Cloud
LANSCOPE
Endpoint Manager

6割以上の企業が対策未実施

情報漏洩リスクに備える！
今すぐ始めるべきシャドーIT対策とは？

chapter

01 シャドー IT のセキュリティ対策

© MOTEX Inc.

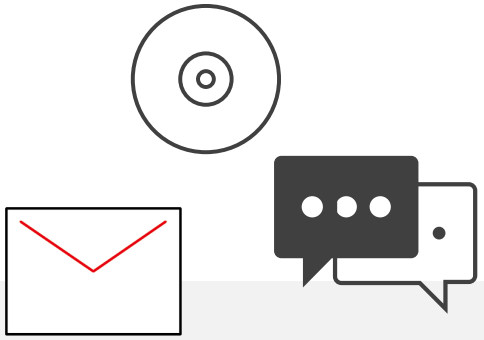
シャドーITとは？

シャドー IT にはさまざまな種類がありますが主に以下の３つになります

最近は、クラウド上で利用するサービスがシャドー IT となるケースが増加

私用デバイス

従業員が個人のデバイス（スマートフォン、タブレット、ノートパソコンなど）を業務に使用すると企業のセキュリティポリシーが適用されないデバイスでのデータアクセスが発生し、セキュリティリスクが高まる。



未承認のソフトウェアやアプリケーション

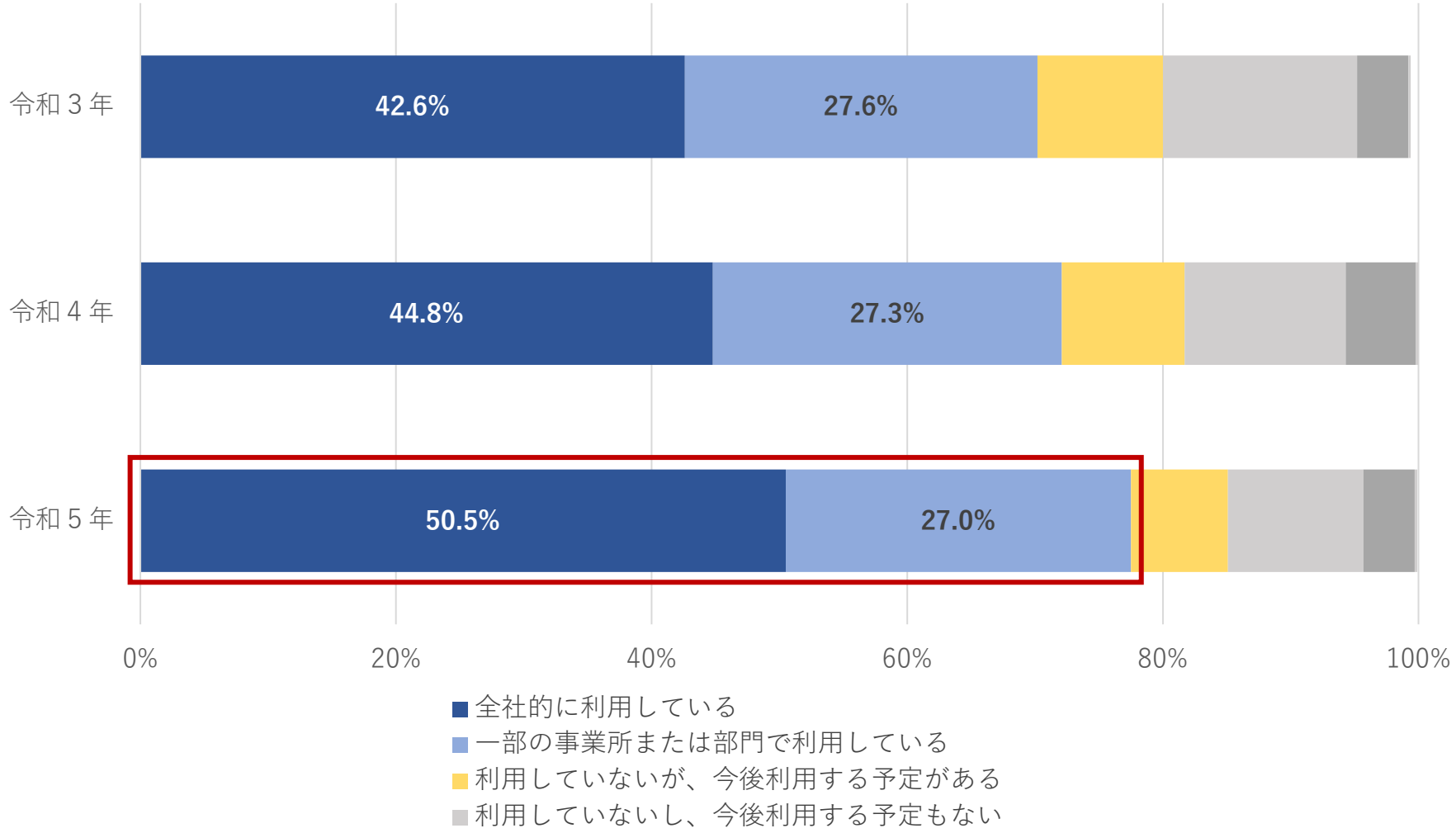
企業が許可していないソフトウェアやアプリケーション（チャットツールなど）をはセキュリティ対策が不十分な場合があり、マルウェアやウイルスの侵入経路となって情報漏洩や不正アクセスのリスクが高まる。

