Cloud
LANSCOPE
Endpoint Manager

企業を守る！

～従業員向け対策チェックリスト付～

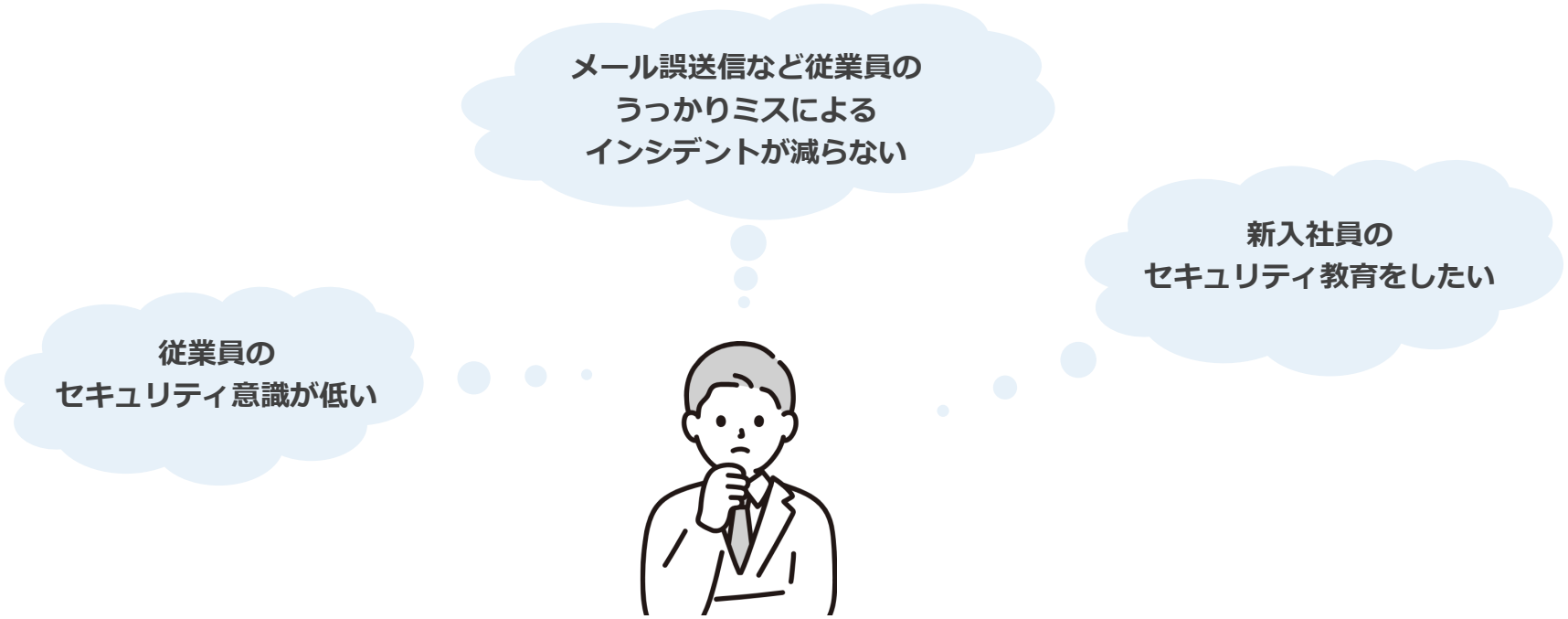
効果的なセキュリティ教育3つのポイントとは？

本資料の目的

近年のビジネス環境では、情報漏洩やサイバー攻撃のリスクが常に存在しています。そのため、従業員のセキュリティ意識を高め、必要な対策を講じることが不可欠となります。しかし、従業員にセキュリティ意識を高めてもらうのに苦労している管理者の方も多いのではないでしょうか。

本資料では、企業の機密情報などを守るために重要な従業員が取り組むべきセキュリティ対策と、従業員にセキュリティ教育を行う上での3つのポイントをご紹介します。また、この3つのポイントに基づいて作成した従業員向けのセキュリティ教育用の参考資料も添付しております。

会社全体のセキュリティの強化にお役立ていただければ幸いです。



こんなお悩みをお持ちの方に、おすすめの資料となっております

従業員がセキュリティホールになっている！？

情報セキュリティ10大脅威でも「不注意による情報漏洩等の被害」は昨年9位から6位へと急浮上
人によるインシデントが脅威に。従業員にセキュリティ意識を持ってもらう必要がある！

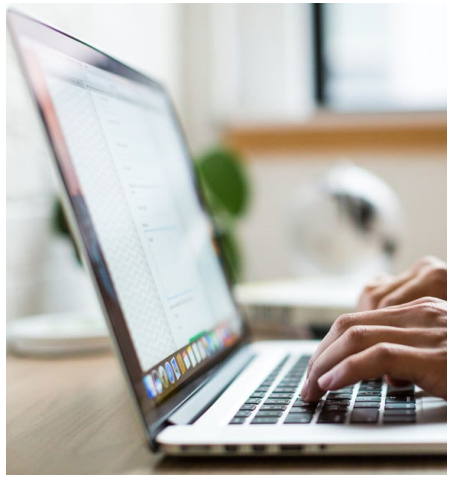
情報セキュリティ10大脅威　2024年度版

	順位	組織	昨年順位	初選出年
外部	1位	ランサムウェアによる被害	1位	2016年
外部	2位	サプライチェーンの弱点を悪用した攻撃	2位	2019年
内部	3位	内部不正による情報漏えい等の被害	4位	2016年
外部	4位	標的型攻撃による機密情報の窃取	3位	2016年
外部	5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位	2022年
内部	6位	不注意による情報漏洩等の被害	9位	2016年
外部	7位	脆弱性対策情報の公開に伴う悪用増加	8位	2016年
外部	8位	ビジネスメール詐欺による金銭被害	7位	2018年
外部	9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位	2021年
外部	10位	犯罪のビジネス化（アンダーグラウンドサービス）	10位	2017年

※引用：IPA「情報セキュリティ10大脅威2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

不注意による情報漏洩等の被害が増える背景

社内規定の不備



外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスを記載した社内規定の不備があると、情報漏洩が起きやすくなる。

セキュリティ意識の低さ

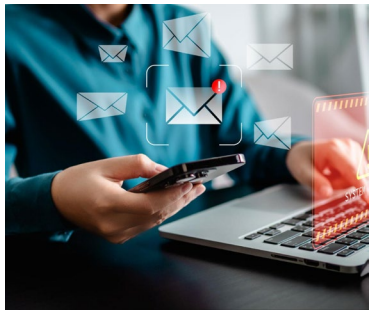
情報セキュリティに対する意識が低く、自身が扱う情報の機密性や重要性等を理解していないため 、誤った情報の取り扱いをしてしまい情報漏洩につながる。

