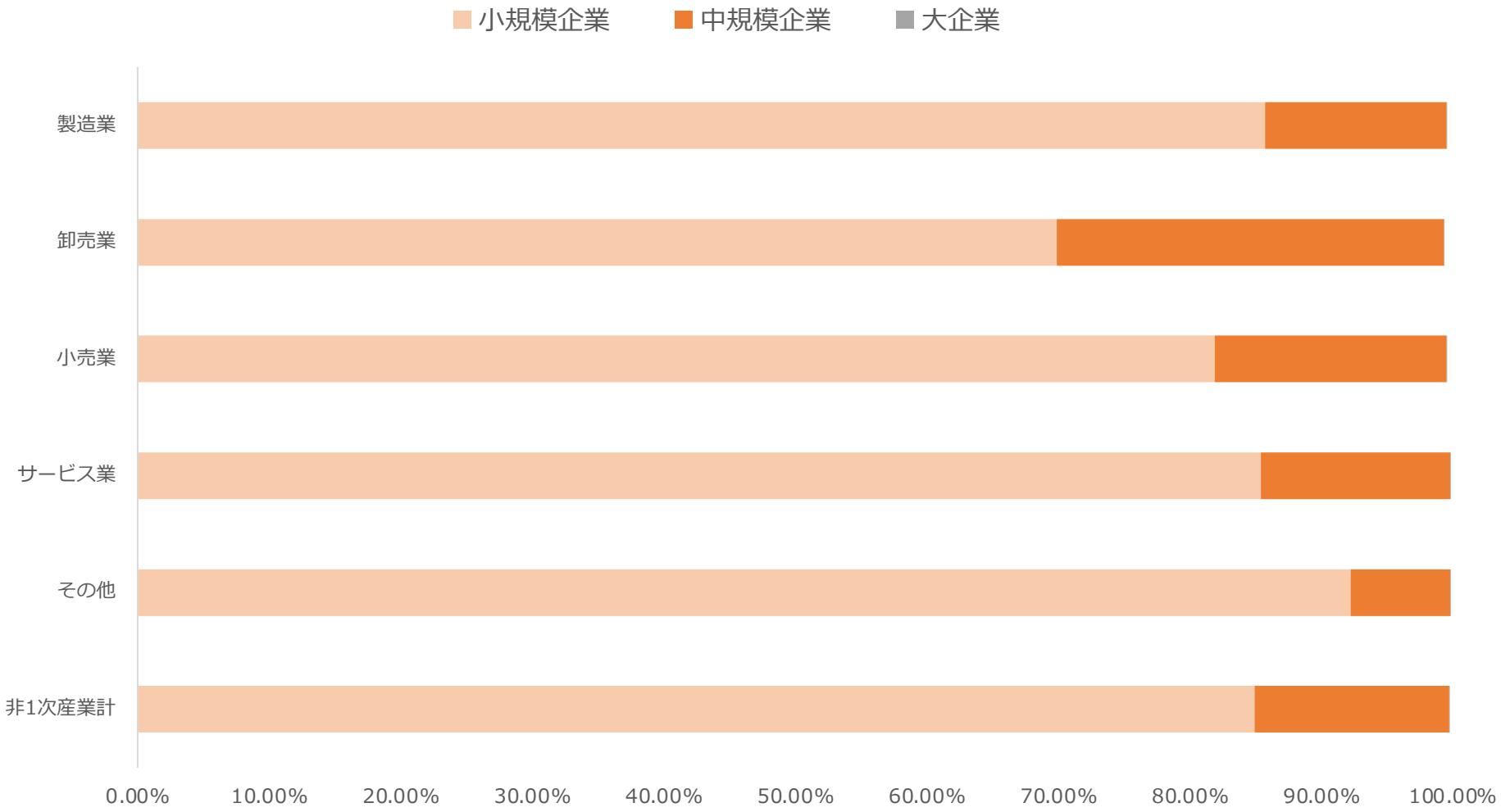
Cloud
LANSCOPE
Endpoint Manager

従業員100名～300名の中小企業様ならではの課題を解決！
事例から見る エンドポイントマネージャー活用術をご紹介

中小企業の割合

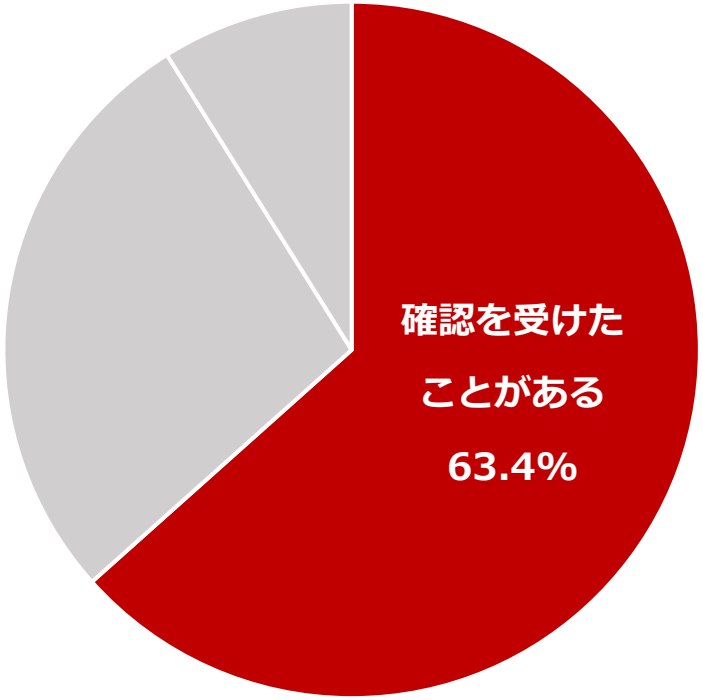
中小企業は日本企業の99%以上を占める



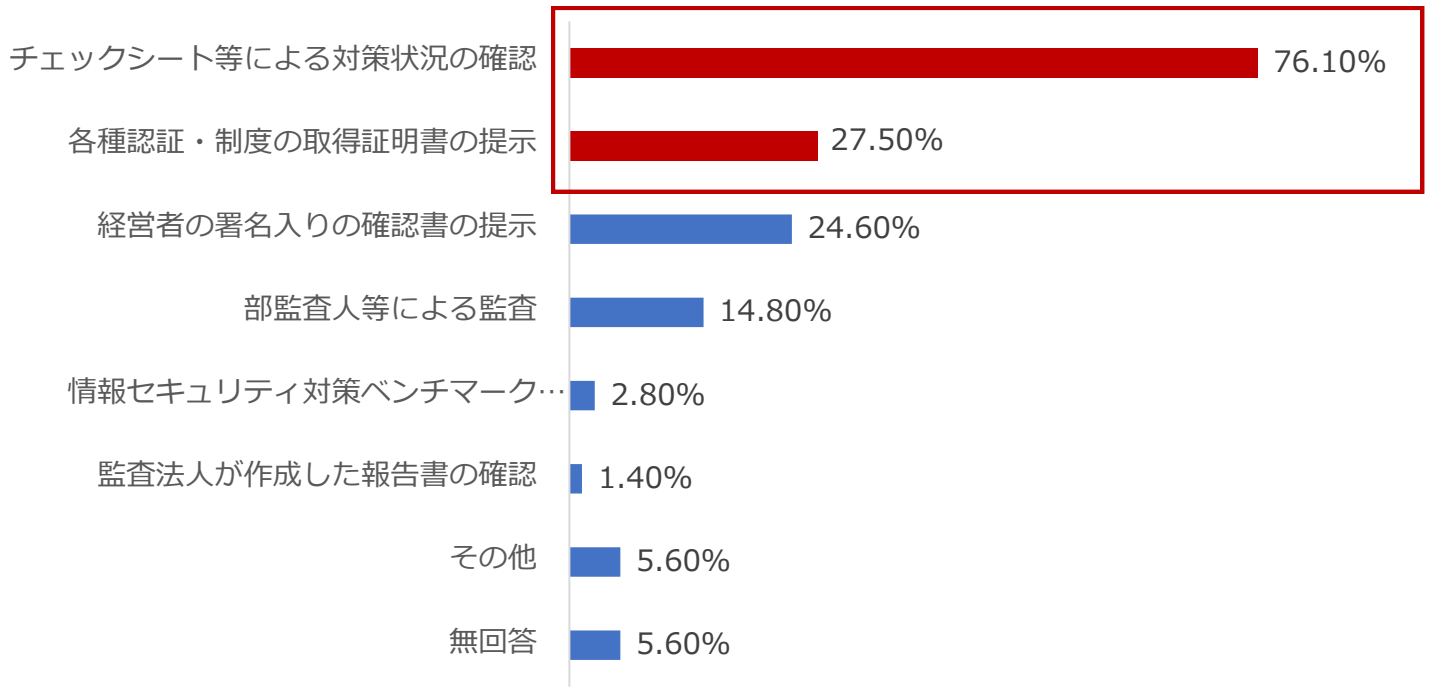
※ 総務省・経済産業省「平成28年経済センサス – 活動調査」

取引先から ISMS や Pマーク等の認証やセキュリティチェックシートの提出が求められる機会が多い

取引先からの情報セキュリティ対策に関する要求実態※



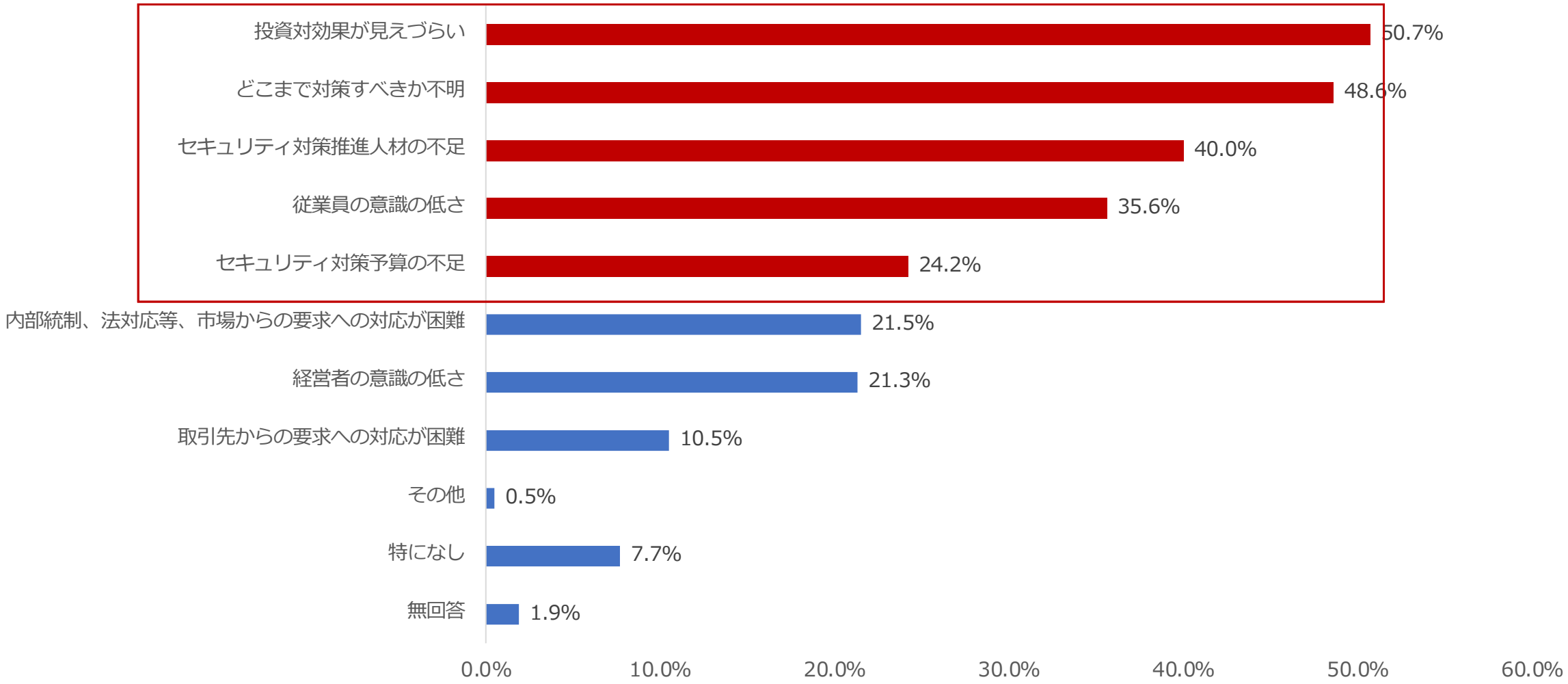
取引先からの情報セキュリティ対策確認方法※



※独立行政法人　情報処理推進機構中小企業の情報セキュリティ対策　確認手法に関する実態調査

中小企業のセキュリティ課題

