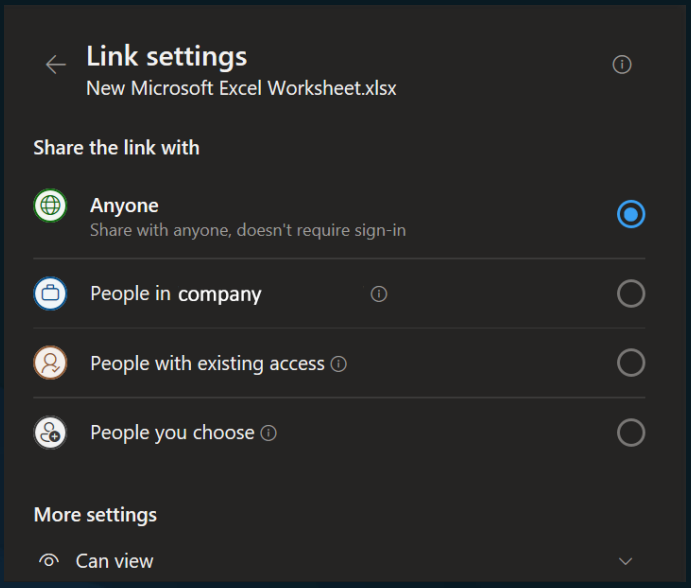
Copilotは、SharePointやOneDriveに保存されたWord、Excel、PowerPoint、Outlook、Teamsなどすべてのマイクロソフト 365アプリケーションのコンテンツにアクセスして情報を収集し、わずか数秒でまとめることが可能です。

Copilotは検索時に、ユーザーが権限を持つすべてのデータへアクセスできるため、不適切なデフォルトの権限設定によって本来アクセスできないはずの機密情報（個人データ、セキュリティ関連情報、事業数値、給与情報など）に、SharePointやOneDrive上で遭遇してしまうことがあります。

Copilotは、ユーザーが権限を持つSharePoint上のすべてのデータにアクセスします。

具体例：

例えば、ある従業員が「共有」機能を使ったリンクで、機密の事業数値を含むExcelファイルを上司にすばやく簡単に共有したとします。問題となるのは、デフォルトの共有設定により、組織内の全員、あるいはさらに悪いことにリンクを知る誰もがアクセスできてしまうリンクが自動生成される場合です。



たとえ組織内の他の従業員がこのドキュメントの存在を知らず、リンクを受け取っていなかったとしても、Copilotはすでにアクセスできる状態にあるため、その情報を読み取り、他の従業員の検索結果に反映させてしまう可能性があります。

