LANSCOPE
Endpoint Manager Cloud

情報漏洩はなぜ起きるのか？

不正のトライアングル理論から学ぶ内部不正の原因と対策

～IPA の内部不正防止ガイドラインを基にしたチェックリスト付～

はじめに

情報漏洩事件の原因は様々ですが、内部不正による情報漏洩はいまだに減らない傾向にあります。昨今の大きな情報漏洩事件も内部不正によるものが多く、組織にとって深刻な問題となっています。

IPA（情報処理推進機構）が毎年発表している「情報セキュリティ10大脅威」でも、内部不正は常にランクインしており、これは情報セキュリティにおいて重要な課題であることを示しています。機密情報のアクセス制限や従業員の教育、監視体制の強化など、対策は様々あります。しかし、業務上どうしても機密情報へのアクセスが必要な人もいるなかで、完全な対策を講じることは難しいのが現状です。そのため、内部不正が起こりにくい体制の構築が必要です。

体制を構築するうえでまず、内部不正のメカニズムを理解することが重要です。内部不正が起こる背景には、従業員の不満やストレス、報酬への不平等感、倫理観の欠如、内部不正ができる環境などが考えられます。これらの要因を把握し、適切な対策を講じることが求められます。

今回は、内部不正のメカニズムを理解し、内部不正を起こさないための対策や体制をどのように作っていけばいいのかご紹介します。

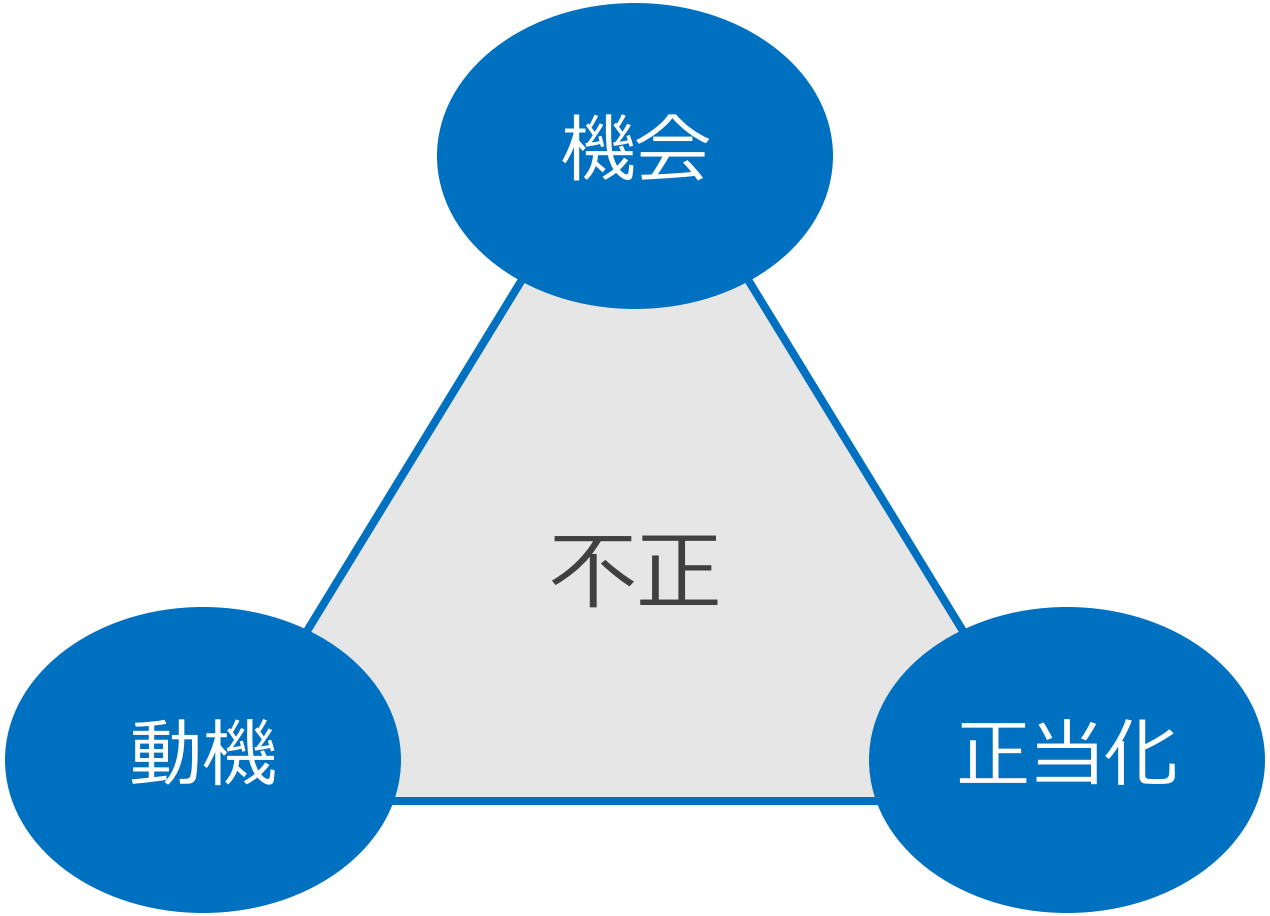
情報セキュリティ10大脅威 2023

順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏洩
5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
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏洩等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

