LANSCOPE cloud

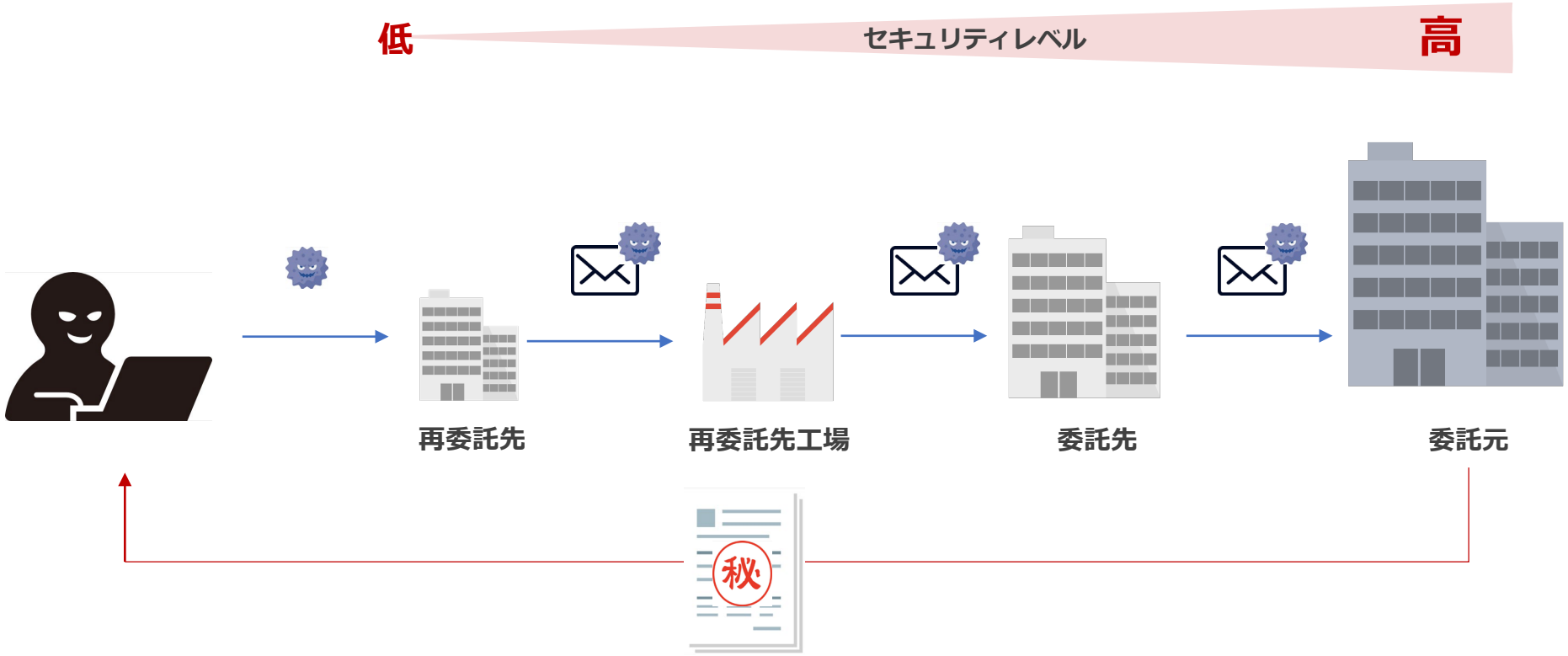
中堅・中小企業も他人ごとではない！？

事例から考えるサプライチェーンのリスクと対策とは？

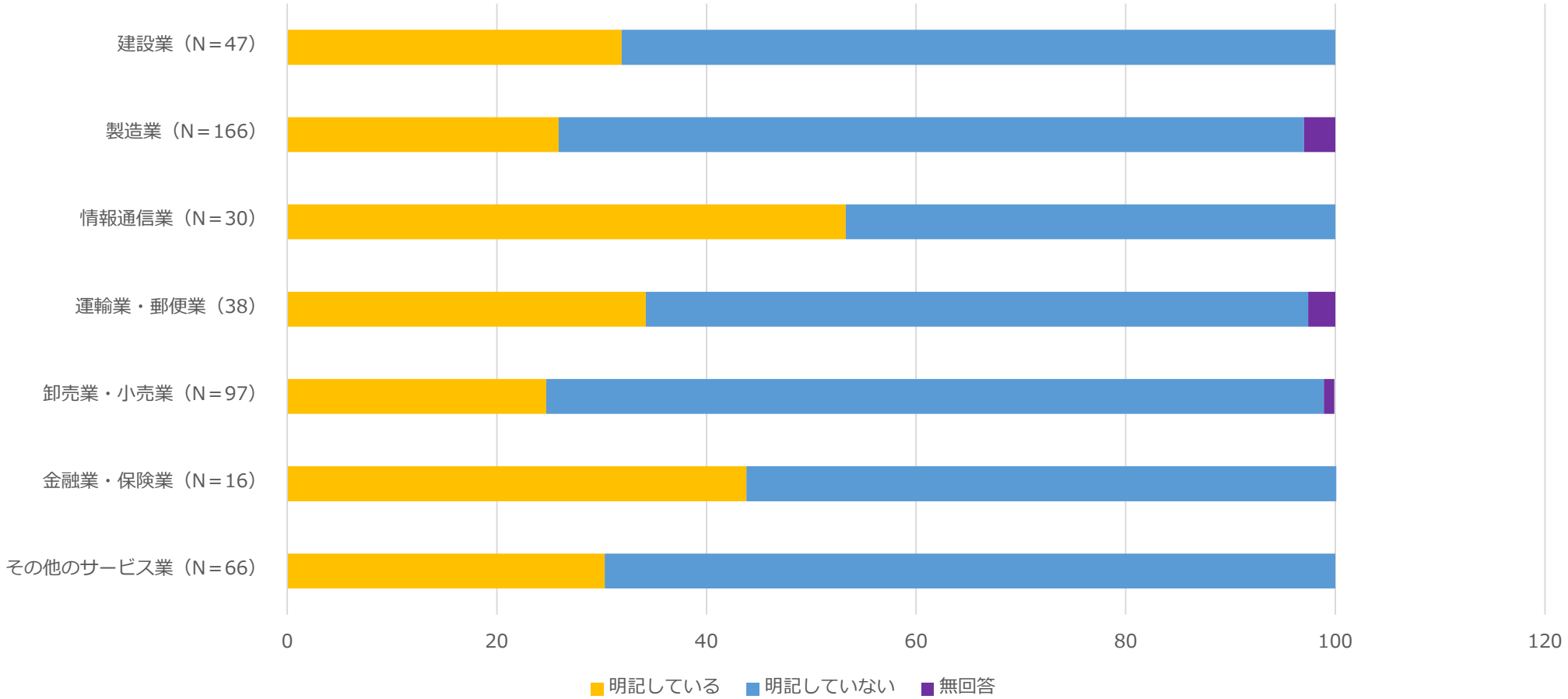
中小企業が狙われる！？サプライチェーン攻撃とは？

セキュリティ対策の甘いサプライチェーンの企業にサイバー攻撃を行い、踏み台にして本命に侵入

直接の被害組織だけでなく、複数の関係者に甚大な被害をもたらすリスク



情報通信業以外の委託元は過半数が、実施すべき情報セキュリティ対策を委託先に明示していない。特に、製造業では71.1%、卸売業74.2%と顕著



※独立行政法人 情報処理推進機構 「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」