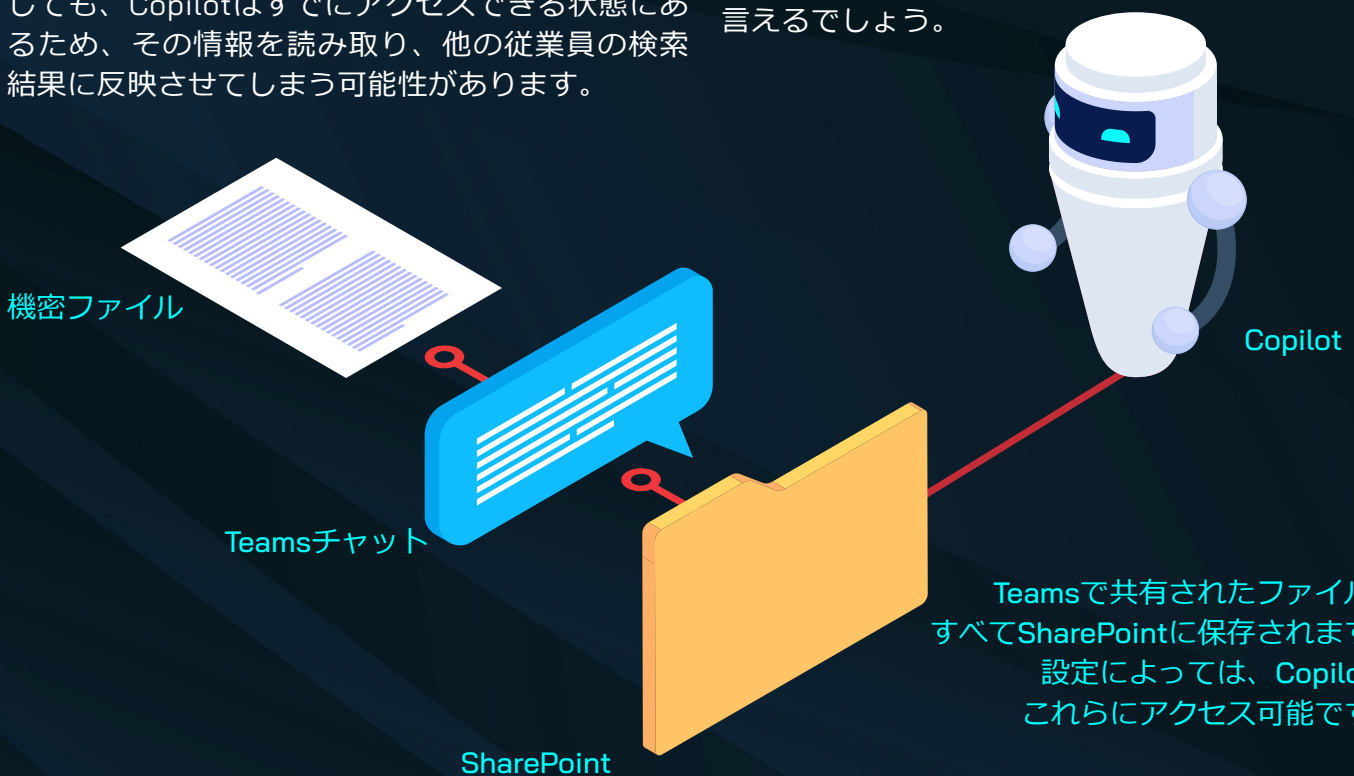
Microsoft　Teamsで共有されたドキュメントはSharePointに保存される

Teamsでのファイル共有も、共有設定が適切でない場合はCopilotに絡むデータ漏えいのリスクを高めます。Teamsのチャットでファイルが共有されると、そのファイルはSharePoint内のチームサイトに保存されますが、このことを理解しているのはごくわずかだけです。

個人チャットまたはグループチャットでアップロードされたファイルは、OneDriveの「Microsoft Teamsチャットファイル」フォルダーに格納されます。プライベートチャネルの場合は、そのチャネル専用の独立したSharePointサイトが作成され、そのドキュメントライブラリにはプライベートチャネルのメンバーのみがアクセス可能です。

つまり、すべてのファイルはTeams内に直接ではなく、それぞれ異なるSharePointサイトに保存されていますが、Copilotはこれらのサイトにもアクセス可能だということです。
さらに問題となるのは、組織外のMicrosoft 365ゲストユーザーがCopilotを利用し、本来アクセスリンクを知らない組織情報に、アクセスできてしまうケースです。

これは、CISOや管理者にとって警戒すべき事態と言えるでしょう。



Microsoft 365データには強固な権限管理が必要

Copilotは、ユーザーが少なくとも閲覧権限を持つすべての組織データを利用・表示することが可能です。そのため、「Need-to-Knowの原則」、すなわちMicrosoft 365における最小限のアクセス権限の付与を厳格に実施することが重要です。

つまり、ユーザーには業務に必要なデータへのアクセスのみを許可し、その他の権限は付与しないということです。これらのアクセス権限は、組織内でユーザーの役割が変わった際には更新する必要が生じます。