従業員に抑えてもらいたい4つのセキュリティ対策

企業・組織では、様々な機密情報を扱います
従業員のうっかりミスから情報漏洩が起きないよう、日々注意してもらう必要があります

01

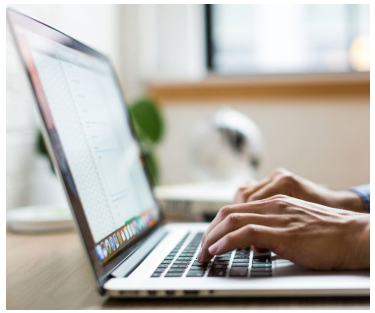
電子メールの利用ルール



不振なメールの開封によるウイルス感染やメール誤送信による情報漏洩などを防ぐためのルール

02

無線LAN・インターネット利用ルール



セキュリティリスクのある無線 LAN の利用や Web サイトの閲覧によるインシデントを防ぐためのルール

03

情報の取り扱いのルール

重要情報の保管方法や持ち出しルール、バックアップなど企業の機密情報を守るためのルール

04

事務所の安全管理 情報の安全な処分

事務所に保管されている、重要情報の書類や PC、USB メモリなどの情報資産を守るためのルール

※IPA_５分でできる自社診断シートを参考に作成

身に覚えのない電子メールは疑ってみる

ウイルス感染のリスクがあるので、身に覚えのないメールの添付ファイルやURLリンクへのアクセスに気をつける。

対策例

- 不審な電子メールは安易に添付ファイルを開いたり、URLリンクにアクセスしない。
- 不審な電子メールの情報を社内で共有する。
- メールソフトに迷惑メール対策機能がある場合は有効にする。

宛先の送信ミスを防ぐ

電子メールや FAX の送り先を間違えると情報漏洩につながります。送付時には送り先を十分確認する。また、メールアドレスを誤って他人に伝えてしまうことも情報漏洩になるので複数人に送付する時も十分確認する。

対策例

- 電子メールやFAXを送る前に送信先を再確認する。
- 複数の送信先アドレスを受信者に表示しない場合は、BCCを使う。
- メールソフトに宛先チェック、送信保留、取り消しなど誤送信防止機能がある場合は有効にする。

重要情報を送信する時は保護する

重要情報を電子メールで送る場合は、本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付する。パスワードはその電子メールには書き込まず、電子メール以外の手段で通知する。

対策例

- 重要情報は文書ファイルに書いて強固なパスワードで保護する、パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SMS）などの別手段で知らせる。

無線LANの盗聴や無断使用を防ぐ

適切なセキュリティ設定がされていない無線LANは、通信内容の盗聴、不正接続されて犯罪行為に悪用される可能性がある。無線LANの盗聴対策や無断使用を防止するようにセキュリティ設定をする。

対策例

- 強固な暗号化方式（WPA2 または WPA3）を選択。
- パスワードの初期設定が簡単なものである場合は、文字数を増やし、文字、数字、記号含め辞書にある英単語は使わず容易に推測されないようにする。
- モバイルルーターやスマートフォンのテザリング機能を使わないときにはオフにする。

インターネットを介したトラブルを防ぐ

悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性がある。また、SNS などに秘密情報を勝手に掲載して会社に被害を及ぼすこともあるので気を付ける。

対策例

- 利用する際の注意・制限のルールに従ってインターネットを利用する（SNSに秘密情報や個人情報を記載しないなど）

バックアップを行う

故障や誤操作、ウイルス感染などで、PC やサーバーの中に保存したデータが消えてしまうことがあるため、不測の事態に備えバックアップを取得しておく。

対策例

- 定期的に重要情報をバックアップ。
- バックアップに使用する装置・媒体は、バックアップ時のみ PC と接続。
- バックアップに使用する装置・媒体は複数用意し、そのうち１つは遠隔地に保存。

重要情報の放置をしない

机の上に放置された情報は、誰かに持ち去られたり、盗み見られたりする危険性がある。重要情報は放置せず、保管場所を定め、作業に必要な場合のみ持ち出し、終了後には戻す。

対策例

- 机の上をきれいにして、重要書類は鍵付き書庫に保管する。
- 秘密情報または個人情報を含む書類やUSBメモリなどの電子媒体を保管する場合は、鍵付き引き出しやケースに保管し、利用時以外は施錠する。

機器・備品の盗難防止対策

ノートPCやタブレット端末、USBメモリなどは手軽に持ち運べる便利さがある反面、盗難や紛失の危険性も高まる。利用しない場合は、安全な場所に保管するなどの対策をする。

対策例

- 退社時に机の上のノートPCやタブレット端末、備品を引き出しにしまう。
- 秘密情報または個人情報を含むデータはPC上には保存しない。

事務所の戸締まりに気を配る

最終退出者と退出時間の記録を残して、最終退出者は責任をもって施錠する。施錠と退出記録の管理をする。

対策例

- 鍵の管理を徹底する。
- 最終退出者は事務所を施錠し退出の記録（日時、退出者）を残す。

機器を勝手に操作させない

PC 作業の途中で席を離れたり、パスワードなしでログインできる PC など、PC を誰でも操作できる状態にしない。

対策例

- 離席時に PC にスクリーンロックをかける。
- 退社時に PC をシャットダウンする。
- 不特定多数の人がいる場所では PC にのぞき見防止フィルタを取り付ける。

見知らぬ人には声をかける

関係者以外の事務所への立ち入りは情報を盗み取られる危険性があります。サーバーや書庫・金庫など、重要な情報の保管場所の近くは無断で立ち入りができないようにする。

対策例

- 見知らぬ人は事務所に入れない。
- 見知らぬ人には声をかける。

情報は安全な方法で持ち出す

重要情報を社外へ持ち出す場合、盗難・紛失のリスクがあります。ノート PC、スマホのパスワードを設定、データファイルの暗号化などの対策を行っておく。

対策例

- ノート PC・スマホ・USB メモリなどはパスワードロックをかける。
- カフェやホテル、駅など公共の場所で仕事するときは PC や書類を放置しない。

情報を安全に処分する

重要情報を廃棄する場合は、書類の場合はシュレッダー、データの場合は消去用ソフトウェアを利用するなど、媒体ごとに適切な方法で処分する。

対策例

- 書類は細断する、電子データは消去ソフトを利用。
- 電子媒体を物理的に壊してから処分。
- 専門サービスに書類の溶解、電子データの消去処分を委託して証明書を取得。

従業員に抑えてもらいたいセキュリティ対策は多岐にわたる
沢山のルールをそのまま通知して本当に伝わるのだろうか。。。？

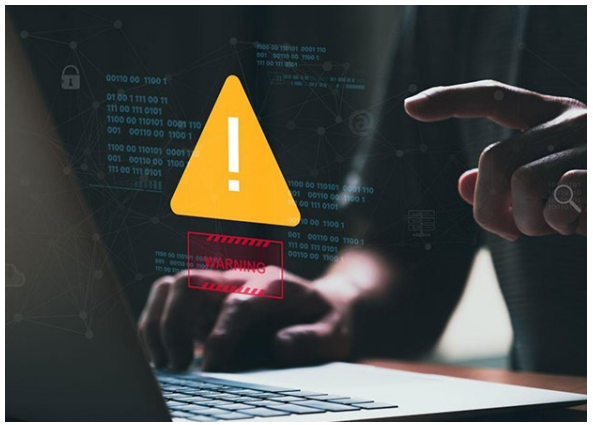
ルールを通知する前に、セキュリティ対策の必要性を理解してもらうのが必要…
どうやって理解してもらえばいいのか？

セキュリティインシデントは誰にでも起こり得るものであると理解してもらい
セキュリティ対策を自分ごととして捉えてもらうことが重要です

企業が守るべき資産について伝える

企業にとって守るべき資産にどのようなものがあるのかを理解してもらう。
また、セキュリティ対策は企業の資産を守るために必要なことだと伝える。

企業の資産に潜む脅威について伝える



企業が守るべき資産には、内部からの情報漏洩、外部からはサイバー攻撃と常に情報漏洩のリスクを抱えていることを伝える。
万が一インシデントが起きたときの企業へのダメージにどんなものがあるのかも伝える。

