MOTEX

情シス1,000人に聞いた！

Microsoft 365の利用における企業のセキュリティ対策に関する

エムオーテックス株式会社

本調査について

昨今、多くの企業で導入が進んでいるMicrosoft 365。

様々なアプリケーションの利用を通じて、働き方の効率化や生産性の向上を支援できる一方で、
不正アクセスや内部不正、設定ミスなどを起因とした様々な情報漏洩のリスクが存在しています。

そこで今回、企業の情報システム部担当者1,000名にMicrosoft 365のセキュリティ対策に関する調査を行いました。

本調査では、Microsoft 365を利用している企業様の回答からセキュリティ対策の状況や課題を知ることができます。
皆様がより良いセキュリティ体制を構築できるよう、本調査結果がお役に立てば幸いです。

エムオーテックス株式会社

chapter

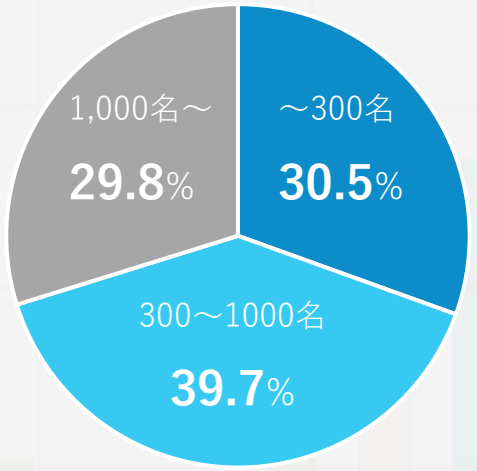
01. 調査結果

本調査について

調査概要　**Microsoft 365の利用における企業のセキュリティ対策に関する実態調査**

- 調査期間：2025年2月
- 調査方法：インターネット調査
- 調査人数：1,062名
- 調査対象：従業員規模300名未満、従業員規模300名～1,000名未満、
  及び従業員規模1,000名以上の企業の情報システム担当者かつPC管理の担当者
- モニター提供元：PRIZMAリサーチ

