Microsoft

新時代のコンプライアンス リスクに備えるセキュリティ対策

Microsoft 365 E5 の
コンプライアンス管理

INDEX

第 1 章

ハイブリッド ワーク時代の コンプライアンス対策

社外で勤務するリモートワークやクラウド サービスを活用したコミュニケーションが普及したことにより、

働き方改革の推進や生産性の向上が期待できる反面、

内部不正やハラスメントが検知しにくくなるといった「コンプライアンス リスク」の問題を抱えている企業も増えているようです。

場所や時間にとらわれずに働くハイブリッド ワークの時代において、

変容するリスクに合わせたコンプライアンス対策についてご説明します。

新時代のコンプライアンス対策とは？

まずは、自社におけるコンプライアンス リスクをチェックしてみましょう。

リモートワーク中に私有パソコンに機密情報を容易にダウンロードできたり、

簡単にメール送信できたりする環境ではありませんか？

また、周りの目がなかったりネットを介した会話だったりすることが原因で、

言動がハラスメントまでエスカレートしている社員はいませんか？

CHECK

リモートワークで増えるコンプライアンス リスク

- ☐ 機密情報を容易にダウンロード、私有エリアに保存、メールや SNS などで共有できてしまう
- ☐ 秘密保有や社内規定を遵守していない行動を制御できていない
- ☐ 会社の PC を使わずに私用 PC で業務している社員がいる
- ☐ VPN 機器が不足している
- ☐ ビデオ通話ツールやチャットツールで言動がエスカレートしている社員がいる

HINT!

ニューノーマル時代のリスクを軽減する Microsoft 365 E5 のコンプライアンス対策

マイクロソフトが提供しているクラウドサービスの法人向けプラン「Microsoft 365 E5」のツールやソリューションを用いたコンプライアンス対策は、企業の情報漏洩・内部不正・ハラスメントといったリスクを軽減します。また、コンプライアンスリスクの評価や機密データの管理体制と保護を行い、規制要件にも対応します。

Microsoft 365 E5 の内部リスク対策

Information Protection & Governance（データ保護とガバナンス）

マイクロソフト製品、サードパーティのクラウドストレージ、クラウドサーバー、オンプレミスサーバーなど、あらゆる場所に存在する重要なデータを横断的に管理・制御します。

Insider Risk Management（内部リスクの特定）

ユーザーの行動を分析し、セキュリティ違反やデータ流出などの重大な内部関係者リスクを特定、対処します。また、メールやチャット、SNS などからハラスメントの兆候を検知し、対処することができます。

Discover & Respond（迅速なデータ調査）

関連データの迅速な調査と対応を可能とします。ログの長期保管を行い、さらにその膨大なログデータにアクセスする際の高い検索性能により、監査作業を効率化します。

Compliance Management（コンプライアンス マネジメント）

世界中のデータ保護規制に対して、自社がどこまで対策できているのかをスコアリング。さまざまな規制に対して自社が抱えるリスクを可視化し、対策を管理できます。

ワード解説

内部リスクとは？　IT を介したリスクのうち、マルウェアなどの外部からの攻撃（外部リスク）ではなく、組織の内部が原因になるリスクのこと。

主な内部リスク
- 機密情報を含むデータの流出
- 知的財産（IP）の盗用
- 法令遵守違反
- 詐欺
- インサイダー取引

第 2 章

コンプライアンス対策を
実践してみよう

ここからは、あなたの会社がコンプライアンス リスクにどの程度対応できているのかを、

具体的にチェックしていきましょう。

そのうえで、Microsoft 365 E5 で使えるツールやソリューションを活用した、

実践的な課題の解決策をご案内します。

パスワード付き zip ファイルでデータを共有していませんか？

資料などのデータを送る際、パスワード付き zip ファイルをメールに添付して送信し、
パスワードを別のメールで後送している方も多いのではないでしょうか。
実はこの方法だと、悪意ある第三者にメールを傍受されてしまえば
二通とも相手に丸見えになってしまうのであまり意味がありません。
そのうえ、暗号化されたデータはセキュリティ システムをすり抜けてしまう場合があるので、
偽装したマルウェアを素通ししてしまうなどのリスクにもつながります。
日本政府はすでにこの運用方法を廃止しており、それに呼応して多くの企業が、
より安全なファイル共有方法への切り替えを進めています。

HINT!