情報漏洩の脅威は身近なものと感じてもらう

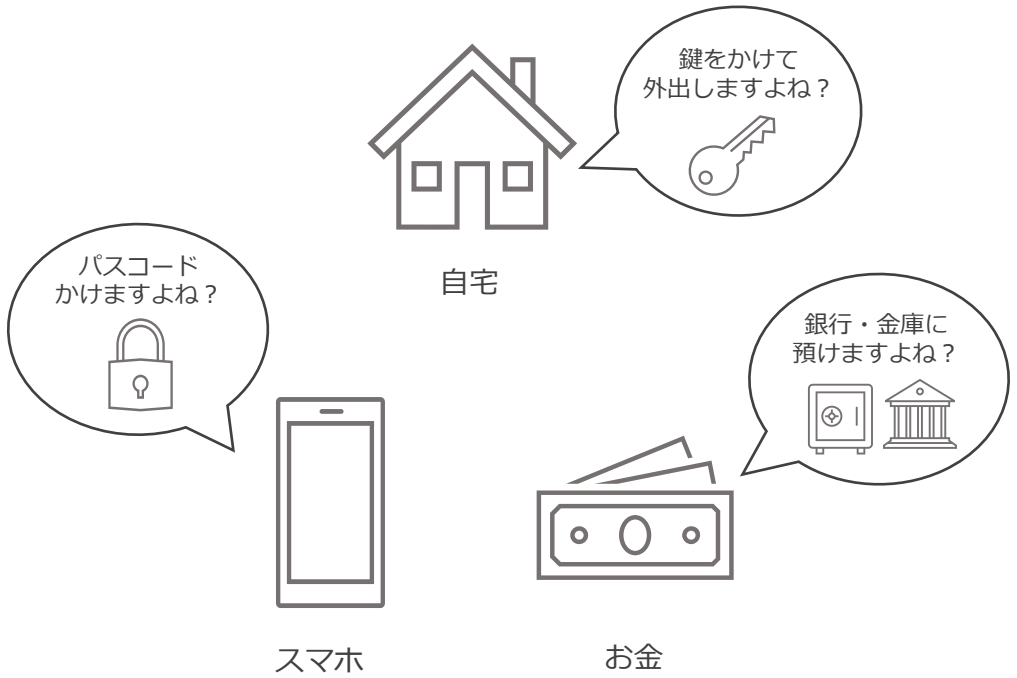
情報漏洩の脅威は、誰にでも起きる可能性があるということを伝える。よくあるインシデント事例を例に、注意すべき点を伝えセキュリティ対策を自分事として捉えてもらう。

参考資料：従業員向けセキュリティ教育　～対策チェックリスト付～

※自社向けにアレンジして、従業員へのセキュリティ教育にご活用ください

企業の資産は企業活動において外部に漏らすことのできない重要な情報資産が多く存在します
個人で管理している資産にはセキュリティ対策していますよね？会社の資産にもセキュリティ対策が必要です

個人が所有する資産



企業が所有する情報資産

今は多くの情報資産はデータで保管されているため PC から簡単にアクセス可能に
便利になった反面、情報漏洩リスクも増えています

内部からの情報漏洩、外部からはサイバー攻撃と常に情報漏洩のリスクを抱えている
個人で注意していても情報漏洩リスクは常に存在している

民放のニュースで取り上げられるなど、社会問題となる場合も
自社だけでなく、取引先・お客様にも被害が及ぶ可能性があります

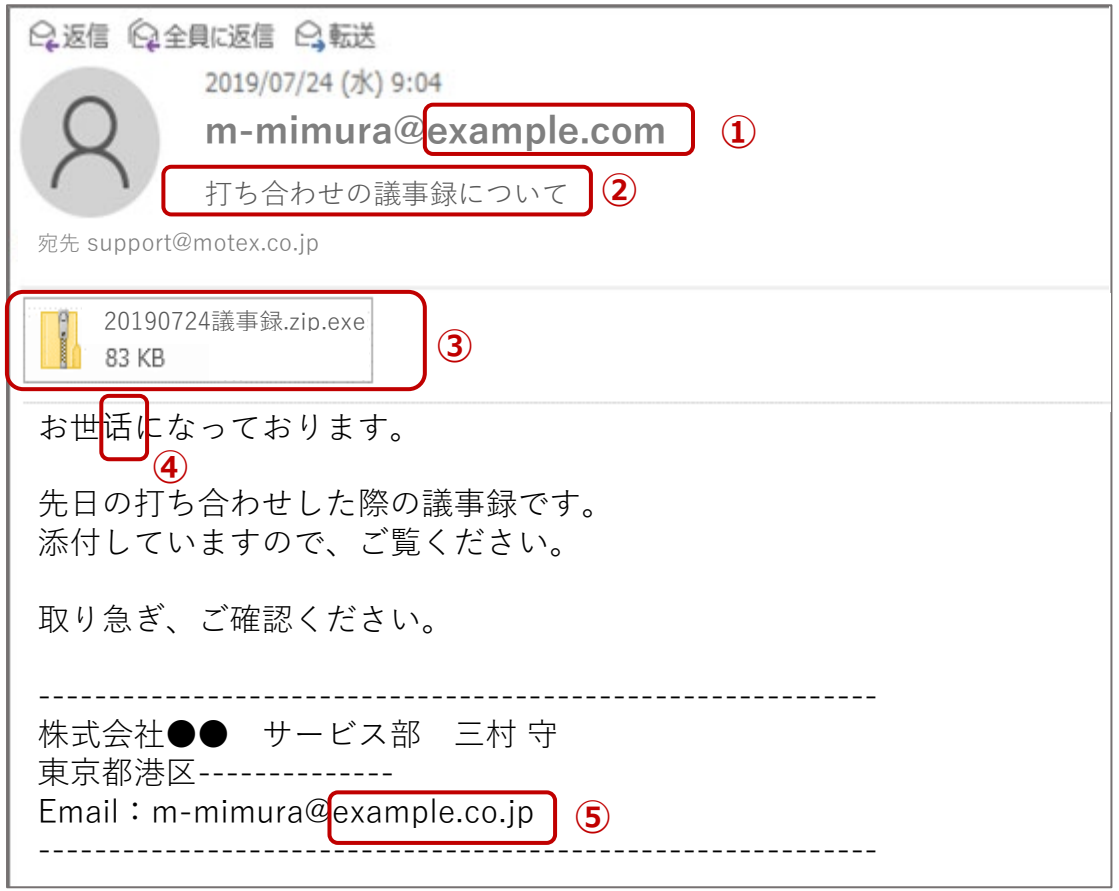
某自動車メーカー ランサムウェア被害	某大手自動車メーカーと取引関係にある部品メーカーがランサムウェアの被害を受けた。サーバや PC の一部でデータが暗号化され、「3日以内に我々に連絡しなければデータを公開する」という脅迫メッセージが届き、自動車メーカーの国内全工場が稼働を停止するという大きな影響が出た。
某官公庁 USB メモリ紛失未遂	某官公庁で全市民の個人情報が入ったUSBメモリを委託企業側が一時紛失。USBメモリには名前や住所、生年月日、住民税額のほか、児童手当と生活保護の受給世帯の口座情報などが入っていた。紛失した担当者は社内規定や個人情報の取り扱いルールを理解していなかった。

