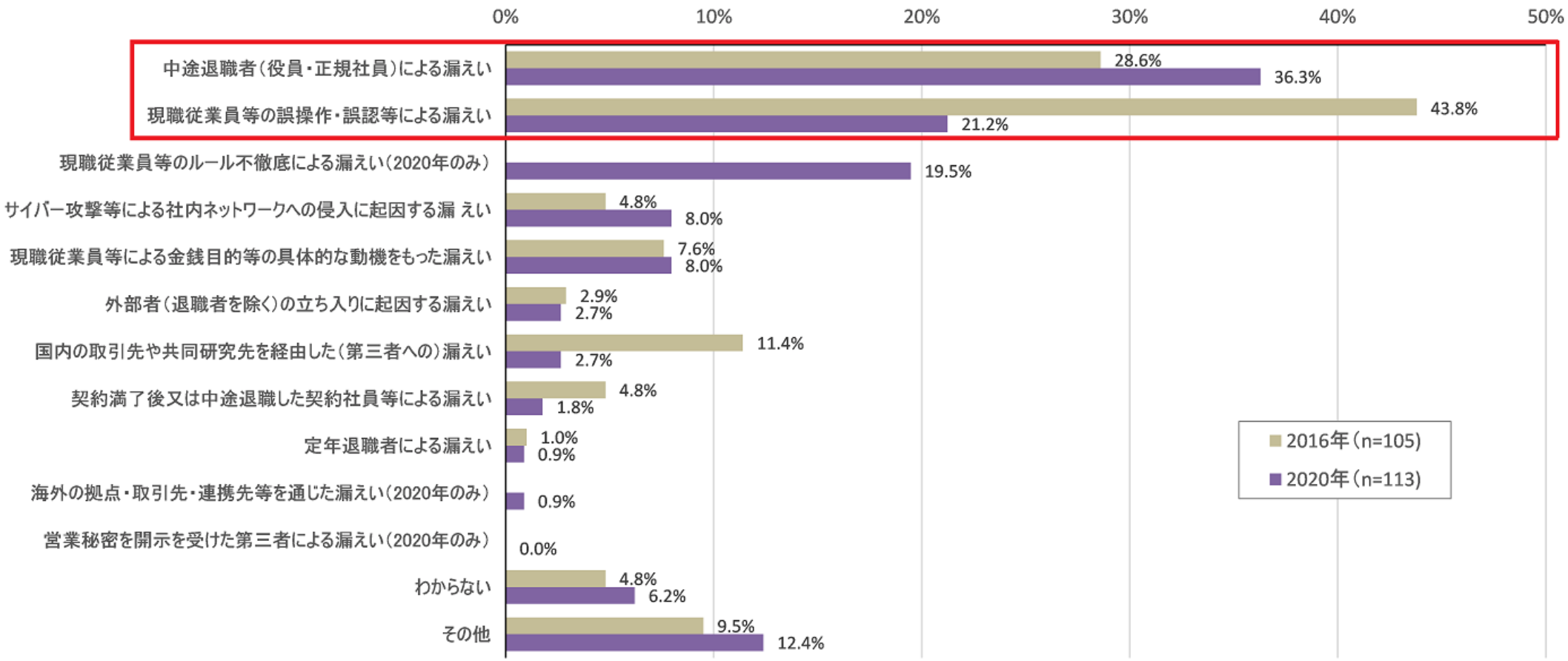
LANSCOPE cloud

知らなかったでは済まされない

改正個人情報保護法に備える

外部指摘で初めて発覚するケースも・・・自社のみならず委託先やグループ内など範囲が広いケースが増加

価値がある情報が故に社内や関係者からの悪意のある情報漏えいが急増しています



※引用IPA「企業における営業秘密管理に関する実態調査2020」報告書

社会情勢に合わせて３年ごとに見直し！2020年6月に改正個人情報保護法が公布されました

2005年4月に「個人情報」を保護するための法律として「個人情報保護法」が施行。その後も平成27年の個人情報保護法の改正以来、社会情勢の変化に伴い見直しが行われています。今回の改正は、令和元年１月に示した「３年ごと見直しに係る検討の着眼点」に即し、３年ごとに個人情報保護法の見直しを受け、反映したものです。

見直しの基準となる５つの視点

個人の
権利利益保護

外国事業者による
リスク変化への対応

保護と利用の
バランス

AI・ビッグデータ時代
への対応

国際的潮流との
調和

※引用元：PPC個人情報保護委員会「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱（概要）

改正個人情報保護法の６つのポイント！漏えい時の報告義務の強制とペナルティ制度が強化されています

1	個人の権利の在り方	利用停止・消去等の個人の請求権について、個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和する。保有個人データの開示方法について、電磁的記録の提供を含め、本人が指示できるようにする。個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。６ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。オプトアウト規定により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。
2	事業者の義務の在り方	漏えい等が発生し、個人の権利利益を害するおそれがある場合に、委員会への報告及び本人への通知を義務化する。違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する。
3	自主的な取組の仕組み	認定団体制度について、現行制度に加え、企業の特定分野(部門)を対象とする団体を認定できるようにする。
4	データ利活用の施策	イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。
5	ペナルティの強化	委員会による命令違反・委員会に対する虚偽報告等の法定刑を引き上げる。データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、法人に対しては行為者よりも罰金刑の最高額を引き上げる（法人重科）
6	法の域外適用・越境移転	日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

※引用：個人情報保護委員会事務局「改正個人情報保護法の基本」https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf

2. 事業者の義務が追加

情報漏えい時の報告が努力義務から義務化！現在のプライバシーポリシーの見直しが急務です

漏えい等が発生した時
個人情報保護法委員会と本人への通知が義務化

質的に侵害のおそれが大きい類型と、量的に侵害のおそれが大きい類型が報告等義務の対象となります。報告の方法も速報と確報に分けて報告することが求められています。

違法や不当な行為を助長する不適正な方法により
個人情報を利用してはならない旨が義務化

利用目的の範囲内での利用という制限に加え、違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならないことが義務化されました。

公表等事項として、事業者の住所及び代表者の氏名・
安全管理措置の内容・利用目的の特定の充実が追加

事業者の住所や法人の場合における代表者の氏名が公表等事項に追加、事業者が保有個人データについて講じている安全管理措置の内容も、改正法の施行令において公表等事項に加えられました。

「質的」「量的」に侵害の恐れが大きい類型に対して報告が求められています

単に漏えいしたデータ数だけで判断するのではなく、個人の権利利益に対する影響が大きいと考えられる、個人データの性質・内容、規模等が考慮されています

事態の類型	漏えい等報告・本人通知が必要となる場合	件数	例外
個人データの性質	要配慮個人情報の漏えい（おそれも含む）	１件以上	「高度な暗号化等の秘匿化」がされた個人データ
個人データの内容	財産的被害が発生するおそれがある場合（例：クレジットカード番号やインターネットバンキングのＩＤ・パスワード等）（おそれも含む）	―	
漏えい等の態様	故意による漏えい（例：不正アクセスや従業員による持ち出し等）（おそれも含む）	―	
大規模な漏えい	個人データの性質・内容、漏えい等の態様を問わず、大規模な個人データの漏えい	1000件以上	
漏えい等のおそれ	上記のおそれがある場合	―	

要配慮個人情報

本人の人種、信条、社会的身分、病歴、犯罪 の経歴、犯罪により害を被った事実など

財産的被害が発生するおそれがある場合

クレジットカード番号やインターネットバンキングのID・パスワード情報など

故意による漏えい

類型的に二次被害が発生するおそれがある不正アクセスや従業員による持ち出しなど

大規模な情報漏えい

内容が個人情報でなくても一定数以上の大規模な漏えい※1000人を基準

「おそれ」がある場合

漏えいの懸念があり漏えいが確定していない段階
※被害を最小限に

法定刑が個人・法人共に概ね引き上げ！特に法人の罰金刑の上限額が大きく引き上げられました

措置命令・報告義務違反の罰則について法定刑を引き上げ　/　法人に対する罰金刑を引き上げ

命令違反や虚偽の報告を抑止する効果を見越し、法定刑の引き上げが実施、特に法人は罰金刑が大幅に引き上げられています。

■ 改正前後の法定刑の比較

表1 改正前後の法定刑の比較

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会 からの命令への違反	行為者	６月以下	**１年以下**	３０万円以下	**100万円以下**
	法人等	-	-	３０万円以下	**１億円以下**
個人情報データベース等の不正提供等	行為者	１年以下	１年以下	５０万円以下	５０万円以下
	法人等	-	-	５０万円以下	**１億円以下**
個人情報保護委員会 への虚偽報告等	行為者	-	-	３０万円以下	**５０万円以下**
	法人等	-	-	３０万円以下	**５０万円以下**