効率的な権限管理は、法規制の観点からも不可欠です。

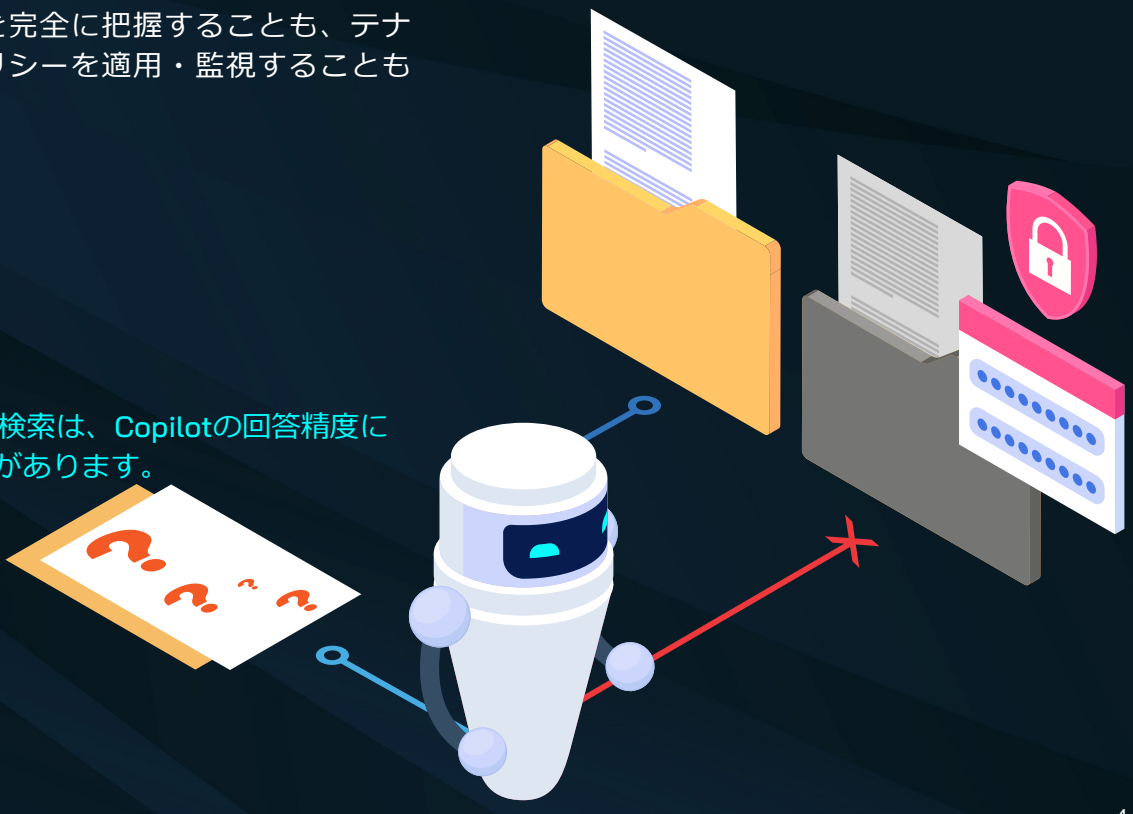
組織情報へのアクセスについては、法的要件も満たす必要があります。これらの要件は、組織の所在地や対象となるデータの種類など、さまざまな要因によって異なります。
特にNIS2指令の施行以降は、業種も管理者やCISOの今後の業務負荷を大きく左右する要因となっています。

Microsoftの既存ツールでは、組織内で付与されているすべての権限を完全に把握することも、テナント全体の権限ポリシーを適用・監視することも不可能です。さらに、Microsoftツール内での設定変更は、変更時点以降に作成・共有されたファイルにしか適用されません。

そのため安易な対応として、ファイル共有を全面的にブロックしたり外部共有を禁止したりして、組織内共有についても厳格なデフォルト権限を設定してしまうことがよくあります。しかし、そうするとユーザーは別の方法でファイルを共有するようになります。その結果、機密文書がサードパーティのクラウドストレージや個人用メールを介して共有されるようになり、CISOや管理者はさらに把握不可能となってしまいます。

Microsoftの「制限付きSharePoint検索」設定は解決策にはならない

Microsoftも、SharePointにおけるCopilot検索に問題が起こり得ることを認識しています。2024年4月、Microsoftは管理者向けに「制限付きSharePoint検索」設定をパブリックプレビューとして公けにしました。これにより、全社検索およびCopilot検索の対象を、選択したSharePointサイトのみに制限することが可能になります。