内部犯行による情報漏えい事件だけでなく、誤送信やPC・スマホの紛失による事故が絶えない

委託元の業務用サーバ内に置かれた
委託元社員専用フォルダに不正にアクセス

委託先社員が委託元の業務用サーバ内に置かれた委託元社員専用フォルダに不正にアクセスし、内部情報を閲覧していたことを、委託元社員が発見。
委託先社員が不正に取得した内部情報は、次期ネットワークシステムに関する、他社提案書や参考見積等が含まれていた。

委託先が提供するシステムに第三者による不正アクセスがありお客様情報が漏えい

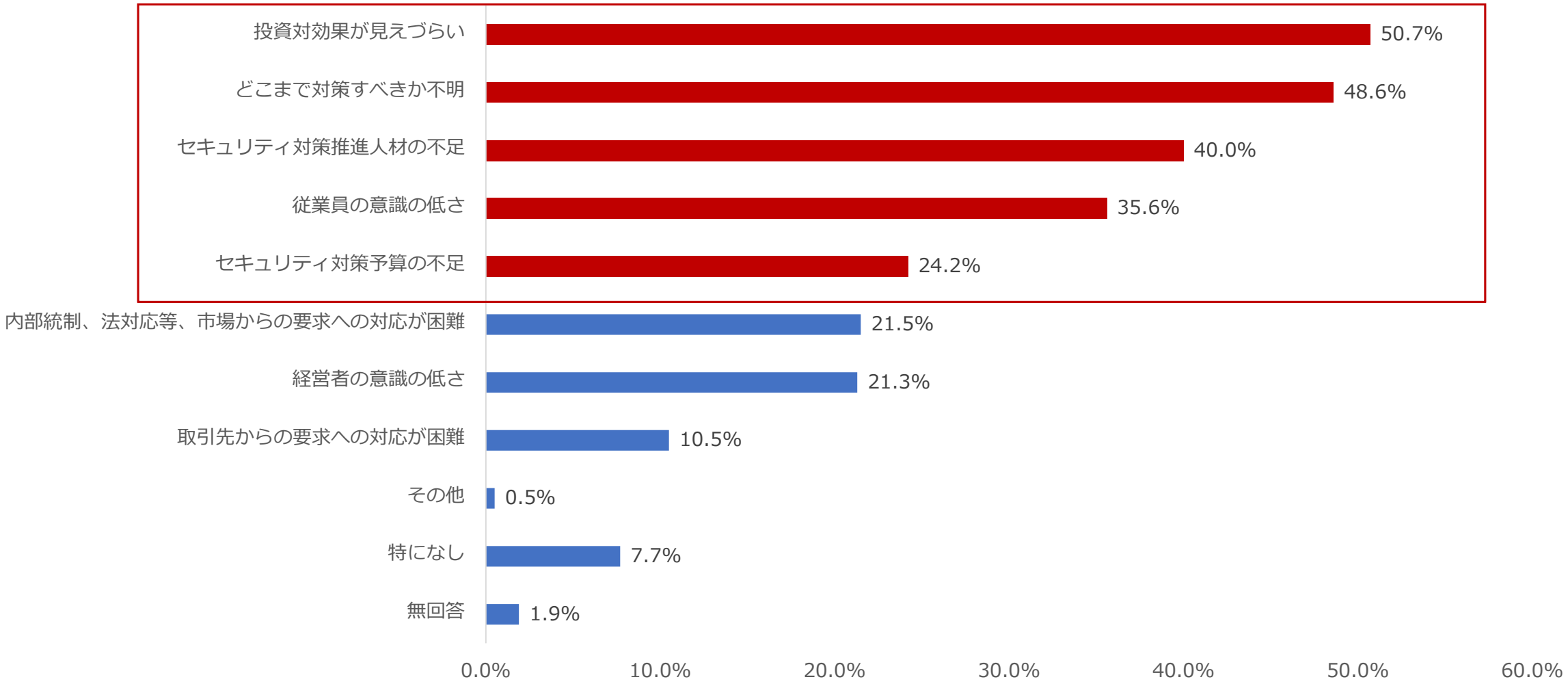
委託先が提供するシステムにおいて委託元のECサイトを運営していた。委託元のECサイトでサーバートラブルが発生したためメンテナンスをしたところ、
一部のお客様の情報が漏えいした可能性があることが判明。