※引用：個人情報保護委員会「令和２年 改正個人情報保護法について」https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

個人情報保護のために必要な４つの「安全管理措置」が掲げられています

事業者が個人情報の漏えいや滅失などの防止等のためにもうけられたのが「安全管理措置」（個人情報保護法20条）です

8-3 **組織的安全管理措置**	（1）組織体制の整備　（2）個人データの取扱いに係る規律に従った運用 （3）個人データの取扱状況を確認する手段の整備　（4）漏えい等の事案に対応する体制の整備 （5）取扱状況の把握及び安全管理措置の見直し
8-4 **人的安全管理措置**	従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。
8-5 **物理的安全管理措置**	（1）個人データを取り扱う区域の管理　（2）機器及び電子媒体等の盗難等の防止 （3）電子媒体等を持ち運ぶ場合の漏えい等の防止　（4）個人データの削除及び機器、電子媒体等の廃棄
8-6 **技術的安全管理措置**	（1）アクセス制御　（2）アクセス者の識別と認証　（3）外部からの不正アクセス等の防止 （4）情報システムの使用に伴う漏えい等の防止

情報を安全に保全するために、組織的にルールや体制構築することが求められています

（1） 組織体制の整備	**安全管理措置を講ずるための組織体制を整備しなければならない。** ・個人データの取扱いに関する責任者の設置及び責任の明確化　・個人データを取り扱う従業者及びその役割の明確化 ・上記の従業者が取り扱う個人データの範囲の明確化　・個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化 ・個人データの漏えい等の事案の発生又は兆候を把握した場合の責任者への報告連絡体制 ・法や個人情報取扱事業者で整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制
（2） 個人データの取扱いに係る規律に従った運用	**あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。** ・整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。 ・個人情報データベース等の利用・出力状況　・個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ・個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） ・個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）
（3） 個人データの取扱状況を確認する手段の整備	**個人データの取扱状況を確認するための手段を整備しなければならない。** ・個人情報データベース等の種類、名称　・個人データの項目　・責任者・取扱部署　・利用目的　・アクセス権を有する者 等
（4） 漏えい等の事案に対応する体制の整備	**漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。** ・漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡　・個人情報保護委員会等への報告　・再発防止策の検討及び決定　・事実関係及び再発防止策等の公表等
（5） 取扱状況の把握及び安全管理措置の見直し	**個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。** ・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。・外部の主体による監査活動と合わせて、監査を実施

従業者に個人データの適正な取扱いを周知徹底・教育することを求められています

従業者の教育	・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む。

個人情報の取り扱いに関わる機器をセキュアに管理するためのルール・体制構築が求められています

（1） 個人データを取り扱う区域の管理	**個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域及びその他の個人データを取り扱う事務を実施する区域について、それぞれ適切な管理を行わなければならない。** ・入退室管理及び持ち込む機器等の制限等。入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 　└間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止
（2） 機器及び電子媒体等の盗難等の防止	**個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。** ・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。）
（3） 電子媒体等を持ち運ぶ場合の漏えい等の防止	**個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。** ・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・封緘、目隠しシールの貼付けを行う。・施錠できる搬送容器を利用する。
（4） 個人データの削除及び機器、電子媒体等の廃棄	**個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。** ・（個人データが記載された書類等を廃棄する方法の例）焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 ・（個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例）情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。 ・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。

個人データ自体に対してセキュアに管理を行うためのルール・体制構築が求められています

（1） アクセス制御	**担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。** ・個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。
（2） アクセス者の 識別と認証	**個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。** ・（情報システムを使用する従業者の識別・認証手法の例）ユーザーID、パスワード、磁気・ICカード等
（3） 外部からの 不正アクセス等の防止	**個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。** ・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。
（4） 情報システムの使用に 伴う漏えい等の防止	**情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。** ・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。

従来の「個人情報保護法」で定められたガイドラインに加え、時勢を踏まえ改正
情報漏えい時には報告が「完全義務化」、法令違反時の罰則金が引き上げされるなど厳格化

1. 情報漏えい時の報告が、**努力義務** から **完全義務化** へ

2. 報告は **速報** と **確報** の二段階で報告

3. 罰則引き上げ！ 法人は **最大１億円** の罰則

LANSCOPEで対応できる改正個人情報保護法対策

情報漏えいをさせない体制と、万が一の対策

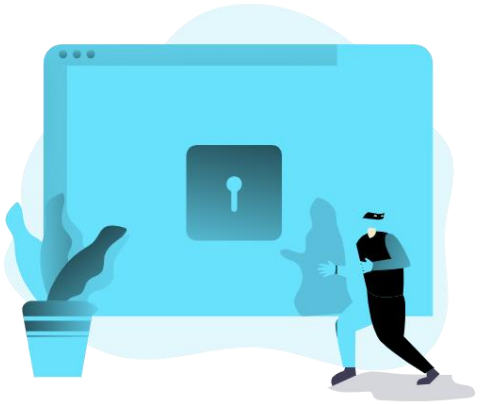
「安全管理措置」で求められている講ずべき措置に対し、様々な対策が行えます

LANSCOPE は情報漏えいをさせない「体制構築」と「万が一の対応」が可能です

情報漏えい対策

「組織的安全管理措置」「技術的安全管理措置」対応として誰が・どのデータに対し・何を行ったか**操作履歴を取得、問題操作をリアルタイムに察知・対策する**ことで情報漏えいをさせないための体制づくりを支援します。

外部脅威対策



「技術的安全管理措置」対応として、常に最新のバージョンを保てているかどうか、**脆弱性の有無を可視化**。対策することでセキュリティホールを無くし、外部からの脅威対策を打つことが可能です。

セキュリティ啓蒙

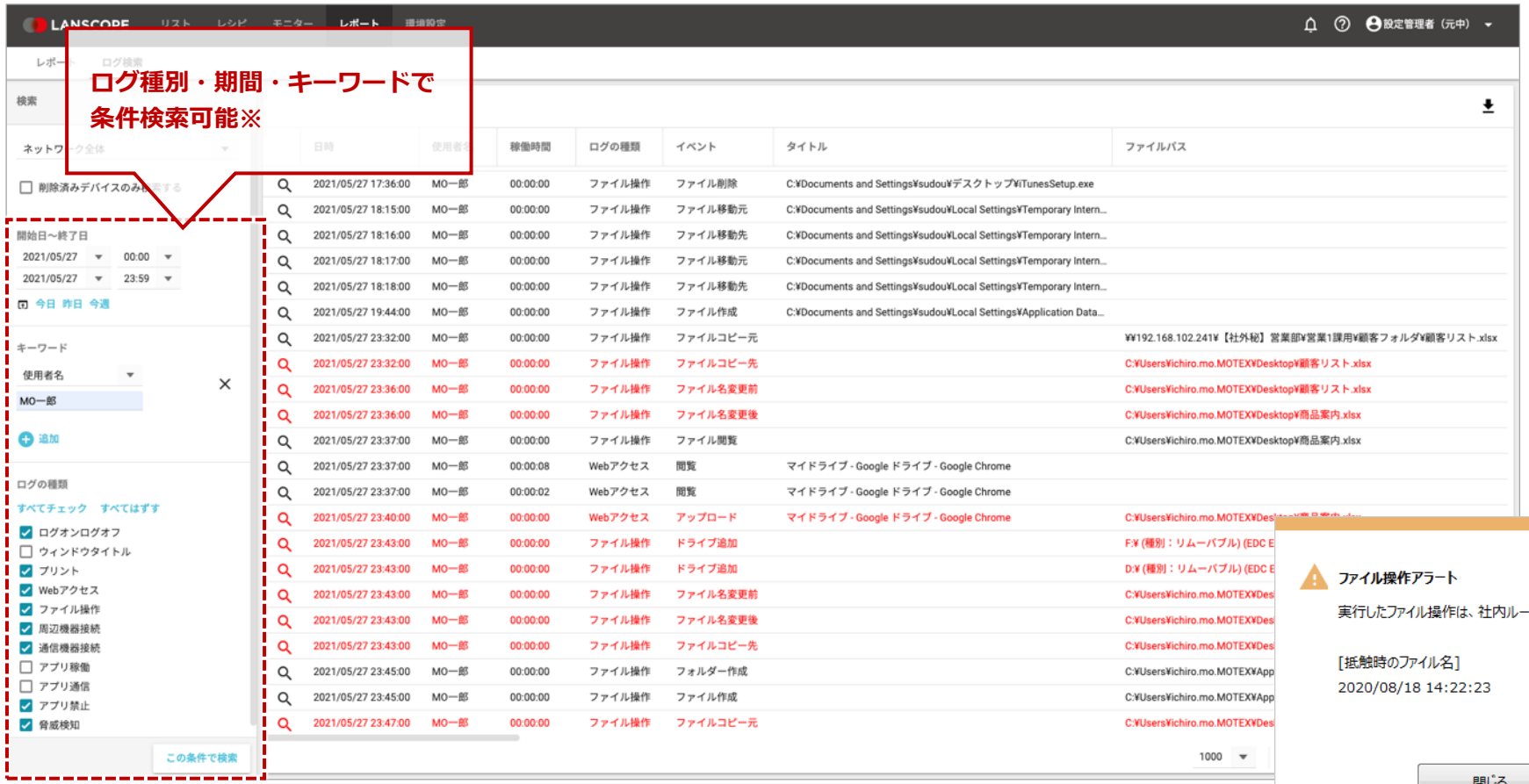
「人的安全管理措置」対応として、従業員に対する**セキュリティ教育で周知・教育・訓練**するための様々な啓蒙コンテンツを提供しています。