会社規模内訳

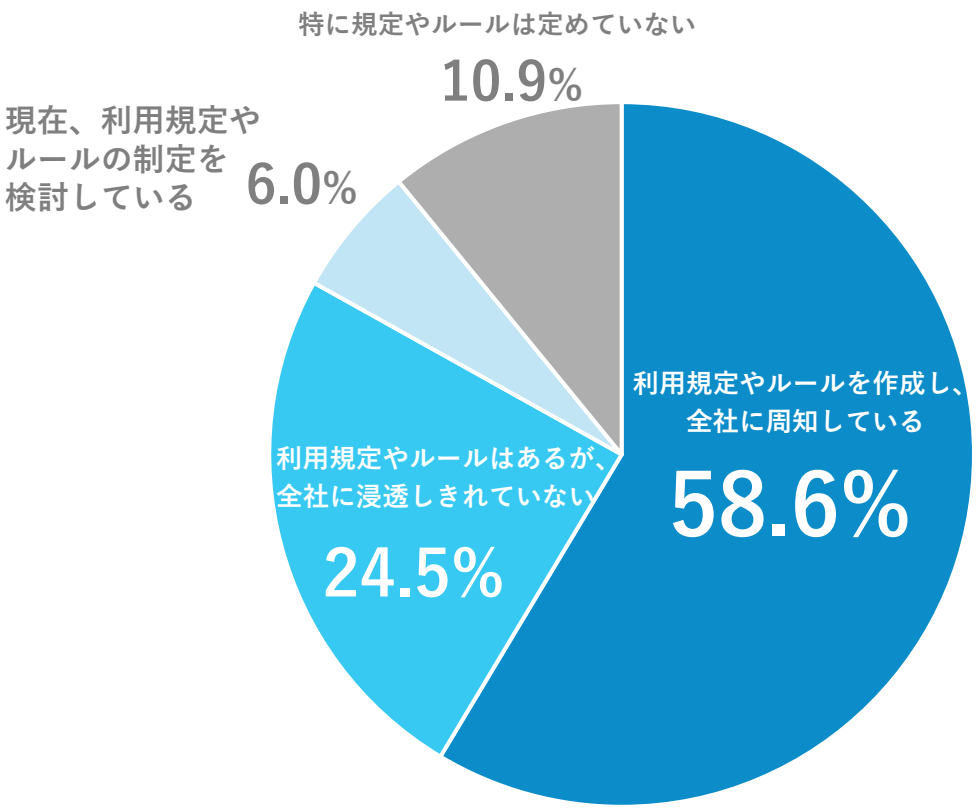


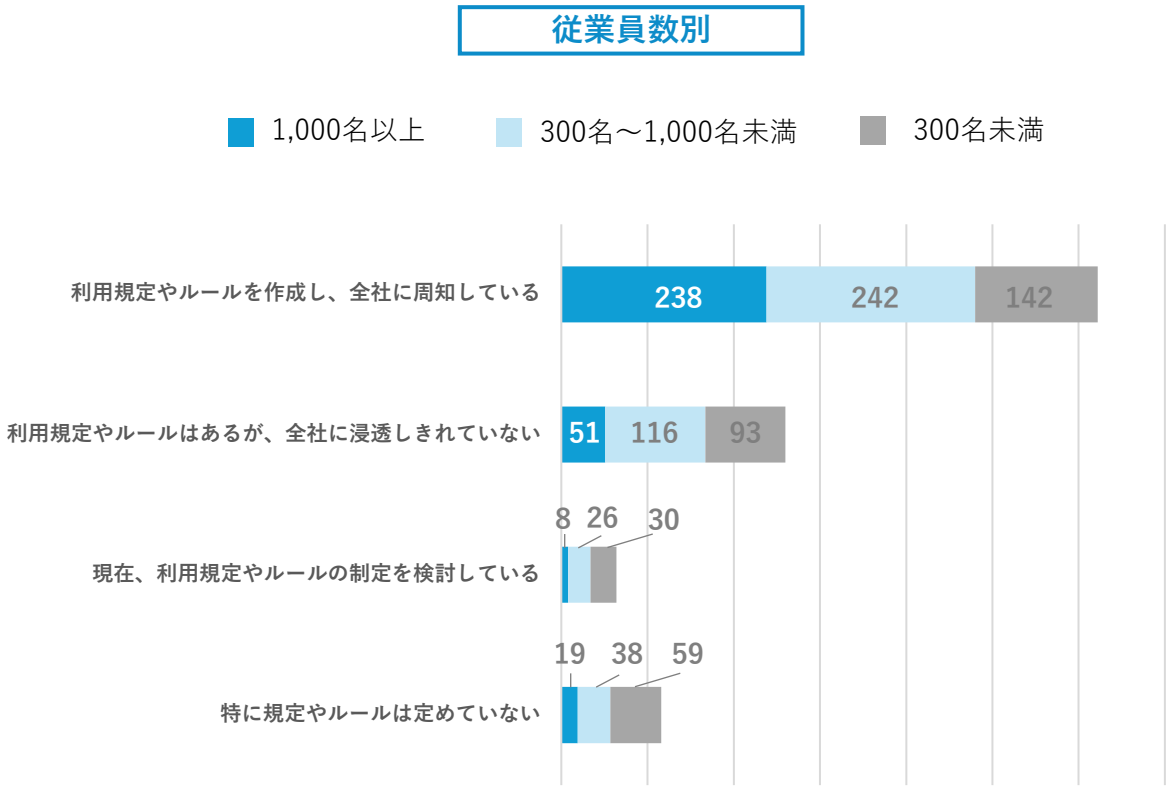
調査項目について

No	アンケート項目
1	Microsoft 365を社内利用するうえで、利用規定やルールを定めていますか？
2	Microsoft 365のセキュリティ対策として、現在対策中、または対策を検討しているものを教えてください
3	Microsoft 365のセキュリティ設定として実施しているものはありますか？
4	Microsoft 365の社外共有リンクの設定について、対象ユーザーをどの範囲まで許可していますか？
5	Microsoft 365のゲストユーザー招待の設定はどの範囲まで許可していますか？
6	Microsoft 365を運用する中で、過去にヒヤリハットはありましたか？
7	Microsoft 365の監査ログを定期的に確認していますか？
8	Microsoft 365監査ログの定期的な確認ができていない理由はなぜですか？
9	現在お使いのMicrosoft 365のプランを選択してください
10	Microsoft 365の監査ログについて何日以上の保管が必要と考えていますか？

Microsoft 365の利用ルール

Q.1 Microsoft 365を社内利用するうえで、利用規定やルールを定めていますか？ （有効回答数：1,062）

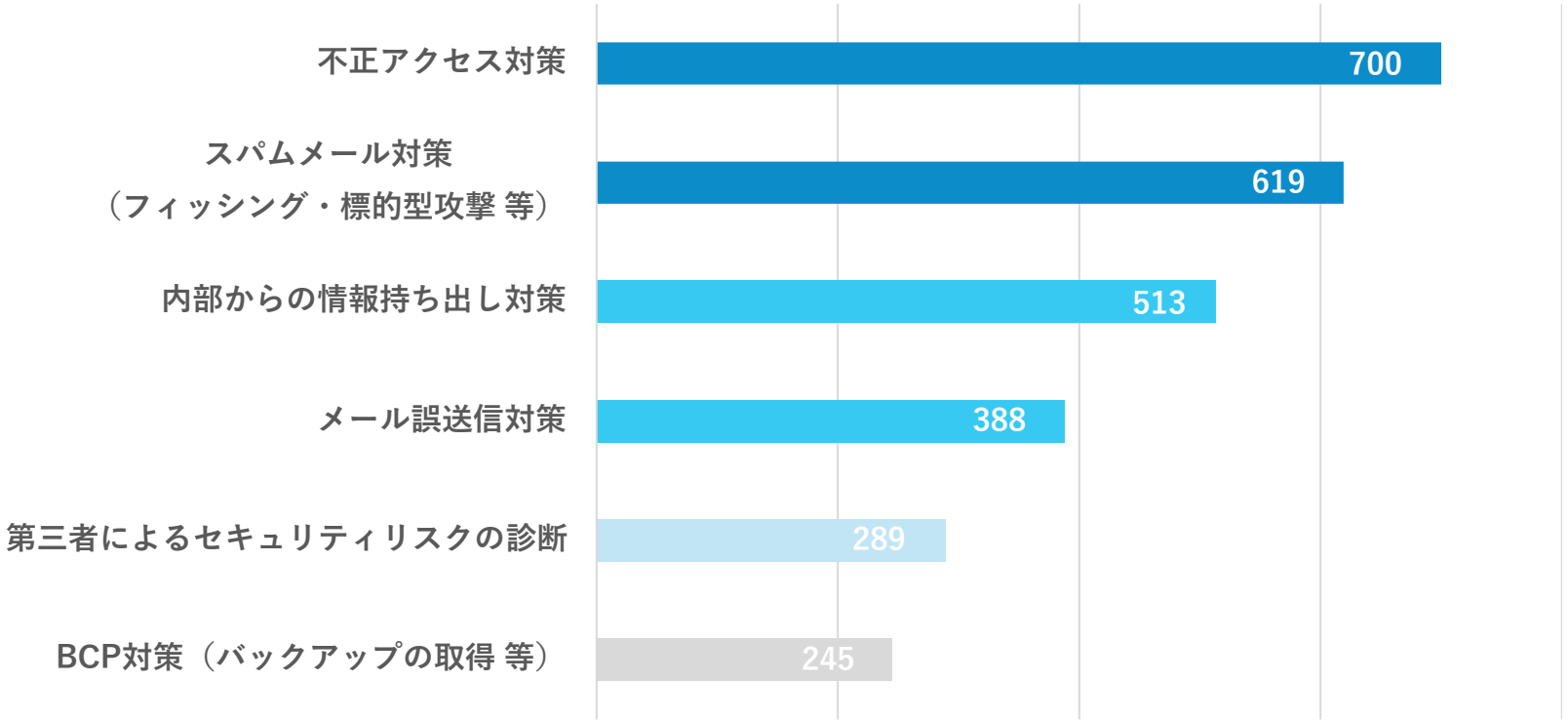




Microsoft 365の利用規定やルールを定めている組織は8割以上となっており、Microsoft 365に対するセキュリティ意識が高まっていることが分かる。
また、従業員数別の回答結果には大きな差は見られず、組織規模にかかわらずルールの策定がスタンダードに。