※引用：IPA「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html

内部不正が起こるメカニズムを分析した「不正のトライアングル」理論（※）

「機会」 「動機」「正当化」3つの要素が揃ったときに内部不正が発生しやすいとされている



※ 「アメリカの犯罪学者ドナルド・R・クレッシー氏が提唱で、組織内の要員が不正を起こすメカニズムを分析した理論

不正のトライアングルの3つの要素と具体例

機会

不正行為を行うための状況や環境が整っていること

- 内部統制が不十分で監視が甘い
- 操作ログの取得など不正行為を監視するシステムがない
- 機密情報へのアクセス制限の管理をしていない
- USBなど外部記録メディアへの書き出しが簡単にできる

動機

不正行為を行うための心理的な要因

- 経済的な困窮、借金など金銭問題
- 金銭を得たいという欲求
- 労働環境によるストレス
- 会社への不満
- 地位や名誉が欲しい（早く出世したい、成果を出したいなど）

正当化

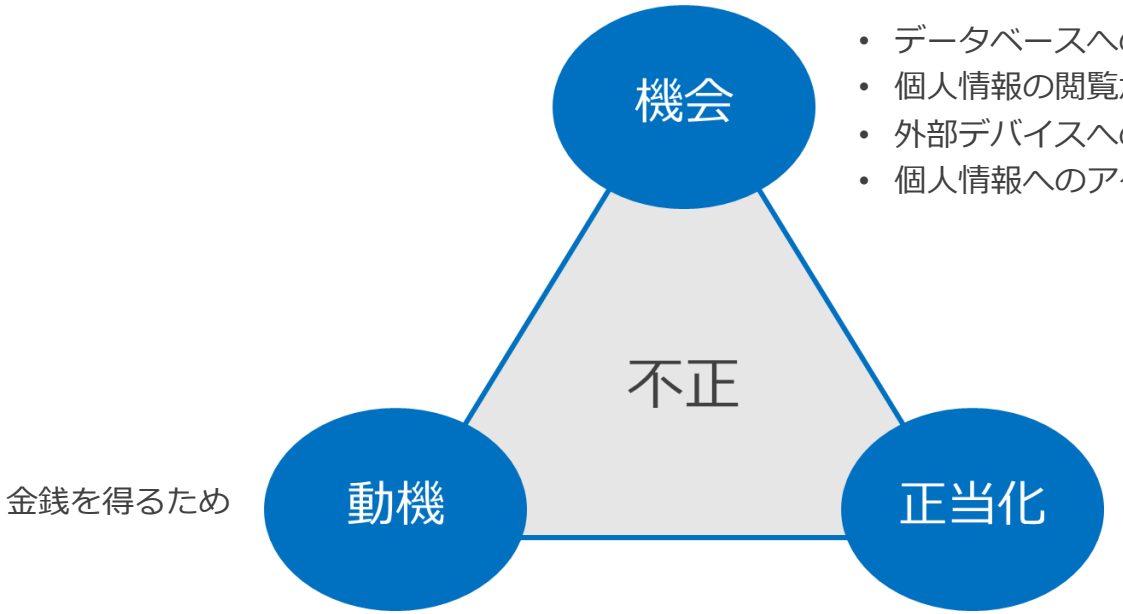
自分の行為を正当化するための言い訳や理由

- 自分を適切に評価しない会社が悪い
- 影響は小さいのでこれくらいの不正は問題ないだろう
- 給料など待遇を良くしない会社が悪い

例：不正のトライアングルの視点からみる情報漏洩事件

実際に起きた情報漏洩事件に不正のトライアングルの3要素はあったのか？

某大手通信教育業者 情報の持ち出し	某大手通信教育業者で約4,858万人の個人情報が流出。データベースの管理を請け負っていたグループ企業の元派遣社員が会社PCに個人情報を保管し、自身のスマートフォンにデータをコピーして持ち出していた。個人情報は名簿業者に売却。元派遣社員は不正競争防止法違反で逮捕されている。