Microsoft 365 E5 のデータ共有ツールを活用しよう

MERIT 1

オンラインストレージ「OneDrive for Business」での共有

OneDrive for Business は Microsoft 365 のオンライン ファイル ストレージです。ストレージに保存したファイルやフォルダを、共有リンク（URL）で相手に共有できます。リンクの有効期限やパスワードの設定、ダウンロードの可否などの細かい設定をすることもできます。共有リンクはあとから削除することもできるので、誤送信してしまった場合でも安心です。

MERIT 2

ワークスペース「Teams」「SharePoint」での共有

会社や部門内であれば、Teams や SharePoint Online が便利です。チャット上で簡単にデータを共有でき、フォルダを作成してチーム内で管理することも可能です。さらに、パスワードを設定する必要もなく、共同作業も可能なので、生産性も向上させられます。また、ユーザーごとにアクセス権限を制御したり、データ損失防止（DLP）機能によって、機密性の高いファイルが外部に共有された場合は自動的に削除したり、機密情報の投稿をブロックしたりすることが可能です。

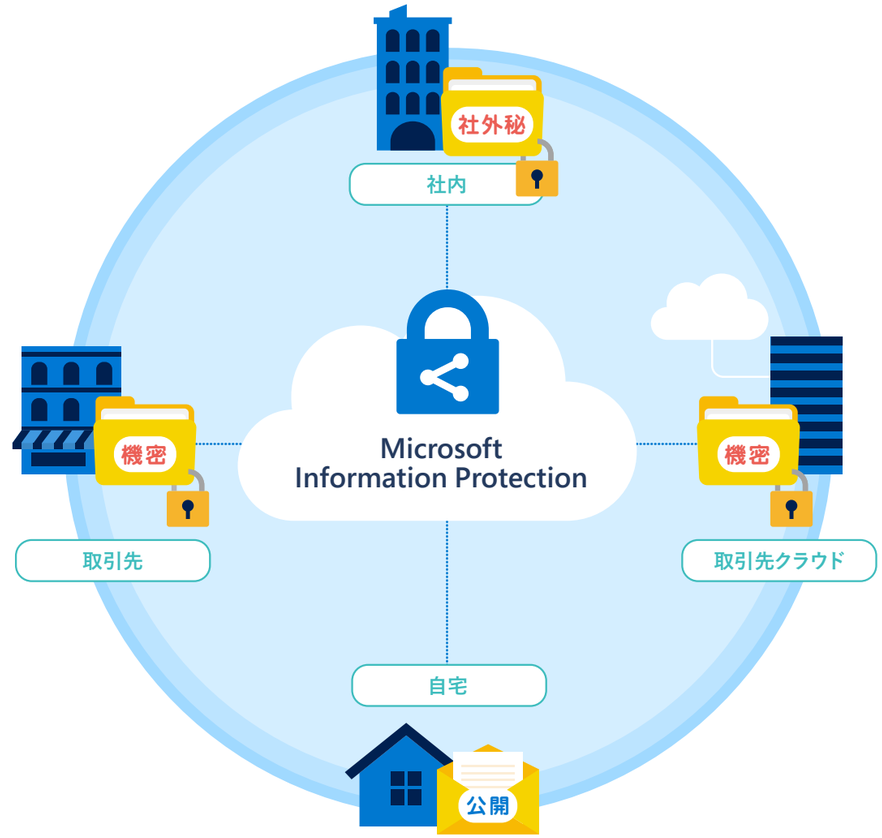
リモートワークでも機密情報を守れていますか？

リモートワークの普及により、これまでは社外に持ち出せなかったり、
特定の人しかアクセスできなかったりと、場所に依存した方法で管理されていた機密情報も、
さまざまな場所で扱う必要が出てきました。
当然、これらの情報や文書を保護する必要があります。
Microsoft 365 E5 の機能を活用すれば、
情報や文書が社内にあっても社外にあっても、自動的に保護することができます。

HINT!