情報漏えい対策

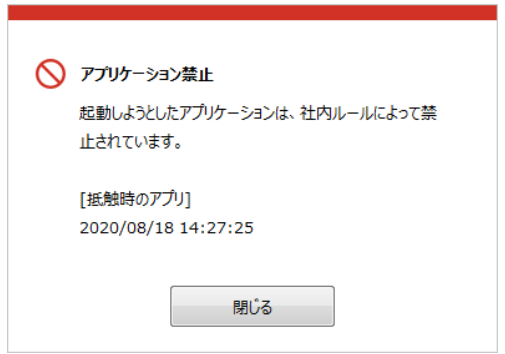
操作ログ管理・BitLocker管理・盗難紛失対策

どのPCで・誰が・いつ・どんな操作をしたかを記録し、万が一情報漏えいが発生した際に報告に活用できます

正しい操作を証明するための証跡や、違反操作があった場合、ユーザーや管理者に通知し抑止効果を発揮



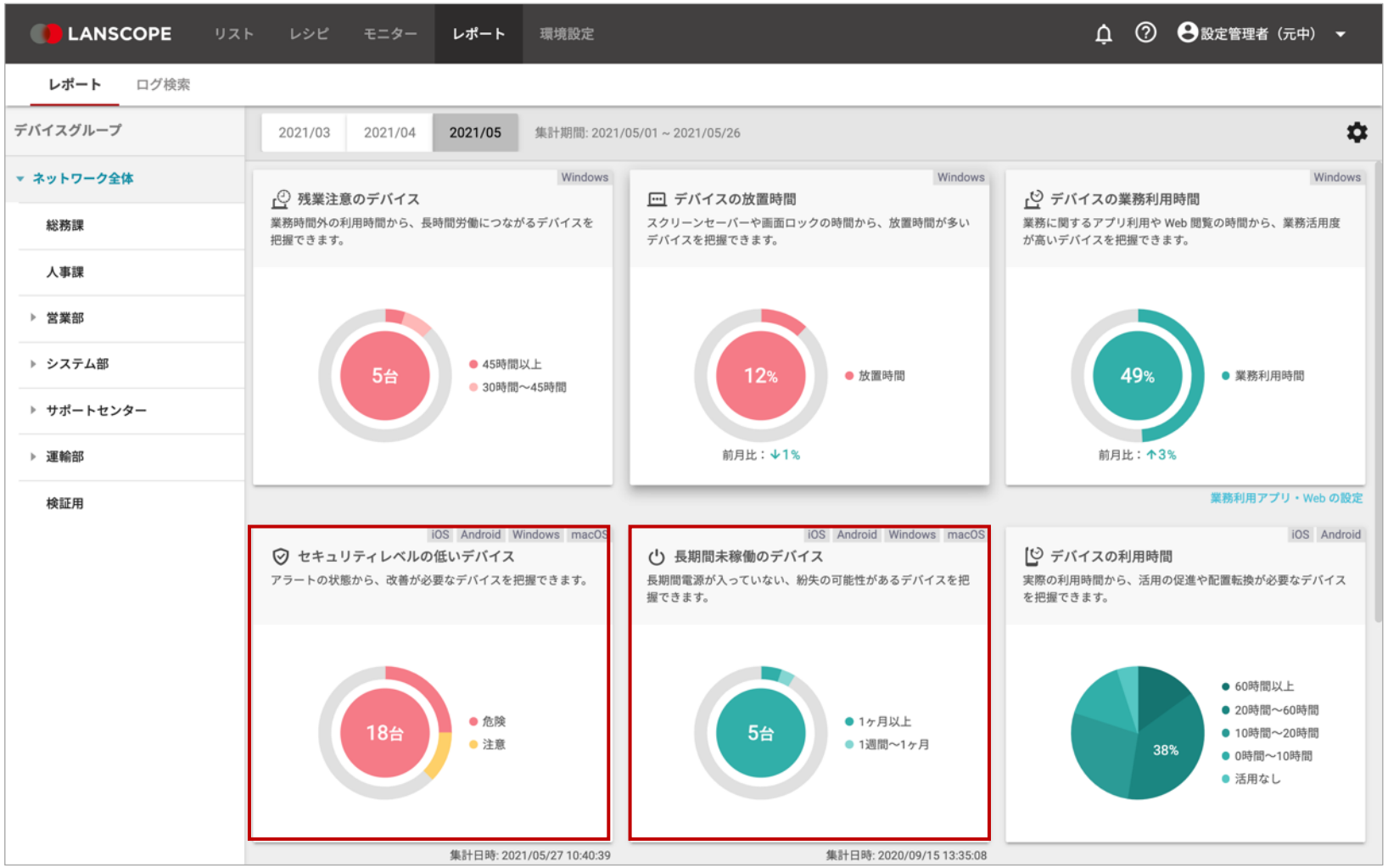
取得できる操作ログ（Windows）
ログオン・ログオフログ
ウィンドウタイトルログ・アプリ利用ログ
ファイル操作ログ（コピー／移動／作成／上書き／削除／名前の変更）
記録メディアの追加／削除、書込みログ
Web サイト閲覧ログ
Web サイト アップロード／ダウンロード／書込みログ
プリントログ
通信機器接続ログ（Wi-Fi／Bluetooth）



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

※ 管理コンソール上で検索できるログは当日を含む過去100日分です。
※ 期間・対象デバイスを指定し CSV 形式で一括出力が可能です。指定できる期間は過去2年分です。
別途オプション（ログ運用オプション）を購入することで、過去5年分を指定して出力可能です。