- データベースへのアクセス権限を保有
- 個人情報の閲覧が可能
- 外部デバイスへのデータ書出し制御はなし
- 個人情報へのアクセスアラート設定なし

金銭を得るため

派遣社員であることから、
待遇が悪いなど会社への
不満があった？？

「機会」「動機」「正当化」3つの要素を発生させない環境づくりが重要

「機会」を減らす

不正を行わせない
システムを構築する

- **内部統制の強化**
  操作ログを取得し定期的にログチェックを行う。USBなどによる情報の持ち出し制限を行う。
- **権限の分散**
  業務を複数の担当者に分散。一人の従業員が大きな権限を持たないようにする。
- **アクセス制限**
  情報へのアクセスは必要な従業員に限定する。

「動機」を減らす

会社への不満、ストレス、
評価への不満などを解消

- **コミュニケーション**
  従業員が意見や悩みを相談できる環境を整え、ストレスを減らす。
- **適切な報酬制度**
  労働に対する報酬が適切であることを確認し、不正行為への動機を減らす。

「正当化」を回避する

自分の行為を正当化する
ための言い訳や理由

- **従業員の教育**
  セキュリティインシデントのリスクへの理解、適切な対応方法を教育する。
- **企業倫理の強化**
  企業の倫理規定や行動規範を明確にし、従業員に理解してもらう。
- **内部通報制度**
  不正行為を見つけやすくし、正当化される前に対処できるようにする。

IPA のガイドラインを基にした内部不正チェックリスト※

うちの会社は大丈夫？内部不正チェックリスト40項目のうち、17項目は不正のトライアングルに該当

チェック項目	3つの要素	対策方法
基本方針		
内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか？	-	社内ルールの整備
「基本方針」に基づき対策を実施するためのリソースが確保されるよう、必要な決定、指示をしていますか？	-	社内ルールの整備
経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか？（ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はありません。）	-	社内ルールの整備
総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していますか？	-	社内ルールの整備
秘密指定		
重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか？	-	社内ルールの整備
重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていますか？	-	社内ルールの整備
重要情報を含む電子文書には、内部者が分かるように機密マーク等の表示をしていますか？	-	社内ルールの整備
アクセス権指定		
情報システムを管理・運営する担当者は、利用者ID及びアクセス権の登録・変更・削除等の設定手順を定めて運用していますか？	-	社内ルールの整備
情報システムを管理・運営する担当者は、異動又は退職により不要となった利用者ID及びアクセス権を、ただちに削除していますか？	-	社内ルールの整備
複数のシステム管理者がいる場合は、情報システムの管理者IDごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか？ また、システム管理者が一人の場合は、ログ等により監視していますか？	機会	IT資産管理ツール
情報システムでは、共有IDや共有のパスワード・ICカード等を使用せず、個々の利用者IDを個別のパスワード・ICカード等で認証していますか？	-	社内ルールの整備

※ IPA「組織における内部不正防止ガイドライン」を基に作成

IPA のガイドラインを基にした内部不正チェックリスト※

チェック項目	3つの要素	対策方法
物理的管理		
重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していますか？	-	社内ルールの整備
PC等の情報機器やUSBメモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理・保護していますか？	機会	IT資産管理ツール
情報機器や記憶媒体を処分する際には重要情報が完全消去されていることを確認していますか？	-	社内ルールの整備
モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていますか？	機会	IT資産管理ツール
個人のモバイル機器及び記録媒体の業務利用及び持込を制限していますか？	機会	IT資産管理ツール
技術・運用管理		
モニタリングシステムが提供する AI監視機能等（例： ふるまい解析機能）の有効性を評価していますか？	-	監視ツール
組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトやSNS、外部のオンラインストレージ等の使用を制限していますか？	機会	IT資産管理ツール
委託先等の関係者への重要情報の受渡しは、受渡しから廃棄迄を含めて管理していますか？	-	社内ルールの整備
インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し暗号化等で保護していますか？	-	暗号化ツール
組織外部で利用・取り扱い可能な重要情報を限定し、重要情報や情報機器を保護していますか？	-	社内ルールの整備
組織外で重要情報を用いた業務を行う際に、周囲の環境やネットワーク環境等を考慮して保護していますか？	-	社内ルールの整備
委託する業務内容に応じたセキュリティ対策を契約前に確認・合意し、契約期間中にも契約通りにセキュリティ対策が実施されていることを確認していますか？	-	社内ルールの整備
原因究明と証拠確保		
重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか？（推奨）	機会	IT資産管理ツール
システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか？	機会	IT資産管理ツール