どんなセキュリティインシデントがあるのかを知っておき
万が一の場合に少しでも気づけるようリスクに備えることが重要

よくあるセキュリティインシデント①

取引先からのメールのように見えますが
どこか違和感のある部分はないでしょうか？

添付ファイルを開いたらマルウェアに感染。。。
よくあるメールを装って添付ファイルを開かせて感染させる手口が増えている



① 差出人のメールアドレスがフリーのメールアドレス

② 内容確認を仰ぐような件名

ex. 議事録等内部文書の送付、公的機関からのお知らせ、その他注意喚起

③ 添付ファイル

・拡張子(exe)とアイコン(zip)があっていない

・二重拡張子/実行形式(exe)の拡張子

④ 日本語では使用されない漢字が使われている

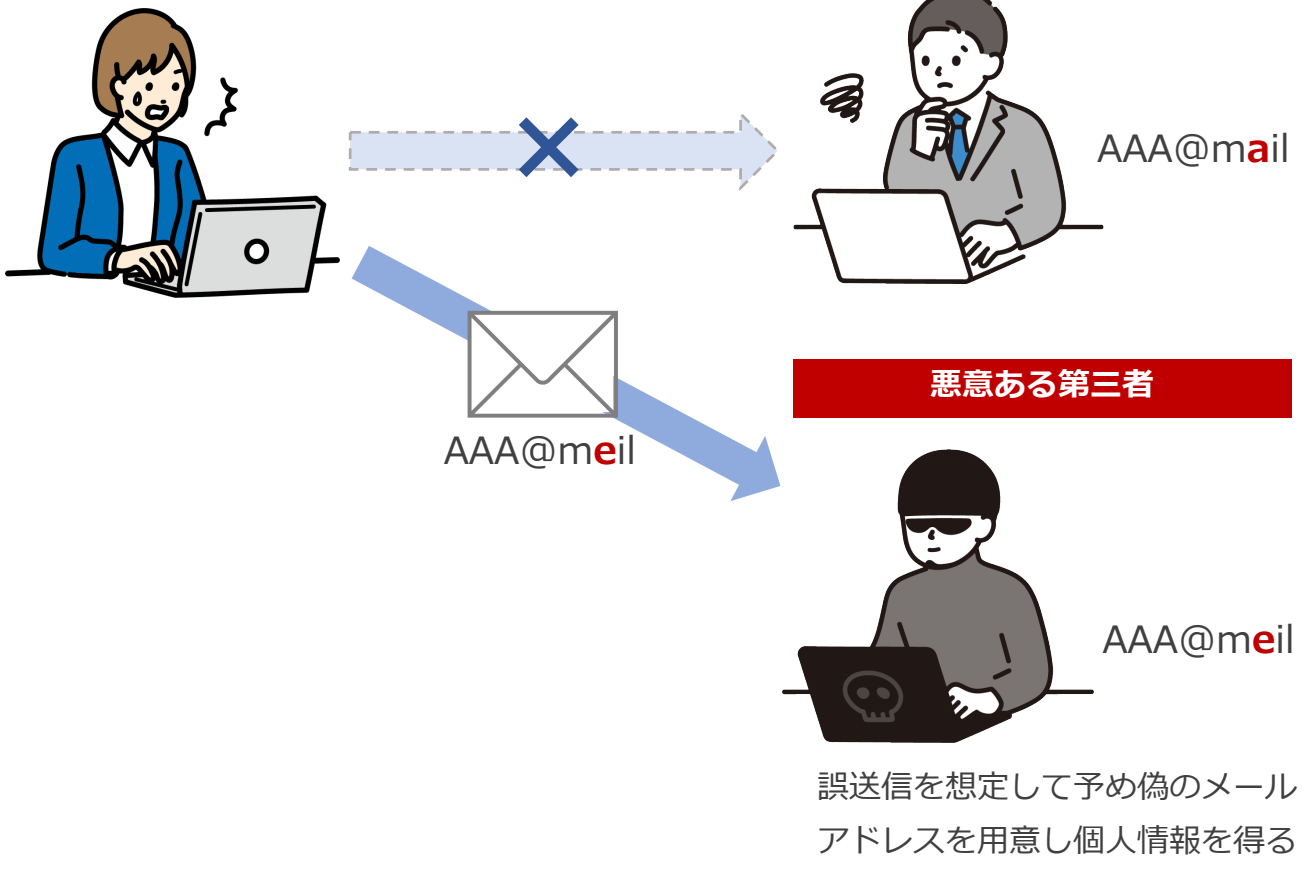
⑤ 差出人のメールアドレスと署名のメールアドレスが異なる

（ドメインが異なる）

注意すべきポイント

- 差出人のメールアドレスがフリーメルアドレスになっていないか
- 直接添付されているファイルにはマルウェアを疑う
- 差出人や添付ファイルが怪しい場合は開かない

メールの宛先、送付ファイルの間違えなどによる誤送信は個人情報漏洩につながります
最近は、誤送信を想定した偽のメールアドレスを用意した悪意ある第三者に個人情報が渡ることも



注意すべきポイント

送付前に確認

- 宛先・CC・BCCは間違えていないか
- メールアドレスに誤字はないか
  例：「mail」を「meil」と記載
- 送付するファイルに誤りはないか
- 送付相手の社名・名前に誤りがないか

送付後に確認

- 送信が問題なく行われたか
- 送付前と同様、宛先、ファイル、社名、名前を確認

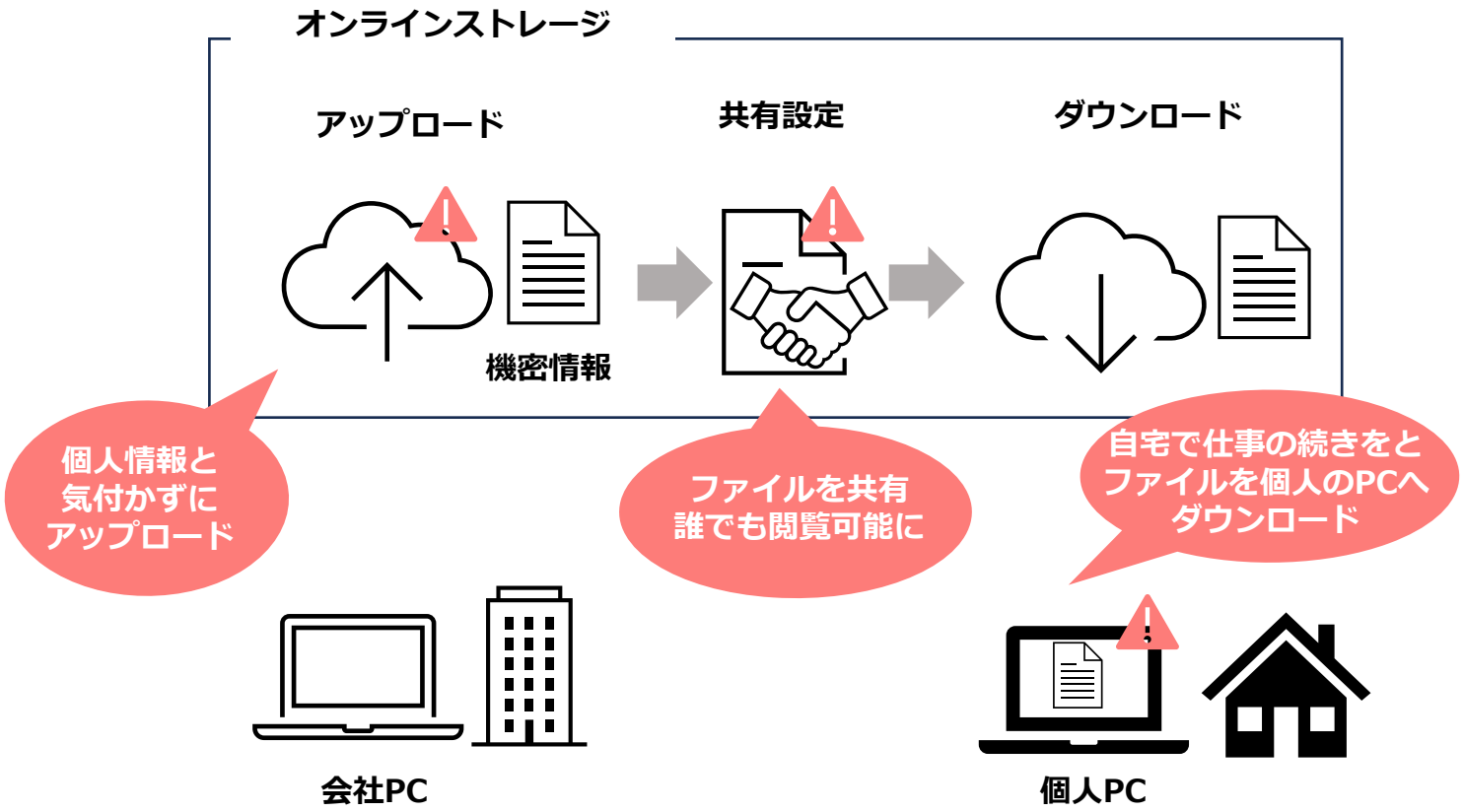
リモートワークの普及もあり PC の持ち出しが増えている
カフェや電車などにうっかりおいてくるケースも