コスト・対策範囲・従業員の意識などセキュリティ対策の実施に課題を感じている



※独立行政法人　情報処理推進機構中小企業の情報セキュリティ対策　確認手法に関する実態調査

導入事例から見る「これだけは押さえておきたいセキュリティ対策」

・導入事例①　IT 資産管理（PC・スマホ）
・導入事例②　情報漏洩対策（PC）
・導入事例③　脆弱性・標的型攻撃対策（PC）
・導入事例④　盗難紛失対策（スマホ）
・導入事例⑤　アプリ管理（スマホ）

PC・スマホ・タブレットの一元管理を実現
クラウド型のIT資産管理で煩雑な台帳管理からの脱却

サービス業

職員数	250名
管理台数	400台

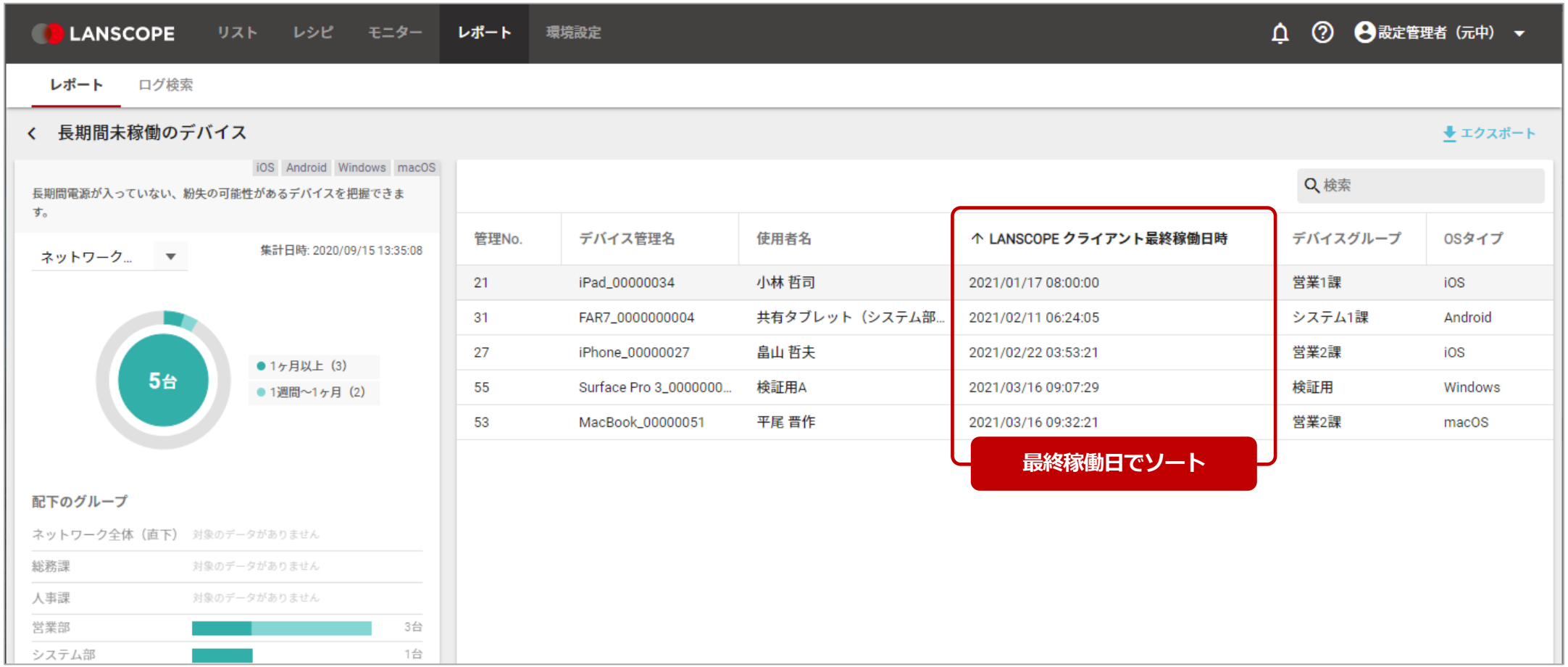
対象OS：Windows / iOS / Android / macOS

ー デバイスの台数や種類が増加するほど煩雑になる資産管理をエージェントをインストールするだけで常に最新の台帳を管理できる

これまで各拠点の担当者が定期的に Excel を更新して資産管理台帳の作成していましたが、作成に工数がかかるだけでなく、最新の情報を確認することができないのが課題でした。
エンドポイントマネージャーでは、エージェントをインストールするだけで、簡単に台帳を作成することができ、PC・スマホをまとめて管理することができるので、大幅な工数削減を実現できました。

ー 『長期間未稼働のデバイス』＝『紛失や故障の恐れのあるデバイス』を管理し、抜け漏れないのないIT資産管理を実現

これまで、デバイスの管理を個人に任せており、「本当に対象のデバイスが存在するのか？」が不明瞭で、中にはデバイスが故障しているにも関わらず1年以上放置されていたこともありました。エンドポイントマネージャーでは、デバイスの稼働状況を簡単に把握することができ、長期間未稼働のデバイスをすぐに特定することができました。
利用者に確認すると、実は全く使っていないデバイスであったことが判明したこともあり、不要なデバイスを無くすことでコスト削減に繋げることもできました。また、1ヶ月以上未稼働のデバイスがある場合、管理者メールで通知が飛ぶように設定しているので、管理コンソールにログインせずとも常に状況を把握することができた点も良かったです。