収集したログを自動でレポーティング！様々な視点からセキュリティリスクの有無を把握できます



<レポート活用例>

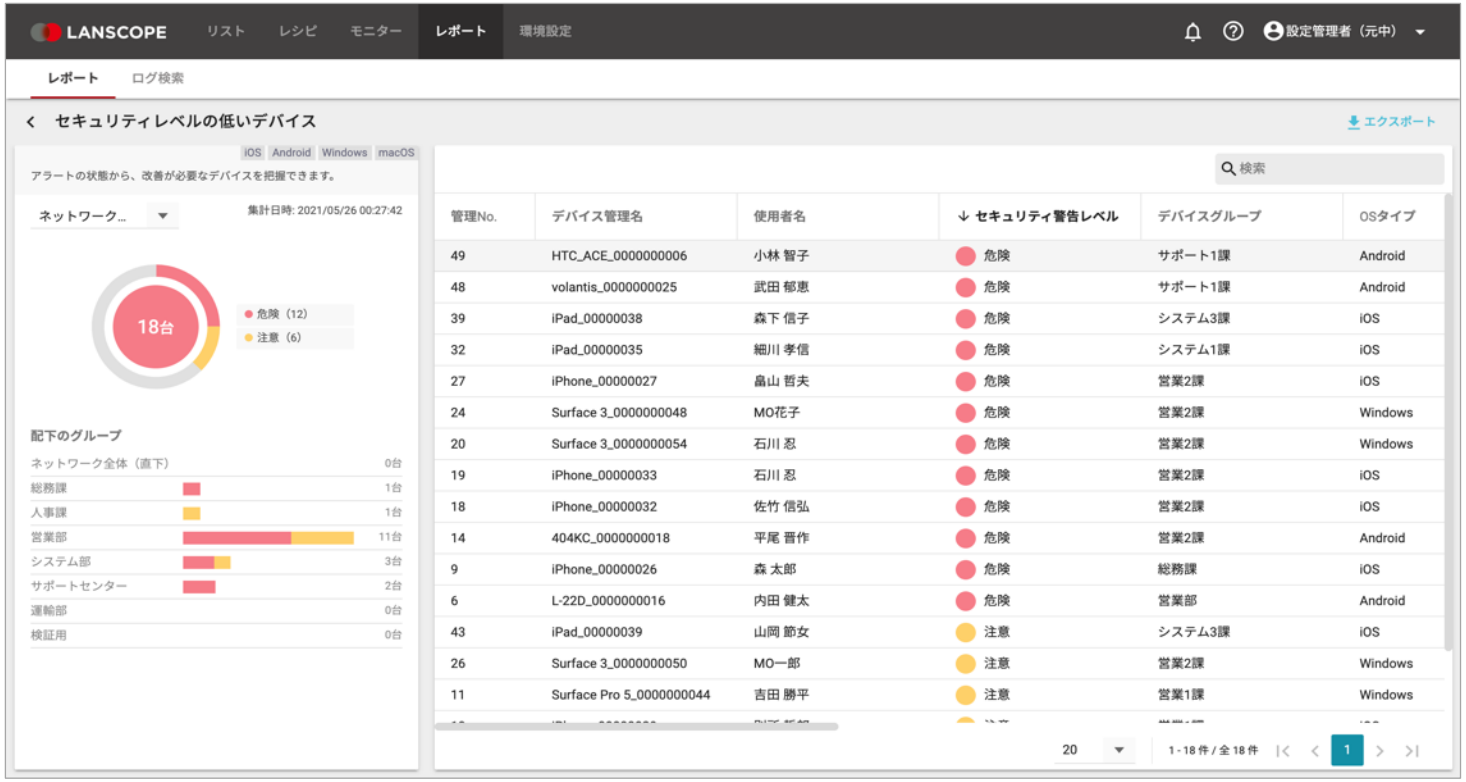
- **セキュリティレベルの低いデバイス**

  アラートの状態から改善が必要なデバイスを把握できます。セキュリティレベルは、「危険」「注意」で表示され、対策の有無を一目で把握できます

- **長時間未稼働のデバイス**

  長時間電源が入っていないデバイスの台数を表示。未稼働＝故障以外にもデバイス紛失の可能性があるため、対策する必要があります

クリックすると詳細情報を表示！デバイスがルールに従って適切に利用されているかを把握

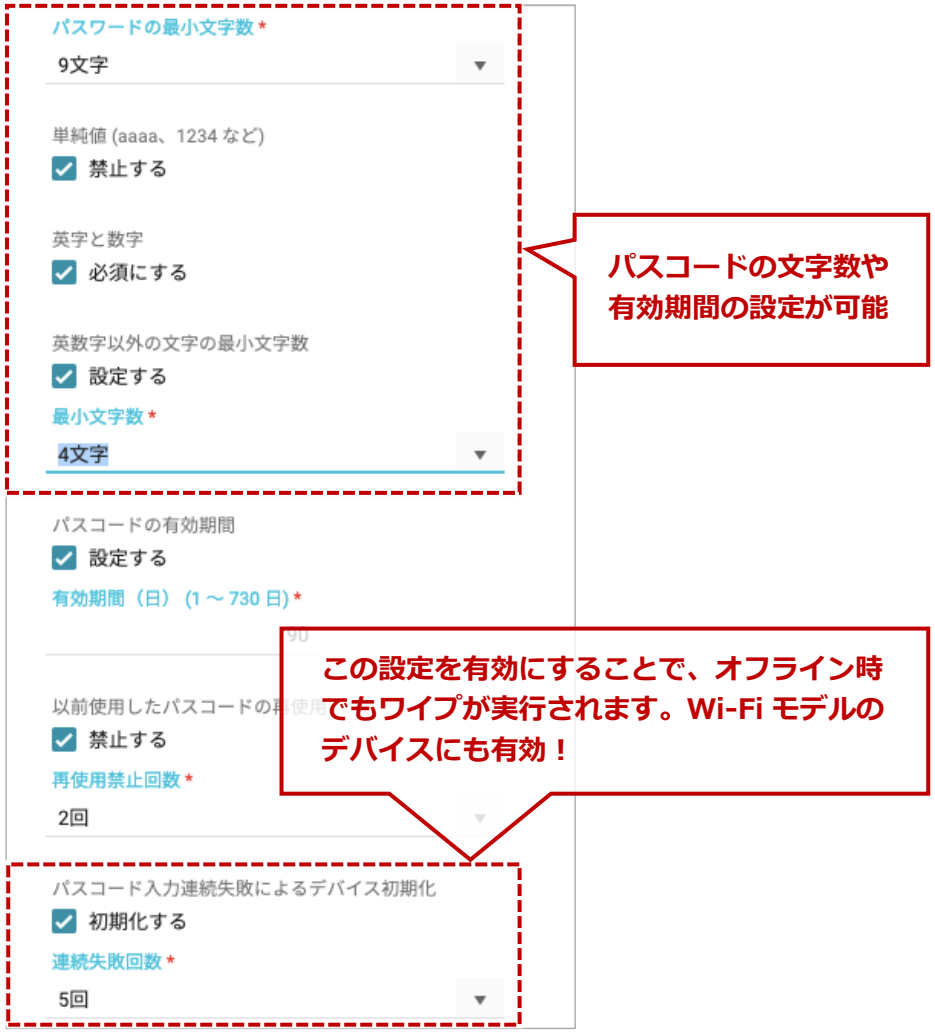


危険/注意の警告レベルを設定し、柔軟な設定が可能！

設定したアラートは「危険」「注意」のレベルに振り分けることが可能です。アラート内容を管理者に通知することも可能で、例えば「『危険』のアラートが発生した時のみ、管理者にメールを送る」など柔軟な設定・管理を実現します。

設定できるアラート	i	A	W	m
パスワードポリシーに準拠していない	○	○	—	—
パスコードロックの設定がオフになっている	○	—	—	—
デバイスが管理外になっている	○	—	○	○
LANSCOPE Client のバージョンが最新になっていない	○	○	○	—
未稼働期間が指定された期間を超過している	○	○	○	○
空き容量が不足している	—	○	○	○
位置情報が取得されない設定になっている	—	○	○	—
指定したアプリがインストールされていない	○	○	○	○
指定したアプリがインストールされている	○	○	○	○
指定したアプリが実行された	—	○	—	—
新しくアプリがインストールされた	○	○	○	○
新規プロファイルがインストールされた	○	—	—	○
デバイスの設定がリモート操作の実行条件を満たしていない	—	○	○	—
デバイスが不正に改造されている（Jailbreak/root化）	○	○	—	—
SDカードが抜き差しされた	—	○	—	—
SIMカードが抜き差しされた	○	○	○	—
OS バージョンが指定した範囲外になっている	○	○	—	—
もうすぐリース切れになる	○	○	○	○

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の設定項目	Androidの設定項目※
パスコードの最少文字数	パスワードの最少文字数
単純値（aaaa、1234など）を禁止	使用しなければならない文字の種類
英字と数字が必要	パスワードの有効期間
英数字以外の文字の最少文字数	パスワードの有効期限を事前の通知
パスコードの有効期間	以前使用したパスワードの再使用を禁止
以前使用したパスコ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
パスコード入力連続失敗によるデバイス初期化	パスワード入力連続失敗によるデバイス初期化
パスコードの設定ルールを一括で設定・配布	スリープ開始までの最大許容時間
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	

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。情報漏えいを防ぐためにも、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。