※ IPA「組織における内部不正防止ガイドライン」を基に作成

IPA のガイドラインを基にした内部不正チェックリスト※

チェック項目	3つの要素	対策方法
人的管理		
すべての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか？	正当化	従業員教育
教育を定期的に繰り返して実施し、教育内容を定期的に見直して更新していますか？	正当化	従業員教育
従業員の行動や心身の状態のモニタリングの目的が、従業員の適正かつ健全な就業を支援し、従業員を内部不正から 保護するためであることを、就業規則で広く 周知していますか？	正当化	従業員教育
派遣労働者による重要情報の漏えい等の不正行為が発生しないように、派遣元と協力して、秘密保持義務を課していますか？	正当化	社内ルールの整備
雇用の終了時に秘密保持義務を課す誓約書の提出を求めていますか？ （推奨）	-	社内ルールの整備
役職員の雇用終了時および請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却または完全消去し、情報システムの利用者IDや権限を削除していますか？	-	社内ルールの整備
コンプライアンス		
就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか？	-	社内ルールの整備
役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等を要請していますか？	-	社内ルールの整備
職場環境		
公平で客観的な人事評価を整備するとともに、業績に対する評価を説明する機会を設ける等、人事評価や業績評価の整備を推進していますか？ （推奨）	動機	社内ルールの整備
業務量及び労働時間の適正化等の適切な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していますか？ （推奨）	動機	社内ルールの整備
相互監視ができない環境における単独作業を制限し、単独作業には事前承認、事後確認等の手続きを定めていますか？ （推奨）	機会	社内ルールの整備
事後対策		
内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保していますか？	-	社内ルールの整備
内部不正者に対する処罰を検討し、内部不正の事例を内部に告知することを検討していますか？	正当化	社内ルールの整備
組織の管理		
内部不正と思わしき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していますか？	正当化	社内ルールの整備
内部不正対策の項目を抽出し、定期的及び不定期に確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していますか？	正当化	社内ルールの整備