導入事例② 情報漏洩対策（PC）

社員への啓蒙でセキュリティモラルの向上
有事の際でもすぐに対応できる環境の構築

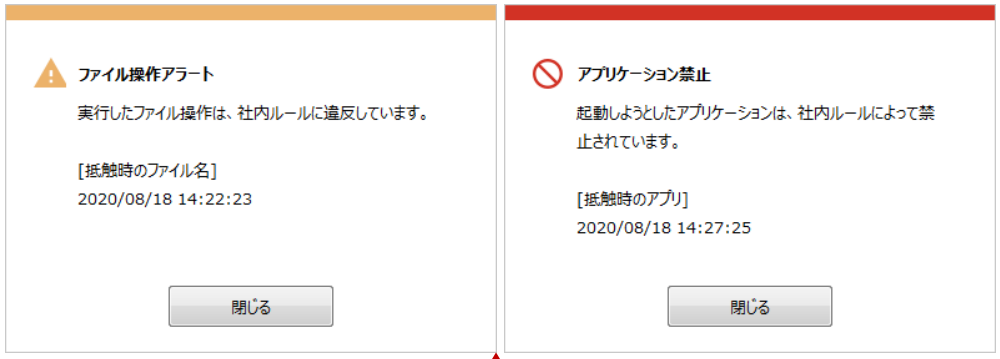
製造業

職員数	150名
管理台数	200台

対象OS：**Windows**　iOS　Android　macOS

ー 「どの部署の」「誰が」「いつ」「何をしたのか」をログで保存。違反操作をした場合はポップアップで通知することでセキュリティ意識の向上

弊社では社内規定で記録メディアの利用やオンラインストレージなどの利用を禁止しておりますが、従業員のセキュリティ意識が低いのが課題でした。
エンドポイントマネージャーでログを取得することで、有事の際の対応も可能となり、ポップアップによる啓蒙により従業員のセキュリティモラル向上に繋がりました。
今後はセキュリティ以外の観点でもログを有効活用し、従業員の働き方の見える化にも活用していきたいと考えています。



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

ー 私有のUSBなど記録メディアの利用を制御し、会社支給のUSBのみを利用許可に設定！

私有の USB の利用は社内規定で禁止しておりましたが、社内規定だけでは統制することができず、実際は私有の USB を利用している従業員がいる状態でした。
エンドポイントマネージャーでは、PC 単位・グループ単位で記録メディアの利用を制御することができ、USB を挿入するだけで簡単に除外登録することができました。
現在は、会社支給の USB のみを利用許可にし、不許可の USB が挿入されるとポップアップで警告を表示し、利用できないように制御しています。

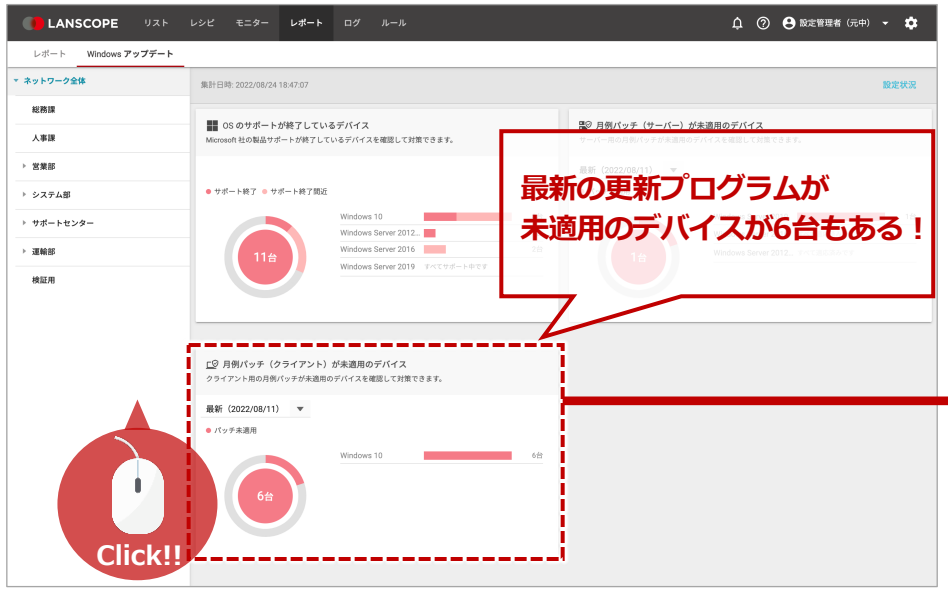
①	記録メディアの利用を読み取り専用（書き込み不可）または禁止に設定できます。
②	①で「読み取り専用」または「禁止」に設定している場合に、会社支給の記録メディアなど、例外的に利用を許可する記録メディアを設定することができます。 【除外設定方法】 ・一度挿入された記録メディアを登録する ・ベンダーID / プロダクトID を登録する ・フレンドリーネーム / デバイスの説明のキーワードを登録する
③	禁止されて記録メディアが挿入された場合に注意喚起のメッセージをポップアップで通知することができます。 

