Cloud
LANSCOPE
Endpoint Manager

長期休暇中はインシデントが増える！？

～対策チェックリスト付～

長期休暇前後にやっておくべきセキュリティ対策

04

はじめに

企業は業務の継続性を確保するため、長期休暇期間中の問題に対処できるよう対策を講じる必要があります。
特に、情報システム部門は、業務に関わるシステムの安全性やセキュリティの確保など企業の業務継続において極めて重要な役割を果たします。

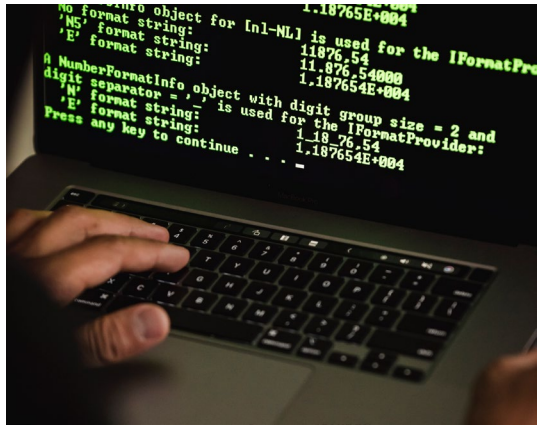
長期休暇期間中は、システム管理者が不在、人員が少ないなど通常と異なる状況になるため障害やインシデントが発生した場合、
対応に遅れが出てしまい、休暇明けからの業務に支障が出るリスクがあります。

本資料では、このような状況にならないために長期休暇期間の前後に企業がやっておくべき対策について解説いたします。
尚、本資料は、内閣官房内閣サイバーセキュリティセンター「春の大型連休に向けて実施いただきたい対策について」を基に作成しています。

長期休暇期間中に発生するリスクとは？

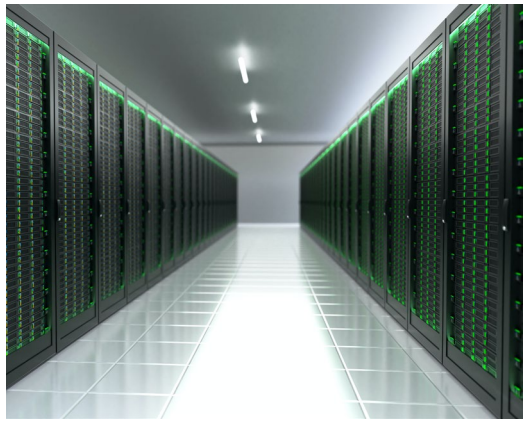
長期休暇期間中は、システム管理者が不在になる、人員が通常より少ない等いつもとは違う状況となり以下のようなリスクが発生します。

サイバー攻撃



長期休暇期間中はセキュリティ担当者が不在となりやすい、休暇期間でメールが溜まり確認がおろそかになりやすいなどの背景から、サイバー攻撃が増加する傾向があります。

システム障害



システム障害が起きた場合、迅速にリカバリーが行われないと、休暇明けに業務が再開できないリスクがあります。またサービスの停止により、お客様への影響が生じる可能性もあります。

人の不注意によるミス

休暇中で PC やスマートフォンを持ち帰ることによる紛失リスクや、休暇中の人員不在による業務負荷の増加によりミスが起きやすくなりインシデントが発生するリスクが高まります。

インシデント発生時の対応の遅れ

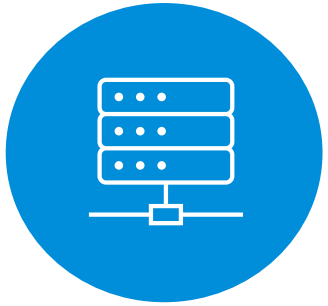
長期休暇期間中は人員が少ないため、サイバー攻撃などの検知が遅れる場合も。攻撃の検知・対処が遅れて被害が拡大するリスクがあります。

長期休暇に備えてやっておくべきセキュリティ対策

長期休暇におけるセキュリティ対策では、「休暇前」「休暇後」それぞれの対策・対応が重要です。

休暇前の対策

インシデント対応手順
連絡体制の確認



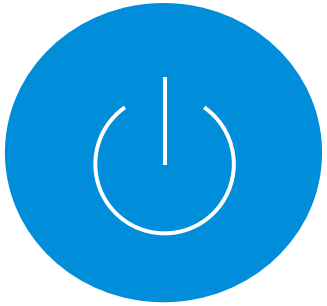
バックアップ対策

アクセス制御対策

ソフトウェアの
脆弱性対策

利用機器に
関する対策

休暇明けの対策



電源を落としていた
機器に関する対応

ソフトウェアの
脆弱性対策

不正プログラム
感染の確認

各種ログの確認

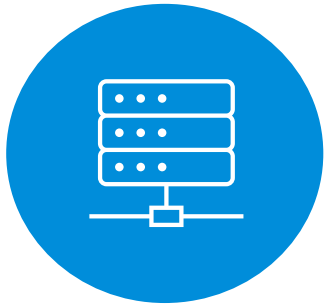
休暇前の対策

長期休暇期間中はサイバー攻撃を受ける可能性が高まります。休暇前には、あらゆるリスクに備えた対策を実施しておきます。

インシデント対応手順 連絡体制の確認

- 休暇期間中の監視体制を確認
- システムアラート等の監視体制を強化
- セキュリティインシデント対応手順を確認
- 連絡体制を最新の組織に合わせて更新

バックアップ対策



- 重要なデータや機器設定ファイルに対するバックアップ対策を実施
- バックアップデータはネットワークから切り離すなどの対策を検討

アクセス制御対策

- アクセス権限の確認、多要素認証の利用、不要なアカウントの削除
- 利用者にパスワードが単純でないか確認
- 外部ネットワークからアクセス可能な機器へのアクセスは必要最低限に設定