万が一の対策として暗号化は必須！OS 標準搭載の BitLocker を活用するための機能を搭載

BitLocker 設定有無の確認

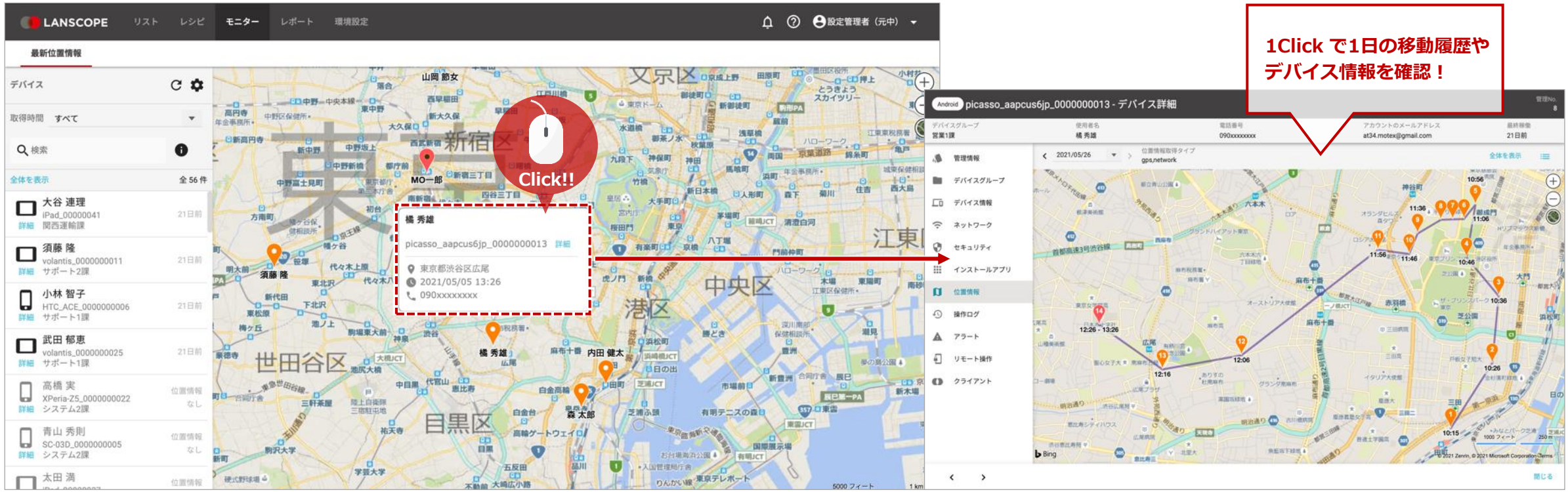
BitLocker を利用したリモートワイプが実行できるよう設定が有効になっているか確認できます。

BitLocker 回復キーの管理

回復キーを自動収集できるので、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。

情報漏えい対策

最新位置情報を1画面で表示！その日どのように行動したのか？移動履歴の取得！



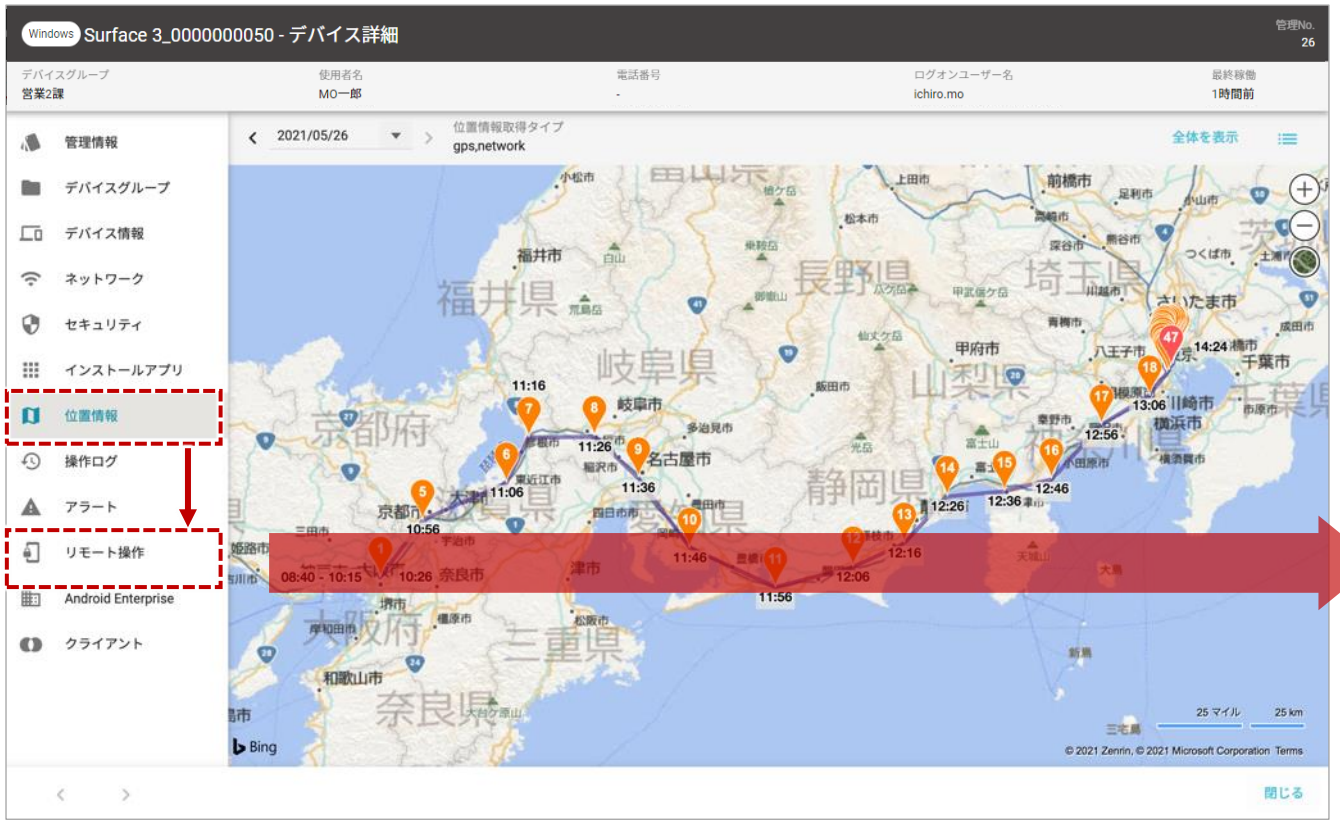
複数の位置情報をまとめて見たい時に最適！

一般的な MDM 製品の場合、1台ずつ Google Map にリンクし位置情報を確認しなければならず、複数のデバイスの位置情報を確認したい時に不便です。LANSCOPE なら、管理コンソールに地図画面を組み込んだ設計のため、他ページにリンクする必要なくコンソール上で確認できます。

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。

紛失時の対策は位置の確認とリモートロック・ワイプ

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えいを防止！



※ 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 はスリープ状態の場合、位置情報が取得できません。
※ Windows Server OS・macOS デバイスは位置情報取得機能には対応していません。

情報漏えい対策

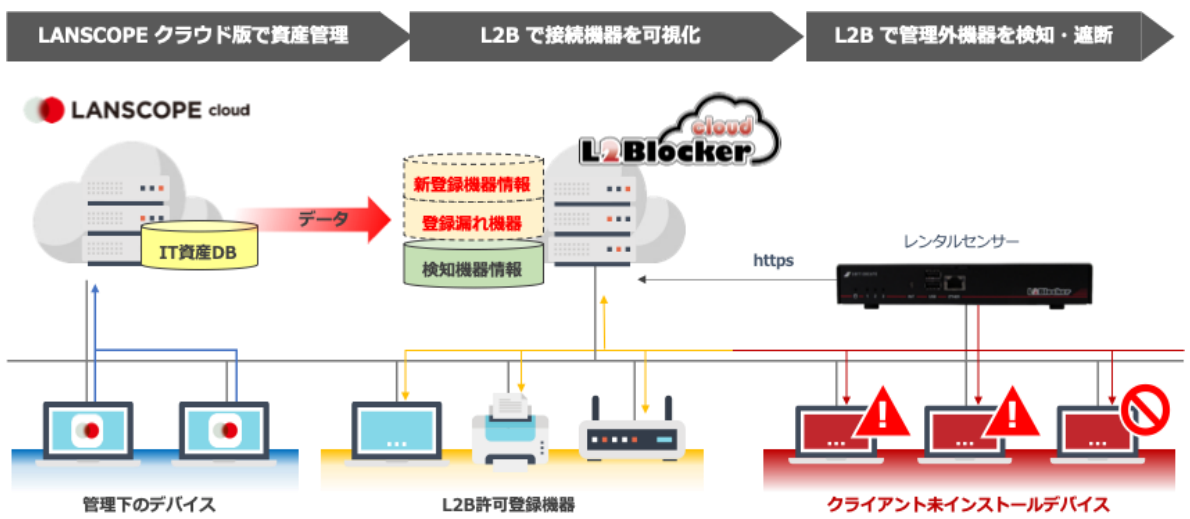
管理外デバイスの社内ネットワークへのアクセスを検知・遮断
LANSCOPE クラウド版の管理下にないデバイスの発見にも貢献します。