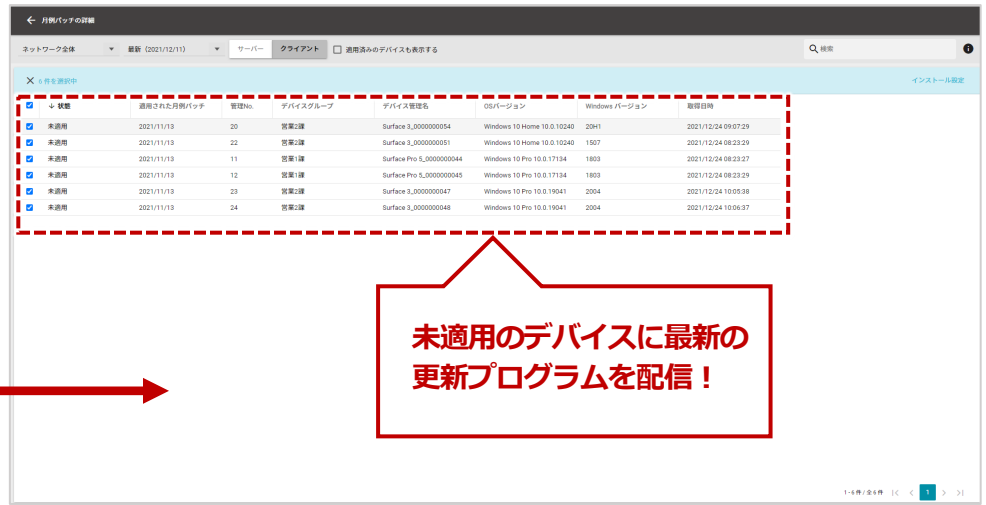
WSUS 未導入でも簡単アップデート管理
パッチ適用状況把握～適用までをエンドポイントマネージャーで実現！

情報・通信業			
職員数	180名	対象OS	Windows / iOS / Android / macOS
管理台数	250台		

ー 常に最新のセキュリティパッチの適用状況を視認性のダッシュボードで把握。

弊社ではこれまで Windows Update の適用は、従業員任せになっており、最新のセキュリティパッチが適用されていないデバイスも多く、社内のセキュリティホールになっていました。
エンドポイントマネージャーでは、WSUS が無くても Microsoft Update Server から常に最新の情報を取得してくれて、視認性の良いダッシュボードから、セキュリティパッチの適用状況を一目で把握することができました。また、未適用デバイスをワンクリックで特定することができ、最新のパッチの適用まで簡単に実行できる点が良かったです。





ー 月額450円で高精度の AI アンチウィルスが利用可能。従来型のようなパターンファイルの管理が不要で、IT 知識が無くても簡単に利用できる

弊社では、一般的なアンチウィルスソフトを導入していましたが、毎日のようにマルウェア感染事件が発生していることから、現在利用しているアンチウィルスで防ぐことができるのか不安でした。また、テレワーク環境下で最新のパターンファイルの適用が遅れるデバイスも多く、いつマルウェア感染が起きてもおかしくない状況でした。
エンドポイントマネージャーと連携する CylancePROTECT は、パターンファイルの管理が不要（年1・2回のモデルの更新のみ）で、あらゆるマルウェアを 99% 検知・隔離できる点が良かったです。また、エンドポイントマネージャーと連携することにより、マルウェアを検知した際の前後操作をワンクリックで確認でき、IT知識が無くても運用できる点も良かったです。

CylancePROTECT × Cloud LANSCOPE Endpoint Manager

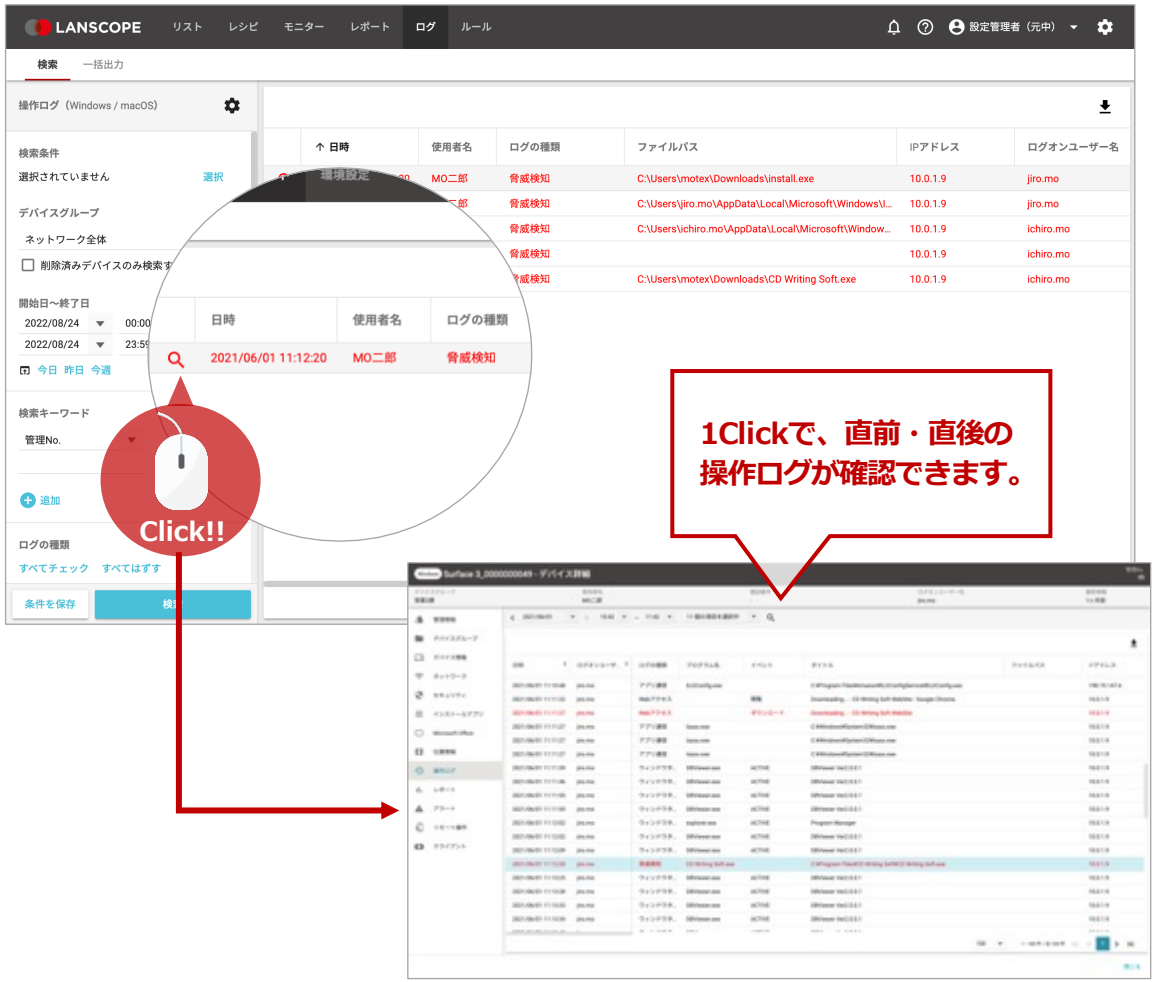
マシーンラーニングの特許技術を活用した「予測脅威防御」で、マルウェアの特徴点を見つけて実行前に検知・隔離します。エンドポイントマネージャー クラウド版と連携*することで、マルウェアに感染してしまった直前の操作を特定。原因の追求や再発防止に活用できます。