鉄道駅にて業務用パソコン
の入ったカバンを盗まれ、顧客情報が漏えい

再委託先社員が、鉄道駅において「業務用パソコン」の入ったカバンを隣に置いて眠ってしまい、目を覚ました時にカバンが無いことに気付いた。
業務用パソコンには数万件の個人情報が含まれていた。

※独立行政法人 情報処理推進機構 「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」

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 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
- 導入事例②　情報漏洩対策
- 導入事例③　脆弱性・標的型攻撃対策
- 導入事例④　盗難紛失対策
- 導入事例⑤　アプリ管理

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

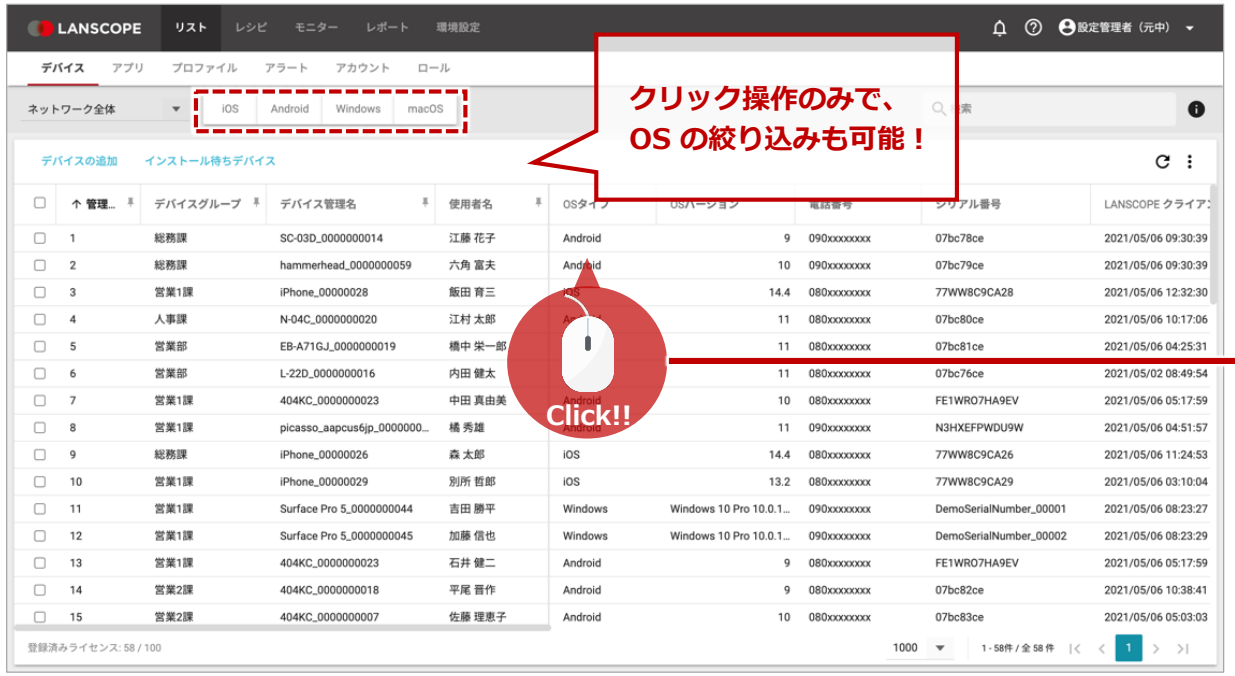
サービス業

職員数	250名
管理台数	400台

対象OS：Windows / iOS / Android / macOS