L2Blocker cloud × LANSCOPE cloud

社内ネットワークへの管理外デバイスからの不正接続を検知・遮断できます。
LANSCOPE クラウド版と連携することで、LANSCOPE クラウド版の管理外の PC を自動検知・遮断し、警告画面から LANSCOPE のクライアントのインストールを誘導することも可能です。

- 2005年販売開始 豊富な導入実績 2,000社以上
- 既存のネットワーク構成を変更することなく導入可能
- 初期費用を抑えて管理サーバーをクラウド化

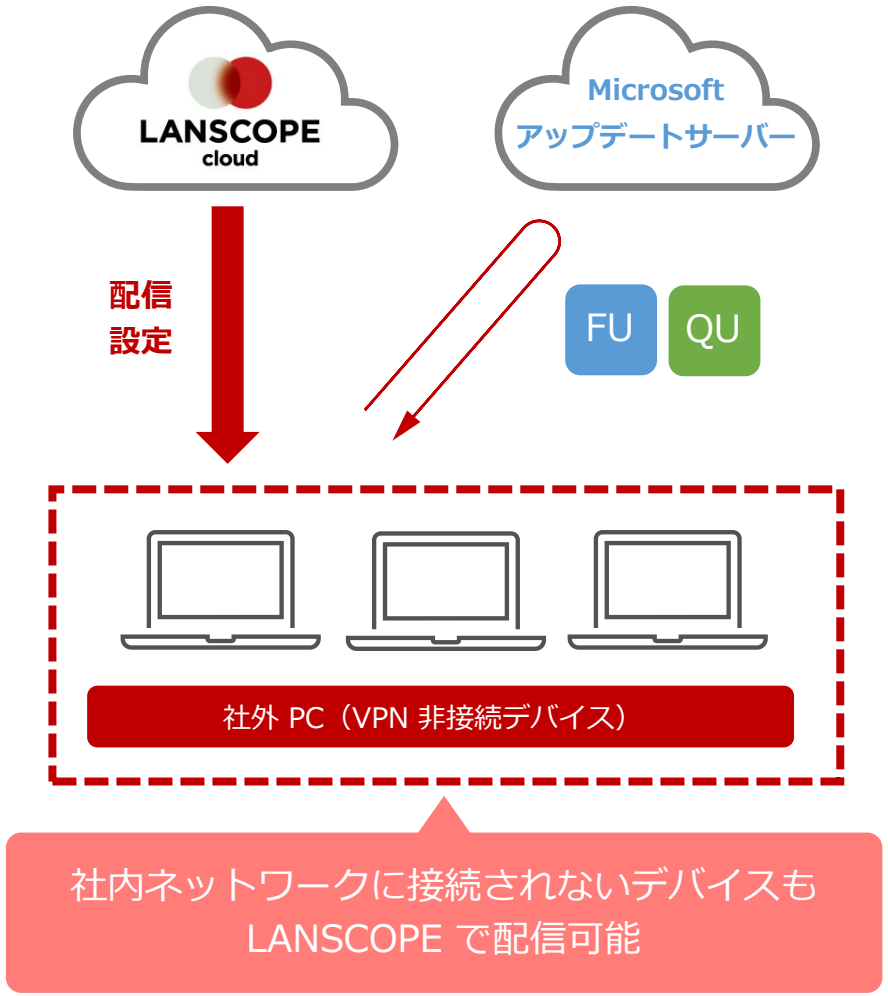
https://www.l2blocker.com/

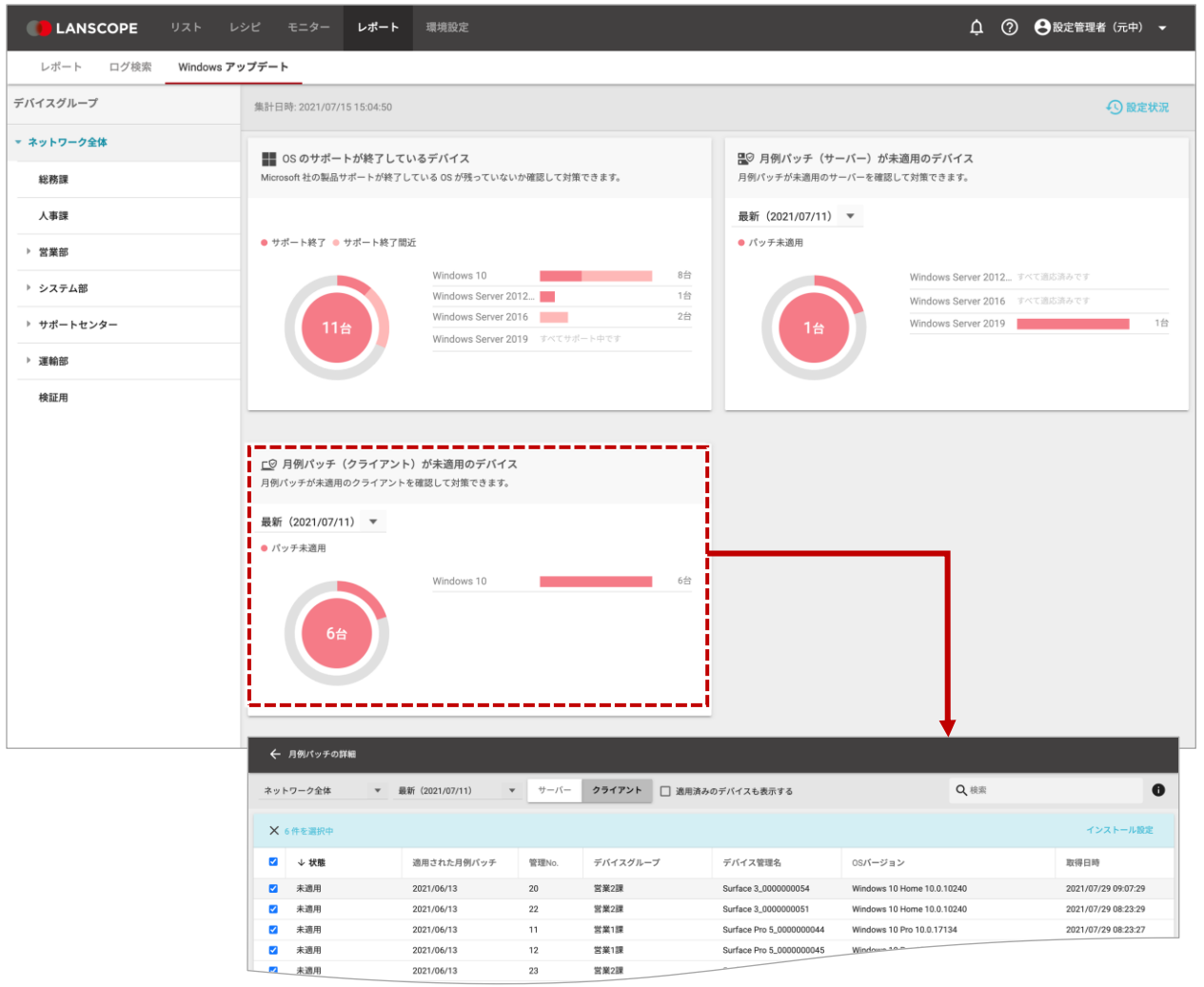


外部脅威対策

脆弱性対策・マルウェア対策

機能更新・品質更新プログラムの適用状況を、“視認性の良い” レポート形式で把握
1Click で未適用デバイスを確認し、最新のプログラムを適用



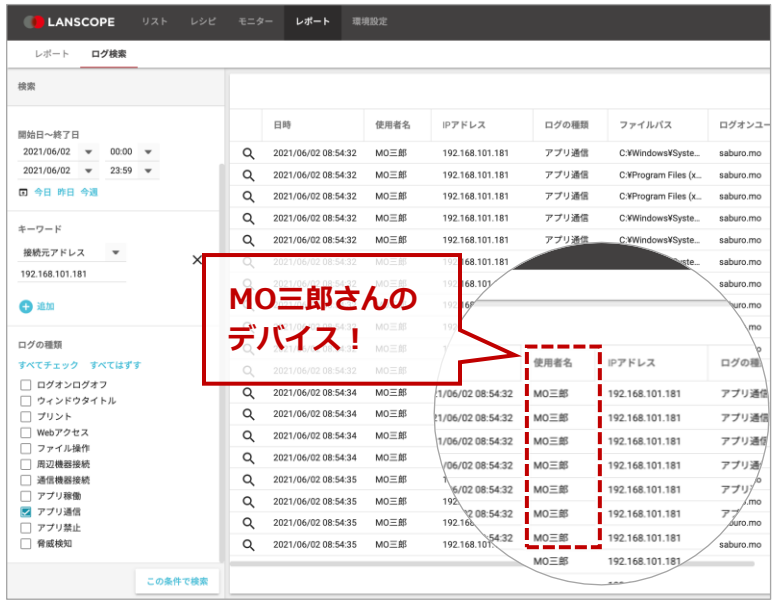


次世代 F/W から不審な通信を検知した場合、取得した操作ログから原因調査を行えます。

次世代 F/W で取得で取得できる情報は、基本的に通信先や通信もとの IP アドレス、使用されたポート番号など限定的です。LANSCOPE では、通信元・通信先の IP アドレスを利用して、以下の調査を行えます。