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

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/



* MOTEX が提供する CylancePROTECT の導入が必要です。
** 2018 NSS Labs Advanced Endpoint Protection Test 結果より

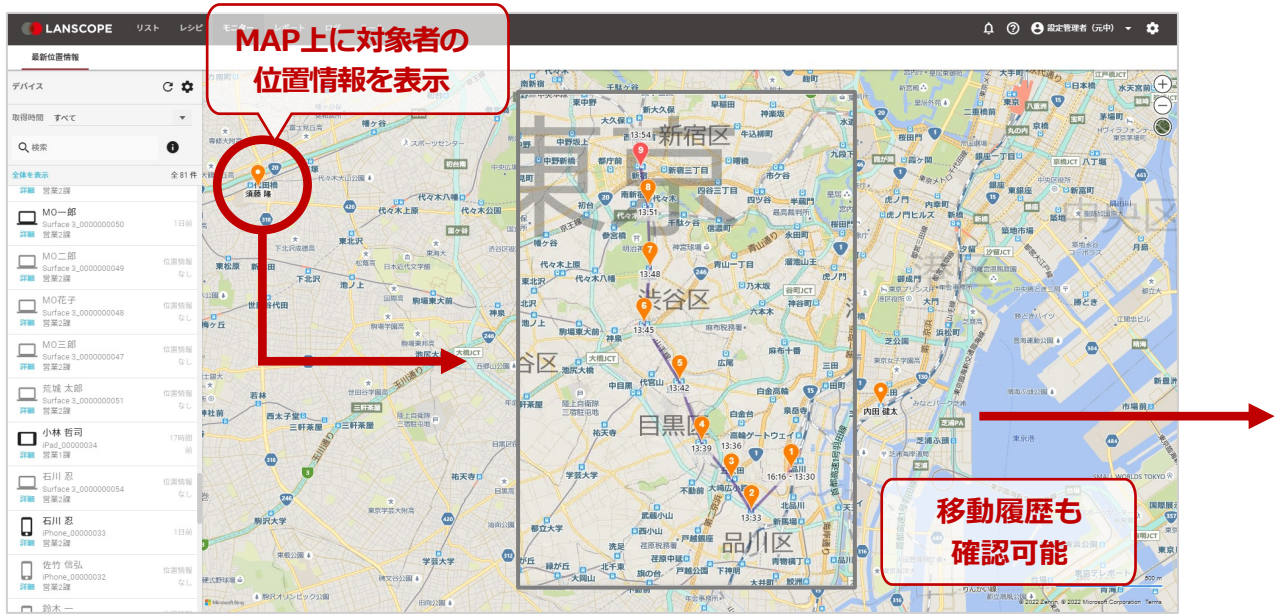
利用者に依存しがちなパスコード設定ルールを統一！
位置情報・リモートワイプで万が一の対策も実現！

卸売・小売業

職員数	140名	対象OS	Windows / iOS / Android / macOS
管理台数	80台		

ー 万が一紛失してしまった場合でも、位置情報を確認し、リモートロック/ワイプで情報漏洩を未然に防ぐ！

弊社では従業員に全員に iPhone・Andorid のスマートフォンを支給していますが、これまでMDMは導入しておらず、盗難・紛失時の対策が不十分な状態でした。特に営業は社外に持ち出して利用するシーンが多く、過去には紛失の事故が発生してしまったこともありました。エンドポイントマネージャーでは、現在の位置情報だけでなく、移動履歴を取得できるために、電源が切れてしまった場合でも、電源が切れる直前までの位置情報を確認できるため、紛失デバイスの発見などにも役立っています。また、万が一デバイスが発見できない場合には、リモートワイプ（データの初期化）を遠隔で行うことができるため、情報漏洩事故を防ぐこともできます。



ー 利用者に依存しがりなパスコードの設定ルールを統一！定期的にパスコードを変更することでより安全なデバイス利用を実現

これまでスマートフォンのパスコードは従業員に任せていましたが、「1234」等の単純値や、中にはパスコードを設定していない従業員も多く、もし紛失事故が発生してしまった場合、情報漏洩事故に繋がりかねない状況でした。エンドポイントマネージャーでは、パスコードの設定の強制はもちろん、最小文字数の指定、1234等の単純値の禁止、パスコードの有効期限なども設定することができました。パスコードを強制化したことで、従業員からパスコードを忘れてしまったといった連絡が入ることもありますが、遠隔でのパスコードリセット※1も可能なため、とても重宝しています。

iOS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
パスコードの設定ルールを一括で設定・配布
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

Androidの設定項目※2
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 Android デバイスの場合、Android Enterprise の利用が必要です。
※2 Android10 以降のデバイスの場合、Android Enterprise の利用が必要です。