セキュリティ対策の状況

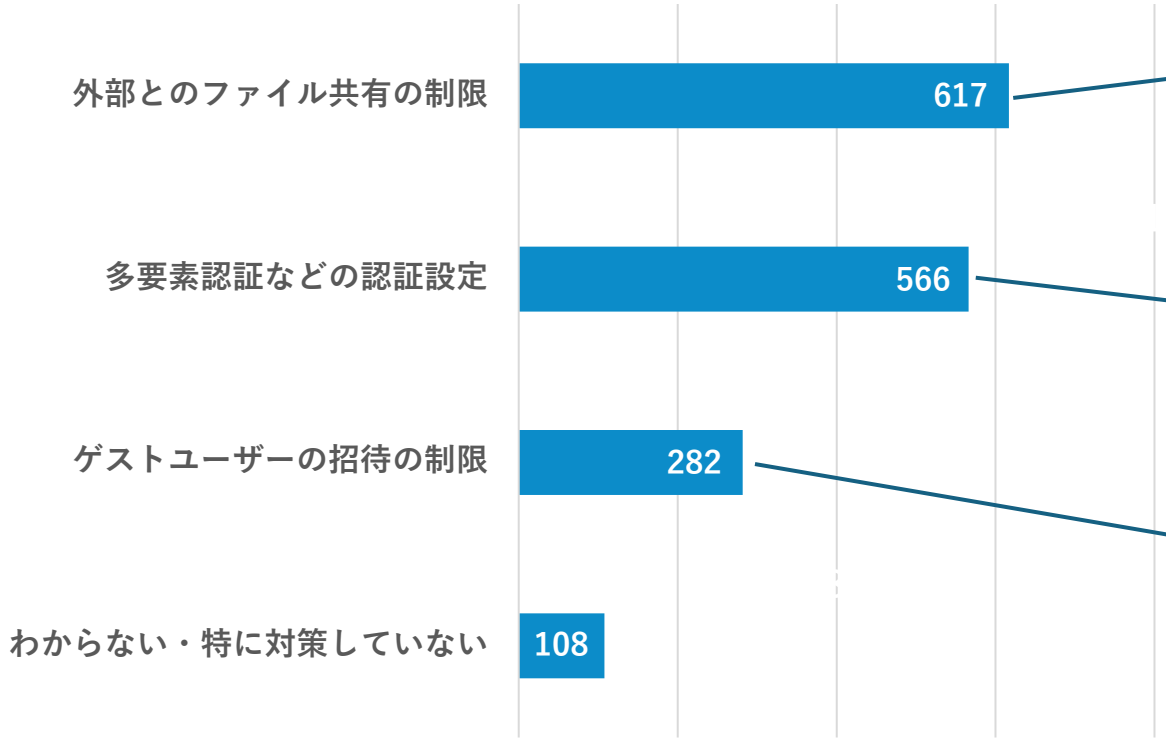
Q.2 Microsoft 365のセキュリティ対策として、現在対策中、または対策を検討しているものを教えてください　（複数選択可　有効回答数：1,062）



多くの組織でMicrosoft 365のセキュリティ対策として対策済み・対策を検討中となっているのが、不正アクセス対策・スパムメール対策（フィッシング・標的型攻撃等）。次いで、内部からの情報持ち出し対策・メール誤送信対策が多く、外部脅威だけでなく内部脅威対策についても注目されていることが分かる。また第三者によるセキュリティリスクの診断を行っている組織も3割近い結果となった。

Microsoft 365の設定について

Q.3 Microsoft 365のセキュリティ設定として実施しているものはありますか？（複数回答可　有効回答数：1,062）



外部とのファイル共有

SharePointやOneDriveで、外部のユーザーに対してファイルなどのコンテンツを共有できる機能

多要素認証などの認証設定

ID・パスワードと合わせて、異なる要素を用いて認証を行う機能
（ex. スマホアプリのワンタイムパスワード、クライアント証明書、生体認証など）

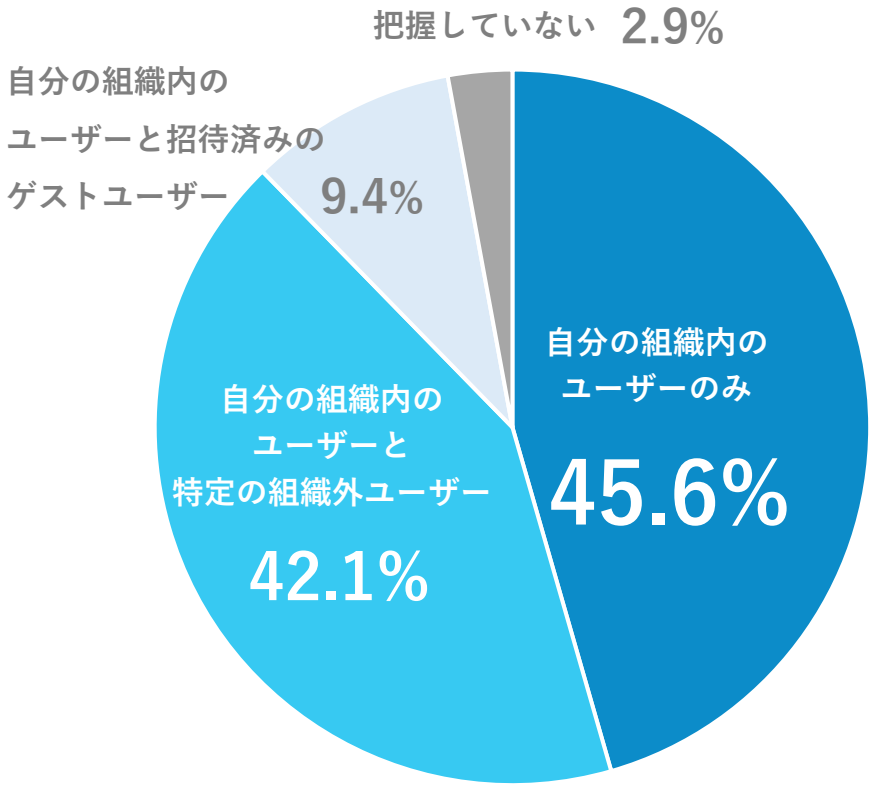
ゲストユーザーの招待

外部からゲストユーザーを招待することで、Teamsをはじめとした
アプリケーション上で共同作業ができる機能

セキュリティ設定として実施しているものについては、ファイル共有の制限や多要素認証が多くみられた。ゲストユーザーの招待については、他の設定項目に比べると設定している企業が少なく、注意すべきポイントの一つと言える。基本的なセキュリティ設定をしっかりと行うことで、外部からの不正アクセスや情報漏洩のリスクを低減することが可能なため、未対応の場合は自社の運用ルールに合わせて見直すことをお勧めする。

Microsoft 365の設定について

Q.4 Microsoft 365の社外共有リンクの設定について、対象ユーザーをどの範囲まで許可していますか？(有効回答数：617)