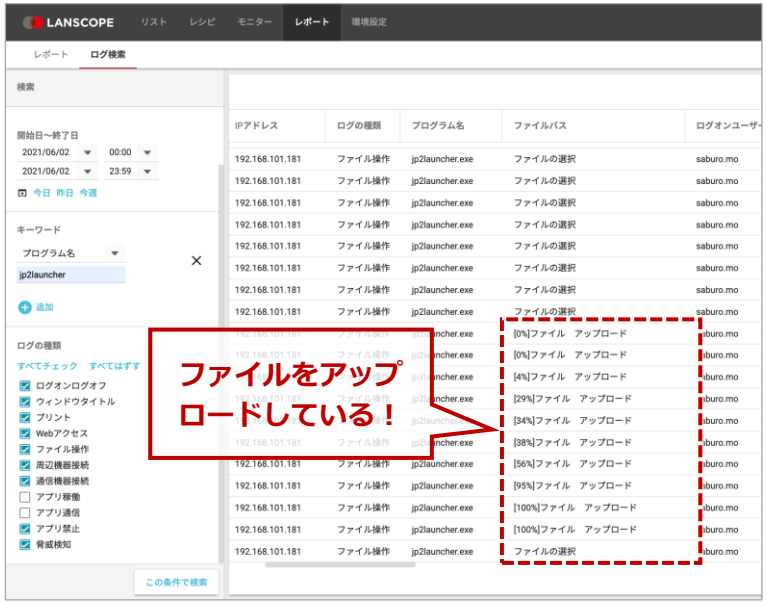
1. どの PC から不審な通信が発せられたのか？
2. 不審な通信の原因となったアプリはどれか？
3. そのアプリを使って何をしていたのか？

Step 1 IP アドレスよりデバイスを特定



Step 2 不審な通信の原因となったアプリを特定

Step 3 このアプリを利用して何をしていたのか確認



Webアクセス状況を把握し、リスクある閲覧をカテゴリ指定で柔軟に制御することが可能

カテゴリ毎にクリックするだけで、関連するWebサイトをを制御！閲覧以外にも書き込み制御も可能

外部脅威対策

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

CPMS Cyber Protection Managed Service × LANSCOPE cloud

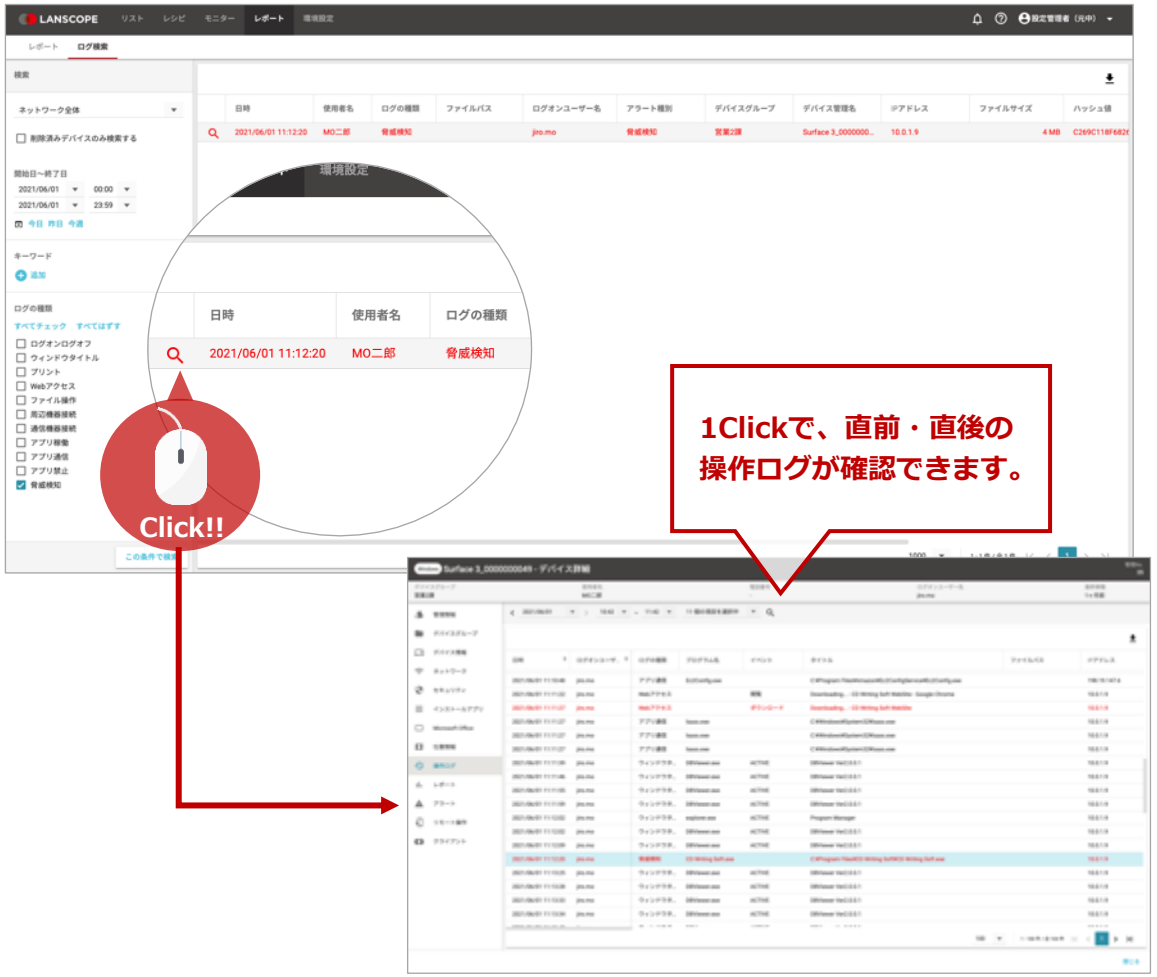
マシーンラーニングの特許技術を活用した「予測脅威防御」で、マルウェアの特徴点を見つけて実行前に検知・隔離します。LANSCOPE クラウド版と連携することで、マルウェアに感染してしまった直前の操作を特定。原因の追求や再発防止に活用できます。