ソフトウェアの 脆弱性対策

- 脆弱性対策の状況を確認
- セキュリティパッチの適用・ソフトウェアのバージョンアップ
- 長期休暇期間中に公表された重要な脆弱性の対応体制を整える

利用機器に関する 対策

- 機器（サーバー、PC、通信回線装置等）のファームウェアを最新にアップデート
- 休暇中に使用しない機器の電源を落とす

休暇前のセキュリティ対策チェックリスト※

チェック項目	チェック
長期休暇期間中のセキュリティインシデント発生時の対処手順及び連絡体制の確認	
長期休暇期間中ではセキュリティインシデントをリアルタイムで認知しづらく対応が遅れがちとなるため、セキュリティインシデントに即応できるよう長期休暇期間中の監視体制を確認し、必要に応じ、システムアラート、各種ログ等の監視体制を強化すること	☐
セキュリティインシデントを認知した際に迅速かつ円滑に対応することができるよう、セキュリティインシデントを認知した際の対処手順（事業継続計画等）の内容を再度確認すること	☐
セキュリティインシデントを認知した際における連絡体制（情報セキュリティインシデントを認知した際における対応等の決定権者及び担当者等の連絡先、連絡が取れなかった場合の予備の連絡先）が最新の情報に更新されていることを確認すること	☐
システムベンダ（保守業者を含む）、回線業者、外部サービス提供者、データセンタ事業者等のサポート窓口やサプライチェーン企業の営業状況、連絡先（夜間・休日等の通常営業時間帯以外の連絡先を含む。）等を確認すること	☐
情報システムを利用する職員等に対して、セキュリティインシデントを認知した場合の報告窓口を周知すること	☐
バックアップ対策の実施	
システムの不具合やランサムウェア等の不正プログラムによるデータ破壊に備えて、重要なデータや機器設定ファイルに対するバックアップ対策を実施するとともに、最新のバックアップが確実に取得されていること、バックアップデータから実際に復旧できることを確認すること	☐
バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討すること	☐
アクセス制御に関する対策	
この機にアクセス権限の確認、多要素認証の利用、不要なアカウントの削除等により、本人認証を強化するとともに、個々の利用者にパスワードが単純でないか確認させること	☐
インターネット等外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定し、管理機能、ポート（例えば、ファイル共有サービス等によく利用される137(TCP/UDP)、138（UDP）、139(TCP)、445(TCP/ UDP)、リモートデスクトップ等で利用される 3389(TCP)など）及びプロトコルを不必要に開放していないことを確認すること	☐

※ 内閣官房内閣サイバーセキュリティセンター「春の大型連休に向けて実施いただきたい対策について」を基に作成

休暇前のセキュリティ対策チェックリスト※

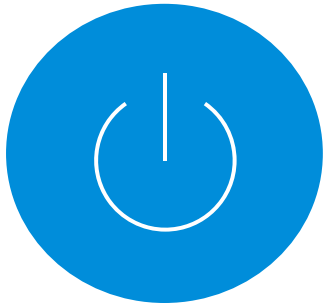
チェック項目	チェック
ソフトウェアに関する脆弱性対策の実施	
脆弱性対策の状況を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行うとともに、直ちに実施することが困難な場合はリスク緩和策を講ずること	☐
休暇期間中に公表された重要な脆弱性情報について遅滞なく確認、対応の検討が行われる体制としておくこと	☐
セキュリティパッチの適用やソフトウェアのバージョンアップについて、やむを得ず長期休暇期間前に実施できない場合、長期休暇期間明け直後は業務システムへのアクセス集中が予想されることから、事前に実施時期のスケジュールを検討すること。	☐
利用機器・外部サービスに関する対策	
外部からの不正アクセスを防止する観点から、機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラなど）等）のファームウェアを最新のものにアップデートすること。	☐
長期休暇期間中に使用しない機器の電源を落とすこと。また、機器に自動起動機能を設定している場合は、長期休暇期間中の設定の要否を検討すること。	☐
この機に使用しない外部サービスの無効化の要否を検討すること。	☐

※ 内閣官房内閣サイバーセキュリティセンター「春の大型連休に向けて実施いただきたい対策について」を基に作成

休暇明けの対策

休暇明けは、サイバー攻撃やウィルス感染・脆弱性への対応有無を確認した上で通常業務に戻していきます。

電源を落としていた機器に関する対応



- 休暇中に電源を落としていた機器は、端末起動後、最初にアンチウイルス当の定義ファイルを確認
- 最新の状態になっていない場合は、更新してから、利用を開始

ソフトウェアの脆弱性対策

- 長期休暇期間中における脆弱性情報を確認
- 必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを実施