Apple Business Manager・Android Enterprise と連動し、効率的なアプリ管理を実現！

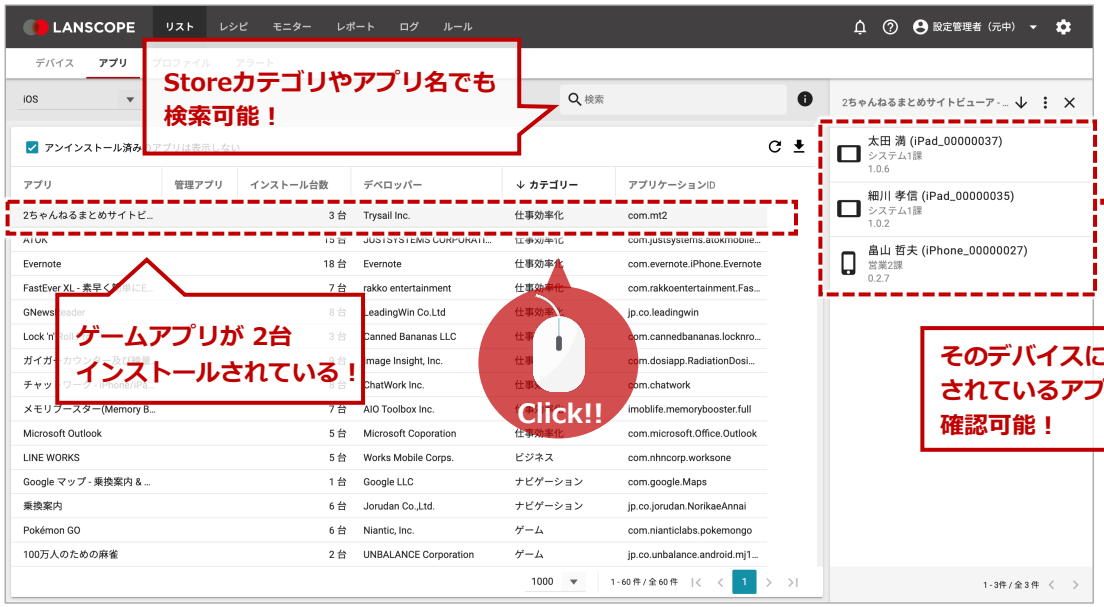
製造業

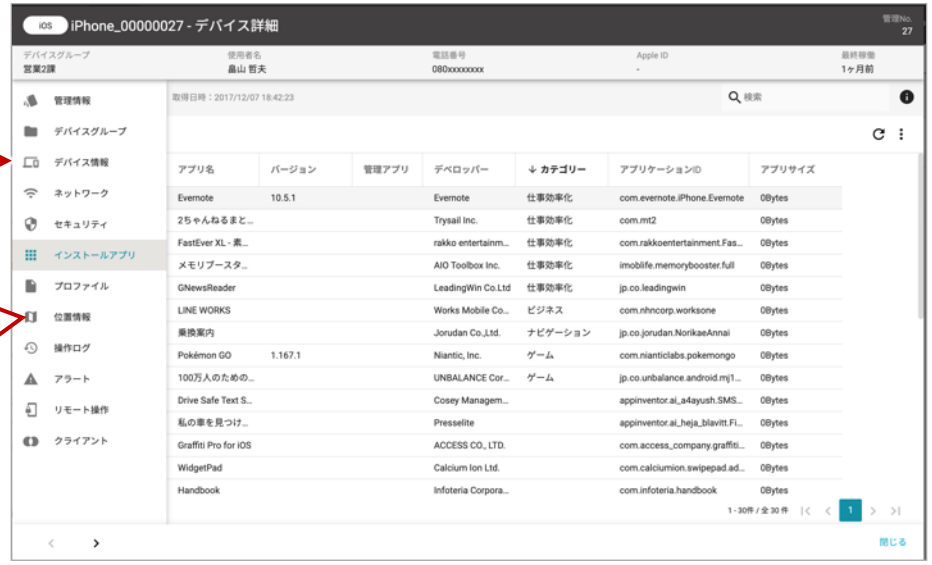
職員数	220名
管理台数	120台

対象OS：Windows / iOS / Android / macOS

ー アプリケーションのインストール状況も簡単に把握。業務に関係の無いアプリケーションの起動も制御可能。

必須のセキュリティアプリケーションがインストールされているか？業務に関係の無いアプリケーションがインストールされていないか？などの情報が把握できていないことが課題でした。
エンドポイントマネージャーでは、アプリケーションを軸にどのアプリケーションがどのデバイスにインストールされているかを一目で把握することができました。
また、iOS・Android においては、Storeカテゴリなども取得できるので、「ゲーム」等の業務外のアプリケーションがインストールされていないかを簡単に把握でき、起動を禁止することが出来た点も良かったです。

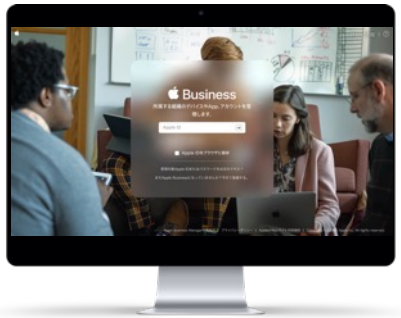




ー Apple Business Manager・Android Enterprise を利用することで、Apple ID・Google アカウント不要でアプリ配信を実現

これまでセキュリティアプリなど業務に必要なアプリをインストールするために、各デバイス毎にApple ID・Google アカウントを取得して管理をしていました。
Apple Business Manager・Android Enterprise とエンドポイントマネージャーを連携することにより、管理者用のアカウントを一つ用意するだけで、Apple ID・Google アカウントをデバイスに設定することなく、必要なアプリを遠隔でインストールすることができました。また、許可したアプリのみに利用を制限することができるので、業務に関係の無いアプリのインストールの心配も無くなり、効率的かつセキュアなアプリ管理を実現することができました。