注意すべきポイント

- PC 等が入ったカバンは電車の網棚にない
- カフェなど公共の施設では、離席時に PC を放置しない
- 個人情報の入った USB、PC を持ち歩くときは居酒屋など寄り道に気を付けること

ほんの少し気を抜いた瞬間に忘れてしまったり紛失することも
外出時は常にそばに置いておき、目を離さないようにする

個人情報・機密情報などを Microsoft 365 などのオンラインストレージにアップロード 知らずに共有設定にしてしまい外部の人が閲覧できる状態に。。。



注意すべきポイント

- 機密情報を OneDrive などのオンラインストレージにアップロードしない
- 機密情報が含まれるファイルを共有設定しない
- 個人の PC に会社のデータをダウンロードして持ち帰らない

オンラインストレージへのファイルアップロード・共有は意図せず部外者に情報を見られれる可能性がある
また会社 PC と異なりセキュリティ対策が不足している個人 PC はウイルス感染・紛失による個人情報漏洩リスクが高い

一度、ポイントに目を通し業務中に気になる点があれば確認しながら作業してください

確認事項
電子メール受信時
メールに直接添付しているファイルはむやみに開かない
添付ファイル名、拡張子が怪しくないか確認
不審な電子メールのURLはクリックしない
差出人のメールアドレスがフリーメールアドレスになっていないか確認
不審な電子メールは開かずに社内の情報システム部に相談する
電子メール送信時
送信前に再度送付先のメールアドレスが正しいか確認
重要情報は文書ファイルに記載。強固なパスワードで保護した上で、パスワードは別の手段で知らせる
無線 LAN・インターネット利用時
安全に使うために適切な暗号化方式を設定するなどの対策をしている無線LANを利用する
モバイルルーターやスマートフォンのテザリング機能を使わないときにはオフにする
インターネットを介したウイルス感染予防のため業務に関係ないウェブサイトは閲覧しない
SNSに秘密情報や個人情報を記載しない

業務の中で注意して欲しいセキュリティ対策チェックリスト

確認事項
情報を取り扱う時
定期的に重要情報をバックアップをしておく
重要情報が記載された書類や電子媒体は机上やPC上に放置しない
重要書類は鍵付き書庫に保管する。
重要情報が記載された書類や電子媒体は、会社のルールに従って持ち出す（場合によっては申請を行う）
退社時に机の上のノートPCやタブレット端末、備品を施錠できる引き出しにしまう
最終退出者は事務所を施錠し退出の記録（日時、退出者）を残す
業務中の安全管理について
PC にスクリーンロックをかける。
退社時に PC をシャットダウンする
不特定多数の人がいる場所では PC にのぞき見防止フィルタを取り付ける
見知らぬ人には声をかけて事務所に入れない
ノートPC、スマホ、USB メモリなどはパスワードロックをかける。
カフェやホテル、駅など公共の場所で仕事するときは PC や書類を放置しない
書類は細断する、電子データは消去ソフトを利用
重要情報の廃棄は細断するまたは専門サービスに書類の溶解を依頼
電子データの廃棄は、消去ソフトを利用または消去処分を委託して証明書を取得

LANSCOPE で支援するセキュリティ対策

従業員へセキュリティ教育だけでインシデントを防ぐのは困難
万が一に備えて、技術的な対策の実施も重要です

無線LAN・インターネット利用

- フリーWi-Fiなどセキュリティ上安全でないネットワークへの接続確認
- 業務外の Web サイト閲覧や、信頼できない Web サイトへのアクセスがないかを確認
- 業務外のWebサイトの閲覧や Web サイトへのデータのアップロードを制御

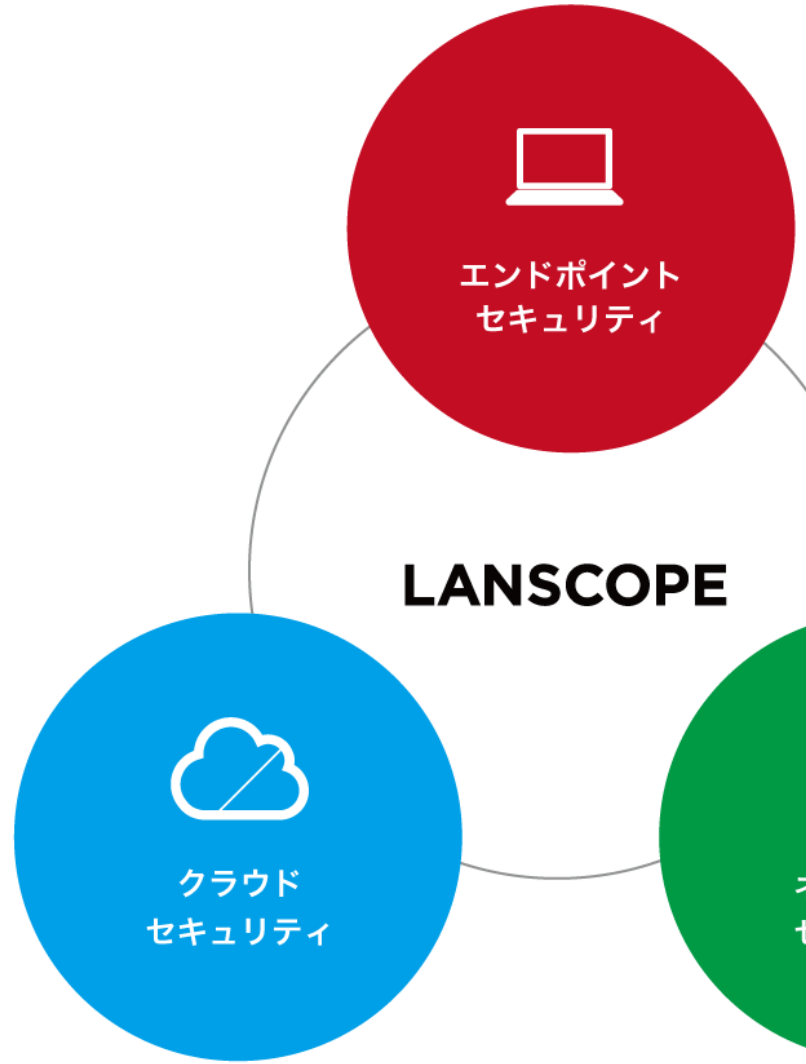
情報の取り扱い

- USB などを用いて、重要情報の持ち出しを許可なく行っていないか確認
- USB などの外部デバイスの利用制限を行う
- ノートPCなど重要情報が入ったデバイスの盗難・紛失対策