会社で契約していないクラウドサービス

企業が正式に契約していないクラウドサービス（SaaS製品など）を従業員が利用することでアクセス権限が不明確になり、セキュリティリスクが増大。

クラウドサービスの利用状況

クラウドサービスを利用する組織は増加傾向で8割近くの組織が利用をしている
一方で、会社に許可なく利用しているシャドー IT が大きな問題になっている

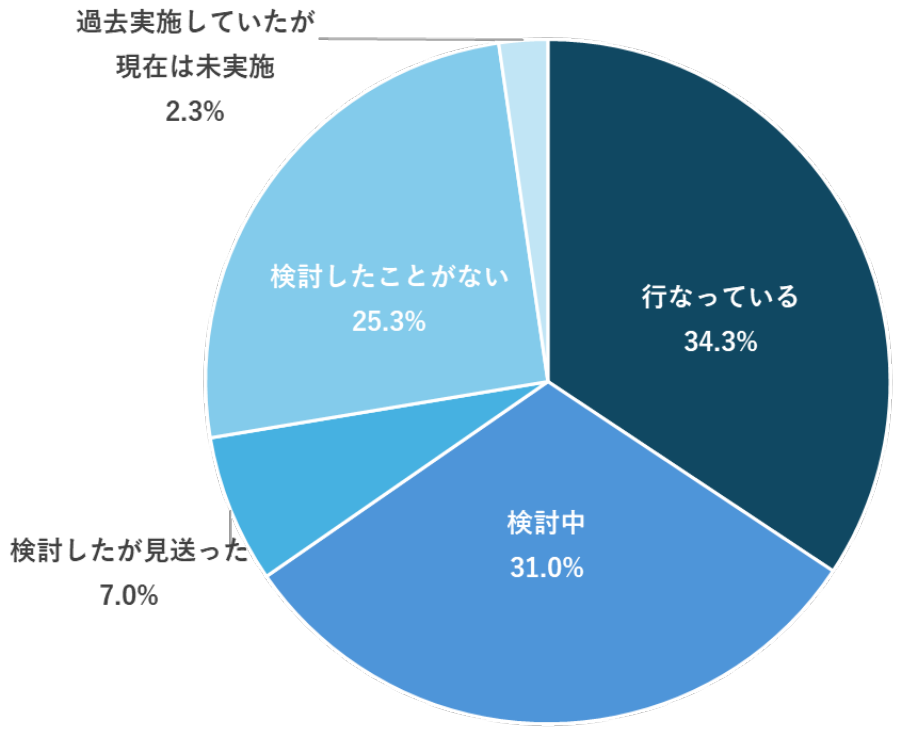


※出典：令和５年　通信利用動向調査報告書（企業編）

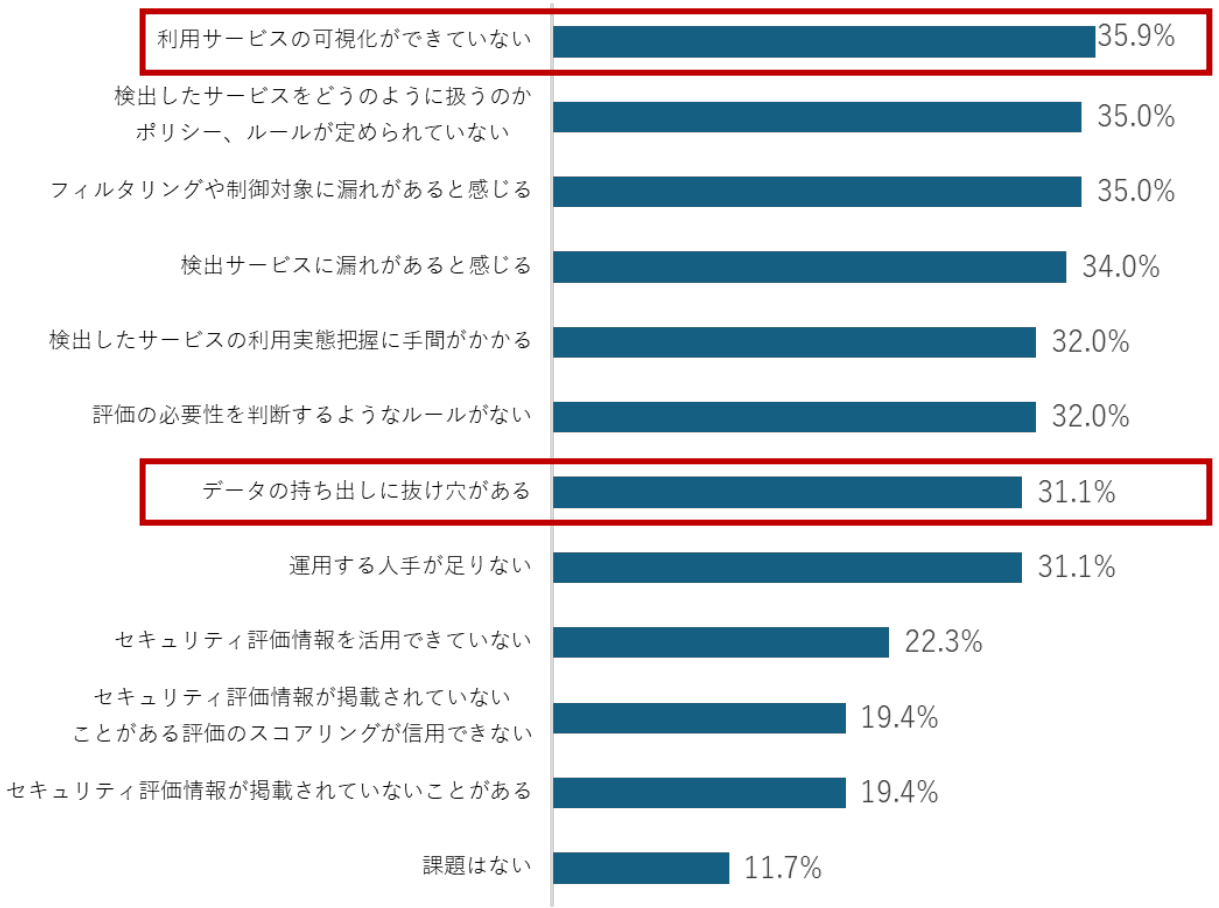
© MOTEX Inc.

6割以上の企業でシャドー IT 対策が行われておらず
対策済みの企業でも利用サービスの把握や利用制限、情報漏洩などに課題を抱えている

Q. あなたのお勤め先では、シャドーIT対策を行っていますか



Q.シャドーIT対策における課題をすべてお選びください（複数回答）

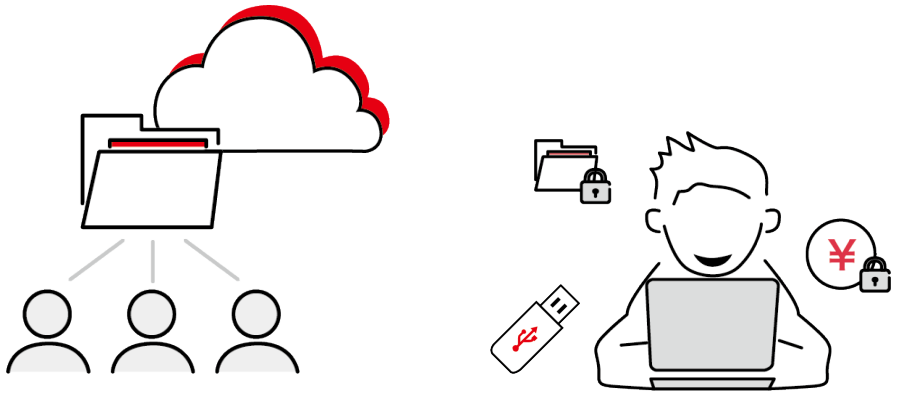


※出典：Assured調べ

© MOTEX Inc.

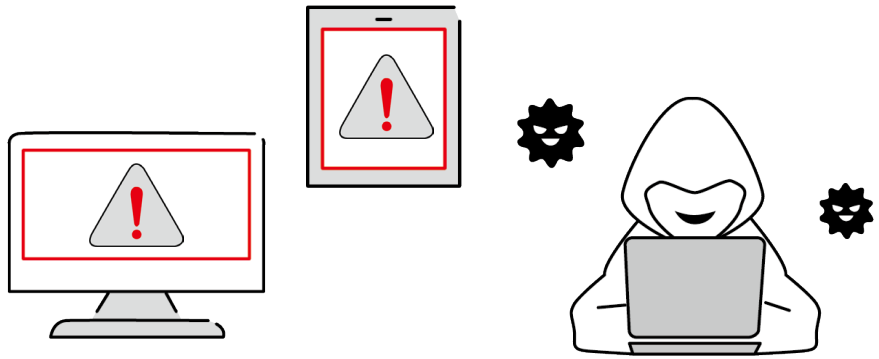
シャドー IT の利用には、不注意や内部不正による情報漏洩、技術的な脆弱性などのリスクが多く存在

情報漏洩のリスク



従業員が未承認のクラウドストレージや個人メールに業務資料を送付することで、機密情報が流出するリスクがあります。また、元従業員が私物の USB やクラウドサービスにデータを保存し、個人 PC にダウンロードすることで機密情報を不正に保管するリスクも存在します。これらは不注意、意図的に関わらず、企業にとって重大なセキュリティリスクとなります。

