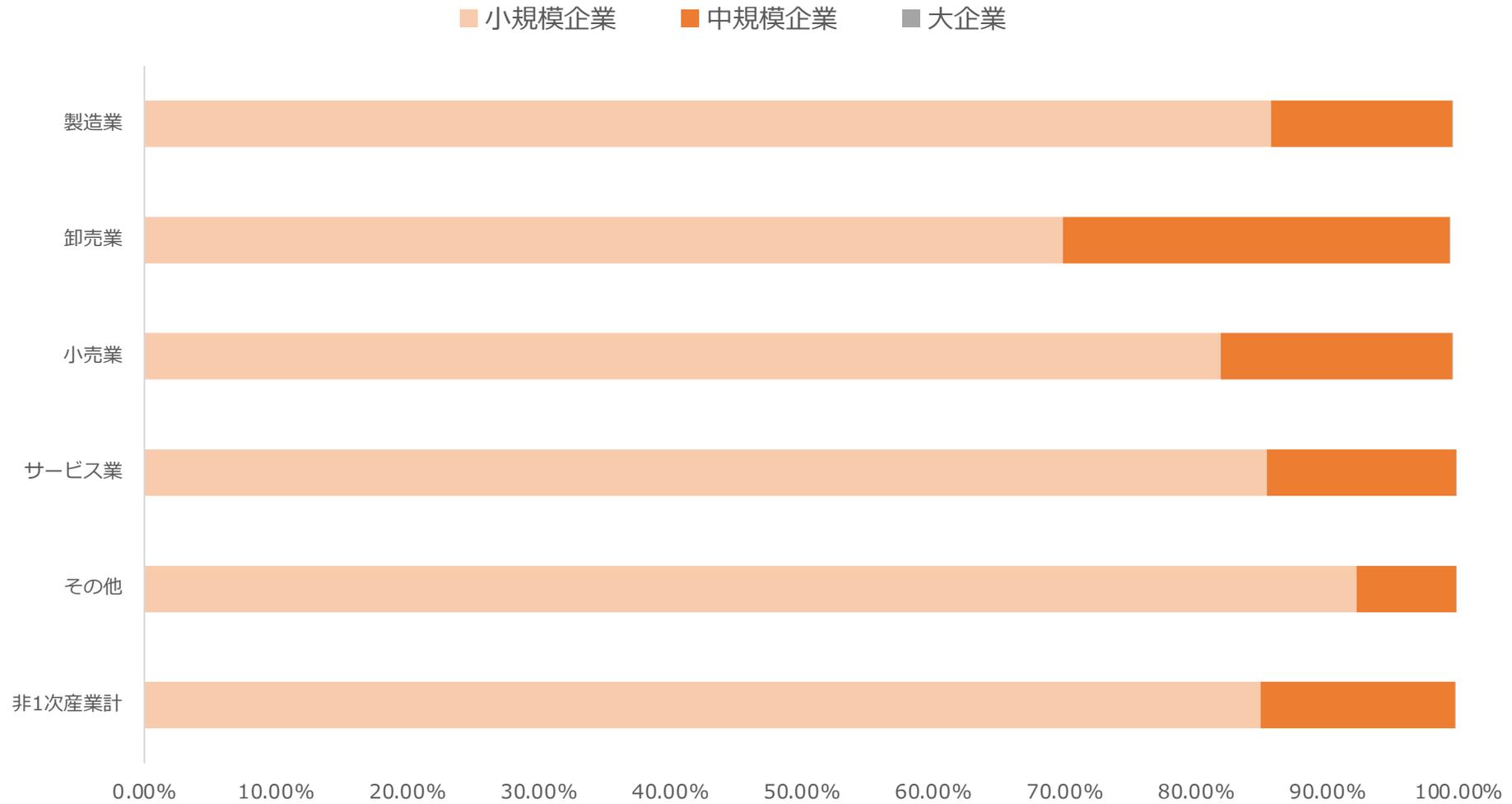




従業員100名～300名の中小企業様ならではの課題を解決！
事例から見る エンドポイントマネージャー活用術をご紹介します

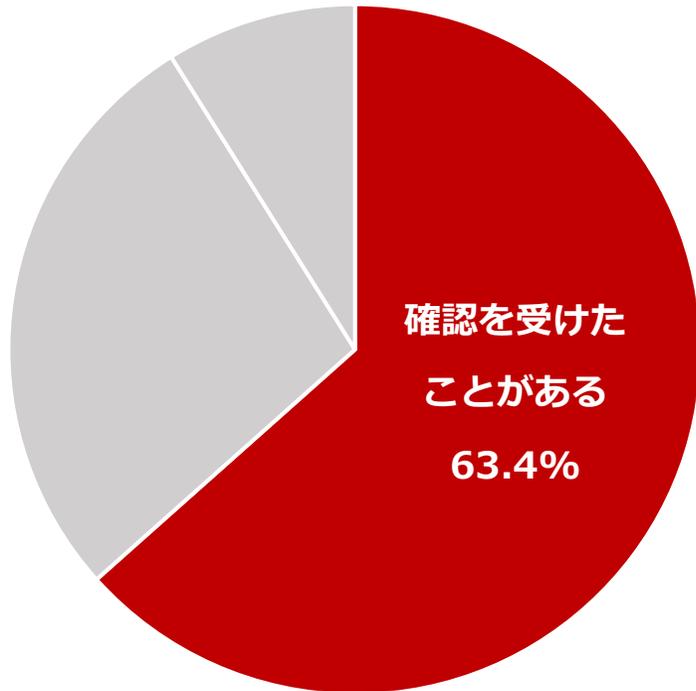
中小企業は日本企業の99%以上を占める



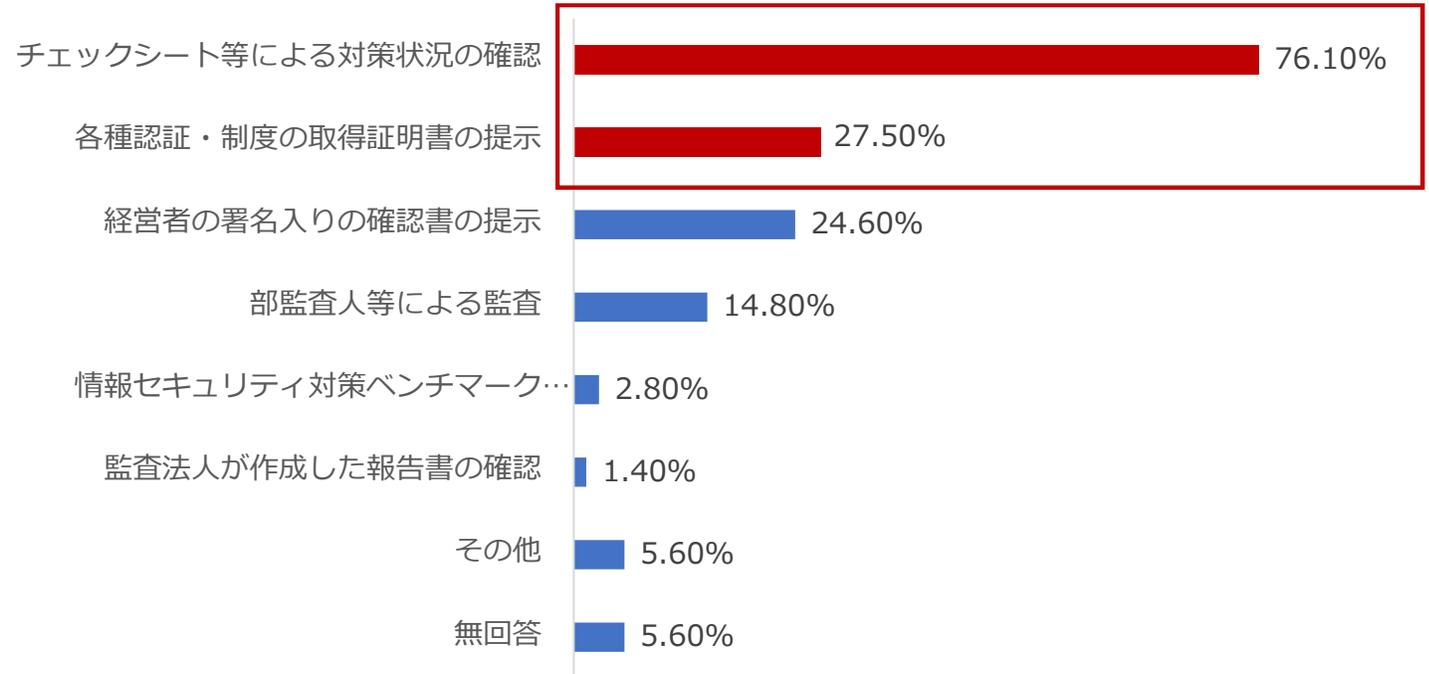
※ 総務省・経済産業省「平成28年経済センサス - 活動調査」

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※

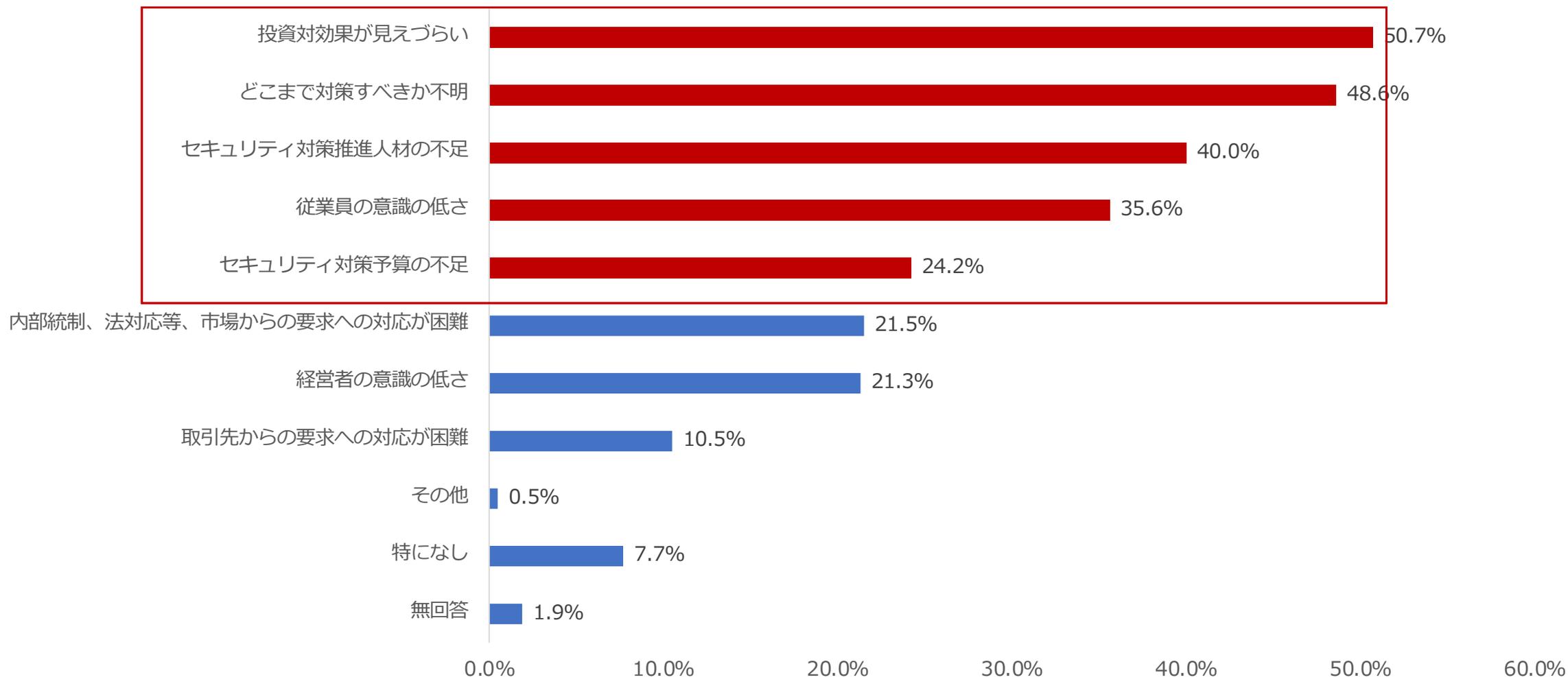


取引先からの情報セキュリティ対策確認方法※



※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

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

— 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。

LANSCOPE リスト レシビ モニター レポート ログ ルール

デバイス アプリ プロファイル アラート