不正プログラム感染の確認

- 休暇中に持ち出しが行われていた PC 等が不正プログラムに感染していないか確認

各種ログの確認

- サーバー等の機器に対する不審なアクセスがないか、ログやアラートで確認
- 不審なログが記録されていた場合は、早急に調査

休暇明けのセキュリティ対策チェックリスト※

チェック項目	チェック
長期休暇期間中に電源を落としていた機器に関する対策	
長期休暇期間中に電源を落としていた機器は、不正プログラム対策ソフトウェア等の定義ファイルが最新の状態となっていないおそれがあることから、端末起動後、最初に不正プログラム対策ソフトウェア等の定義ファイルを確認し、最新の状態になっていない場合は更新作業を実施してから、利用を開始すること。	☐
ソフトウェアに関する脆弱性対策の実施	
長期休暇期間中における脆弱性情報を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行うとともに、直ちに実施することが困難な場合はリスク緩和策を講ずること。	☐
不正プログラム感染の確認	
長期休暇期間中に持ち出しが行われていたパソコン等が不正プログラムに感染していないか、不正プログラム対策ソフトウェア等で確認を行うこと。	☐
サーバ等における各種ログの確認	
サーバ等の機器に対する不審なアクセスが発生していないか、VPN、ファイアーウォール、監視装置等ログやアラートで確認すること。もし何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行うこと。	☐

※ 内閣官房内閣サイバーセキュリティセンター「春の大型連休に向けて実施いただきたい対策について」を基に作成

従業員向けのセキュリティ対策

従業員にも、長期休暇期間中の前後に適切なセキュリティ対策を行ってもらうよう事前に周知しておきます。
また、この機会に改めて社内のセキュリティポリシーを理解してもらい、セキュリティ意識を高めてもらいましょう。