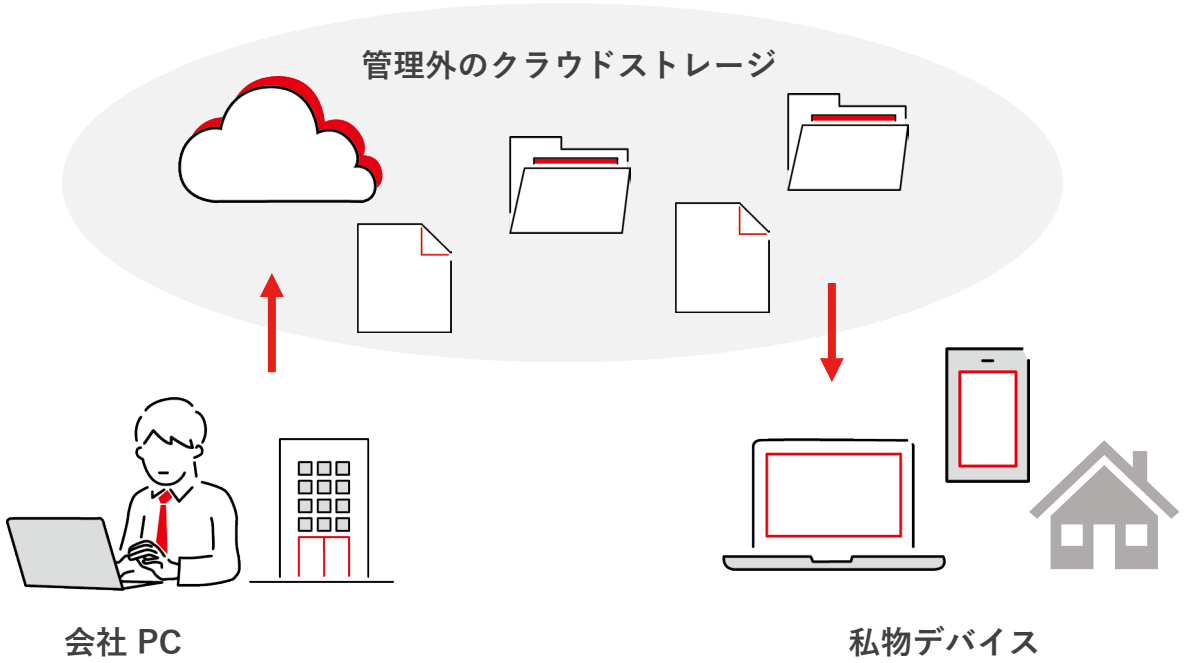
技術的な脆弱性



許可されていないソフトウェアやアプリケーションは情報セキュリティ対策が脆弱なものが多く存在し、これらを業務で利用することで、不正アクセスやマルウェア感染等のリスクが高まります。

© MOTEX Inc.

許可していないクラウドストレージへデータをアップロードして私物デバイスへダウンロード
管理外のクラウドサービス経由での情報持ち出しに気づくことは難しい



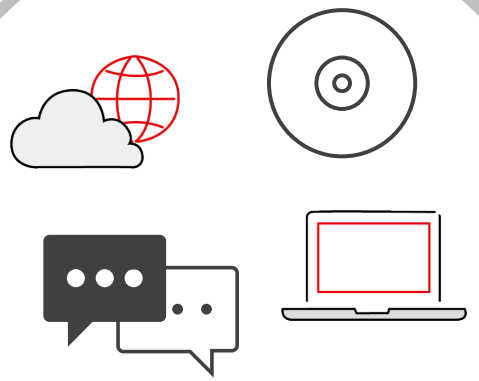
情報漏洩事件の例

総合商社	元従業員がインターネット上でデータを管理するクラウドサービスを使って、営業秘密を個人的に保管してたいことが判明。自宅のパソコンからデータベースに接続し、自動車部品の取引台帳や、海外メーカー向けの新商品の開発提案書などのファイルをダウンロード。その後、自身が管理するクラウド上にデータをアップロードして保管していた。

© MOTEX Inc.

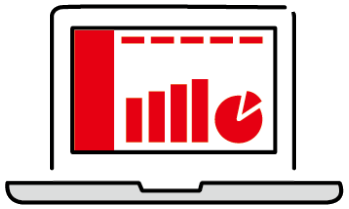
シャドー ITリスクを軽減するには、まずは利用状況の可視化、未承認のシステム利用、データ持ち出しなど問題のある操作の抽出、利用制限の3ステップで行うことが重要

Step1



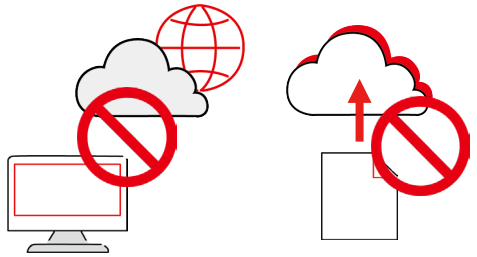
利用状況の可視化

Step2



問題抽出

Step3



利用制限

LANSCOPE を利用すれば上記のステップでシャドー IT 対策を支援します

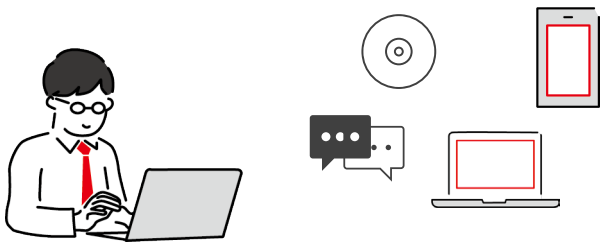
© MOTEX Inc.