ネットワーク全体 iOS Android Windows macOS

デバイスの追加 インストール待ちデバイス

管理	デバイスグループ	使用者名	OSタイプ	OSバージョン	電話番号	シリアル番号	デバイス管理名	LANSCOPE クライア
1	総務課	江藤 花子	Android		9 090xxxxxxx	07bc78ce	SC-03D_0000000014	2022/08/24 09:30:35
2	総務課	六角 富夫	Android		10 090xxxxxxx	07bc79ce	hammerhead_0000000059	2022/08/24 09:30:35
3	営業1課	飯田 育三	iOS		14.4 080xxxxxxx	77WW8C9CA28	iPhone_000000028	2022/08/24 12:32:30
4	人事課	江村 太郎	Android		11 080xxxxxxx	07bc80ce	N-04C_0000000020	2022/08/24 10:17:06
5	営業部	橋中 栄一郎	Android		11 080xxxxxxx	07bc81ce	EB-A71GJ_0000000019	2022/08/24 04:25:31
6	営業部	内田 健太	Android		11 080xxxxxxx	07bc76ce	L-22D_0000000016	2022/08/20 08:49:54
7	営業1課	中田 真由美	Android		11 080xxxxxxx	FE1WR07HA9EV	404KC_0000000023	2022/08/24 05:17:55
8	営業1課	橋 秀雄	Android		11 090xxxxxxx	N3HXEFPWUJ9W	picasso_aapcus6jp_00000000...	2022/08/24 04:51:57
9	総務課	森 太郎	iOS		14.4 080xxxxxxx	77WW8C9CA26	iPhone_000000026	2022/08/24 11:24:55
10	営業1課	別所 哲郎	iOS		13.2 080xxxxxxx	77WW8C9CA29	iPhone_000000029	2022/08/24 03:10:04
11	営業1課	吉田 勝平	Windows	Windows 10 Pro 10.0.1...	090xxxxxxx	DemoSerialNumber_00001	Surface Pro 5_0000000044	2022/08/24 08:23:27
12	営業1課	加藤 信也	Windows	Windows 10 Pro 10.0.1...	090xxxxxxx	DemoSerialNumber_00002	Surface Pro 5_0000000045	2022/08/24 08:23:25
13	営業1課	石井 健二	Android		9 080xxxxxxx	FE1WR07HA9EV	404KC_0000000023	2022/08/24 05:17:55
14	営業2課	平尾 晋作	Android		9 080xxxxxxx	07bc82ce	404KC_0000000018	2022/08/24 10:38:41
15	営業2課	佐藤 理恵子	Android		10 080xxxxxxx	07bc83ce	404KC_0000000007	2022/08/24 05:03:05

登録済みライセンス: 83 / 100

1000 1 - 85件 / 全 85件

iOS iPhone_000000028 - デバイス詳細

取得日時: 2023/05/06 12:32:30

システム

OSバージョン iOS 14.4 (98176)

ネットワーク

セキュリティ

インストールアプリ

プロファイル

位置情報

操作ログ

アラート

リモート操作

クライアント

デバイス情報

位置情報サービス

LANSCOPE Client ID

iPhoneを探す ON

アクティベーションロック ON

最新 iCloud バックアップ日時 2017/12/07 14:38:25

iTunes Store アカウント状態 有効

デバイスの詳細情報も1Clickで確認!