緊急連絡先の確認

- 休暇中にインシデント等が発生した場合の緊急連絡先や報告フローを周知する

PC・スマホ等の持ち出しルールの確認

- 長期休暇期間中に PCやスマホ等の機器や記録メディア等の持ち出しが必要な場合、持ち出しルールを再度通知する

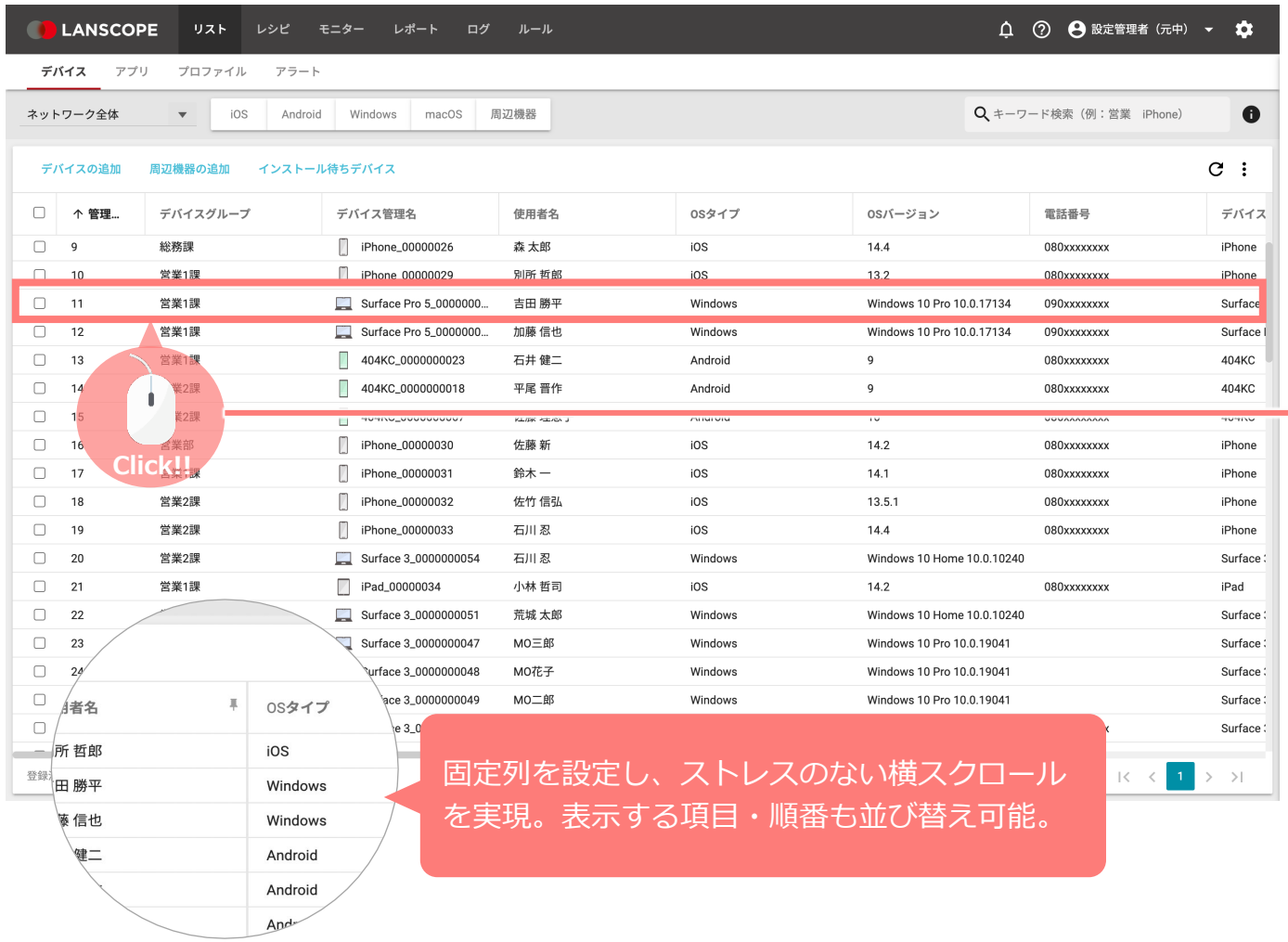
休暇明けメール開封の注意喚起

- 不審な添付ファイルを開いたり、リンク先にアクセスしたりしないよう注意喚起する
- 不審な点があれば、メールを開封する前に、電話等、別の手段で確認するなどの対応方法を周知

エンドポイントマネージャー クラウド版でできる対策

デバイスの所在を問わず、管理下のデバイスの最新情報を自動取得し、一覧で表示

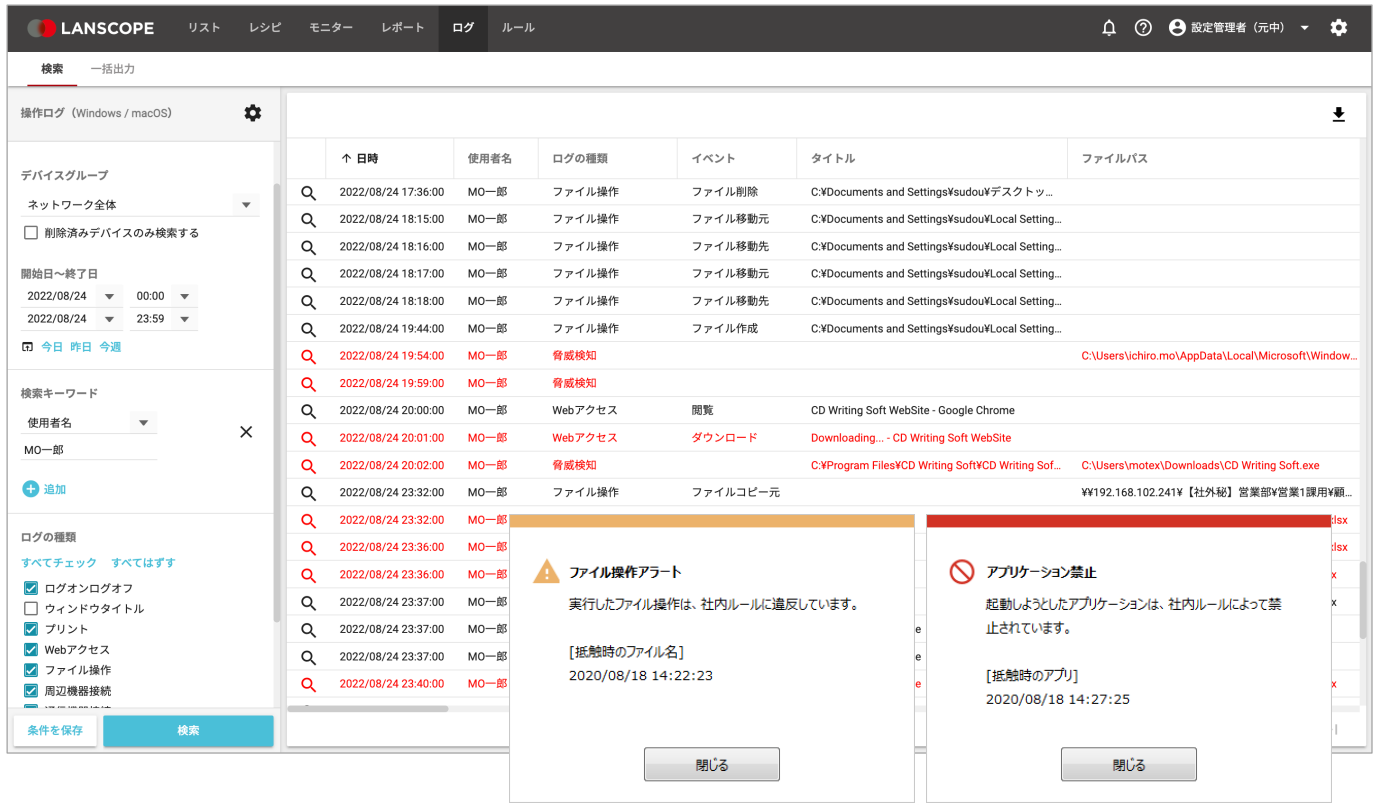
デバイスを特定し、1Click で詳細の資産情報の確認が可能。自動取得できない項目は、任意項目として管理できます。