Microsoft Information Protection で場所を問わずに文書を保護・制御

Microsoft 365 の情報保護ソリューション「Microsoft Information Protection（MIP）」を利用することで、Office ファイル内やクラウド ストレージ、ファイル サーバーなどにある文書に含まれる機密情報の種類や量、信頼度を識別し、自動的に「社外秘」「機密」「公開」など分類してラベルをつけ、ラベルのポリシーに応じて、データの保護や統制を行えます。これにより、取引先に送信してしまったファイルや、社員が自宅に持ち帰った文書でも、二次利用や漏洩を未然に防げます。



膨大な機密情報は安全に管理できていますか？

財務データ、クレジットカード番号、マイナンバー、社員の健康や社会保障に関する情報など、
現代の企業は守るべき情報を膨大に抱えています。
Microsoft 365 では、データ損失防止（Data Loss Prevention /DLP）機能を提供しています。
この機能により、さまざまな場所、さまざまなフォーマットでやりとりされている
機密情報の漏洩や不正利用を防ぐことができます。

HINT!

機密情報を検出・保護する Microsoft 365 E5 の DLP 機能

Azure AD で ID を統合し、シングルルサインオン（SSO）を利用すれば、ユーザーが一度ログインした資格情報がほかのアプリにも使用されることになり、アプリにいちいちサインインする必要がなくなります。ID を一元管理できるようになるので、さまざまな外部アプリケーションの認証レベルの統一することもできます。ユーザーを集中的に管理して、アクセス状況を一元的に把握することも可能です。

機密情報の高度な検出と制御

Microsoft 365 E5 の DLP 機能には、どの情報が重要なのかを検出するための標準テンプレートが 150 種類以上準備されています。この高度なデータ検出機能によって検出された情報を、ポリシーに基づいて管理・制御し、ポリシー違反のアラート提示や、不適切なデータ使用に対する自動削除や閲覧禁止といった制限をかけることができます。

DLP によって保護される範囲

- Exchange Online のメール
- SharePoint Online や OneDrive for Business で共有されたファイル
- Teams チャットやチャネル のメッセージ
- Office アプリ（ Word、Excel、PowerPoint ）
- Windows 10 エンドポイント
- Microsoft 以外のクラウド アプリ（SaaS アプリケーション）
- オンプレミスのファイル共有とオンプレミス の SharePoint

内部リスクに対応できる体制は整っていますか？

リモートワークやクラウド サービスが普及している今、

故意かどうかに関わらず会社の内部にあるリスクは見逃せないほど大きなものになっています。

これまでは、内部リスクが原因で情報漏洩が発生しても気づかれにくく、

事件化して初めて表面化する場合がほとんどでした。

内部不正の証拠を過去にさかのぼって探るのも大変です。

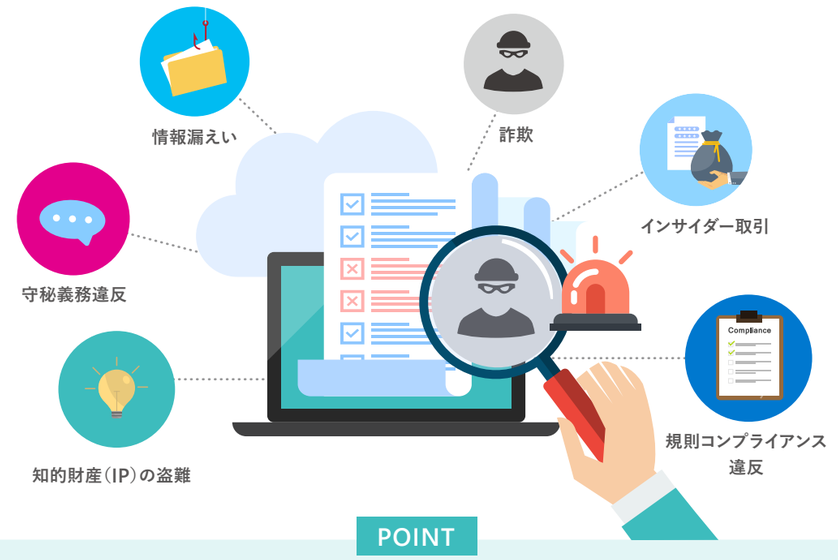
Microsoft 365 E5 の Insider Risk Management (IRM) は、

組織に潜むさまざまなリスクを検出し、不正の調査や対策をサポートします。

HINT!