※ IPA「組織における内部不正防止ガイドライン」を基に作成

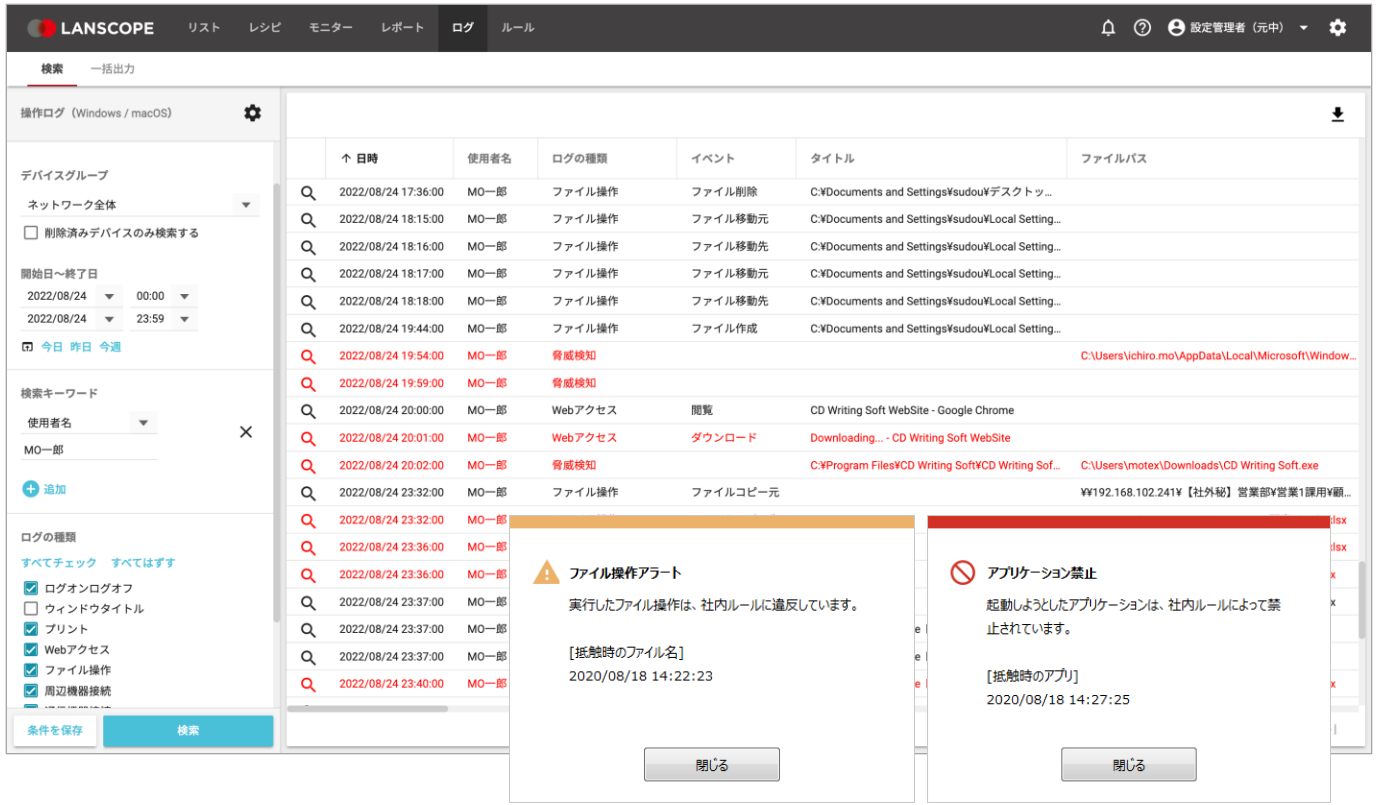
エンドポイントマネージャーで行う内部不正チェック

重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか？

機会

「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

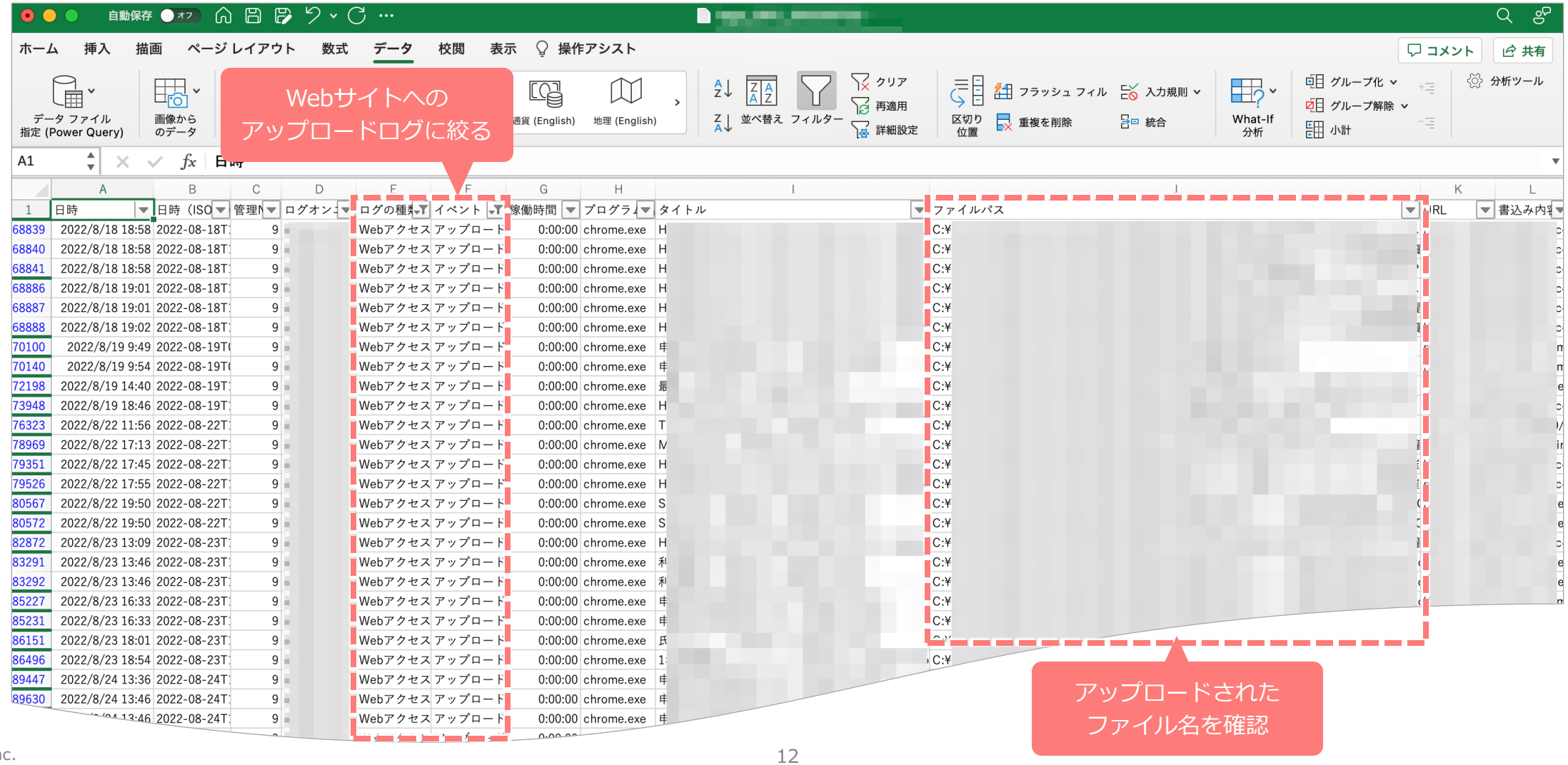
バックグラウンドで稼働しているアプリ情報、通信元／先のIPアドレスやポート番号、アプリのハッシュ値を取得できます。