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

月額450円/台から！
ニーズに合わせて
必要なプランを選択

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



* 2018 NSS Labs Advanced Endpoint Protection Test 結果より

未知・亜種のマルウェアも事前検知・隔離！運用工数を最大限に下げたウイルス対策が実現

AIによる予測防御検知を実行。シグニチャレスなので毎日のアップデートは不要で管理者・従業員にも負荷をかけません

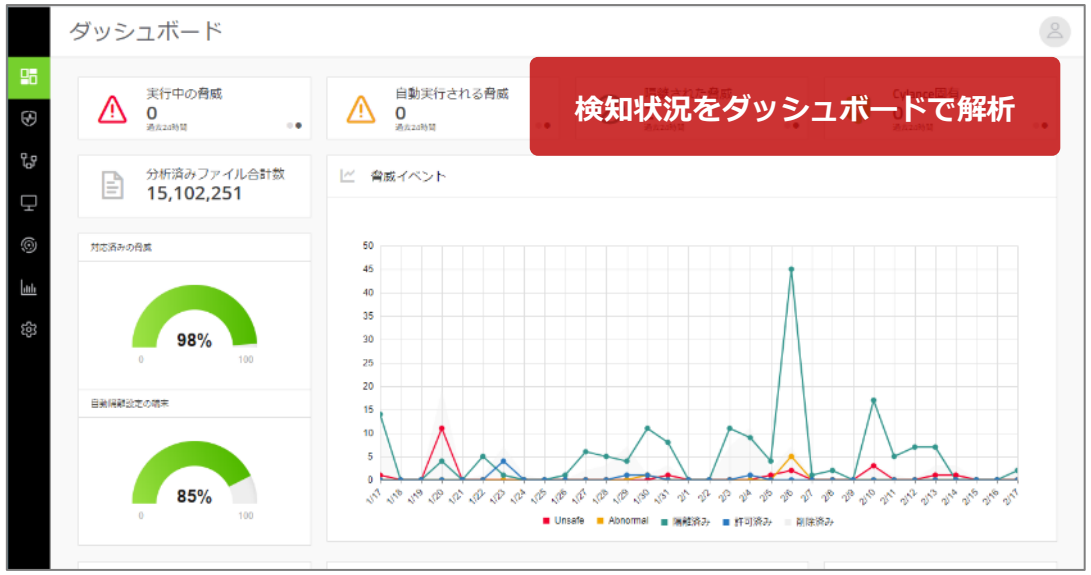
DNAレベルの
マルウェア解析

AIによる自動判断
感染前検知・隔離

シグニチャレス
検知

アップデートは年１
ネットワーク負荷減

非ネット環境下でも
検知・隔離可能



検知したマルウェア以外の「端末に潜む脅威」を発見、攻撃の流れを操作を紐づけて可視化

BlackBerry Protect の検知力に加え、調査・封じ込め・復旧まで一連の対応が可能で、負荷の少ないDER機能です

攻撃防御	検知	調査	封じ込め	復旧
BlackBerry Protect	機械学習を活用したCAE（コンテキスト分析エンジン）で攻撃を検知	BlackBerry Optics インシデントや脅威の根本原因調査	脅威の痕跡が見つかった端末をネットワークから直ちに隔離	リモートスクリプトの実行やフォレンジック用の証拠取得

BlackBerry Protectと統合

AIを活用

予防にフォーカス

※BlackBerry Optics の導入が必要です。詳細はお問合せください

セキュリティ啓蒙

従業員に対するセキュリティ教育で周知・教育・訓練

内部規定等の周知・教育・訓練の実施に最適なのがMOTEXが提供している**「セキュリティブック」**です。全ページWebからPDFを無料ダウンロード可能。
また、本書を元にした社内や学校などでセキュリティの研修で活用できる**「講師用資料」**と、その後の復習に活かせる**「テスト」**も無料でPDFを公開しています。

「セキュリティ 7つの習慣・20の事例」PDFデータは、無料でDLできます！ http://www.motex.co.jp/vision/enlightenment_activity/education_book/

LANSCOPE クラウド版とは

PC・スマホを一元管理！IT資産管理・MDM「LANSCOPE クラウド版」

PC・スマホを一元管理！IT資産管理・MDM

LANSCOPE cloud

- iOS・Android・Windows・macOS を一元管理
- Apple・Google の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/an/

ご検討中のお客様向けコンテンツ

安心してご導入いただけるよう、さまざまなコンテンツをご用意しております。

お申し込みは LANSCOPE クラウド版 製品サイトより可能です。

オンライン商談

お客様の自席で管理コンソールや
ご提案資料をご覧いただきながら
製品をご紹介致します。

60日間無料体験

導入前に LANSCOPE の機能や
操作感を60日間無料で体験できます。
無料体験期間中もサポートセンターを
ご利用いただけます。

資料ダウンロード

導入をご検討いただく際に参考と
なる各種資料をダウンロードできます。

簡単お見積

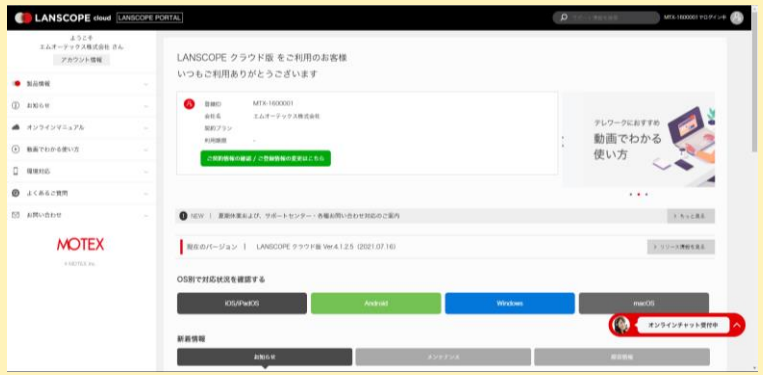
お客様の導入構成に合わせて
価格をご確認いただけます。

LANSCOPE cloud

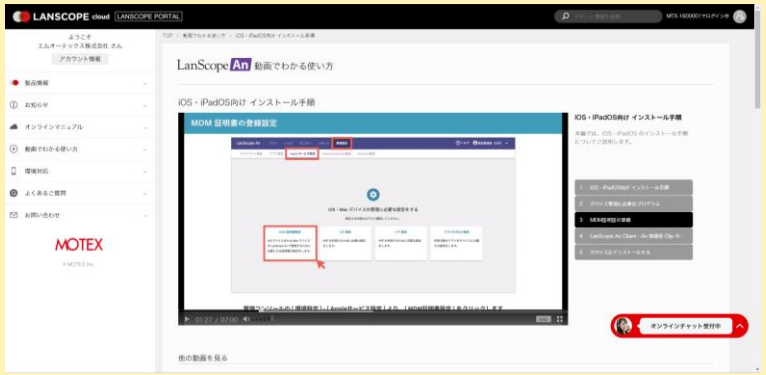
60日間無料体験キャンペーン中

LANSCOPE クラウド版の体験版は 60日間たっぷり利用できます。十分に機能を検証していただき、ご検討ください。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

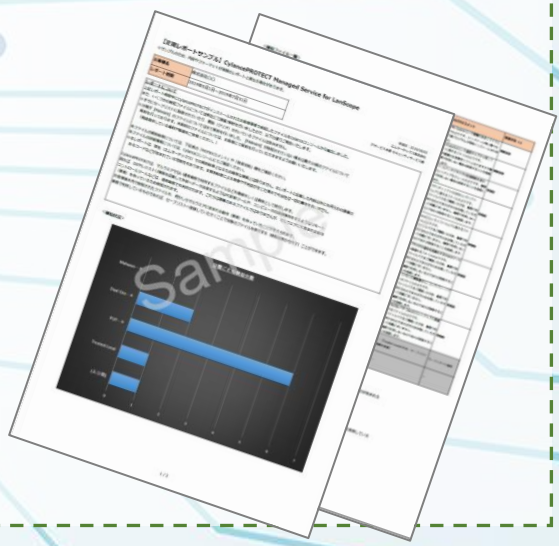
BlackBerry Protect

AIアンチウイルス無料体験実施中

～BlackBerry Protectを気軽に使ってみよう～

最新AIを活用した新技術で超高精度の検知率を誇る「BlackBerry Protect」を**1ヶ月無料**で**何台でも体験**できるキャンペーンがスタートしました。実際に自社のPCにBlackBerry Protectをインストールし、コンソールの操作方法や検知力の高さを体験いただけます。

体験終了後、エムオーテックスにて**検知結果のサマリーレポートをご提供**します。
AIを活用した最新鋭のアンチウイルス製品を、この機会にお気軽にご体験ください！



●お申し込みはこちらから

https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr

本資料は2022年4月施行の「令和２年 改正個人情報保護法について」（2021年7月時点の情報）に基づいて作成しています
あくまで抜粋・まとめ版となりますので、正式版もご参照いただくことを推奨します
個人情報保護委員会：https://www.ppc.go.jp/personalinfo/

エムオーテックス製品に関する問い合わせは下記にて受付いたします
sales@motex.co.jp