内部不正の洗い出しから対処までのワークフローを提供

Microsoft 365 E5 の Microsoft Graph には、ユーザー ID/ デバイス ID、アクセス、コンプライアンス、セキュリティを管理し、データの漏洩や損失から組織を保護する強力なサービスが含まれています。Office 365 やデバイスにおけるユーザーアクティビティを監視して、リスクのあるアクティビティを検出。それを分析し、対処します。ユーザー起点で一連のデータの流れを見るので、調査や対策も簡単。匿名の状態でアラートを確認できるため、先入観なしで調査可能です。過去 1 年のログを遡って調査したり、調査対象者を指定して情報を収集・分析したりできるので、法的な証拠としても利用できます。



POINT

どんな流れで調査できるの？

Microsoft 365 E5 の IRM では、さまざまな種類のユーザーアクティビティを調査することが可能です。これらの疑わしい行為を「調査対象の設定（ポリシー）」→「検出（アラート」→「検査（ケース管理）」→「解決」という流れで調査を進めます。

調査対象の設定（ポリシー） → 検出（アラート） → 検査（ケース管理） → 解決

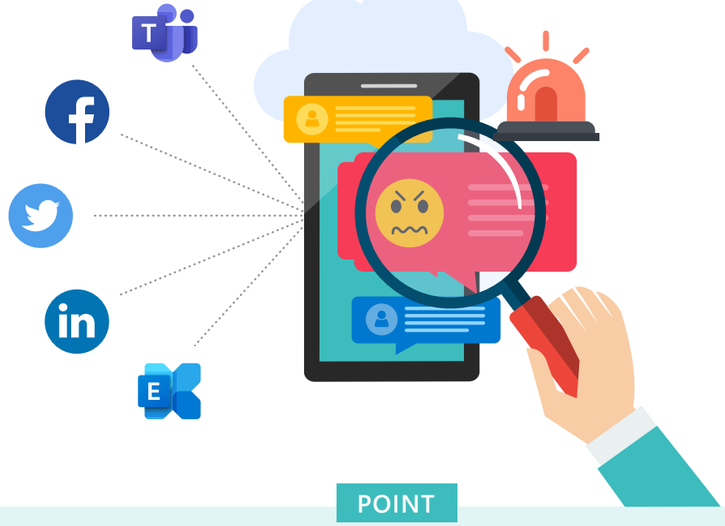
ハラスメント行為、対策をしていますか？

リモートワーク中、本人が目の前にいないこともあり、
チャットやメールでのハラスメントや違法な業務命令をするケースが増えています。
しかし、ハラスメント行為はそもそも発見しにくいうえ、証拠が集めにくく、
言い分が食い違うことも多いため、対応がとても困難です。
Microsoft 365 E5 のコミュニケーション コンプライアンスなら、
ハラスメントにつながりかねないメッセージの兆候を捉えて警告し、
次のアクションにつなげることができます。

HINT!

事前に定義・設定したキーワードから ハラスメント発生を可視化

Microsoft 365 E5 のコミュニケーション コンプライアンスは、Exchange Online や Teams だけでなく、Facebook や Twitter、Linkedin などのサードパーティのソースに至るまで広範なコミュニケーション ツールを監視し、事前に定義・設定したキーワードから、行動規範に違反したハラスメント行為に該当するメッセージを自動的に検知。問題解決に向けた警告やケース化などのアクションを自動で行います。同様のフローで談合などの兆候を見つけることも可能です。



POINT

行動規範への違反が検出されるとどうなるの？

行動規範に反するようなメッセージを検知→警告→問題管理（調査アクション）→ ドキュメントのレビュー→ユーザーアクティビティ履歴の確認という流れで問題が調査されます。管理部門から法務や人事部門へのエスカレーションも自動化することができます。

メッセージを検知 → 警告 → 問題管理（調査アクション） → ドキュメントのレビュー → ユーザーアクティビティ履歴の確認

チャットや Web 会議のリスク管理はできていますか？

チャットアプリや Web 会議ツールは、今や効率的なビジネスには欠かせません。
社外のユーザーを招待したり、機密情報を取り交わしたりと、
セキュリティ対策が必要とされるやりとりも増えており、
安心して使えるツールを選ぶことが大切です。
Microsoft 365 E5 の「Teams」は、ビジネス シーンでの利用を想定した、
セキュリティ対策万全のコラボレーション ツールです。

HINT!