一 『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が。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、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。

LANSCOPE リスト レシビ モニター レポート 環境設定

設定管理者 (元中)

レポート ログ検索

長期間未稼働のデバイス

iOS Android Windows macOS

長期間電源が入っていない、紛失の可能性があるデバイスを把握できません。

ネットワーク... 集計日時: 2020/09/15 13:35:08

5台

- 1ヶ月以上 (3)
- 1週間~1ヶ月 (2)

配下のグループ

- ネットワーク全体 (直下) 対象のデータがありません
- 総務課 対象のデータがありません
- 人事部 対象のデータがありません
- 営業部 3台
- システム部 1台

管理No.	デバイス管理名	使用者名	↑ LANSCOPE クライアント最終稼働日時	デバイスグループ	OSタイプ
21	iPad_00000034	小林 哲司	2021/01/17 08:00:00	営業1課	iOS
31	FAR7_0000000004	共有タブレット (システム部...	2021/02/11 06:24:05	システム1課	Android
27	iPhone_00000027	畠山 哲夫	2021/02/22 03:53:21	営業2課	iOS
55	Surface Pro 3_00000000...	検証用A	2021/03/16 09:07:29	検証用	Windows
53	MacBook_00000051	平尾 晋作	2021/03/16 09:32:21	営業2課	macOS

最終稼働日でソート

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

対象OS

管理台数 200台

Windows

iOS

Android

macOS

「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。

LANSCOPE リスト レシビ モニ

検索 一括出力

操作ログ (Windows / macOS)

どのPCで・いつ・誰が

どのくらい・何をしたか

日時	ユーザー名	ログの種類	イベント	タイトル	ファイルパス
2022/08/24 17:36:00	MO一部	ファイル操作	ファイル削除	C:\Documents and Settings\vsudou\デスクトップ...	
2022/08/24 18:15:00	MO一部	ファイル操作	ファイル移動元	C:\Documents and Settings\vsudou\Local Setting...	
2022/08/24 18:16:00	MO一部	ファイル操作	ファイル移動先	C:\Documents and Settings\vsudou\Local Setting...	
2022/08/24 18:17:00	MO一部	ファイル操作	ファイル移動元	C:\Documents and Settings\vsudou\Local Setting...	
2022/08/24 18:18:00	MO一部	ファイル操作	ファイル移動先	C:\Documents and Settings\vsudou\Local Setting...	
2022/08/24 19:44:00	MO一部	ファイル操作	ファイル作成	C:\Documents and Settings\vsudou\Local Setting...	
2022/08/24 19:54:00	MO一部	脅威検知		C:\Users\Vichiro.mo\AppData\Local\Microsoft\Window...	
2022/08/24 19:59:00	MO一部	脅威検知			
2022/08/24 20:00:00	MO一部	Webアクセス	閲覧	CD Writing Soft WebSite - Google Chrome	
2022/08/24 20:01:00	MO一部	Webアクセス	ダウンロード	Downloading... - CD Writing Soft WebSite	
2022/08/24 20:02:00	MO一部	脅威検知		C:\Program Files\CD Writing Soft\CD Writing Sof...	C:\Users\vmotex\Downloads\CD Writing Soft.exe
2022/08/24 23:32:00	MO一部	ファイル操作	ファイルコピー元		\\192.168.102.241\【社外】営業部\営業1課用\V観...
2022/08/24 23:32:00	MO一部	ファイル操作	ファイルコピー先		C:\Users\Vichiro.mo\MOTEX\Desktop\顧客リスト.xlsx
2022/08/24 23:36:00	MO一部	ファイル操作	ファイル名変更前		C:\Users\Vichiro.mo\MOTEX\Desktop\顧客リスト.xlsx
2022/08/24 23:36:00	MO一部	ファイル操作	ファイル名変更後		C:\Users\Vichiro.mo\MOTEX\Desktop\商品案内.xlsx
2022/08/24 23:37:00	MO一部	ファイル操作	ファイル閲覧		C:\Users\Vichiro.mo\MOTEX\Desktop\商品案内.xlsx
2022/08/24 23:37:00	MO一部	Webアクセス	閲覧	マイドライブ - Google ドライブ - Google Chrome	
2022/08/24 23:37:00	MO一部	Webアクセス	閲覧	マイドライブ - Google ドライブ - Google Chrome	
2022/08/24 23:40:00	MO一部	Webアクセス	アップロード	マイドライブ - Google ドライブ - Google Chrome	C:\Users\Vichiro.mo\MOTEX\Desktop\商品案内.xlsx