制限付きSharePoint検索は、Copilotの回答精度に影響を与える可能性があります。

ただし、これはきめ細かい設定の余地がない機能です。SharePointサイトを丸ごと許可するか、丸ごとブロックするかのどちらかしかありません。

この設定を有効にすると、Copilotを利用しないユーザーも含め、検索体験全体に影響が及びます。Copilotが利用できる情報も少なくなるため、正確で網羅的な回答を提供する能力にも影響が出る可能性があります。

したがって、Copilotを最適に活用するという観点からも、これは解決策にはなり得ません。

ファイルに常に正しい権限が設定され、Copilotの検索結果に対象ユーザー向けのファイルのみが表示されるようにするには、Microsoft 365全体で大規模かつ効率的なデータライフサイクル管理を実現するソリューションが必要です。

365 Permission ManagerでCopilot対応を実現する

定義された権限ポリシーを遵守するために急務となっているのは、何千ものSharePointサイトを持つ大規模テナントにも無理なく対応できる、スケーラブルなツールです。

Hornetsecurityの365 Permission Managerを使えば、アクセスと権限を効果的に監視・管理することが可能です。特にCopilotに対しては、権限管理を簡素化することで、情報が意図せず拡散してしまうのを防ぐことが可能です。

Microsoftの複数の純正ツールを行き来する必要はなく、365 Permission Managerは、管理者やCISOがM365環境の権限を包括的に把握し、コンプライアンスポリシーを定義し、違反を防止・是正するための、便利で使いやすいインターフェースを提供します。

365 Permission ManagerがTeams、SharePoint、OneDrive、Groupsを含むMicrosoft 365インフラの保護と最適化をどのように支援するか、ぜひご確認ください。

- **Explore（把握）** – 権限の明確でシンプルな概要を取得
- **Manage（管理）** – すぐに使えるベストプラクティス、またはカスタムの共有ポリシーを割り当て
- **Monitor & Audit（監視・監査）** – コンプライアンスポリシー違反に関するアラートを受け取り、対処

365 Permission Managerによって
Microsoft 365におけるデータ漏えいリスクを低減し、コンプライアンスを向上

365 Permission Managerの利点

包括的な監視

» 365 Permission Managerは、SharePoint、OneDrive、Microsoft TeamsにおけるM365権限の把握を支援します。高度なフィルター機能により、外部ユーザーやゲストがアクセスできる要素を確認することが可能です。さらに、ファイル、サイト、フォルダーが組織外の関係者と共有された場合、管理者やCISOに通知されます。

権限ポリシーのカスタマイズ

» 365 Permission Managerを使用すると、あらかじめ定義された権限ポリシーを設定したり、独自のポリシーを作成したりすることが可能です。これらは必要に応じて、サイト、フォルダー、ファイルの各レベルで適用可能で、画一化されたポリシーしか提供しないMicrosoft 365の純正ツールとは異なります。

大規模な権限管理

» 365 Permission ManagerのControl Panelでは、任意の数のテナントやグループの権限を同時に一括で調整可能です。これにより時間と手間が削減され、従業員の権限をコンプライアンスに準拠した状態に保つことが可能です。

常に状況を把握

» 違反が発生した場合、管理者またはCISOに警告メッセージが送信されます。関係するユーザーや、サイト、ファイル、フォルダーが示されます。これにより、データ漏えいを防ぐための即時対応が可能になります。違反は個別に、または一括操作によって承認・却下することが可能です。

» 特に便利な機能がTo Doリストです。各SharePoint Onlineサイトに適用されたポリシーの違反がすべて一覧表示されます。これらの違反の大規模な是正が可能で、業務上の正当な理由がある場合は例外を設定することも可能です。従業員にも責任の所在が明確になり、自身が所有するサイトのOneDriveやSharePointサイトに関するポリシー違反については、メールで通知されます。

権限ポリシーの遵守、情報およびデータの保護、組織内でのCopilot利用への備えなど、いずれの目的であっても、365 Permission Managerはこれらの要件すべてに応えるよう設計されており、CISOや管理者はより安全でコンプライアンスに準拠した形で、Copilotの導入や活用が可能になります。