操作ログ取得

「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。

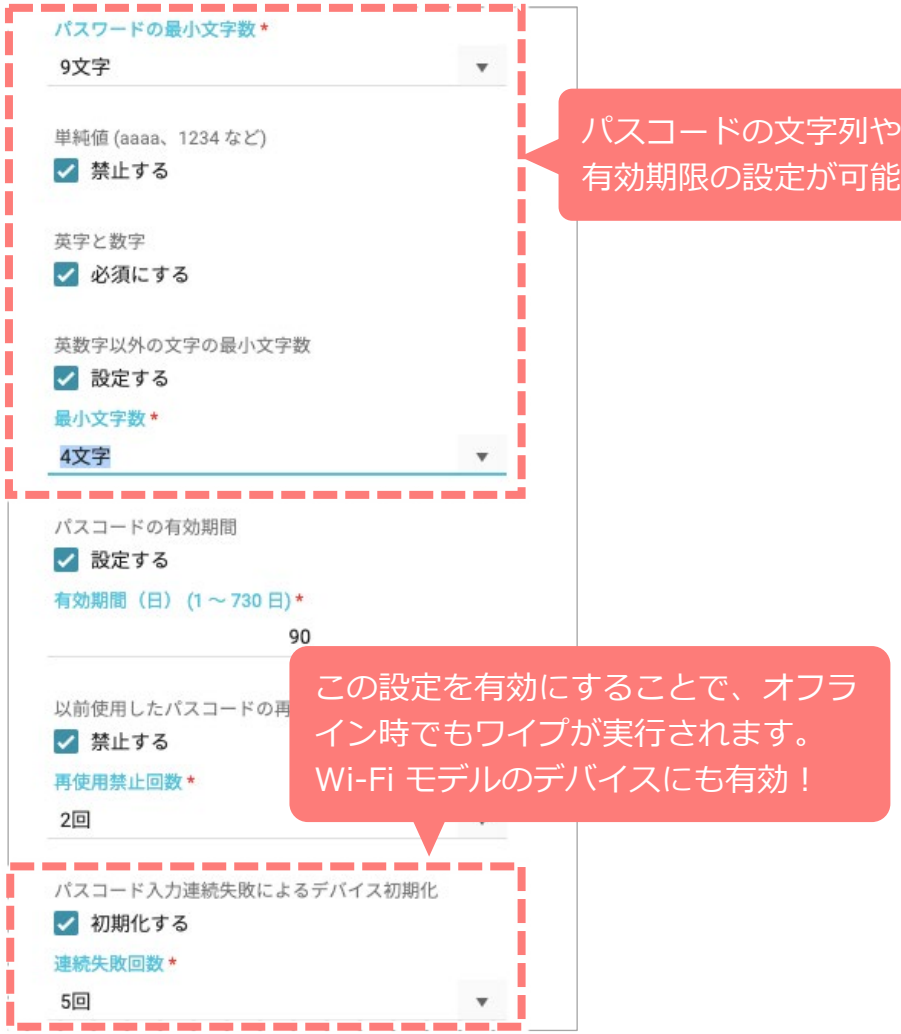
プリントログ
印刷状況を記録し、ドキュメントやプリンター、PCごとに印刷枚数を集計できます。