Apple Business Manager



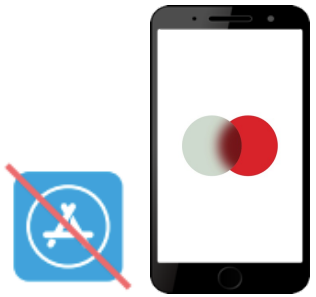
入手したアプリ

連携

エンドポイントマネージャー

配信

App Store を禁止していても管理可能



Android Enterprise

連携

エンドポイントマネージャー

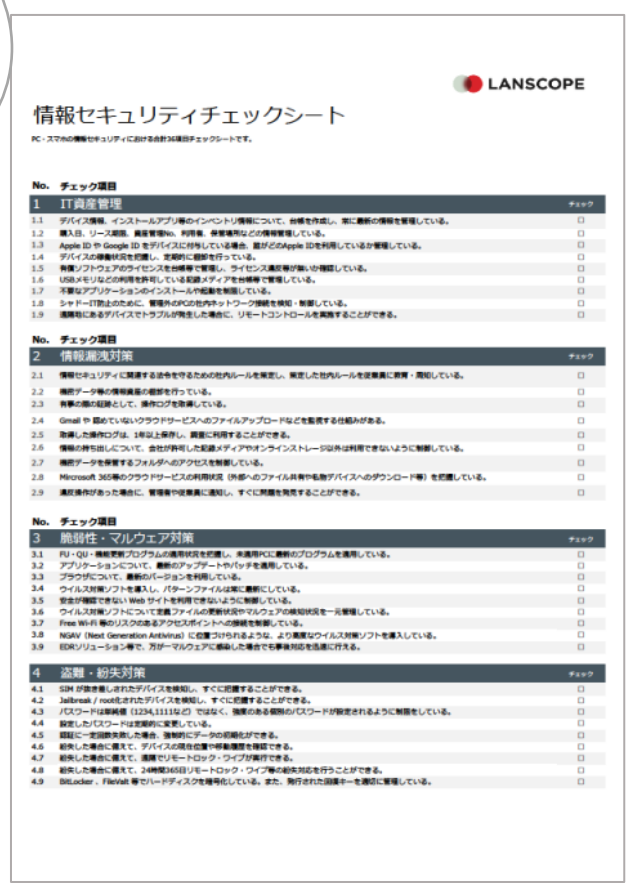
配信

許可したアプリのみPlay ストアに表示

情報セキュリティチェックシート無料配布中！

PC・スマホ管理における最低限押さえておきたい管理項目をまとめたチェックシートを無料配布中！

全36項目から自社の
課題をチェック！



LANSCOPE

情報セキュリティチェックシート

PC・スマホの情報セキュリティにおける合計36項目チェックシートです。

No.	チェック項目	チェック
1	**IT資産管理**	
1.1	デバイス情報、インストールアプリ等のインベントリ情報について、台帳を作成し、常に最新の情報を管理している。	□
1.2	購入日、リース期限、資産管理No、利用者、保管場所などの情報管理している。	□
1.3	Apple ID や Google ID をデバイスに付与している場合、誰がどのApple IDを利用しているか管理している。	□
1.4	デバイスの稼働状況を把握し、定期的に棚卸を行っている。	□
1.5	有償ソフトウェアのライセンスを台帳等で管理し、ライセンス違反等が無いか確認している。	□
1.6	USBメモリなどの利用を許可している記録メディアを台帳等で管理している。	□
1.7	不要なアプリケーションのインストールや起動を制限している。	□
1.8	シャドーIT防止のために、管理外のPCの社内ネットワーク接続を検知・制御している。	□
1.9	遠隔地にあるデバイスでトラブルが発生した場合に、リモートコントロールを実施することができる。	□

No.	チェック項目	チェック
2	**情報漏洩対策**	
2.1	情報セキュリティに関連する法令を守るための社内ルールを策定し、策定した社内ルールを従業員に教育・周知している。	□
2.2	機密データ等の情報資産の棚卸を行っている。	□
2.3	有事の際の証跡として、操作ログを取得している。	□
2.4	Gmail や 認めていないクラウドサービスへのファイルアップロードなどを監視する仕組みがある。	□
2.5	取得した操作ログは、1年以上保存し、調査に利用することができる。	□
2.6	情報の持ち出しについて、会社が許可した記録メディアやオンラインストレージ以外は利用できないように制御している。	□
2.7	機密データを保管するフォルダへのアクセスを制御している。	□
2.8	Microsoft 365等のクラウドサービスの利用状況（外部へのファイル共有や私物デバイスへのダウンロード等）を把握している。	□
2.9	違反操作があった場合に、管理者や従業員に通知し、すぐに問題を発見することができる。	□

No.	チェック項目	チェック
3	**脆弱性・マルウェア対策**	
3.1	FU・QU・機能更新プログラムの適用状況を把握し、未適用PCに最新のプログラムを適用している。	□
3.2	アプリケーションについて、最新のアップデートやパッチを適用している。	□
3.3	ブラウザについて、最新のバージョンを利用している。	□
3.4	ウイルス対策ソフトを導入し、パターンファイルは常に最新にしている。	□
3.5	安全が確認できない Web サイトを利用できないように制御している。	□
3.6	ウイルス対策ソフトについて定義ファイルの更新状況やマルウェアの検知状況を一元管理している。	□
3.7	Free Wi-Fi 等のリスクのあるアクセスポイントへの接続を制御している。	□
3.8	NGAV（Next Generation Antivirus）に位置づけられるような、より高度なウイルス対策ソフトを導入している。	□
3.9	EDRソリューション等で、万が一マルウェアに感染した場合でも事後対応を迅速に行える。	□

4	**盗難・紛失対策**	
4.1	SIM が抜き差しされたデバイスを検知し、すぐに把握することができる。	□
4.2	Jailbreak / root化されたデバイスを検知し、すぐに把握することができる。	□
4.3	パスワードは解読容（1234,11111など）ではなく、強度のある個別のパスワードが設定されるように制限をしている。	□
4.4	設定したパスワードは定期的に変更している。	□
4.5	認証に一定回数失敗した場合、強制的にデータの初期化ができる。	□
4.6	紛失した場合に備えて、デバイスの現在位置や稼働履歴を確認できる。	□
4.7	紛失した場合に備えて、遠隔でリモートロック・ワイプが実行できる。	□
4.8	紛失した場合に備えて、24時間365日リモートロック・ワイプ等の紛失対応を行うことができる。	□
4.9	BitLocker、FileVault 等でハードディスクを暗号化している。また、発行された回復キーを適切に管理している。	□

情報セキュリティ36項目チェックシート

https://www.lanscope.jp/tips/25032/

設定したポリシーや取得した情報をそのまま製品版へデータ引き継ぎが可能です

エンドポイントマネージャー 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。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。

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	03-5460-0775
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）
E-mail お問い合わせ	support@motex.co.jp