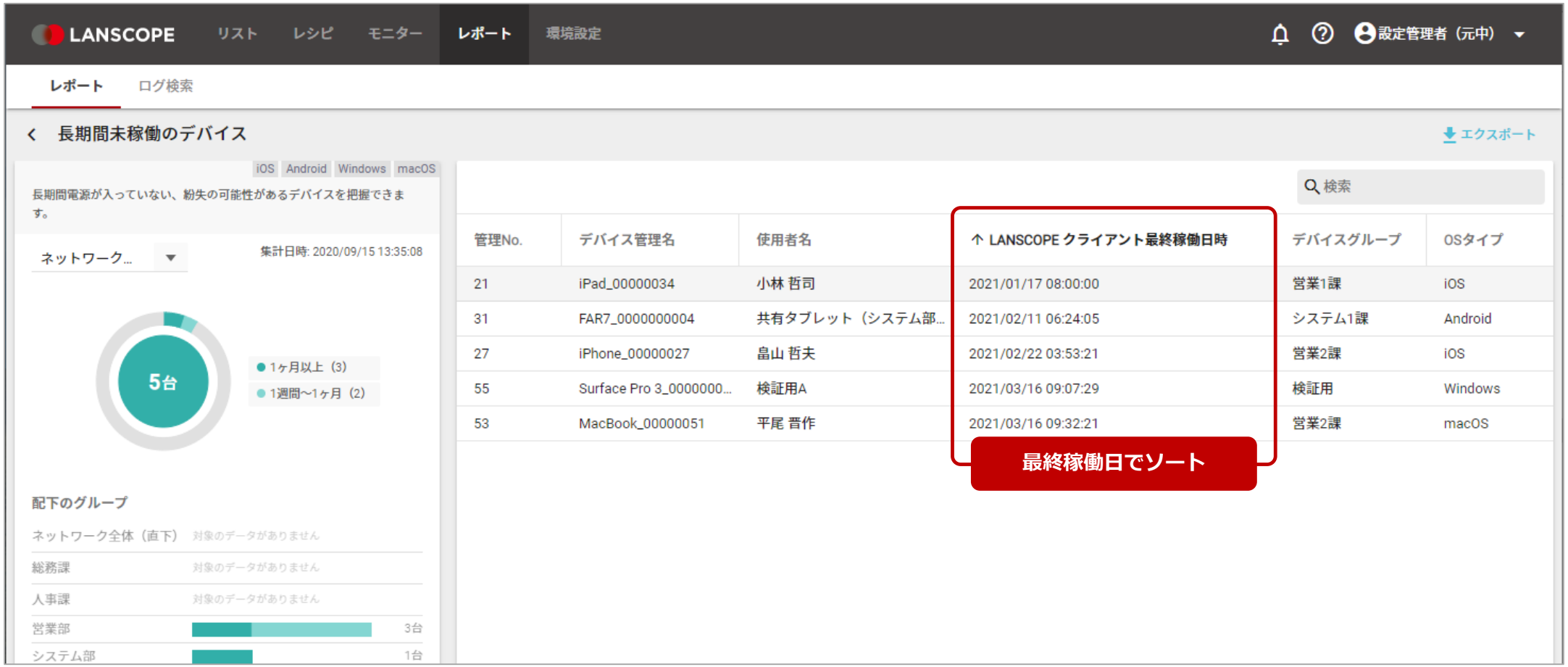
ー デバイスの台数や種類が増加するほど煩雑になる資産管理をエージェントをインストールするだけで常に最新の台帳を管理できる

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。
LANSCOPE 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。LANSCOPE 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。



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

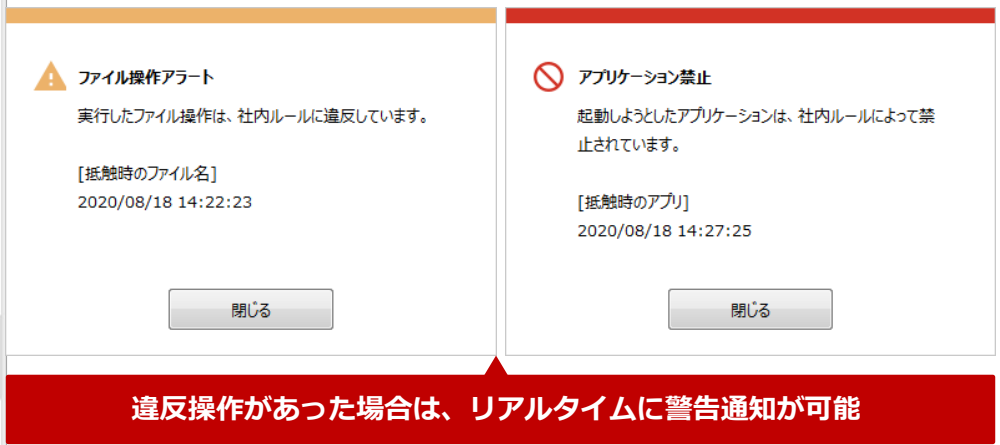
製造業

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。
LANSCOPE 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。
LANSCOPE 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。