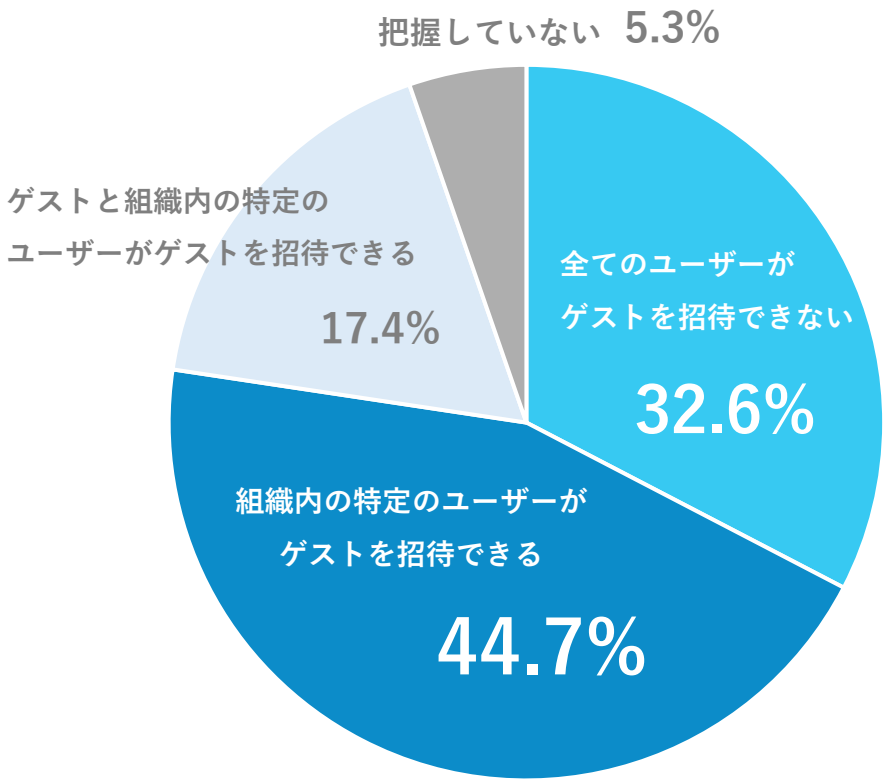


	解説	外部への共有
自分の組織内のユーザーと招待済みのゲストユーザー	組織内部のユーザー、サインインしているゲストユーザーに対しては問題無くコンテンツを共有できます。外部ユーザーに共有することはできません。共有が必要な場合はゲストユーザーとして、自組織への招待が必要です。	可能
自分の組織内のユーザーと特定の組織外ユーザー	組織内部のユーザー、サインインしているゲストユーザーに対しては問題無くコンテンツを共有できます。外部のユーザーやMicrosoft 365のアカウントを持っていないユーザーに対しては、メールアドレスへ送信した認証コードを入力する必要があります。 外部の一般ユーザーに対して共有する場合はこの設定を使うこととなります。	可能
自分の組織内のユーザーのみ	組織内部のユーザーのみに対してコンテンツを共有できます。 ゲストユーザーや外部のユーザーに対して共有することはできません。	不可 （最も制限的）

Microsoft 365の設定について、SharePointやOneDriveのデータ共有を、自分の組織内のユーザーのみに限定している企業が約4割、一方で半数以上の企業が、ゲストユーザーや組織外のユーザーにデータ共有することを許可しているという結果に。特定の組織外ユーザーへの共有のみ制限しているものの、機密情報などの社外共有が可能となるため、定期的なモニタリング等が必要と言える。

Microsoft 365の設定について

Q.5 Microsoft 365のゲストユーザー招待の設定はどの範囲まで許可していますか？（有効回答数：282）



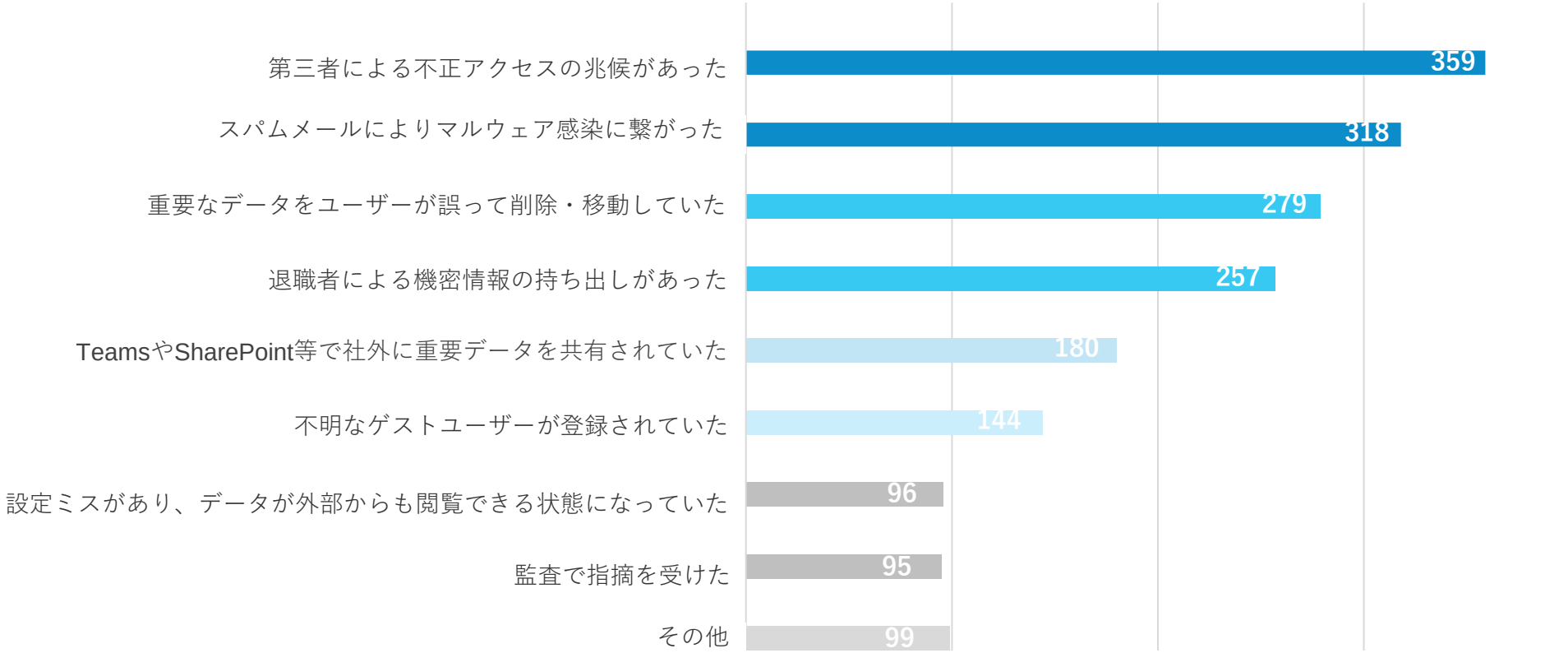
	解説	ゲストの招待
ゲストと組織内の特定のユーザーがゲストを招待できる	運用上ゲストユーザーが必要な場合はこの設定になります。特定の管理者ロールに割り当てられているユーザーのみがゲストユーザーを招待できます。（特定の管理者ロールをゲストユーザーにも設定できます）	可能
組織内の特定のユーザーがゲストを招待できる	同上ですが、ゲストユーザーは設定できません。	可能
すべてのユーザーがゲストを招待できない	ゲストユーザーを招待できない設定です。	不可（最も制限的）

6割以上の組織で、ゲストユーザーを招待できる設定で運用していることが判明した。ゲストユーザーの招待は、社外とのコミュニケーションを効率化できるメリットがある一方で、対象のゲストユーザーが増えると管理が煩雑になるだけでなく、意図しないセキュリティ事故が発生するリスクも高まる。
こうした事態を防ぐためにも、ゲストユーザーの定期的な棚卸が必要といえる。