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。

休暇前に改めて、パスコードの設定ルールを見直してセキュリティを強化！



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。

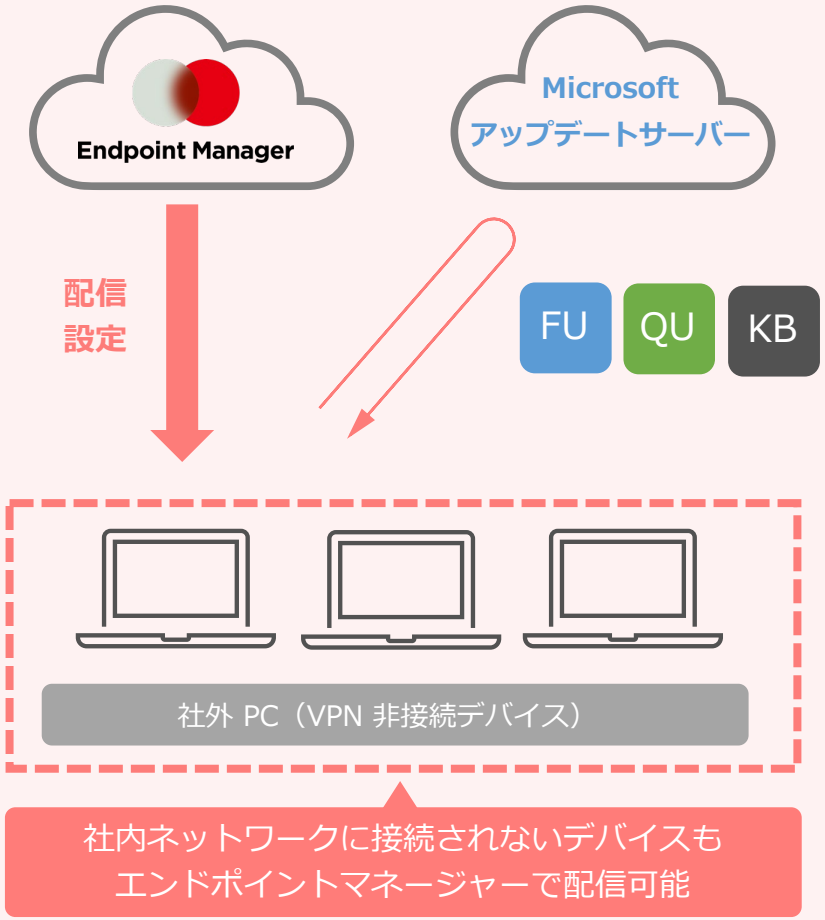
紛失リスクに備える事後対策：位置情報の確認※・リモートロック・ワイプ

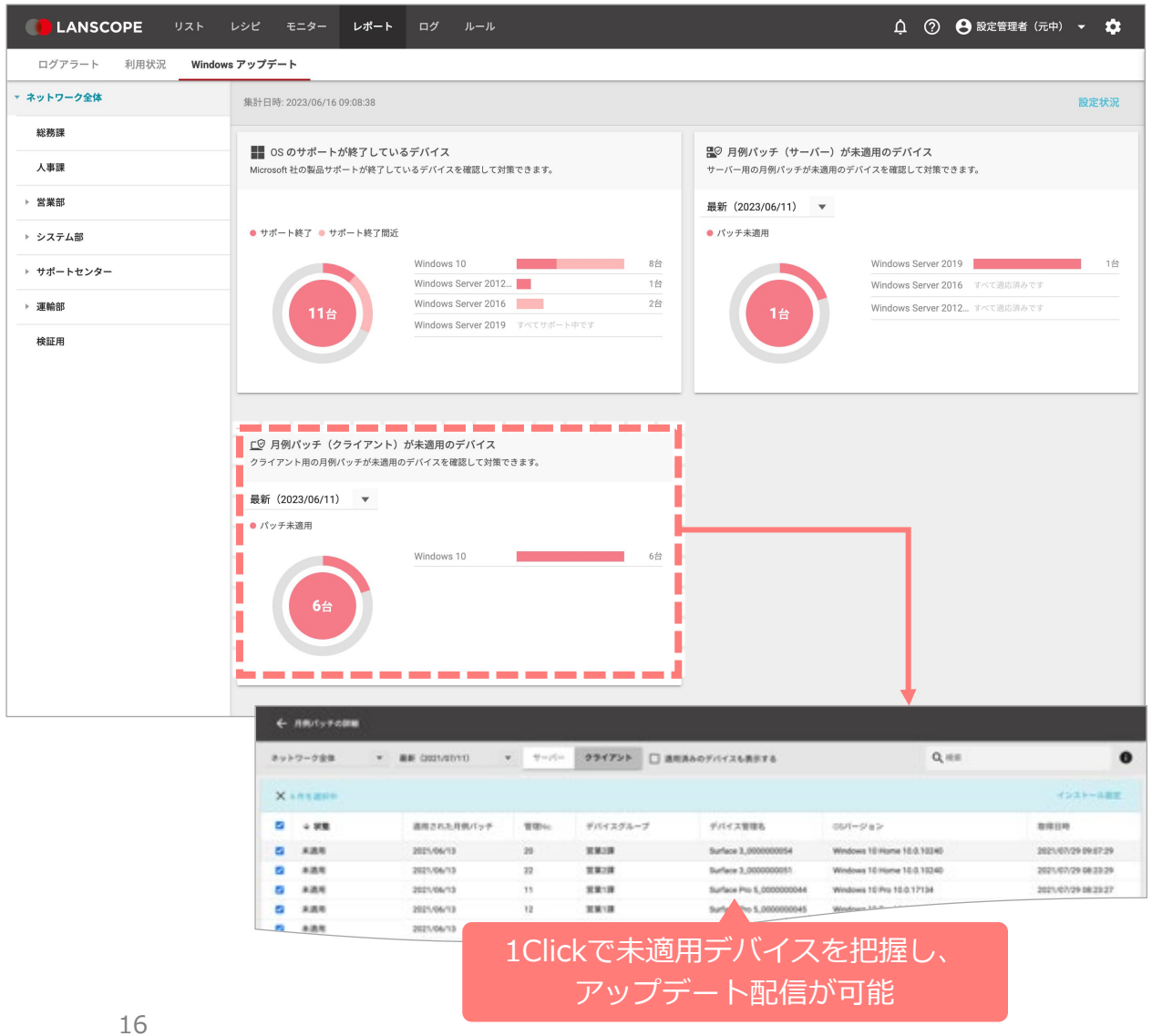
万が一休暇中に PC を紛失した際も位置情報から所在確認
遠隔でリモートロックやワイプを実行し情報漏洩を防止！