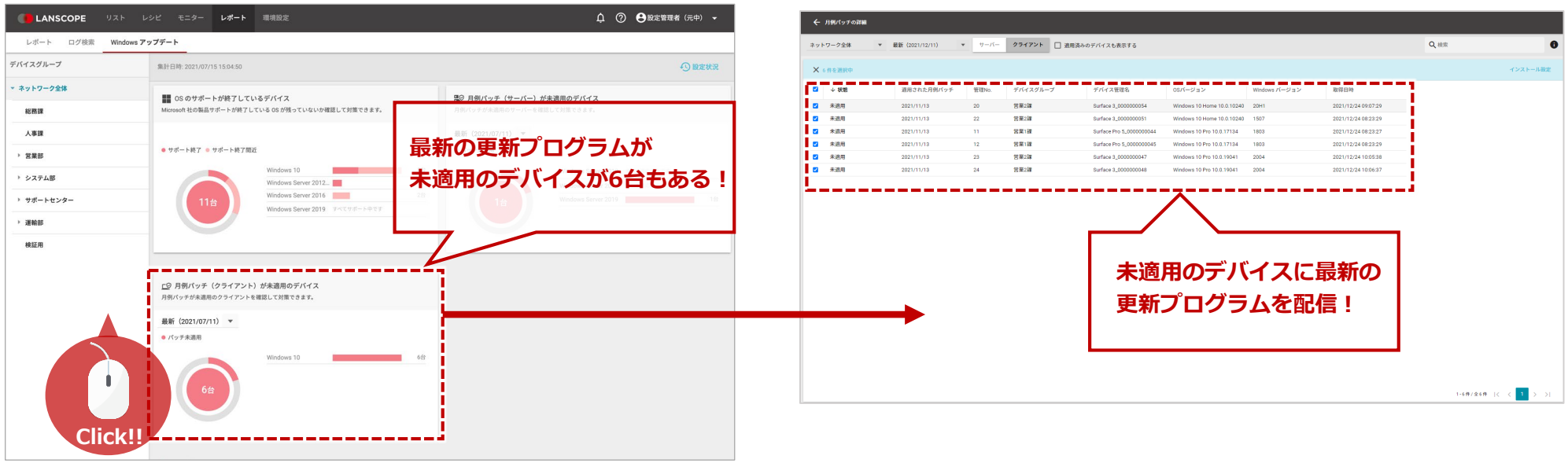
①	記録メディアの利用を読み取り専用（書き込み不可）または禁止に設定できます。
②	①で「読み取り専用」または「禁止」に設定している場合に、会社支給の記録メディアなど、例外的に利用を許可する記録メディアを設定することができます。 【除外設定方法】 ・一度挿入された記録メディアを登録する ・ベンダーID / プロダクトID を登録する ・フレンドリーネーム / デバイスの説明のキーワードを登録する
③	禁止されて記録メディアが挿入された場合に注意喚起のメッセージをポップアップで通知することができます。 

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LANSCOPE 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。LANSCOPE 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

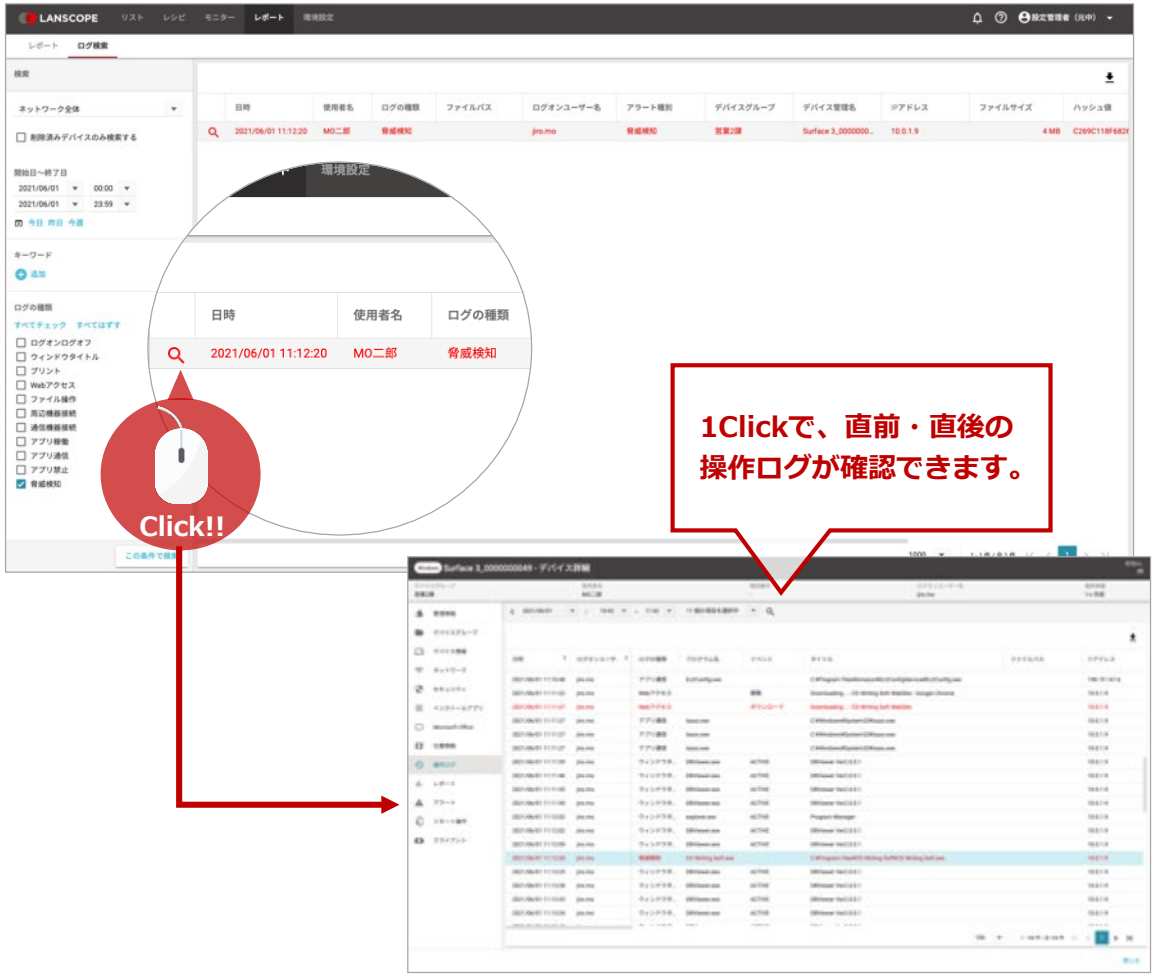
弊社では、一般的なアンチウィルスソフトを導入していましたが、毎日のようにマルウェア感染事件が発生していることから、現在利用しているアンチウィルスで防ぐことができるのか不安でした。また、テレワーク環境下で最新のパターンファイルの適用が遅れるデバイスも多く、いつマルウェア感染が起きてもおかしくない状況でした。
LANSCOPE と連携する BlackBerry Protect は、パターンファイルの管理が不要（年1・2回のモデルの更新のみ）で、あらゆるマルウェアを 99% 検知・隔離できる点が良かったです。
また、LANSCOPE と連携することにより、マルウェアを検知した際の前後操作をワンクリッ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