インシデントの有無について

Q.6

Microsoft 365を運用する中で、過去にヒヤリハットはありましたか？（複数回答可　有効回答数：1,062）

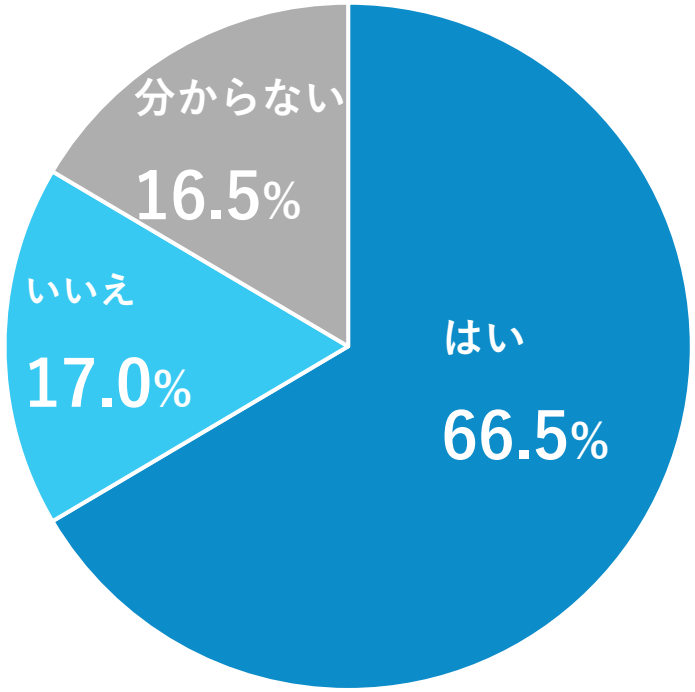


Microsoft 365を運用する中で、過去に発生したインシデントとして、不正アクセスやメール経由でのマルウェア感染などの外部脅威が上位に挙がった。次いで、ユーザーのミスによるデータ削除、退職予定者による情報持ち出しなどが多く、内部脅威についても対策が必要と言える。また、TeamsやSharePointで組織外にデータを共有されていた、または不明なゲストユーザーが登録されていたなどの事案は、Microsoft 365の設定を見直すことで防ぐことができる可能性もあるため、注意したいポイント。