※ 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。

休暇前後に Windows アップデートの適用状況を確認し、脆弱性の有無を把握

Windows アップデート管理のイメージ

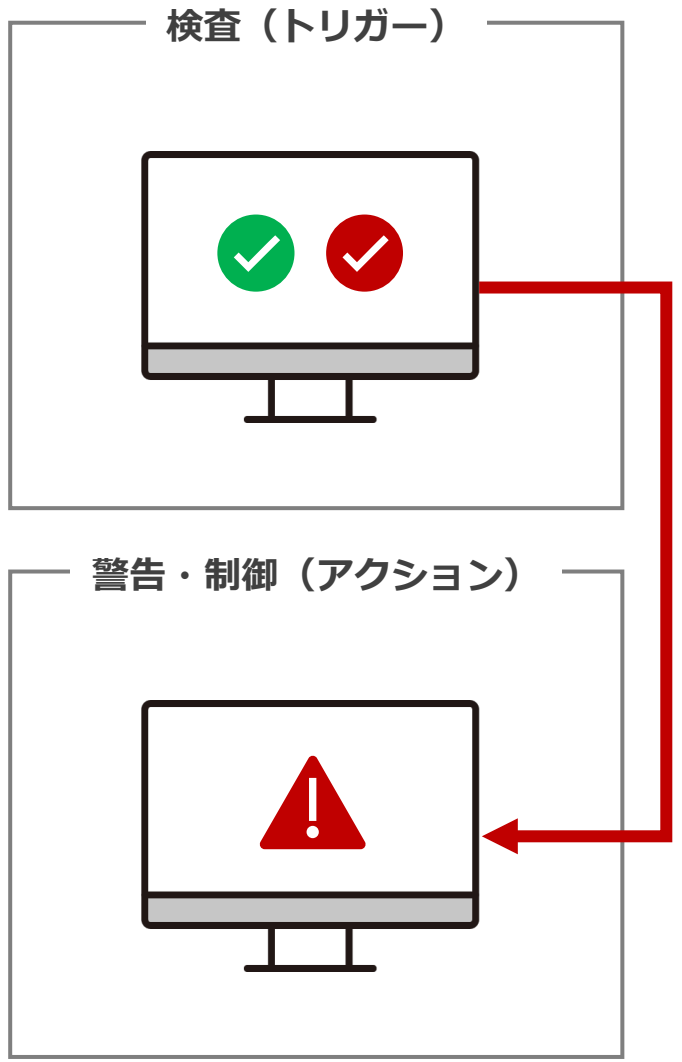




「古い OS を利用していないか」「セキュリティソフトがインストールされているか」など検査項目に違反があった場合に、警告・制御・特定アプリの起動を自動実行

▼トリガー・アクション一覧

	トリガー名	概要
検査（トリガー）	Windows OS バージョン検査	利用している OS バージョンが指定したバージョン外の場合に検査違反と判定します。
	Windows セキュリティパッチ検査	指定したセキュリティパッチがインストールされていない場合に検査違反と判定します。
	アプリインストール検査	指定したアプリがインストールされていない場合に検査違反と判定します。
	アプリバージョン検査	インストールされているアプリが指定したバージョン外の場合に検査違反と判定します。
	プロセス起動検査	指定したアプリが起動していない場合に検査違反と判定します。
	特定宛先への NW 疎通検査	指定したネットワークと疎通が取れていない場合に検査違反と判定します。
警告/制御（アクション）	不適合警告	警告ダイアログを表示し、警告内容と必要な設定内容などを案内します。
	IP アドレス指定制御	あらかじめ指定した IP アドレス以外への接続を禁止できます。
	ドメイン名指定制御	あらかじめ指定したドメイン名以外への接続を禁止できます。
	特定 URL ブラウザアクセス	ブラウザを起動して、指定した Web サイト が表示されます。
	指定アプリ起動	PC にインストールされているアプリを実行します。