LANSCOPE で利用状況の可視化～利用制限までを支援
SaaS 管理製品と併用すれば、昨今利用が増えているクラウドサービスの可視化も可能です

LANSCOPE

利用状況の可視化

デバイスのハードウェア、ソフトウェア情報を収集して資産情報を可視化



従業員のハードウェア、ソフトウェア情報を自動収集し、一覧情報を作成して資産情報を可視化。会社が許可していないシステム（シャドー IT）がないか把握できます。

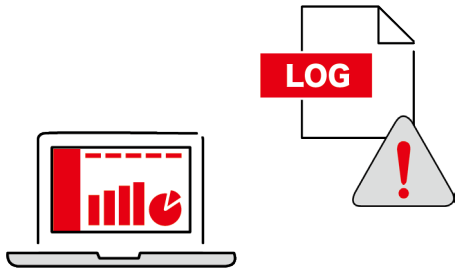
＋

クラウドサービスの可視化 SaaS管理製品

社内で利用されているSaaS製品を自動的に検出。
許可されていないSaaS製品を把握します。

問題抽出

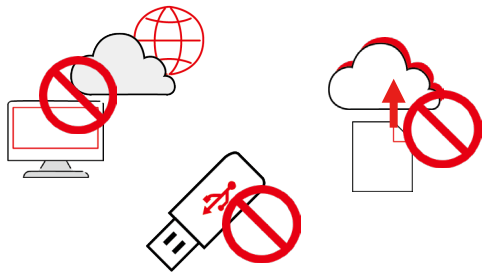
アラート操作の抽出



PC 操作ログの取得、分析を行い、クラウドストレージへのデータアップロードなど、情報漏洩リスクにつながるアラート操作を抽出します。

利用制限

シャドー IT の利用制限



私物 USB メモリへの書込みや許可していないソフトウェアの利用、クラウドストレージへのデータアップロードなどシャドー IT の利用を制限します。

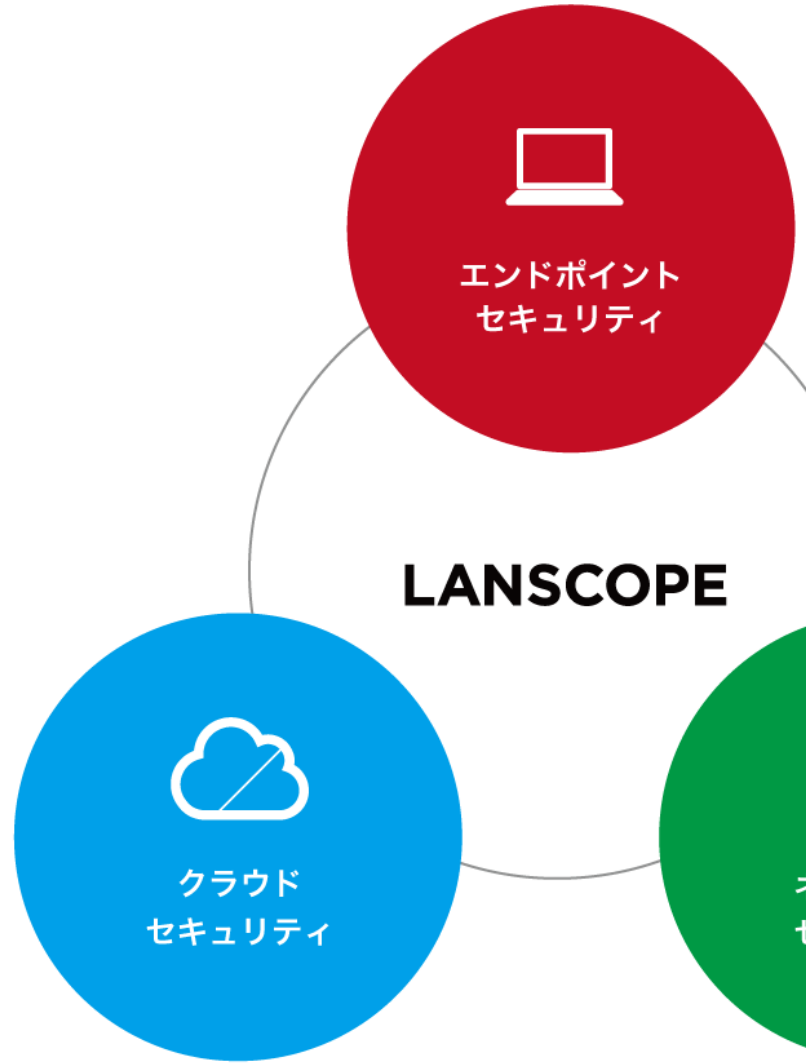
© MOTEX Inc.

chapter

02 LANSCOPE で支援する技術的な対策

© MOTEX Inc.

MOTEX 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・MDR

- 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 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

© MOTEX Inc.

MOTEX が提供するプロダクト・サービス

「LANSCOPE」を通して、お客様の “Secure 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

セキュリティ診断

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 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

© MOTEX Inc.

PC・スマホ・タブレットの一元管理をクラウドで実現
「使いやすい」管理コンソールで、充実の「IT 資産管理機能」と「MDM 機能」を実装

IT review 顧客評価No.1※

使いやすい管理コンソール

充実の PC 管理

操作ログ・セキュリティ
PC 管理に必要な機能を網羅

Apple・Google の認定プログラム対応

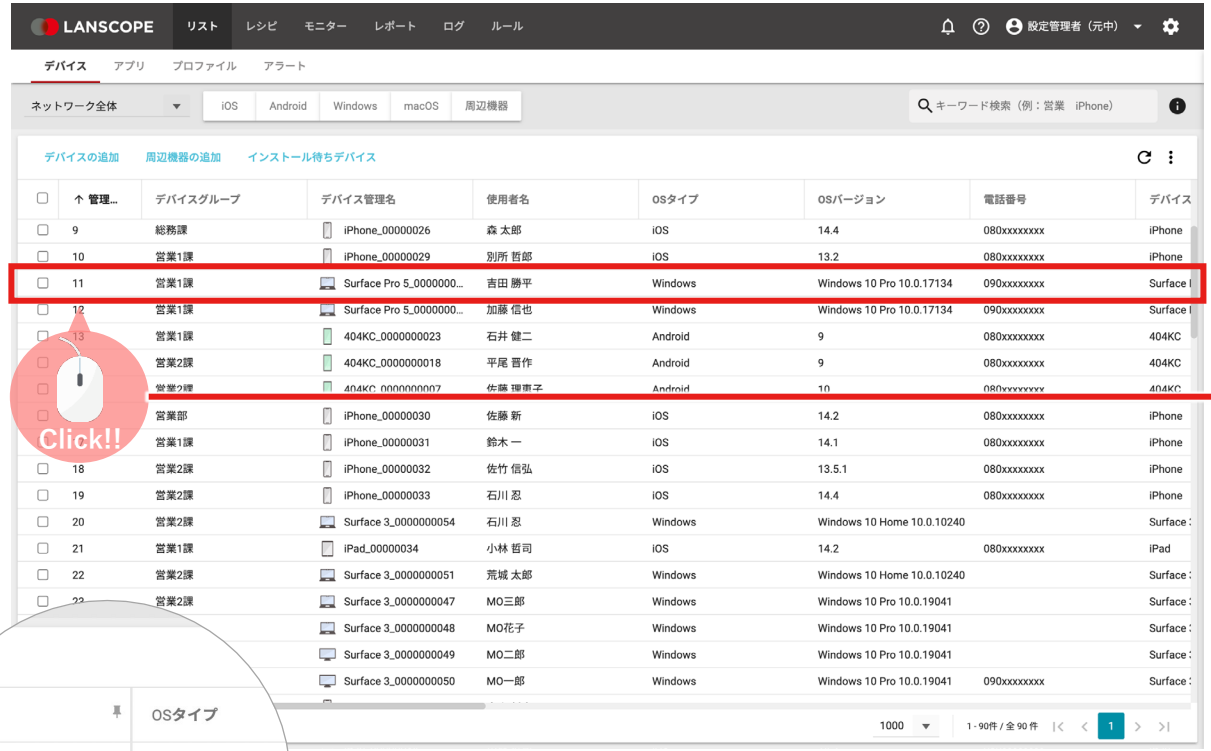
充実の「モバイル管理」

※ IT 資産管理、ログ管理、MDM・EMM、統合運用管理の4部門でLeaderを獲得

© MOTEX Inc.