監査ログ管理について

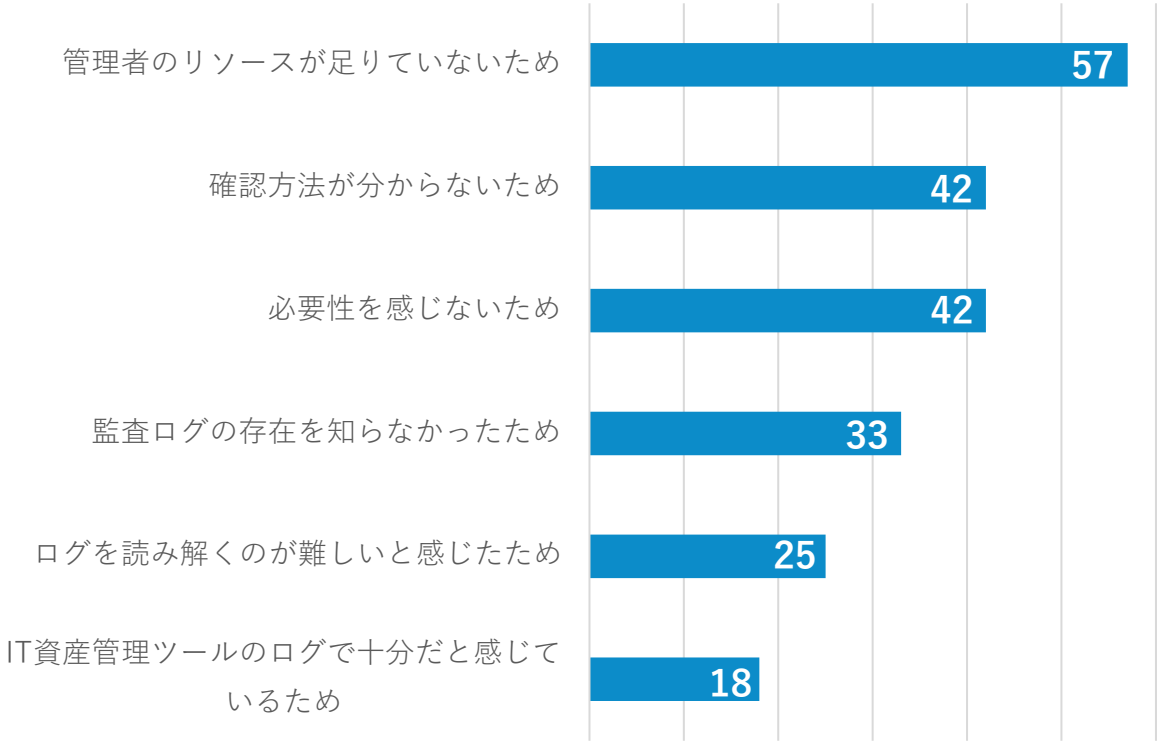
Q.7 Microsoft 365の監査ログを定期的に確認していますか？

（有効回答数：1,062）



Q.8 Microsoft 365 監査ログの定期的な確認ができていない理由はなぜですか？

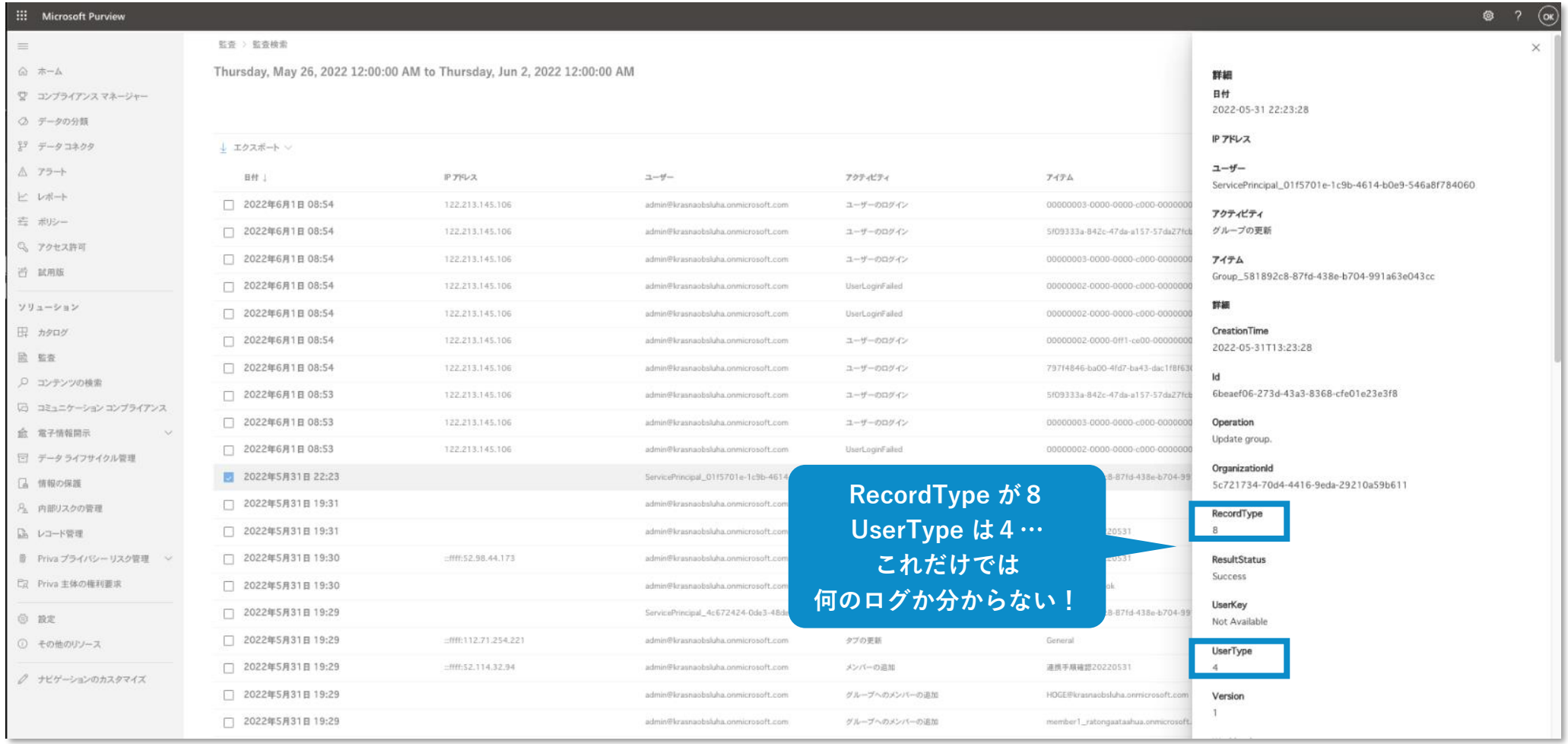
（複数回答可　有効回答数：181）



監査ログを定期的に確認している企業は6割以上となっており、多くの企業でセキュリティ対策として監査ログが活用されているという結果になった。
一方で、「定期的に確認ができていない」「分からない」と回答した企業が約3割となっており、その理由として管理者のリソース不足や確認方法が分からないといった課題が多く見られた。Microsoft 365の監査ログについては定期的な管理が一般的となっているものの、運用におけるハードルも多く存在していることがわかる。

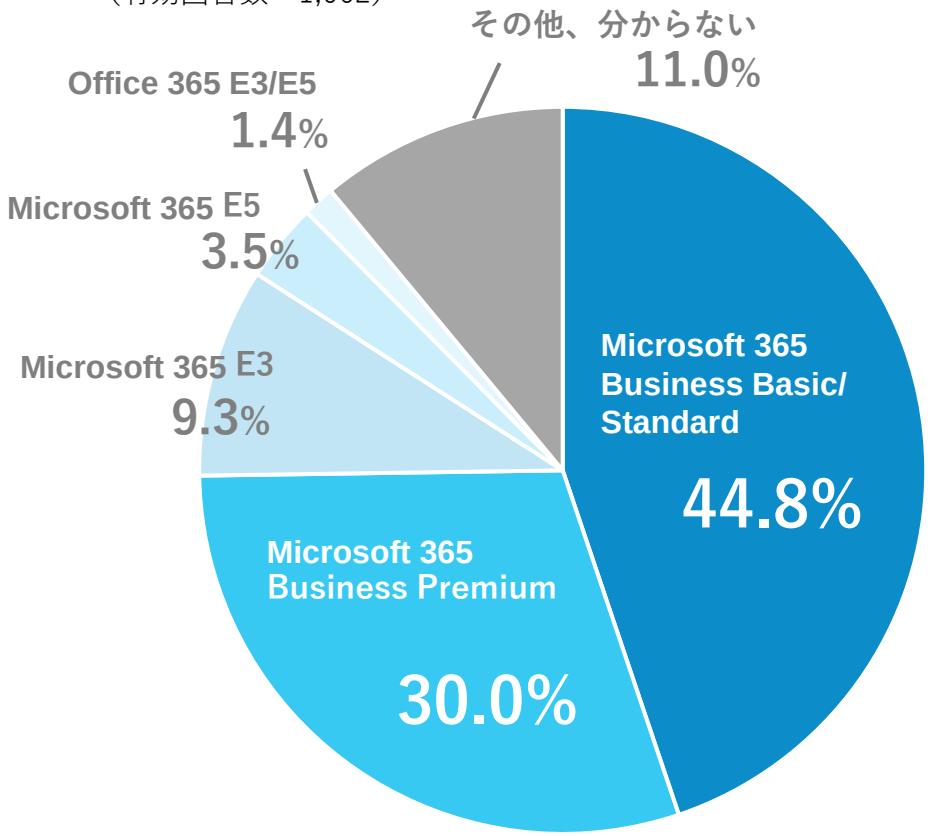
【参考】Microsoft 365の監査ログにおける課題

Microsoft 365上でも監査ログを確認できるものの、RecordTypeやUserTypeなどで表現される値を
Microsoft社が公開している項目と照合しないと読み解けない仕様に・・