※1 macOS は Web サイトの閲覧ログのみ対応しています。
※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。

重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか？

機会

エンドポイントマネージャーは過去2年分の操作ログを保存
期間を指定しログを CSV 形式で一括出力、重要データが持ち出されていないか把握



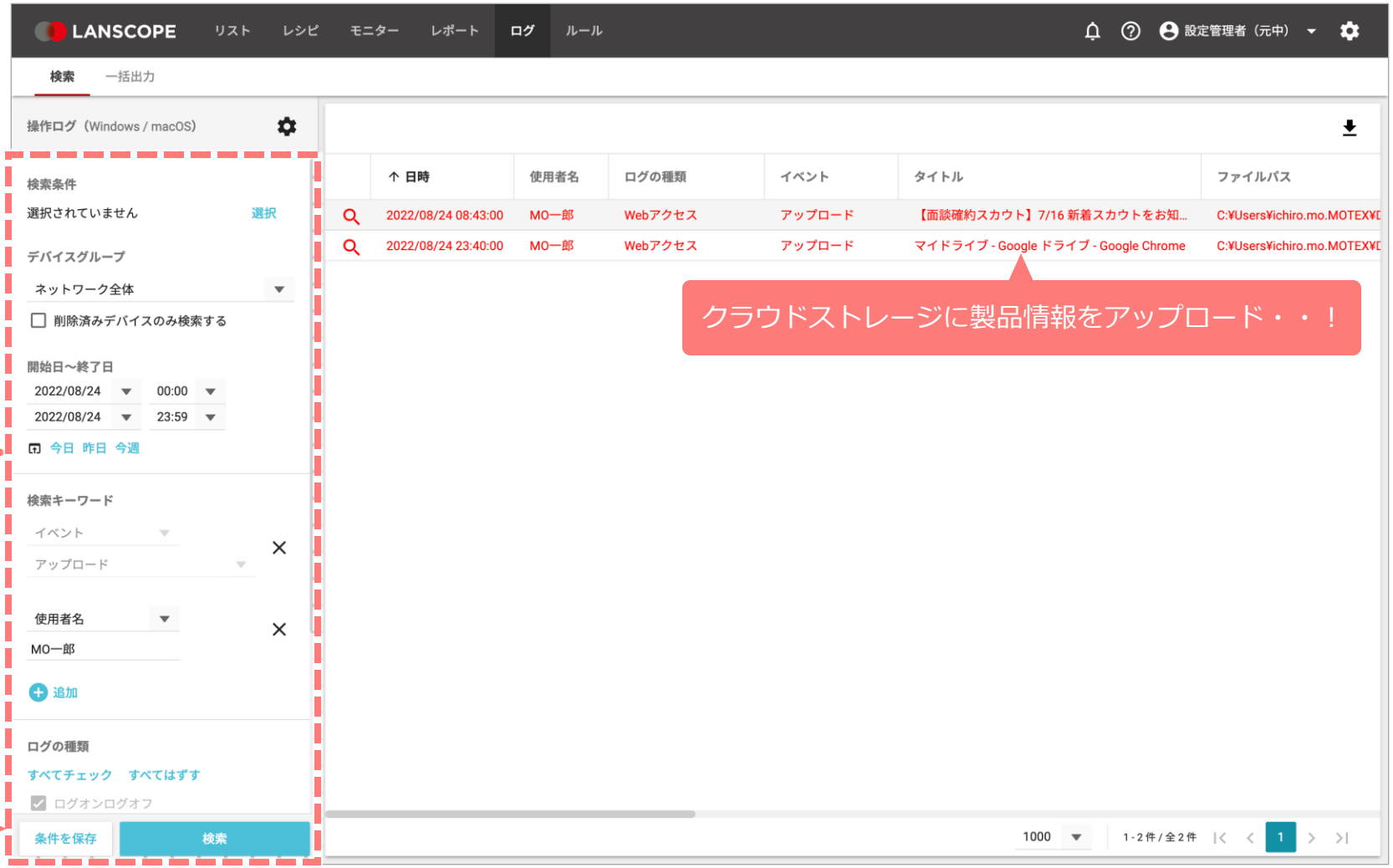
ログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか？