管理下のデバイスの最新情報を自動取得し、一覧で表示

デバイスを特定し、1Click で詳細情報を確認可能。自動取得できない項目は、任意項目として管理できます。



固定列を設定し、ストレスのない横スクロールを実現。
表示する項目・順番も並び替え可能。

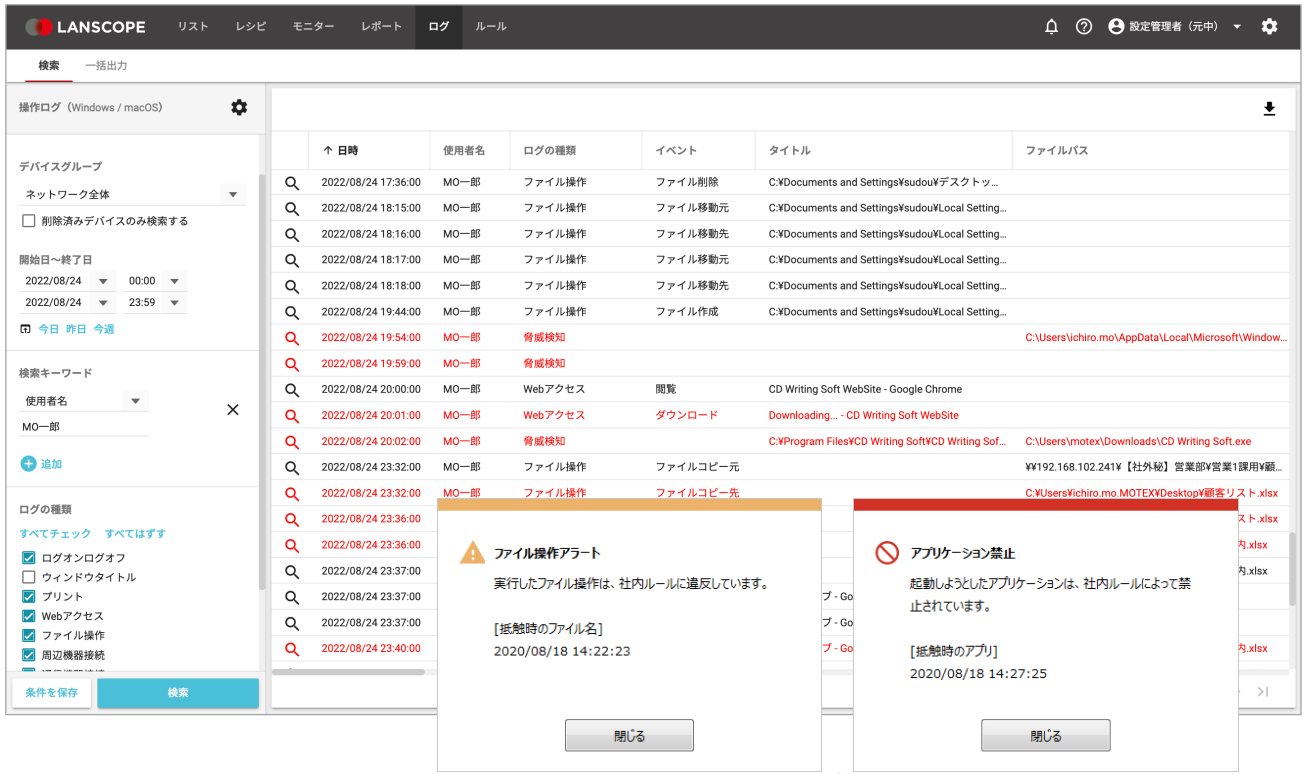
1Clickでデバイスの詳細情報を確認

© MOTEX Inc.

操作ログ取得：シャドー IT の利用状況を把握

「どの部署の」「誰が」「いつ」「何をしたのか」をリアルタイムに取得

取得した操作ログは2年間保存、検索によるログの抽出と CSV ファイルによる出力が可能。ログ運用オプションの導入で最大5年保存されます。



違反操作があった場合は、リアルタイムに警告通知が可能

取得できる操作ログ

ログオン・ログオフログ

電源ON・OFF・ログオン・ログオフのログを取得できます。

ウィンドウタイトルログ

デバイス上での閲覧画面（ウィンドウタイトル・アプリ名）のログを取得できます。

ファイル操作ログ

デバイス上でのファイル操作（ファイル・フォルダのコピー／移動／作成／上書き／削除／名前の変更）でのログを取得できます。

Web アクセスログ※1

Webサイトの閲覧、Webメールやクラウドストレージのアップロード／ダウンロードログを取得できます。

プリントログ

印刷状況を記録し、ドキュメントやプリンター、PCごとに印刷枚数を集計できます。

周辺機器・通信機器接続ログ※2

USB メモリなどの周辺機器、Wi-Fi・Bluetooth などへの接続／切断などのログを取得できます。

アプリ稼働・アプリ通信ログ※3

バックグラウンドで稼働しているアプリ情報、通信元／先のIPアドレスやポート番号、アプリのハッシュ値を取得できます。

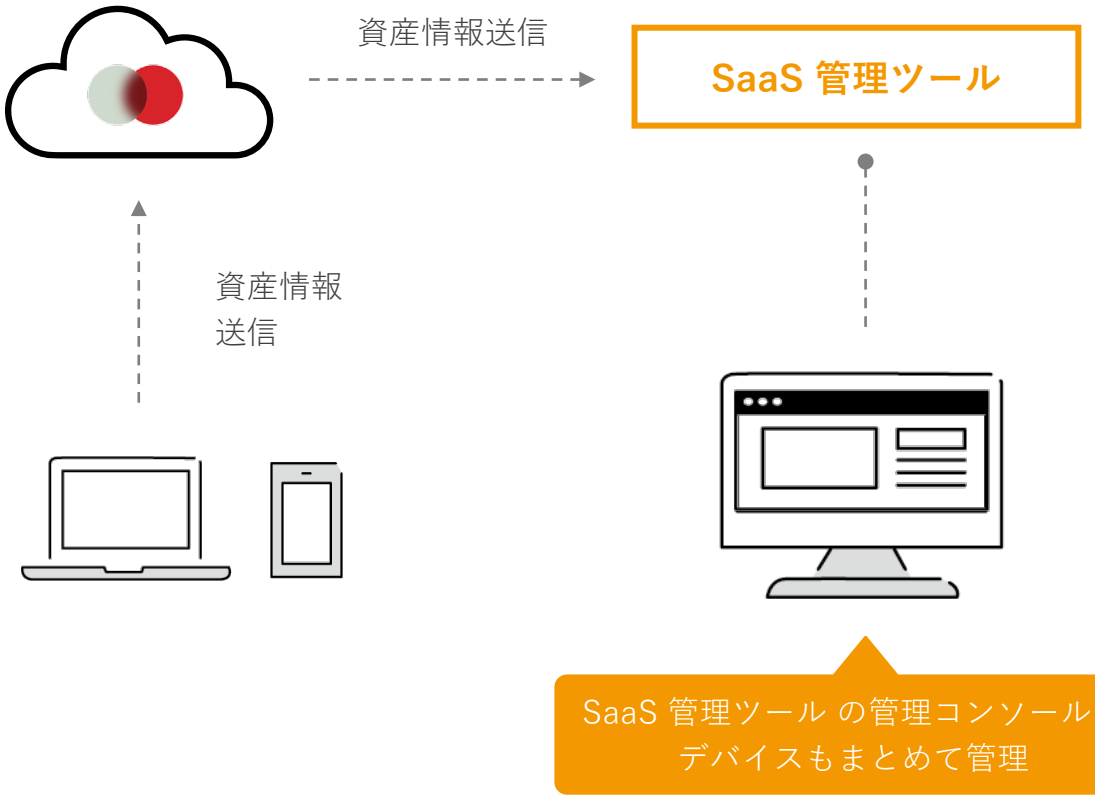
※1 macOS は Web サイトの閲覧ログのみ対応しています。また対応ブラウザは Microsoft Edge・Google Chrome・FireFox・Safari です。
※2 macOS は周辺機器接続ログのみ対応しています。
※3 外部脅威調査オプションの導入が必要です。尚、macOS は非対応です。

© MOTEX Inc.

エンドポイントマネージャーのデバイス情報を SaaS 管理ツールに自動連携
SaaS 管理ツールの管理コンソール上で、人・デバイス・SaaS の統合管理を支援

SaaS 管理ツール × Cloud LANSCOPE Endpoint Manager

「SaaS 管理ツール」は、多様なクラウドサービスとの連携により一元的に社内の SaaS 環境を可視化。クラウドサービスと人（利用者）を紐付けた効率的な管理が可能です。エンドポイントマネージャーとの連携で、人・SaaS に加えて、デバイスの情報も一元管理が可能となり、IT 資産管理の効率化を支援します。