Teams の DLP 機能でリモートワーク中の内部リスクから情報を保護

Teams は、データ損失防止（DLP）機能によって、外部ユーザーと共有された機密性の高いメッセージやファイルを自動的に削除したり、投稿された機密情報を外部ユーザーが開けないように設定したりと、リモートワークで想定される内部リスクから情報を保護します。

POINT

安心・安全に使えるコラボレーション ツール Teams の DLP 機能

会議の制御	外部ユーザーの参加や権限を制御。招いていない人物が勝手に参加することも防げます。
プライバシーを保護	通信内容が広告に使われたり、会議の内容が検閲されたりすることもありません。
組織アカウントを保護	外部ユーザーにも多要素認証を設定したり、条件付きアクセスでパスワードの漏洩を防いだりできるので、安心して外部の人とコラボレーションできます。
脅威対策も万全	悪意あるリンクやマルウェアに感染した添付ファイルへのアクセスをブロックします。

やりとりしてほしくないユーザーの管理はできていますか?

クラウドやコミュニケーション ツールの普及によって、社内のコミュニケーションや
情報共有がスムーズになった一方、柔軟すぎるコミュニケーションが弊害となるケースもあります。
企業・組織には、人事・監査関連情報などの特定部署内に留めておきたい情報や
オープンにやり取りされては困る情報があり、
活発にコミュニケーションされると困るグループや人員が存在するのも確かです。
Microsoft 365 E5 の「情報バリア」は、特定の組織やユーザー間の
コミュニケーションを制限するのに役立ちます。

HINT!

特定ユーザーのコラボレーションを制限する「情報バリア」

Microsoft 365 E5 の情報バリア機能は、個人またはグループが互いに通信し合うのを防ぐために管理者がポリシーを決めることができ、以下のような利益相反リスクまたはポリシー違反が発生した場合に適用されます。

例 1　デイトレーダーから
マーケティング チーム メンバーへの
通話禁止

例 2　機密情報を扱っている財務部の
メンバーに対する、
一部メンバーからの発信禁止

例 3　機密情報を扱うメンバーから、
組織内の一部メンバーに対する
通話・チャットの禁止

例 4　研究チームからの通話やチャットは、
製品開発チーム対象のみ

POINT

どんなやりとりを制限できるの?

Teams、SharePoint オンライン、OneDrive for Business 上の通信ややりとりを制限して、ポリシーに反する情報のやりとりを防止します。

- ユーザーやポータルサイトの検索
- チームやポータルサイトへのメンバーの追加
- 他のユーザーとのチャット、グループチャット
- 会議への招待
- Web 会議での画面の共有
- 電話での通信
- ファイルの共有やアクセス
- ポータルサイトやコンテンツの共有やアクセス

高度なセキュリティ機能をオールインワンで提供

Microsoft 365 E5 では、新時代のビジネス環境に必要な
「ID 保護」「脅威対策」「情報保護」「クラウドセキュリティ」の
4 つのセキュリティ機能がまとめて提供されます。
あとから機能を追加しなくても、Azure AD をはじめとする
さまざまなセキュリティ機能を提供するサービスを常に最新の状態で利用できるため、
各機能を連携させて包括的に組織全体を守ることができます。
同時に、自動化によって管理者の負担も軽減できます。

	Microsoft 365 E3	Microsoft 365 E5
ユーザー / 月	詳しくは、販売パートナー様へお問合せください	
含まれる Office アプリ	Outlook, Word, Excel, PowerPoint, Access, Publisher（Access、Publisher は Windows PC のみ）	
含まれるクラウドサービス	Exchange, OneDrive, SharePoint, Teams, Bookings, Sway, Lists, Yammer, Stream, Power Apps, Power Automate, Planner, ToDo, MyAnalytics	
1 ライセンスでのインストール	最大 5 台の Windows PC / Mac （Web・モバイル版と合わせて最大 15 台のデバイス）	
契約可能な最大ユーザ数	300 人～	
デバイスとアプリの管理	○	○
アイデンティティとアクセスの管理	△ ※	○
脅威対策	△ ※	○
情報保護	△ ※	○
セキュリティ管理	○	○
コンプライアンス管理	△ ※	○

※詳しくはこちらをご確認ください。https://www.microsoft.com/ja-jp/microsoft-365/compare-microsoft-365-enterprise-plans

Microsoft

ご購入前のご相談は「セキュア リモートワーク相談窓口」

0120-167-400

（営業時間：9:00 ～17:30 土日祝日、弊社指定休業日を除く）

詳しくはこちらから

https://www.microsoft.com/ja-jp/microsoft-365

日本マイクロソフト株式会社　〒108-0075 東京都港区港南 2 - 16 - 3 品川グランドセントラルタワー