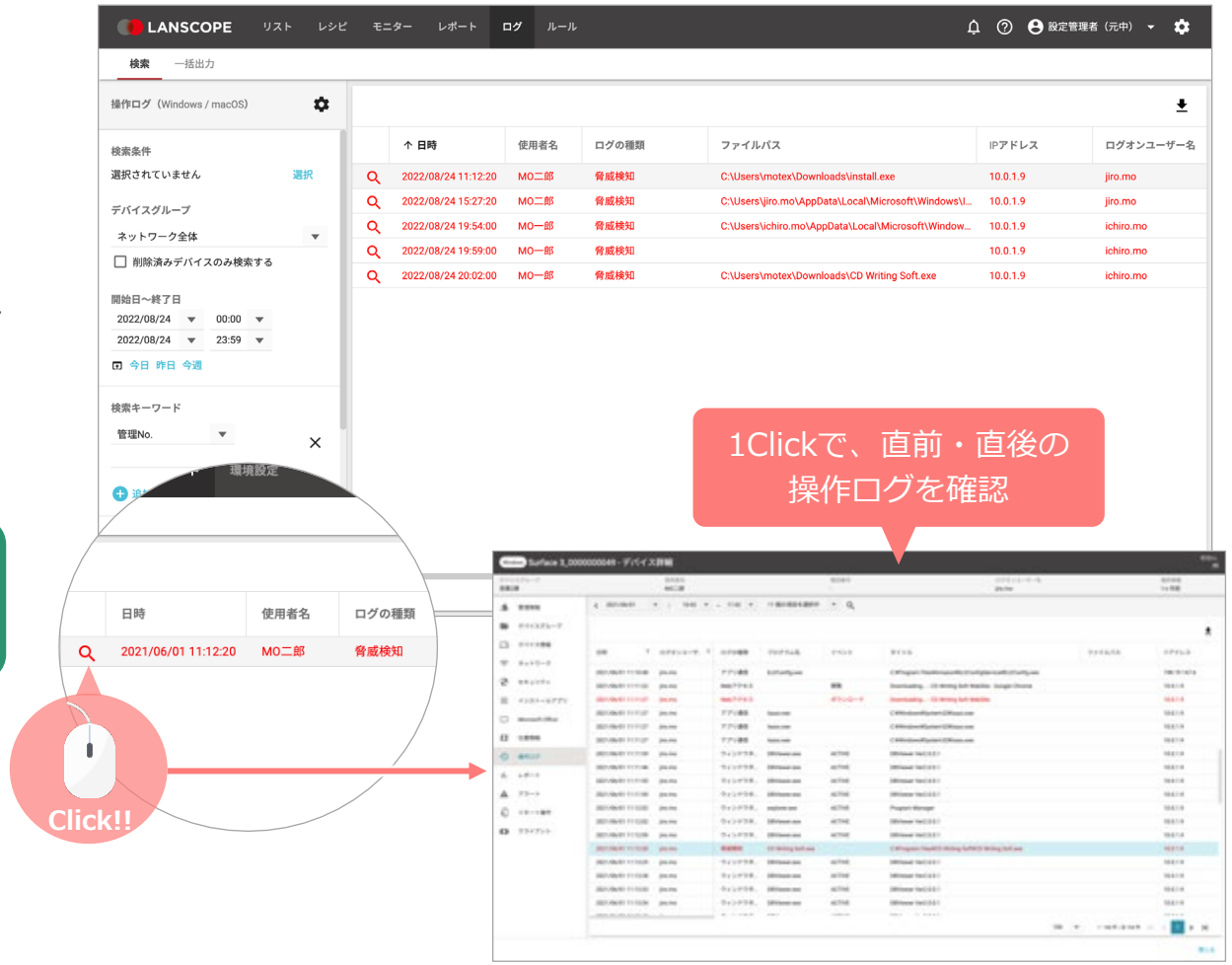
AI を活用した次世代型アンチウイルス製品と連携し、操作ログから、未知・亜種のマルウェア感染原因を特定

LANSCOPE Cyber Protection × Cloud LANSCOPE Endpoint Manager

AI を活用した「予測脅威防御」で、マルウェアの特徴点を見つけて実行前に検知・隔離します。エンドポイントマネージャー クラウド版と連携することで、マルウェアに感染してしまった直前の操作を特定。原因の追求や再発防止に活用できます。

- 検知率は99% *
未知のマルウェアも
検知・隔離
- PC への負荷が小さく
快適なパフォーマンス
を発揮
- クラウド型のため、
サーバー構築や
メンテナンスも不要

https://www.lanscope.jp/cpms/



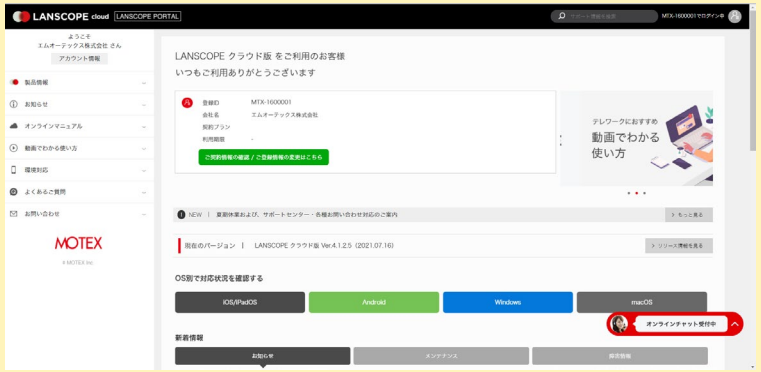
* 2018 NSS Labs Advanced Endpoint Protection Test / Unit 221B 調べ

Endpoint Manager Cloud

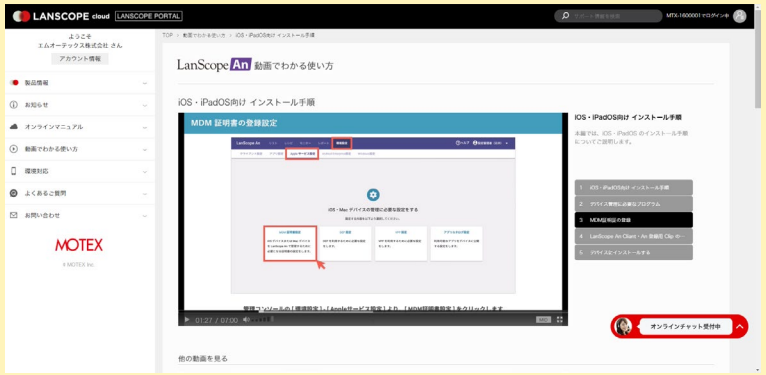
60日間無料体験キャンペーン中

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