連携済 SaaS 管理ツール※

Money Forward Admina　ジョーシス

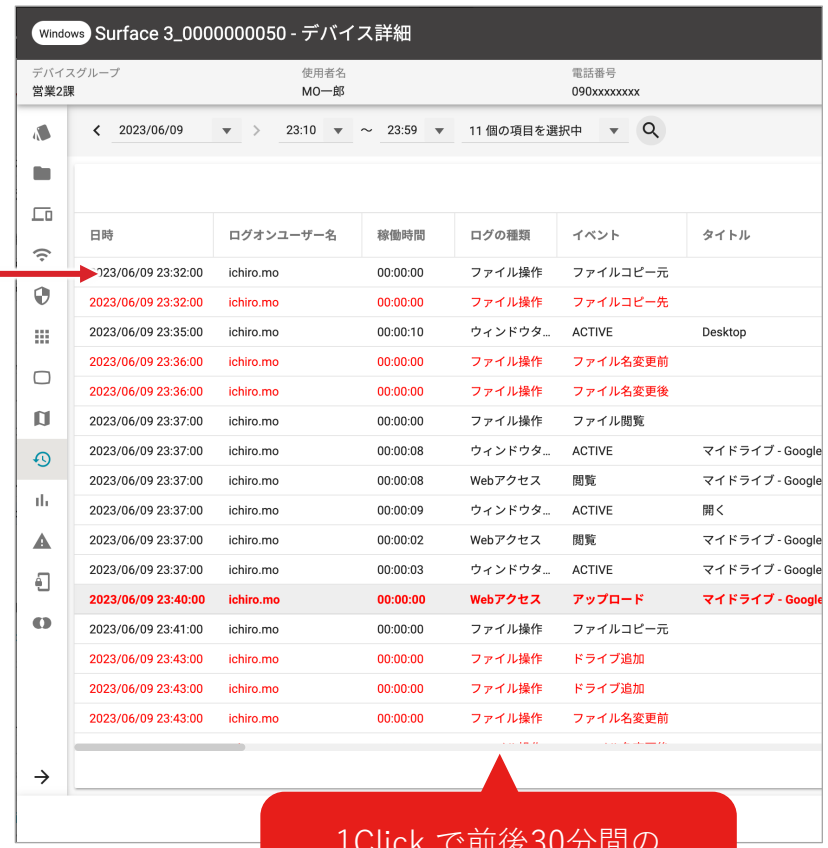
※ マネーフォワードi株式会社「マネーフォワード Admina」（https://admina.moneyforward.com/jp）
※ ジョーシス株式会社「ジョーシス」（https://jp.josys.com/）
※ SaaS 管理ツールの詳細については、各社にお問い合わせください。

© MOTEX Inc.

問題抽出

活用シーンに合わせたテンプレートから検索条件をセット、必要な操作ログを簡単に抽出

検索条件をカスタマイズして、保存も可能。検索から 1Click で前後 30分の操作を抽出。



© MOTEX Inc.

問題抽出

グループ単位で違反操作の発生状況を見える化し、Click 操作で詳細を確認

レポート形式で確認できるアラートは過去3ヶ月分です。

設定できる操作ログのアラート	W	m
指定した文字列が含まれるウィンドウタイトル	○	○
一定枚数以上の印刷	○	○
指定したキーワードがドキュメント名に含まれる印刷	○	○
Web サイト閲覧（タイトル / URL）	○	○
Web サイトのアップロード/ダウンロード（タイトル / URL）	○	—
Web サイトの書き込み（タイトル / URL）	○	—
指定したキーワードが含まれるファイル操作	○	○
ドライブの追加	○	○
ドライブに追加された記録メディアへの書き込み	○	○
ローカル共有フォルダーの作成または書き込み	○	—
Outlook メールへのファイル添付	○	—
機密フォルダー内での操作	○	○
CSV ファイルへの出力	○	○
ネットワーク上の共有フォルダーへの書き込み	○	○
指定した SSID / BSSID への接続	○	—
Bluetooth 接続	○	—

© MOTEX Inc.

問題抽出

操作ログアラートを管理者の Microsoft Teams やメールに通知
通知が届いたら、管理コンソールで詳細をチェックする体制を可能に

メールに通知

LANSCOPEアラート通知

下記時刻に通知対象のアラートログが発生しました。

2024/07/12 17:20-17:30

詳細は各ログのリンクから管理コンソールのログ詳細画面でご確認ください。

ウィンドウタイトル ウィンドウタイトルアラート -> リンク

ファイル操作 キーワードアラート -> リンク

ファイル操作 ドライブ追加アラート -> リンク

ファイル操作 記録メディア書込みアラート -> リンク

ファイル操作 共有アラート -> リンク

ファイル操作 メール添付アラート -> リンク

ファイル操作 機密フォルダーアラート -> リンク

ファイル操作 CSV出力アラート -> リンク

ファイル操作 リモート書込みアラート -> リンク

管理コンソールで確認

対象のログが抽出
1Click で前後30分の操作も確認

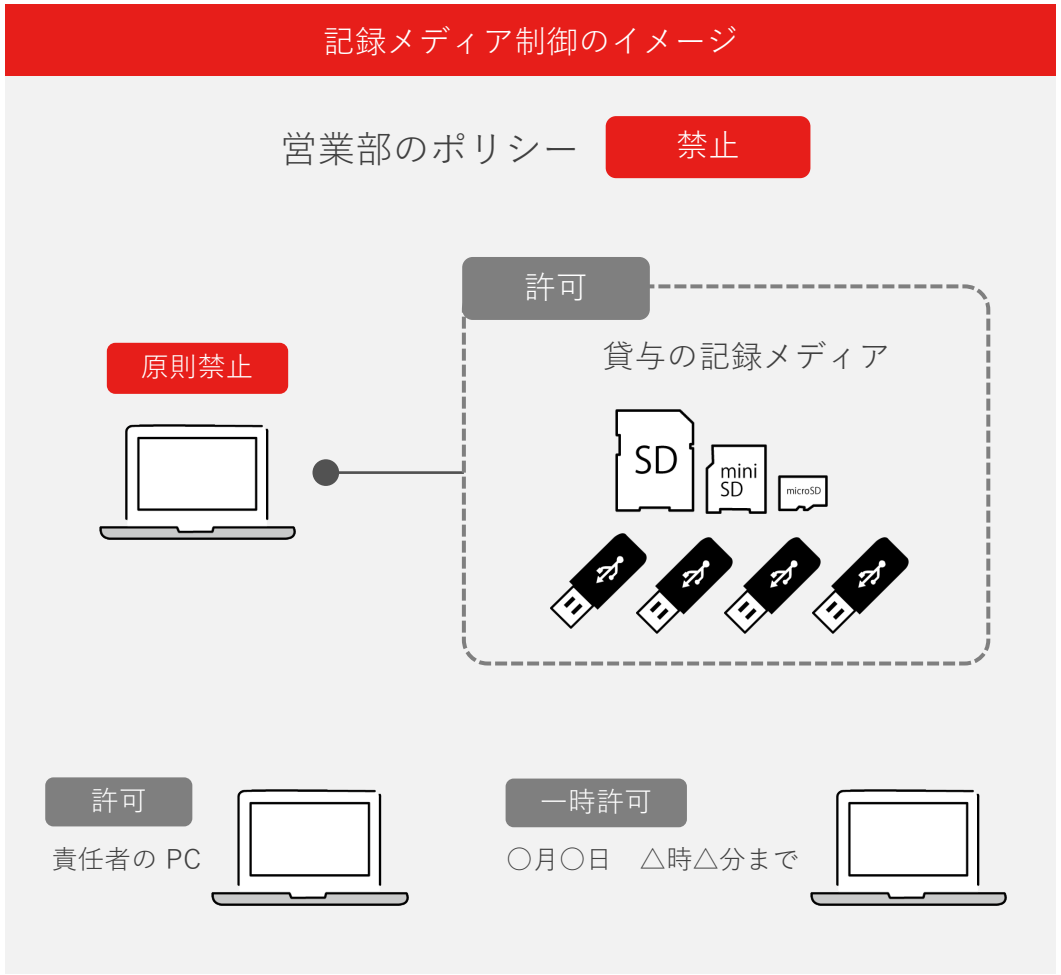
本機能を利用するためには、Power Automate のプレミアムコネクタが利用できる Microsoft アカウントで通知設定を行う必要があります。