安全管理

- デバイスのパスワードポリシーを設定する
- データの暗号化対策を行う

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

セキュリティ教育だけでは防げない技術的な対策を「LANCSOPE」で支援します

エンドポイントセキュリティ

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

クラウドセキュリティ

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

ネットワークセキュリティ

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

PC・スマホ・タブレットの一元管理をクラウドで実現
充実の「IT 資産管理機能」と「MDM 機能」でセキュリティ対策を支援します

Cloud
LANSCOPE
Endpoint Manager

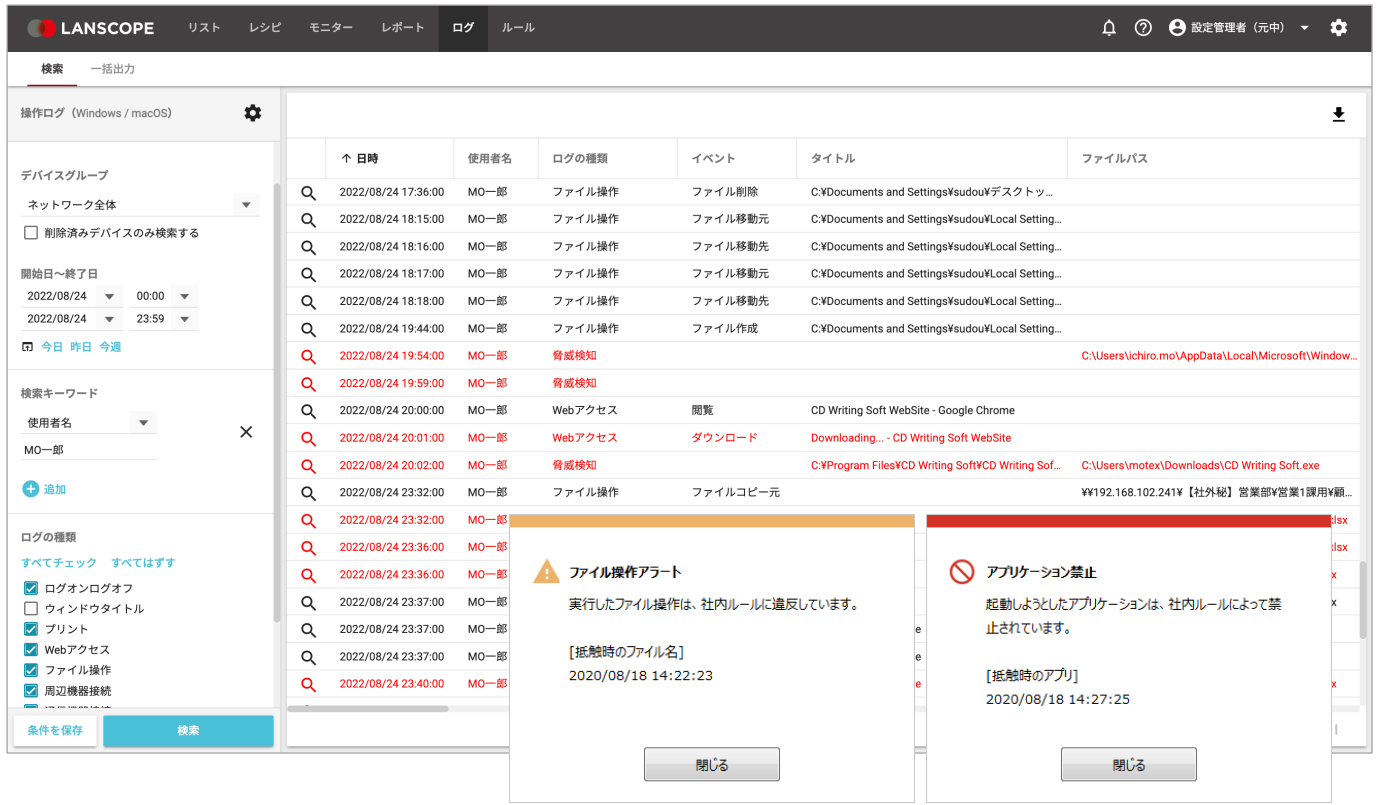
- iOS・Android・Windows・macOS を一元管理
- Apple・Google の認定プログラム対応で充実のモバイル管理
- 操作ログ・ファイル配信・記録メディア制御で PC 管理

資産管理	位置情報取得	レポート
セキュリティ	操作ログ	AE/ABM 対応

https://www.lanscope.jp/endpoint-manager/

「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年間保存され、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。

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

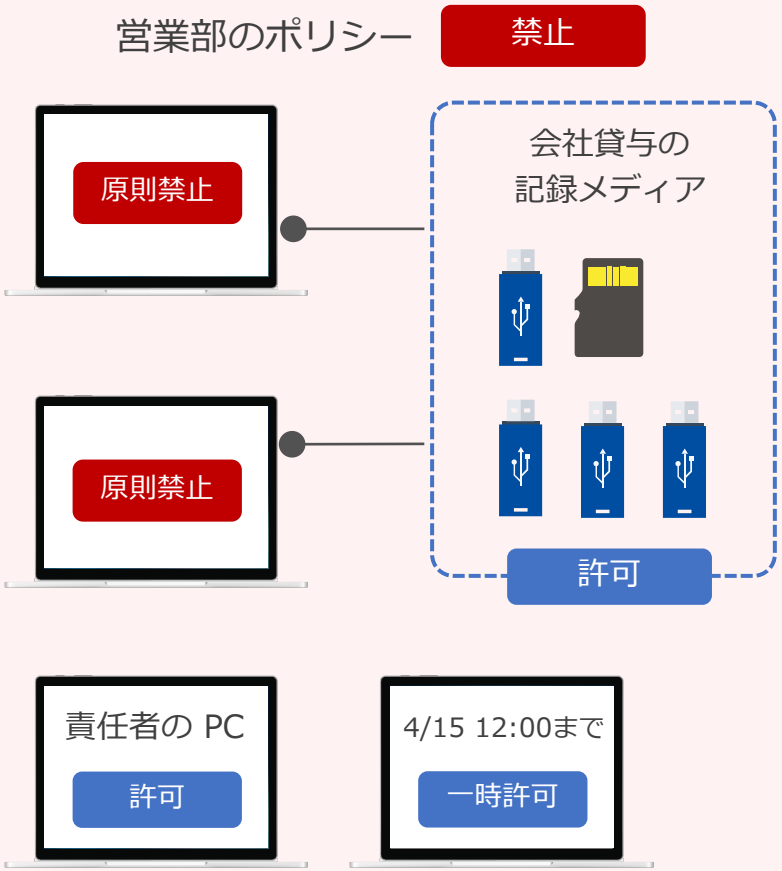
ユーザ設定カテゴリを含めた全26種・148カテゴリで制御が可能です。さらにカテゴリごとにサブカテゴリが設定されており、より詳細な制御が可能です。