BlackBerry Protect × 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/



* MOTEX が提供する BlackBerry Protect 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。
LANSCOPE クラウド版では、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。LANSCOPE 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。

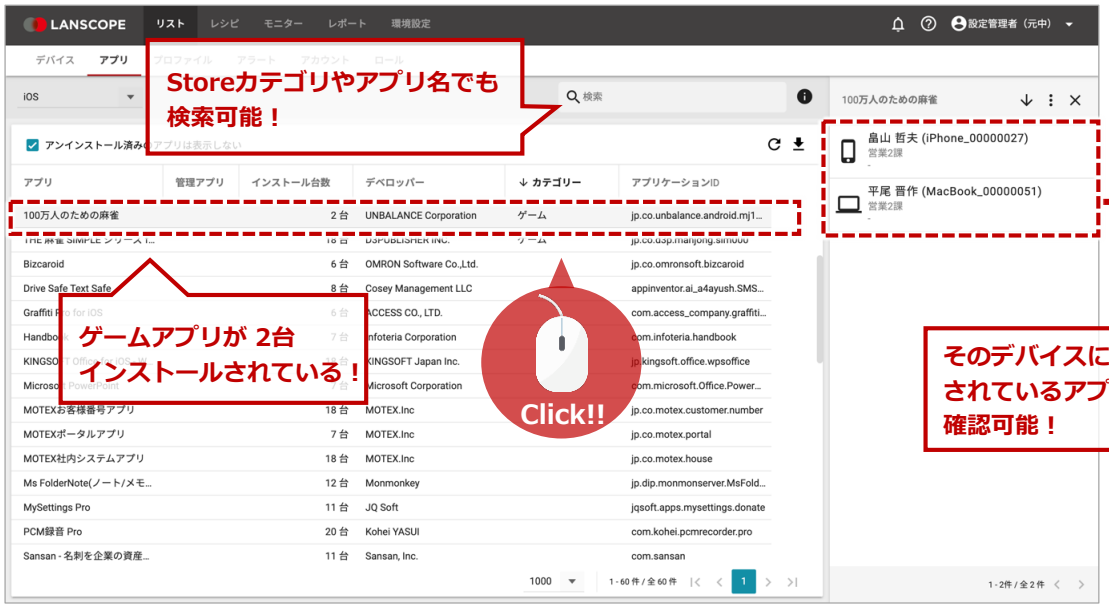
Apple Business Manager・Android Enterprise と連動し、効率的なアプリ管理を実現！

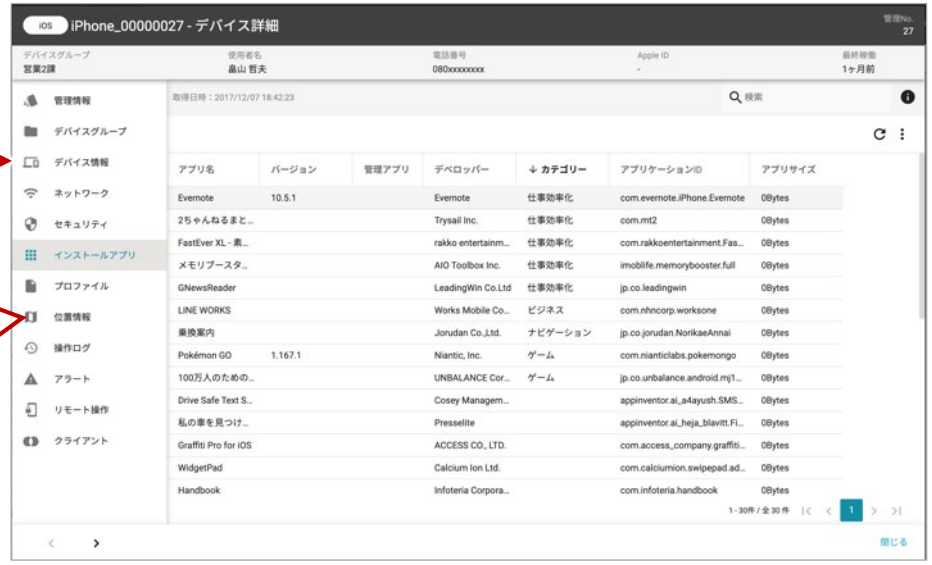
製造業

職員数	220名	対象OS	Windows / iOS / Android / macOS
管理台数	120台		

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。
LANSCOPE 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。