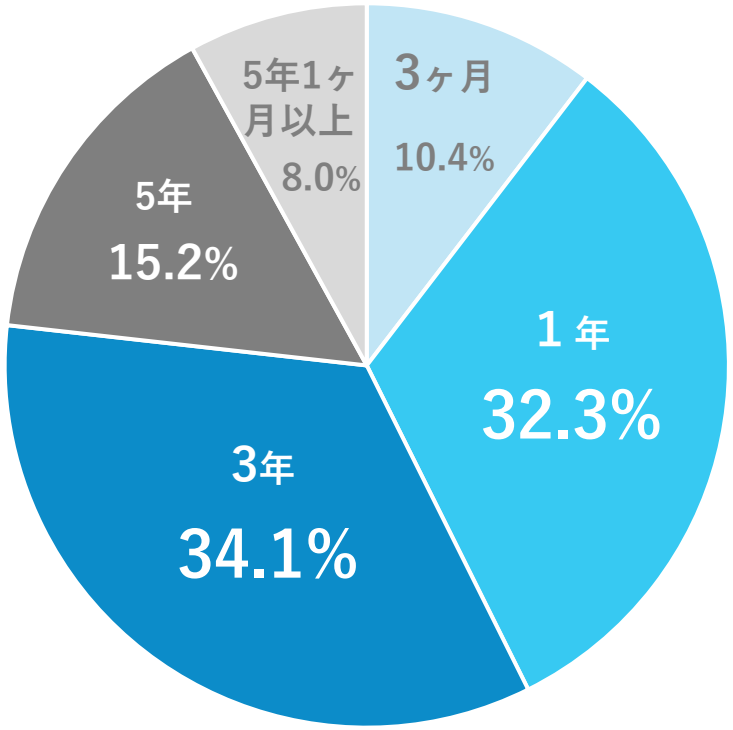


Microsoft 365の利用プラン

Q.9 現在お使いのMicrosoft 365のプランを選択してください
（有効回答数：1,062）



Q.10 Microsoft 365の監査ログについて何日以上の保管が必要と考えていますか？
（有効回答数：847）



Microsoft 365の契約プランについては、ユーザーの利用上限が300名以下のプラン（Microsoft 365 Business Basic・Business Standard・Business Premium）を契約している企業が7割。また、監査ログの保存期間については、「1年以上必要」と答えた企業が約9割という結果に。Microsoft 365のプランでは、E3・E5などの一部プランを除き、最長180日間のログ保存となっており、多くのユーザーの要件を満たせていないことがわかる。

【参考】Microsoft 365におけるログの保存日数比較

Microsoft 365では、1年以上のログ保存に対応するには<u>Microsoft E5（8,208円/月）</u>
もしくは、最低でも<u>月額750円/月のオプション購入</u>が必要…

	Microsoft 365 Business Basic	Microsoft 365 Business Standard	Microsoft 365 Business Premium	Microsoft E3	Microsoft E5	Microsoft F3	Office E1	Office E3	Office E5
ログ保存期間	180日	180日	180日	180日	1年	180日	180日	180日	1年
価格	899円/ユーザー	1,874円/ユーザー	3,298円/ユーザー	5,059円/ユーザー	8,208円/ユーザー	1,199円/ユーザー	1,161円/ユーザー	3,110円/ユーザー	5,359円/ユーザー
ユーザ上限	300	300	300	無制限	無制限	無制限	無制限	無制限	無制限
ログ保存オプション	×	×	×	+750円/月額で1年間保存可能	+250円/月額で10年間保存可能	×	×	+750円/月額で1年間保存可能	+250円/月額で10年間保存可能

※価格はすべて税抜き価格です。

chapter

02 まとめ

まとめ

01 Microsoft 365の利用ルールを定めている企業が8割

Microsoft 365を社内利用する上で、ユーザーに対し何らかの利用規定やルールを定めている企業が8割という結果に。
組織の業務の根幹となるクラウドサービスとして、セキュリティ対策意識の高さがうかがえます。

02 組織外ユーザーへのファイル共有や、ゲストユーザーの招待を許可している企業が多数

外部とのデータ共有、ゲストユーザーの招待設定など、多くの企業で外部のユーザーとの共同業務を許可しているという結果に。
外部とのコラボレーションは利便性が向上する一方で、機密情報の漏洩などのセキュリティリスクがあります。
自社の運用ルールに合わせて、設定の見直しや操作ログのチェックを行うことで、リスクを低減することも重要です。

03 監査ログを定期確認する企業が多い一方で、課題も多く存在

6割以上の企業が、ログの定期的な確認を実施しており、インシデントなどの早期発見を意識しています。
その一方で、約3割の企業はリソース不足や確認方法が分からないという理由から、定期的な確認ができていないという現状も。
管理者のリソースだけでなく、専用のログ管理ツールを併用することでより効率的な管理も可能です。