※ Web フィルタリングはオプション機能になります。

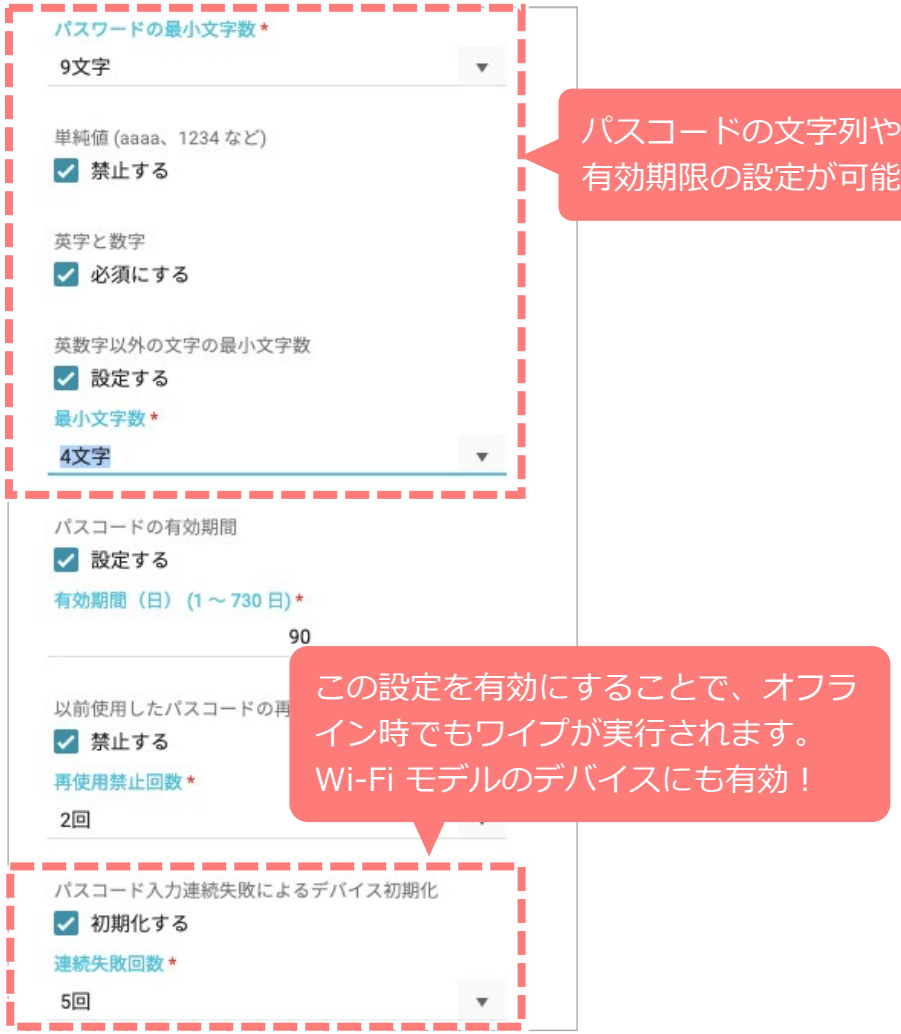
USB メモリなどの記録メディアの利用を制御し、情報漏洩を防止

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



利用者に依存しがちなパスコードの設定ルールを会社で統一！



iOS・macOS の設定項目
パスコードの最少文字数
単純値（aaaa、1234など）を禁止
英字と数字が必要
英数字以外の文字の最少文字数
パスコードの有効期間
以前使用したパスコードの再使用を禁止
パスコード入力連続失敗によるデバイス初期化*1
デバイスロック開始までの最大許容時間
画面ロック解除時のパスコード要求までの最大許容時間
ログイン失敗後の待ち時間*2
パスワードリセットの強制*2

Androidの設定項目
パスワードの最少文字数
使用しなければならない文字の種類
パスワードの有効期間
パスワードの有効期限を事前の通知
以前使用したパスワードの再使用を禁止
以前使用したパスワードの再使用を禁止
パスワード入力連続失敗によるデバイス初期化
スリープ開始までの最大許容時間

*1 macOS はアカウントのロックが行われます。
*2 macOS のみ対応しています。

👉 **パスワードポリシー設定の重要性**

パスワードを設定していない場合、画面ロックの解除は容易です。情報漏洩を防ぐためにも、利用者にパスワードの設定条件を委ねるのではなく、会社のポリシーをデバイスに設定することは、紛失対策の基本と言えます。

⚠ Android10以降のデバイスの場合、Android Enterprise の利用が必要です。

情報を安全に持ち出すためWindows・Mac デバイス 標準搭載の ドライブ・ディスク暗号化機能の運用管理をエンドポイントマネージャーで！

Windows：BitLocker

BitLocker の回復キーを自動取得できるので、デバイス毎にファイルや印刷で保存する必要がなくなります。

macOS：FileVault

FileVault の設定を強制化したり、復旧キーを自動取得します。

情報持ち出しリスクに備える
位置情報から所在確認！遠隔でリモートロックやワイプを実行し情報漏洩を防止！

※ 位置情報の取得のためにはデバイス側で必要な設定があります。詳細はお問い合わせください。また位置情報の取得精度はデバイスに依存します。
※ OSによってリモートロック・ワイプの仕様は異なります。Windows Server OS はリモートロック・ワイプ機能に対応していません。
※ Windows Server OS・macOS は位置情報取得機能には対応していません。
※ Windows はスリープ状態の場合、位置情報が取得できません。