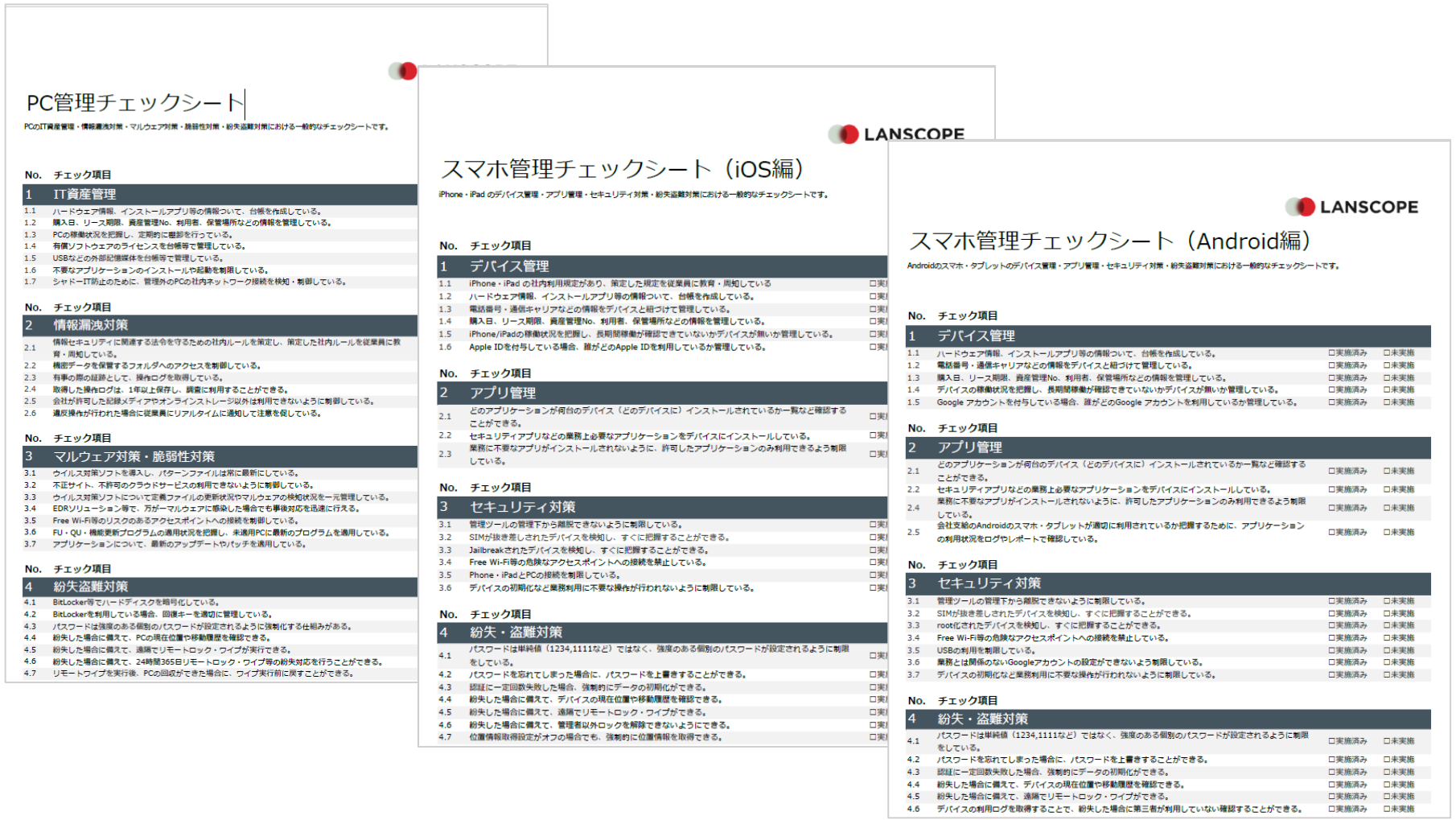
ー Apple Business Manager・Android Enterprise を利用することで、Apple ID・Google アカウント不要でアプリ配信を実現

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LANSCOPE 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。

簡易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！

ご希望の方は『 sales@motex.co.jp 』までお問合せください



PC管理チェックシート

PCのIT資産管理・情報漏洩対策・マルウェア対策・脆弱性対策・紛失盗難対策における一般的なチェックシートです。

No.	チェック項目
1	IT資産管理
1.1	ハードウェア情報、インストールアプリ等の情報ついて、台帳を作成している。
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を管理している。
1.3	PCの稼働状況を把握し、定期的に棚卸を行っている。
1.4	有償ソフトウェアのライセンスを台帳等で管理している。
1.5	USBなどの外部記憶媒体を台帳等で管理している。
1.6	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。
1.7	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。
No.	チェック項目
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	機密データを保管するフォルダへのアクセスを制御している。
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	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。
2.5	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。
2.6	違反操作が行われた場合に従業員にリアルタイムに通知して注意を促している。
No.	チェック項目
3	マルウェア対策・脆弱性対策
3.1	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。
3.2	不正サイト、不許可のクラウドサービスの利用できないように制御している。
3.3	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。
3.4	EDRソリューション等で、万がー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。
3.5	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。
3.6	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。
3.7	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。
No.	チェック項目
4	紛失盗難対策
4.1	BitLocker等でハードディスクを暗号化している。
4.2	BitLockerを利用している場合、回復キーを適切に管理している。
4.3	パスワードは強度のある個別のパスワードが設定されるように強制化する仕組みがある。
4.4	紛失した場合に備えて、PCの現在位置や移動履歴を確認できる。
4.5	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。
4.6	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。
4.7	リモートワイプを実行後、PCの回収ができた場合に、ワイプ実行前に戻すことができる。