機会

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

活用シーンに合わせてテンプレートを用意



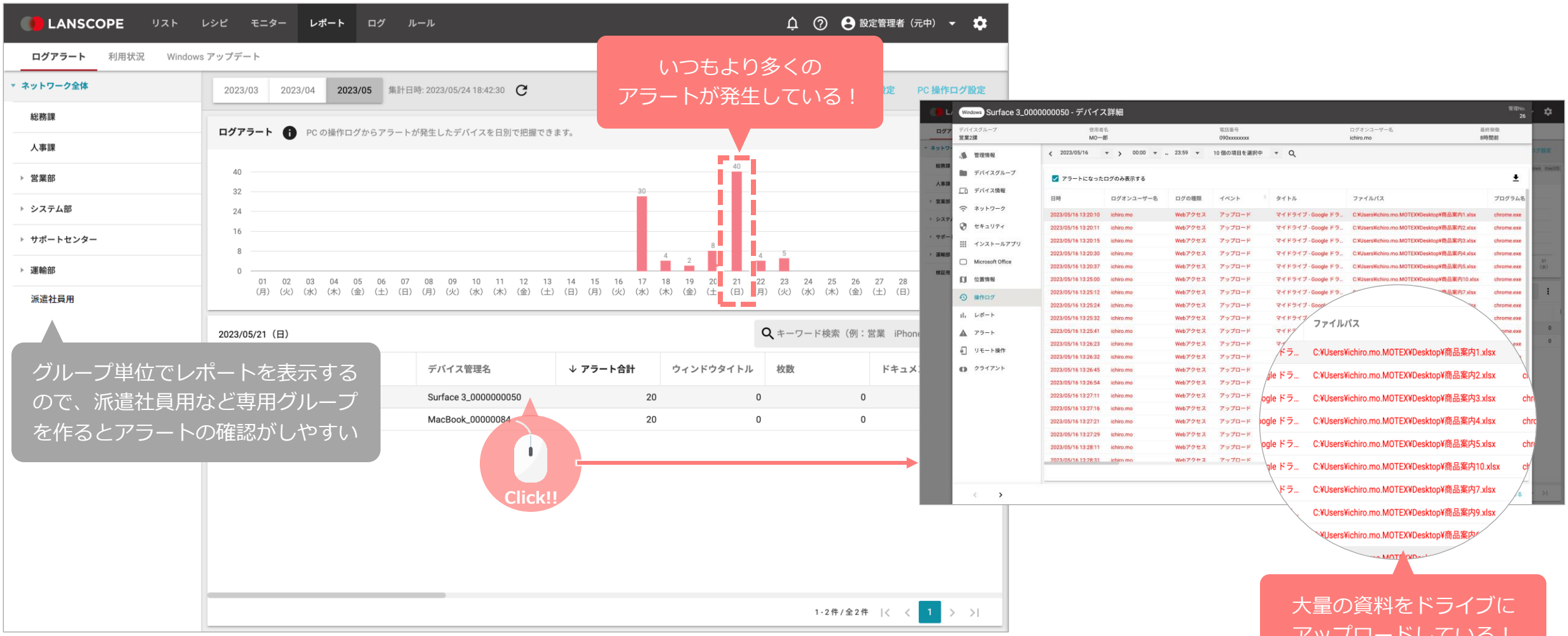
クラウドストレージに製品情報をアップロード・・！

編集した検索条件の保存も可能

ログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか？

機会

日付ごとにアラート数を把握できる視認性の良いレポート
「発生数が極端に多い日」などポイントを絞って、詳細をチェック



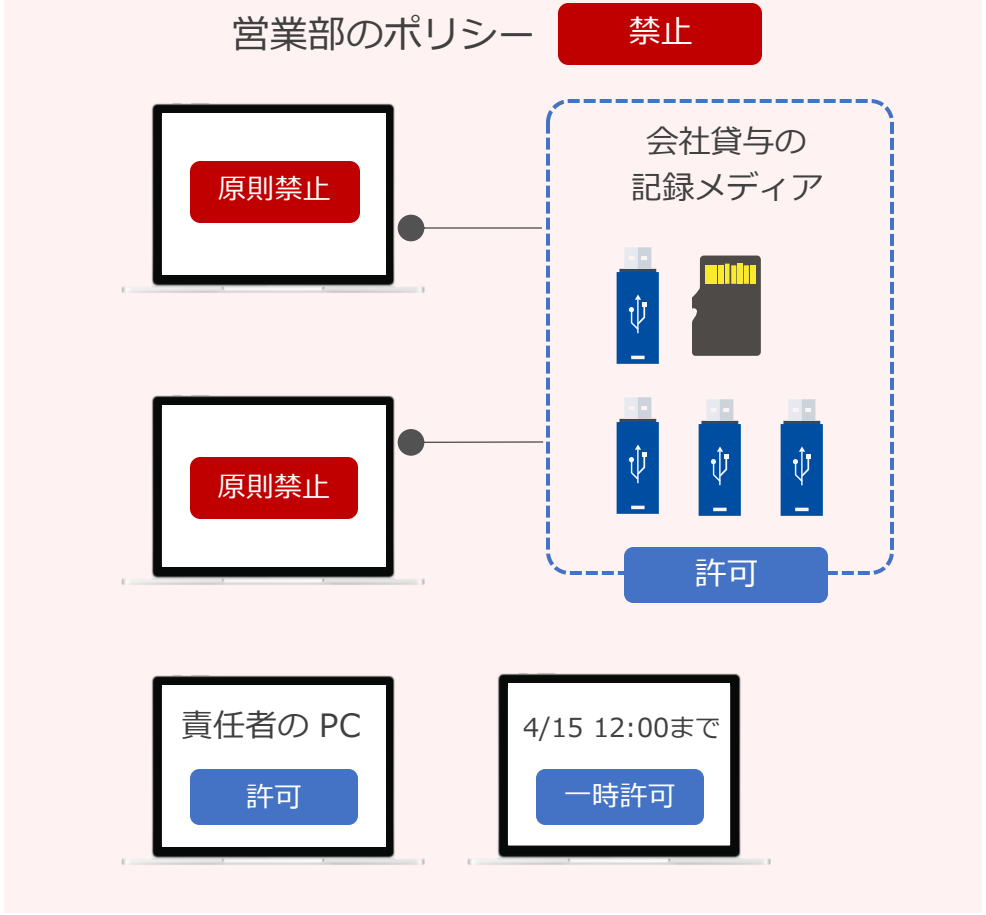
USBメモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理・保護していますか？

機会

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。

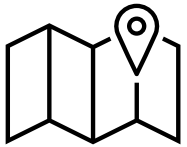
記録メディア制御のイメージ



情報システムの管理者IDごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか？

機会

安全にクラウドサービスをご利用いただけるよう、エンドポイントマネージャーは管理コンソールのセキュリティ機能を実装。管理コンソールのログイン画面に、許可されていない第三者のアクセスを防止する IP アドレス制限や2要素認証、パスワードポリシーの設定が可能です。また管理コンソール上の操作履歴を1年分保存します。

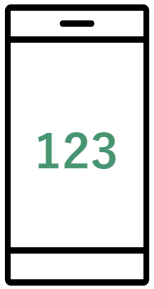


IP アドレス制限

IP アドレスによるアクセス制限を行い、社外 PC などからの不正なアクセスをブロックします。

パスワードポリシー