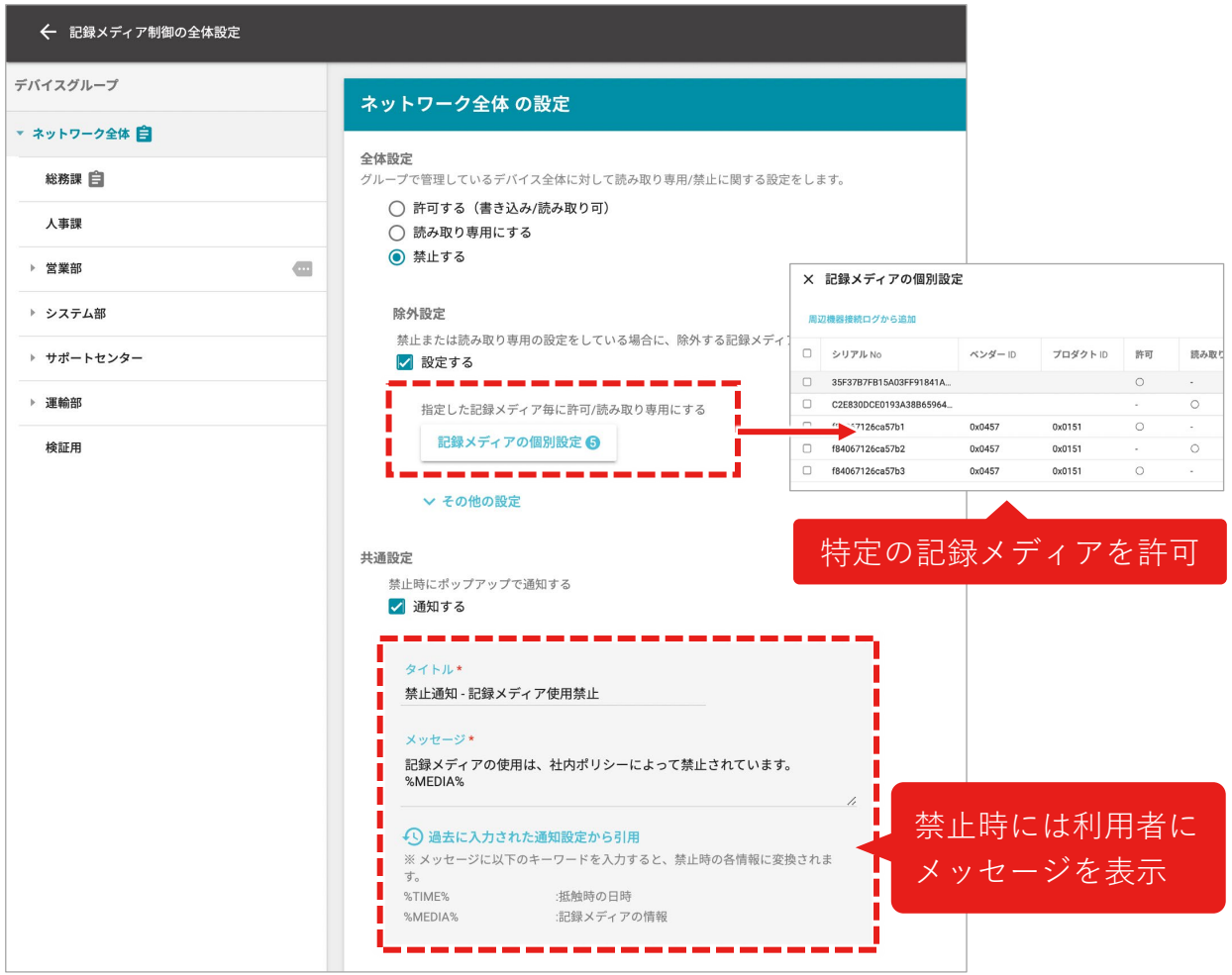
© MOTEX Inc.

USB メモリなどの記録メディアの利用を制御し、情報漏洩を防止

グループ単位で禁止・読取専用・許可のいずれかから基本ポリシーを設定。特定記録メディアのみ許可/特定 PC のみ許可/特定時間のみ許可など柔軟な設定が可能。

記録メディア制御のイメージ





© MOTEX Inc.

Web フィルタリング：組織で許可していないクラウドストレージへのデータ共有を規制

見せたくないカテゴリを指定するだけで関連サイトの閲覧を一括で制御可能

OS によって動作が異なります。事前に体験版環境で動作確認をお願いします。

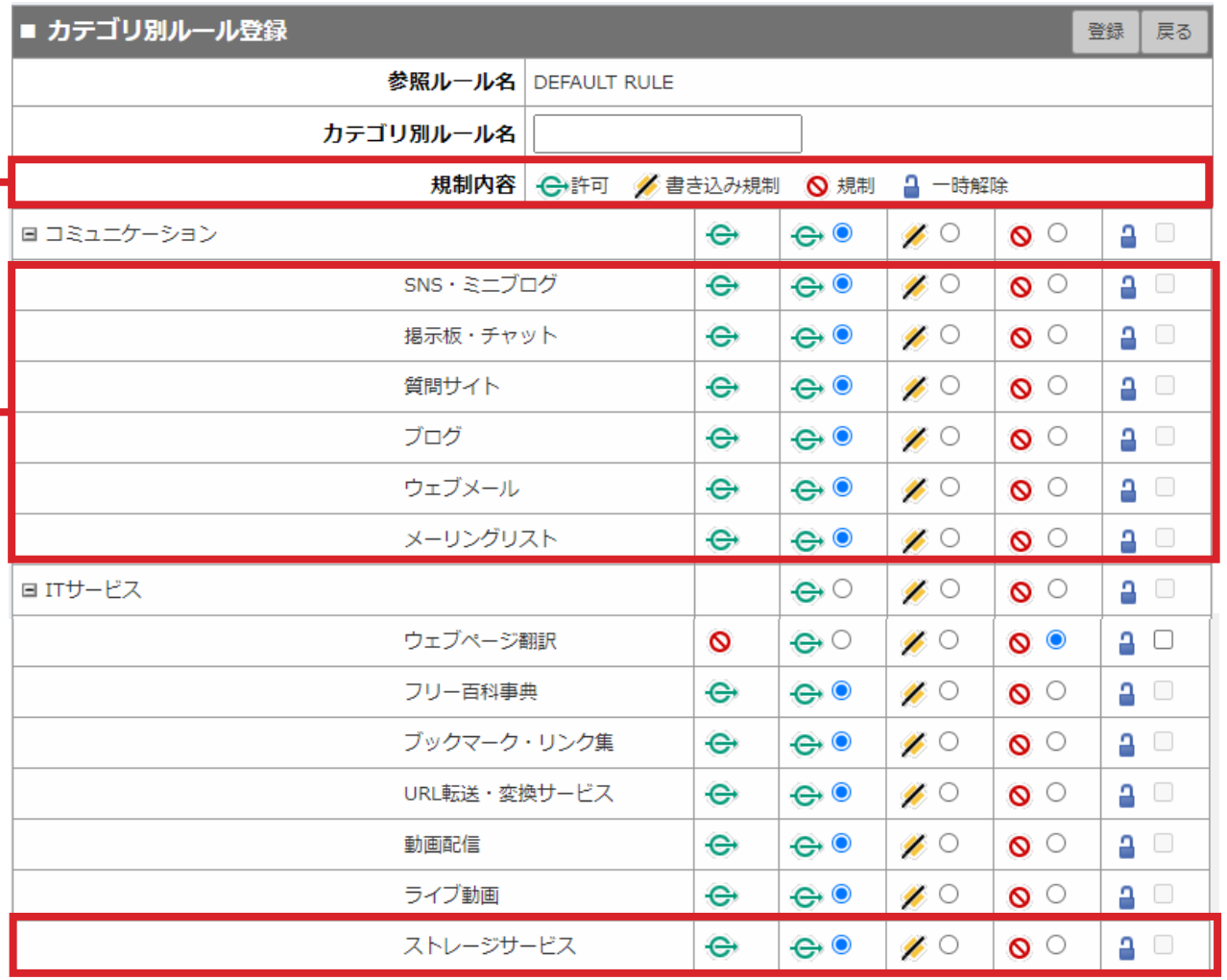
● 規制内容

許可　書き込み規制　規制　一時解除

許可／書き込み規制／規制／一時解除の 4 つの規制が可能です。

● カテゴリ別設定

ユーザ設定カテゴリを含めた全26種・148カテゴリで制御が可能です。さらにカテゴリごとにサブカテゴリが設定されており、より詳細な制御が可能です。



参考：カテゴリー覧例

シャドー IT として利用されやすいカテゴリをまとめて制御

コミュニケーション	
SNS・ミニブログ	SNS(会員向けコミュニティサイト)およびミニブログサービス
掲示板・チャット	ウェブ上の掲示板およびチャットサービス
ウェブメール	ウェブ上でのメールの送受信サービスおよびグリーティングサービスの提供
IT サービス	
ストレージサービス	インターネット上のディスクスペース提供など、各種ストレージサービス

詳細は ALSI 社サイトを参照してください：https://www.alsi.co.jp/security/isgc/database/

※ Web フィルタリングはオプション機能になります。

© MOTEX Inc.