LANSCOPE

スマホ管理チェックシート（iOS編）

iPhone・iPad のデバイス管理・アプリ管理・セキュリティ対策・紛失盗難対策における一般的なチェックシートです。

No.	チェック項目	
1	デバイス管理	
1.1	iPhone・iPad の社内利用規定があり、策定した規定を従業員に教育・周知している	□実
1.2	ハードウェア情報、インストールアプリ等の情報ついて、台帳を作成している。	□実
1.3	電話番号・通信キャリアなどの情報をデバイスと紐づけて管理している。	□実
1.4	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を管理している。	□実
1.5	iPhone/iPadの稼働状況を把握し、長期間稼働が確認できていないかデバイスが無いか管理している。	□実
1.6	Apple IDを付与している場合、誰がどのApple IDを利用しているか管理している。	□実
No.	チェック項目	
2	アプリ管理	
2.1	どのアプリケーションが何台のデバイス（どのデバイスに）インストールされているか一覧など確認することができる。	□実
2.2	セキュリティアプリなどの業務上必要なアプリケーションをデバイスにインストールしている。	□実
2.3	業務に不要なアプリがインストールされないように、許可したアプリケーションのみ利用できるよう制限している。	□実
No.	チェック項目	
3	セキュリティ対策	
3.1	管理ツールの管理下から離脱できないように制限している。	□実
3.2	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。	□実
3.3	Jailbreakされたデバイスを検知し、すぐに把握することができる。	□実
3.4	Free Wi-Fi等の危険なアクセスポイントへの接続を禁止している。	□実
3.5	Phone・iPadとPCの接続を制限している。	□実
3.6	デバイスの初期化など業務利用に不要な操作が行われないように制限している。	□実
No.	チェック項目	
4	紛失・盗難対策	
4.1	パスワードは単純値（1234,1111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。	□実
4.2	パスワードを忘れてしまった場合に、パスワードを上書きすることができる。	□実
4.3	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。	□実
4.4	紛失した場合に備えて、デバイスの現在位置や移動履歴を確認できる。	□実
4.5	紛失した場合に備えて、遠隔でリモートロック・ワイプができる。	□実
4.6	紛失した場合に備えて、管理者以外ロックを解除できないようにできる。	□実
4.7	位置情報取得設定がオフの場合でも、強制的に位置情報を取得できる。	□実

LANSCOPE

スマホ管理チェックシート（Android編）

Androidのスマホ・タブレットのデバイス管理・アプリ管理・セキュリティ対策・紛失盗難対策における一般的なチェックシートです。

No.	チェック項目		
1	デバイス管理		
1.1	ハードウェア情報、インストールアプリ等の情報ついて、台帳を作成している。	□実施済み	□未実施
1.2	電話番号・通信キャリアなどの情報をデバイスと紐づけて管理している。	□実施済み	□未実施
1.3	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を管理している。	□実施済み	□未実施
1.4	デバイスの稼働状況を把握し、長期間稼働が確認できていないかデバイスが無いか管理している。	□実施済み	□未実施
1.5	Google アカウントを付与している場合、誰がどのGoogle アカウントを利用しているか管理している。	□実施済み	□未実施
No.	チェック項目		
2	アプリ管理		
2.1	どのアプリケーションが何台のデバイス（どのデバイスに）インストールされているか一覧など確認することができる。	□実施済み	□未実施
2.2	セキュリティアプリなどの業務上必要なアプリケーションをデバイスにインストールしている。	□実施済み	□未実施
2.4	業務に不要なアプリがインストールされないように、許可したアプリケーションのみ利用できるよう制限している。	□実施済み	□未実施
2.5	会社支給のAndroidのスマホ・タブレットが適切に利用されているか把握するために、アプリケーションの利用状況をログやレポートで確認している。	□実施済み	□未実施
No.	チェック項目		
3	セキュリティ対策		
3.1	管理ツールの管理下から離脱できないように制限している。	□実施済み	□未実施
3.2	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。	□実施済み	□未実施
3.3	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。	□実施済み	□未実施
3.4	Free Wi-Fi等の危険なアクセスポイントへの接続を禁止している。	□実施済み	□未実施
3.5	USBの利用を制限している。	□実施済み	□未実施
3.6	業務とは関係のないGoogleアカウントの設定ができないよう制限している。	□実施済み	□未実施
3.7	デバイスの初期化など業務利用に不要な操作が行われないように制限している。	□実施済み	□未実施
No.	チェック項目		
4	紛失・盗難対策		
4.1	パスワードは単純値（1234,1111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。	□実施済み	□未実施
4.2	パスワードを忘れてしまった場合に、パスワードを上書きすることができる。	□実施済み	□未実施
4.3	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。	□実施済み	□未実施
4.4	紛失した場合に備えて、デバイスの現在位置や移動履歴を確認できる。	□実施済み	□未実施
4.5	紛失した場合に備えて、遠隔でリモートロック・ワイプができる。	□実施済み	□未実施
4.6	デバイスの利用ログを取得することで、紛失した場合に第三者が利用していない確認することができる。	□実施済み	□未実施

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

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。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。

お問い合わせ先

■製品に関するお問い合わせ

エムオーテックス株式会社 営業部

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

■ご導入後の運用に関するお問い合わせ

エムオーテックスサポートセンター

0120-968995

※携帯・PHSからは06-6308-8981

※受付 9:30～12:00/13:00～17:30（月～金）

メールでのお問い合わせ

support@motex.co.jp（※24時間受付）

関連サイト

エムオーテックス株式会社 コーポレートサイト	http://www.motex.co.jp/
LANSCOPE クラウド版 製品サイト	http://www.lanscope.jp/an/
LANSCOPE オンプレミス版 製品サイト	http://www.lanscope.jp/cat/
SYNCPIT 製品サイト	https://www.syncpit.com