IT 資産管理ツールだけでは特定できない、Microsoft 365 経由の情報漏洩経路

Microsoft 365 でのファイル操作や共有状況の把握には、監査ログの取得と解析が必要です。

（従来の範囲）IT 資産管理ツールの領域

ファイルサーバーの「顧客リスト」を「参考データ」に名前変更してアップロード

クラウドサービスの領域

「参考データ」を競合Aに共有、競合Aがダウンロード

Microsoft 365 の利用状況の見える化と社内ルールの通知までを自動化
M365上でのファイル共有による情報漏洩対策はセキュリティオーディターで！

現状把握

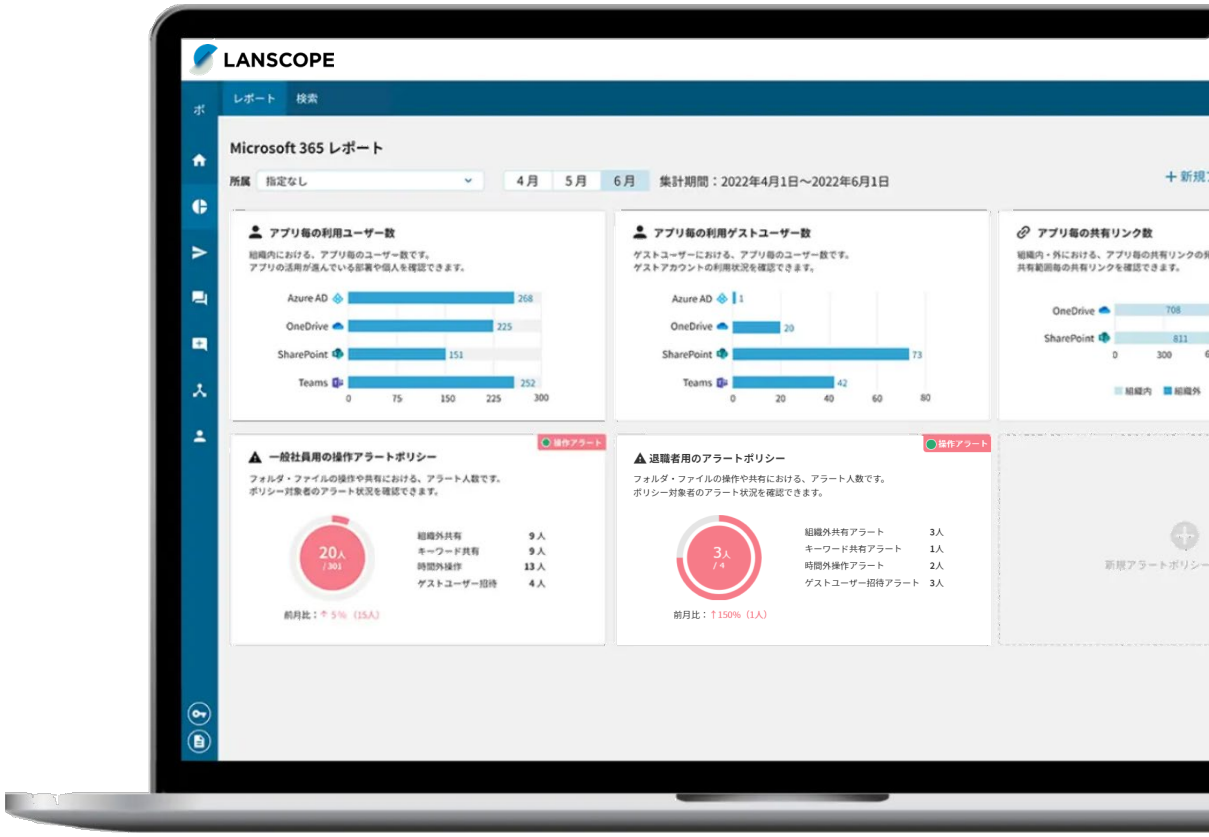
取得したログを分かりやすくレポートに
利用状況とセキュリティリスクを可視化

アラート通知

通知機能で必要な案内・連絡業務を
担当者に代わり、ボットが自動通知

監査ログの保存・出力

Microsoft 365 監査ログを2年間保存
全期間のログを一括出力可能



ファイル共有などのアラートの発生状況を “視認性”の良いレポートで見える化

情報漏洩リスクがあることを管理者に通知するだけでなく、本人にも警告通知が可能です

組織外への共有は
ルールで禁止なのに！
スグに確認だ

管理者

LANSCOPE

【Microsoft 365 組織外共有アラート】
以下のアラートを検知しました。

■組織外共有アラート
日時：2022/4/26　02:38:11
内容：フォルダ/ファイルが組織外に共有されました

■ログ
所属：営業本部/営業1課
ユーザー名：MO　一郎
メールアドレス：ichiro.mo@demo.motex.co.jp
IPアドレス： 203.0.113.10
アクティビティ日時：2022/4/26　02:38:11
アクティビティカテゴリー：共有リンク操作＞共有リンク発行
アクティビティ：共有リンク（特定のユーザー）のユーザー追加
アプリ：OneDrive
ファイルパス:/personal/ichiro.mo_onmicrosoft_com/Documents/社外秘/upload_file.csv

■関連する項目

1.アラート通知があった場合　2.Microsoft 365について

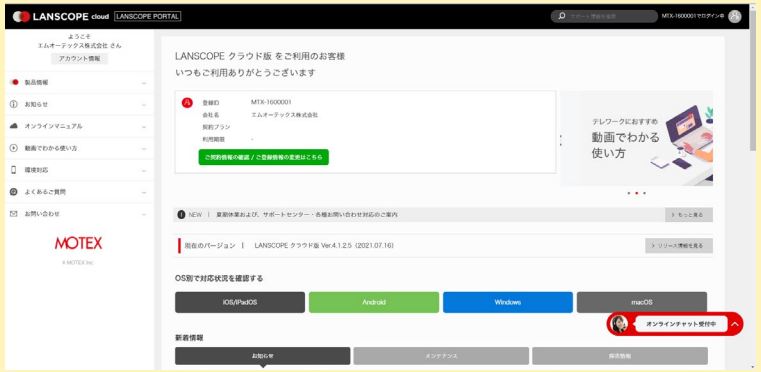
- **組織外共有アラート**
  組織外にフォルダーやファイルを共有するリンクを生成した場合にアラートにします。
- **キーワード共有アラート**
  指定したキーワードを含むフォルダやファイルを共有した場合にアラートにします。
- **時間外操作アラート**
  指定した時間外にアプリの利用があった場合に把握できます。
- **ゲストユーザー招待アラート**
  ゲストユーザーを招待した場合にアラートにします。
- **アラート通知**
  アラートが発生した本人や管理者にビジネスチャットからアラート内容を通知できます。

Endpoint Manager Cloud

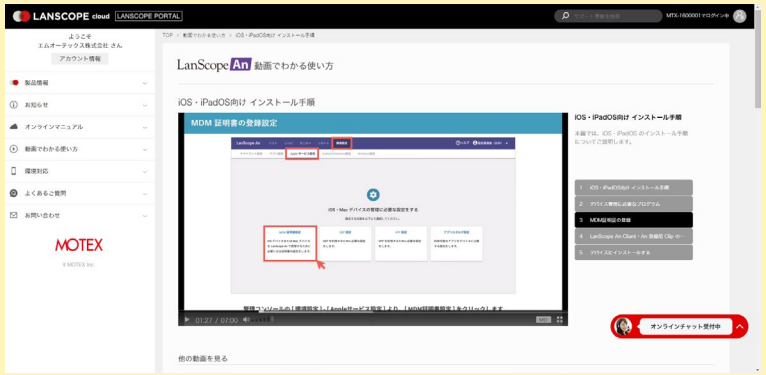
60日間無料体験キャンペーン中

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

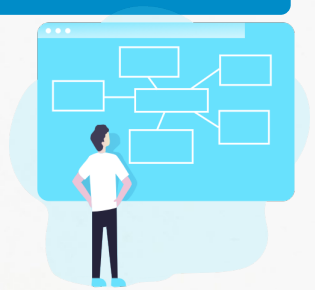
LANSCOPE
Security Auditor

60日間無料体験版 受付中！

「禁止していたはずのゲストユーザー招待が、実際にはいくつかあった。。」
「社外への共有はNGなのに、やっている人が何人もいた！」など、
体験版導入で今まで見えなかったセキュリティリスクがレポートで一目で分かる！
さらに、無料体験版のデータをそのまま製品版へ移行も可能です。

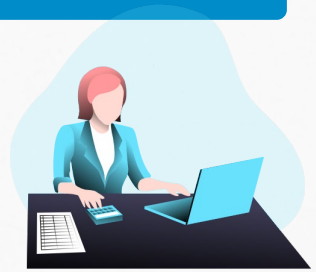
＋　ユーザー様専用サイトの利用

ユーザー様しか利用できない専用サイトを利用できます。マニュアルや活用方法などを掲載しています



＋ ヘルプデスクサポート

ユーザー様と同様に電話やメールによる問い合わせが可能です。お困りごとなどお気軽にご相談ください



https://go.motex.co.jp/l/320351/2018-11-22/21kdt6

製品に関するお問い合わせ

■ 営業本部

大阪本社	06-6308-8980
東京本部	03-3455-1811
名古屋支店	052-253-7346
九州営業所	092-419-2390
E-mail	sales@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	0120-968995 （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）
Email お問い合わせ	support@motex.co.jp