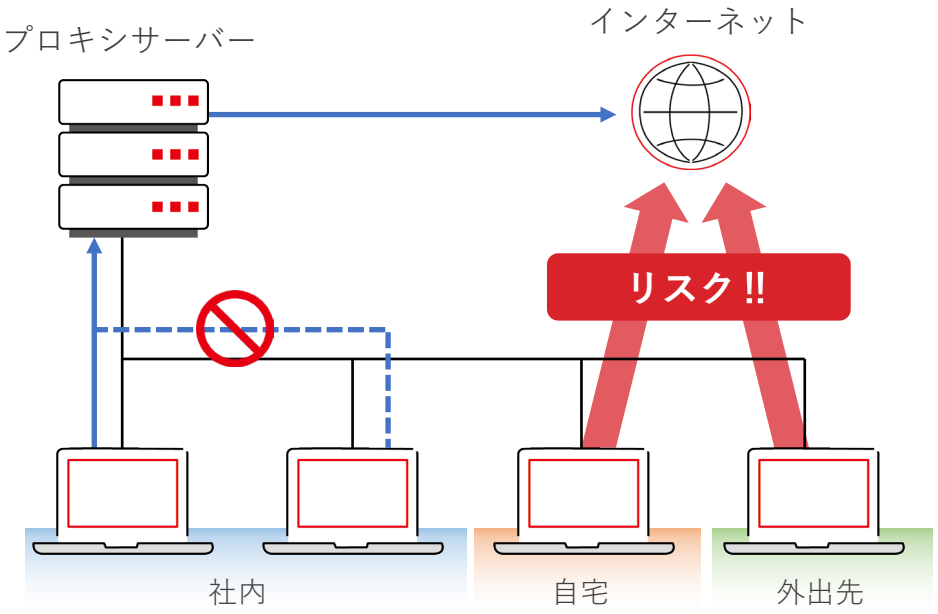
利用制限

社内ネットワークへの接続が必須のプロキシ型と異なり、クライアント型は場所を問わず制御！

テレワークなどで社内ネットワークへの接続をしない Web 閲覧が増えています。Web フィルタリングであればセキュリティの担保も安心

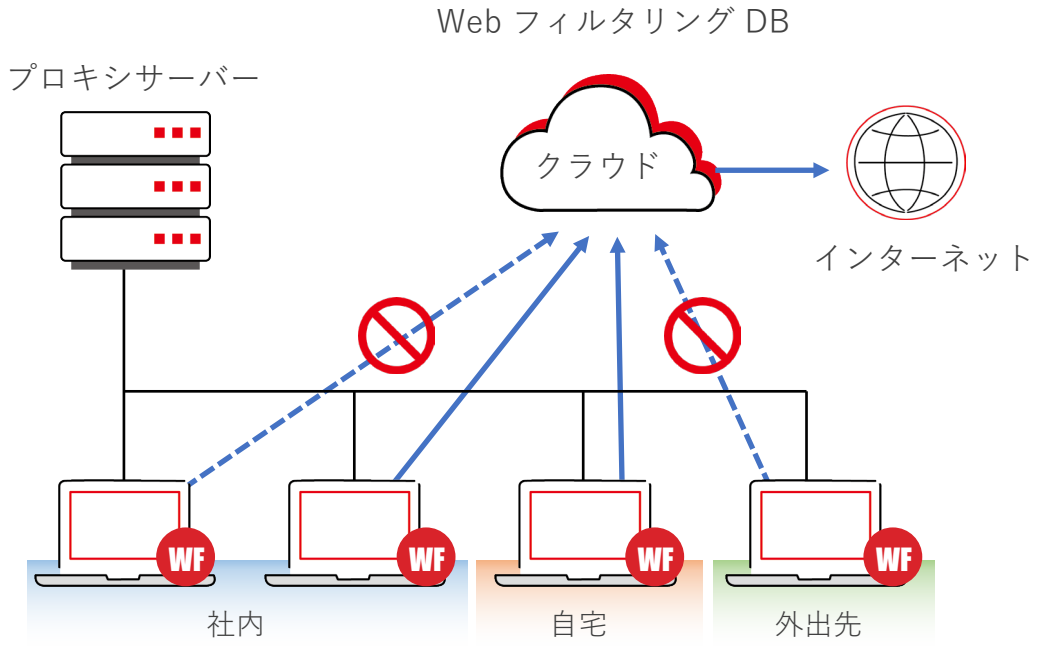
プロキシ型

社内ネットワークに接続端末のみの対策



クライアント型

ネットワークの接続形態を問わず対策が行える



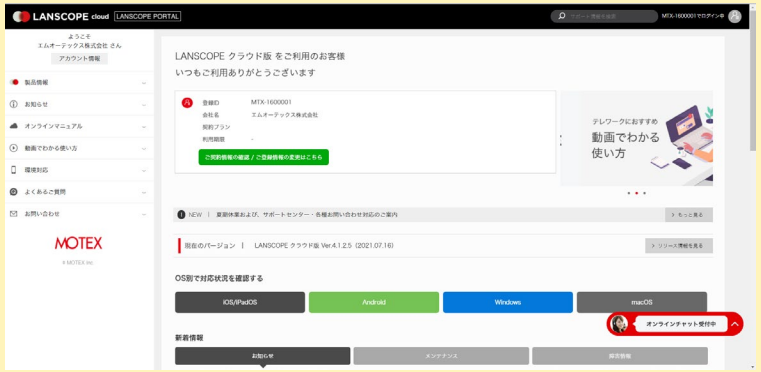
© MOTEX Inc.

Endpoint Manager Cloud

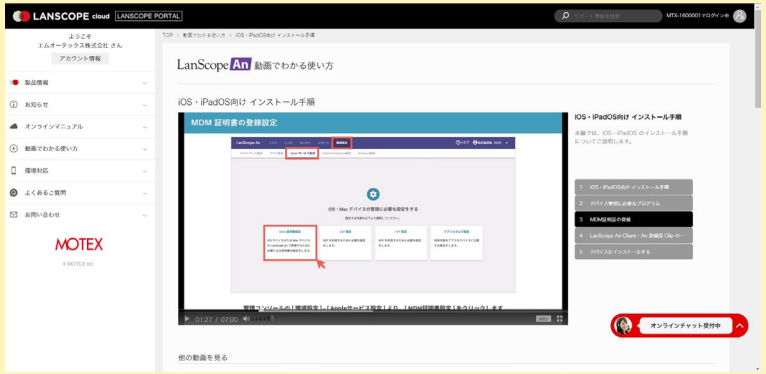
60日間無料体験キャンペーン中

エンドポイントマネージャー クラウド版の体験版は、設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています。

●各種マニュアル・問い合わせが可能



●動画で設定方法を説明



https://go.motex.co.jp/l/320351/2017-06-21/c55z

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

ご導入後の製品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

・記載の会社名および製品名・サービス名は、各社の商標または登録商標です。
・製品の仕様・サービスの内容は予告なく変更させていただく場合があります。
・MOTEX はエムオーテックス株式会社の略称です。

© MOTEX Inc.