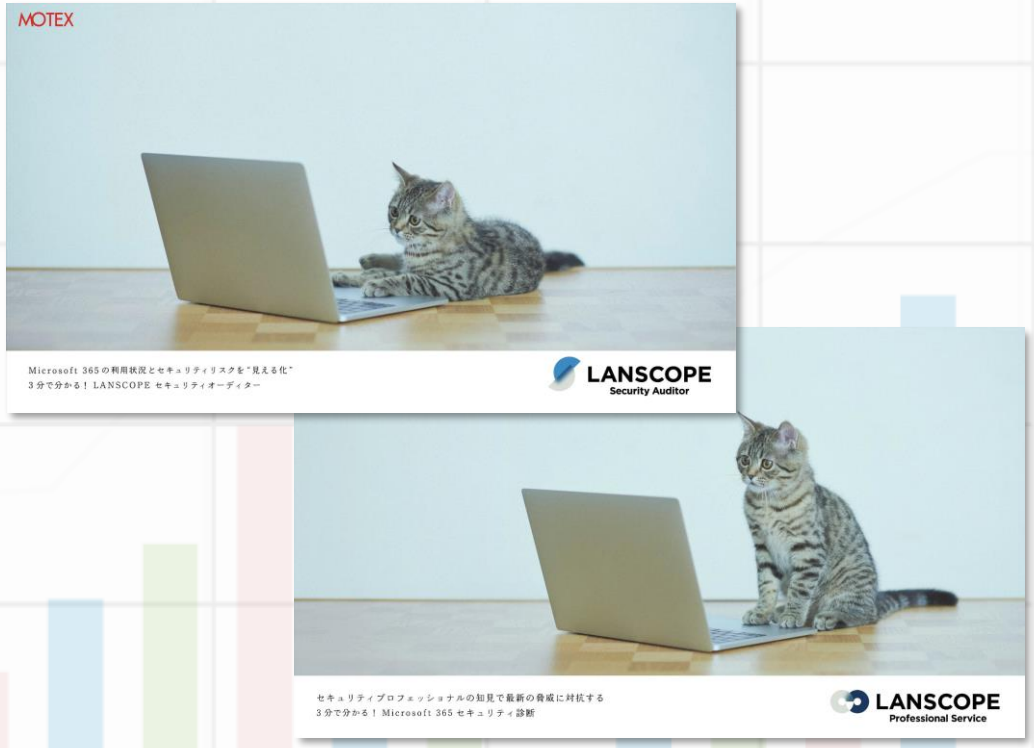
ダウンロードできる資料

- **3分で分かるMicrosoft 365脆弱性診断**

Microsoft 365の設定にセキュリティ上の不備がないか、
セキュリティエンジニアが診断し、結果をレポーティングする
サービスです。

- **3分で分かるLANSCOPE セキュリティオーディター**

解読の難しいMicrosoft 365の監査ログを自動収集し、
分かりやすくレポーティングする製品です。



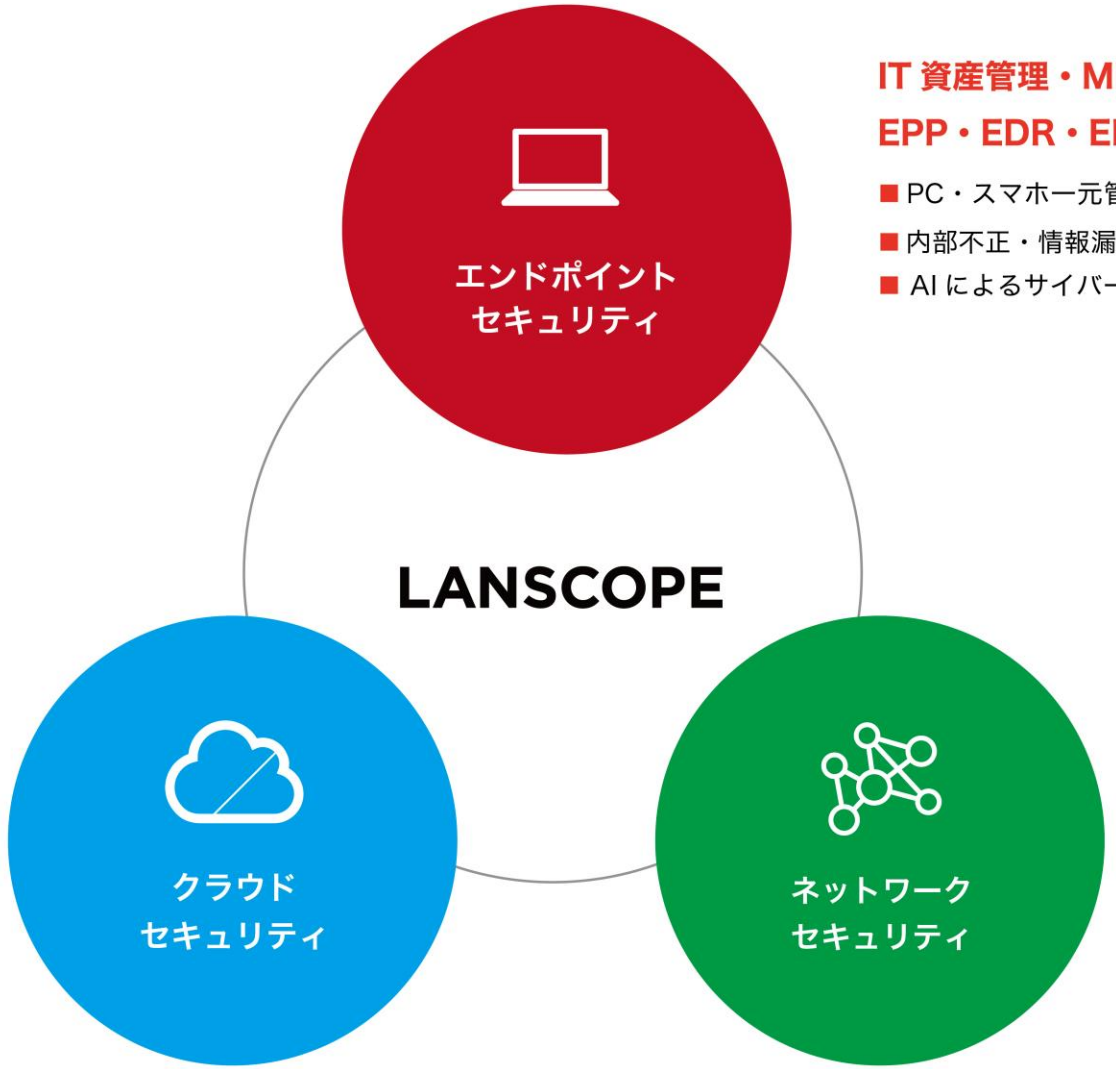
資料をダウンロードする

https://www.lanscope.jp/security-auditor/form-documents/3min_syncpit_doc_SCA028/

chapter

03 LANSCOPEのご紹介

エムオーテックスが提供する3つのセキュリティソリューション



IT 資産管理・MDM
EPP・EDR・EDR

- PC・スマホ一元管理
- 内部不正・情報漏洩対策
- AI によるサイバー攻撃対策

SaaS・IaaS の設定診断
Microsoft 365 監査ログ管理

- 国家資格取得者による設定診断
- 業界トップクラスの診断項目数
- 監査ログの取得・アラート管理

脆弱性診断・AI 型ネットワーク脅威検知
サプライチェーンリスク評価

- AI によるネットワーク監視・遮断
- Web・ネットワークの脆弱性診断
- 外部公開資産の洗い出し・リスク評価

エムオーテックスが提供するプロダクト・サービス

「LANSCOPE」を通して、お客様の “Security Productivity” の実現を支援

エンドポイントセキュリティ | クラウドセキュリティ | ネットワークセキュリティ

統合エンドポイント管理

Endpoint Manager

組織の IT 資産管理・内部不正対策・外部脅威対策をオールインワンで対応

- IT 資産管理・MDM
- 内部情報漏洩対策
- 外部脅威対策

AI アンチウイルス

Cyber Protection

AI を活用したアンチウイルスで未知・亜種の脅威を検知・対処・復旧が可能

- EPP
- EDR
- MDR

リモートコントロール

Remote Desktop

遠隔地のサーバーやPC、スマホへのリモート操作、画面共有などヘルプデスク業務を効率化

- リモートアクセス
- ヘルプデスク効率化

Microsoft 365 セキュリティ

Security Auditor

Microsoft 365の監査ログを取得。利用状況の見える化やアラート管理が可能

- 監査ログ管理
- アラート管理

脆弱性診断

Professional Service

高い技術力を誇るセキュリティエンジニアがWeb・ネットワーク・クラウドの脆弱性を診断

- Web 診断
- ネットワーク診断
- クラウド診断

AI 型ネットワーク脅威検知

DARKTRACE

AI を活用しネットワークを監視、サイバー攻撃や内部不正の兆候を検知・遮断

- NDR
- ネットワーク遮断
- Email 監視

サプライチェーンリスクマネジメント

Panorays

ドメイン情報やオンライン調査票からサプライチェーンリスクを可視化

- セキュリティスコアリング
- ASM

本資料内容についてのご質問や、セキュリティに関するご相談があれば、お気軽にお問い合わせください。

無料Webセミナー

ウイルス対策や情報漏洩対策など
幅広いコンテンツを配信中。
いつでも視聴できるオンデマンド配信も
ございます。

セミナーを確認する

お役立ち資料

今すぐ実践できるセキュリティ対策・
事例、調査データ、プロダクト紹介資
料などご活用ください。

資料をダウンロードする

オウンドメディア Wiz LANSCOPE

安全と生産性の両立を実現するために、
サイバーセキュリティに関わる情報を分
かりやすく伝える
情報サイトです。

ブログを読む

MOTEX

本資料に関するお問い合わせ

■ マーケティング本部
プロダクトマーケティング部
E-mail　product@motex.co.jp

ご導入後のプロダクト利用に関するお問い合わせ

サポートセンター	0120-968-995 （携帯・PHSからは06-6308-8981）
お電話受付時間	9:30～12:00/13:00～17:30（平日、祝祭日除く）
E-mailお問い合わせ	support@motex.co.jp