管理コンソールのパスワード強度・有効期間などポリシーを設定できます。



2要素認証

ログイン時に認証用のモバイルアプリで生成された確認コードの入力を要求できます。

操作履歴

管理コンソールのアカウントの画面閲覧や設定変更などを操作履歴として1年分保存し、閲覧・CSV 出力できます。

重要情報を不正に持ち出し可能なファイル共有ソフトやSNS、外部のオンラインストレージ等の使用を制限していますか？

機会

Web フィルタリングで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
ファイルのアップロードも禁止できます

● 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。

■ カテゴリ別ルール登録　　登録　戻る

参照ルール名	MOTEX
カテゴリ別ルール名	
規制内容	許可　書き込み規制　規制　一時解除

カテゴリ	サブカテゴリ	設定	全て	全て	全て	全て
⊞ ユーザ設定カテゴリ						
⊞ 不法						
⊟ アダルト・フェティシズム						
	アダルト・ポルノ					
	フェティシズム					
⊞ セキュリティ						
⊞ 出会い						
⊞ 金融						
⊞ ギャンブル						
⊞ ショッピング						
⊞ コミュニケーション						

※ Web フィルタリングはオプション機能となります
※ 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

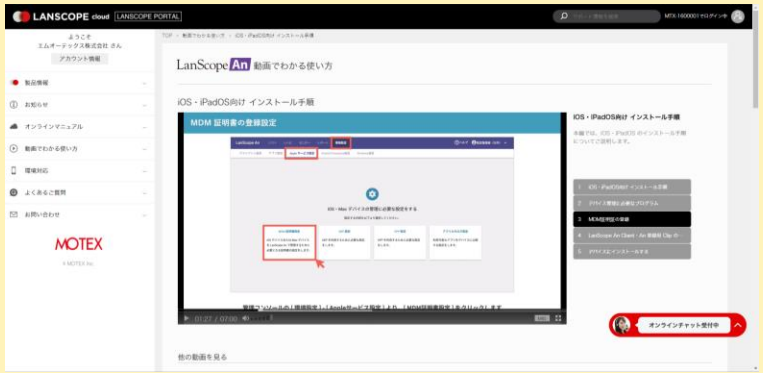
Endpoint Manager Cloud

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

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