条件を保存 検索

ファイル操作アラート

実行したファイル操作は、社内ルールに違反しています。

[抵触時のファイル名]
2020/08/18 14:22:23

閉じる

アプリケーション禁止

起動しようとしたアプリケーションは、社内ルールによって禁止されています。

[抵触時のアプリ]
2020/08/18 14:27:25

閉じる

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。

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

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

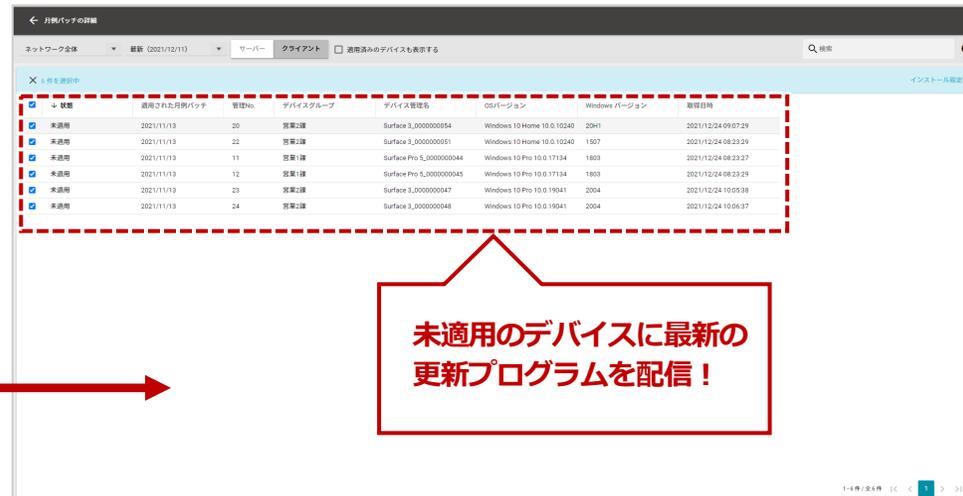
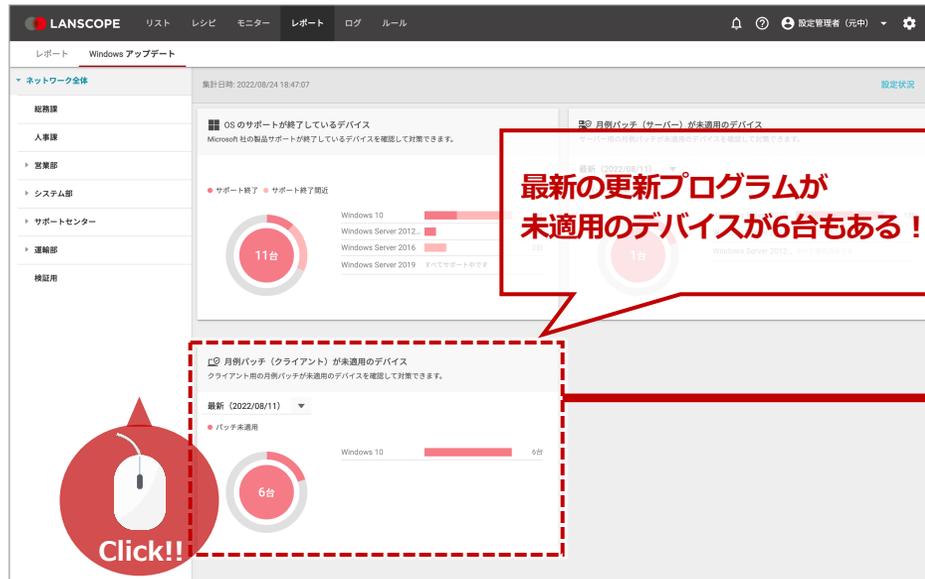
管理台数 250台

対象OS

Windows iOS Android macOS

— 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。



— 月額450円で高精度の AI アンチウイルスが利用可能。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、一般的なアンチウイ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イ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。



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

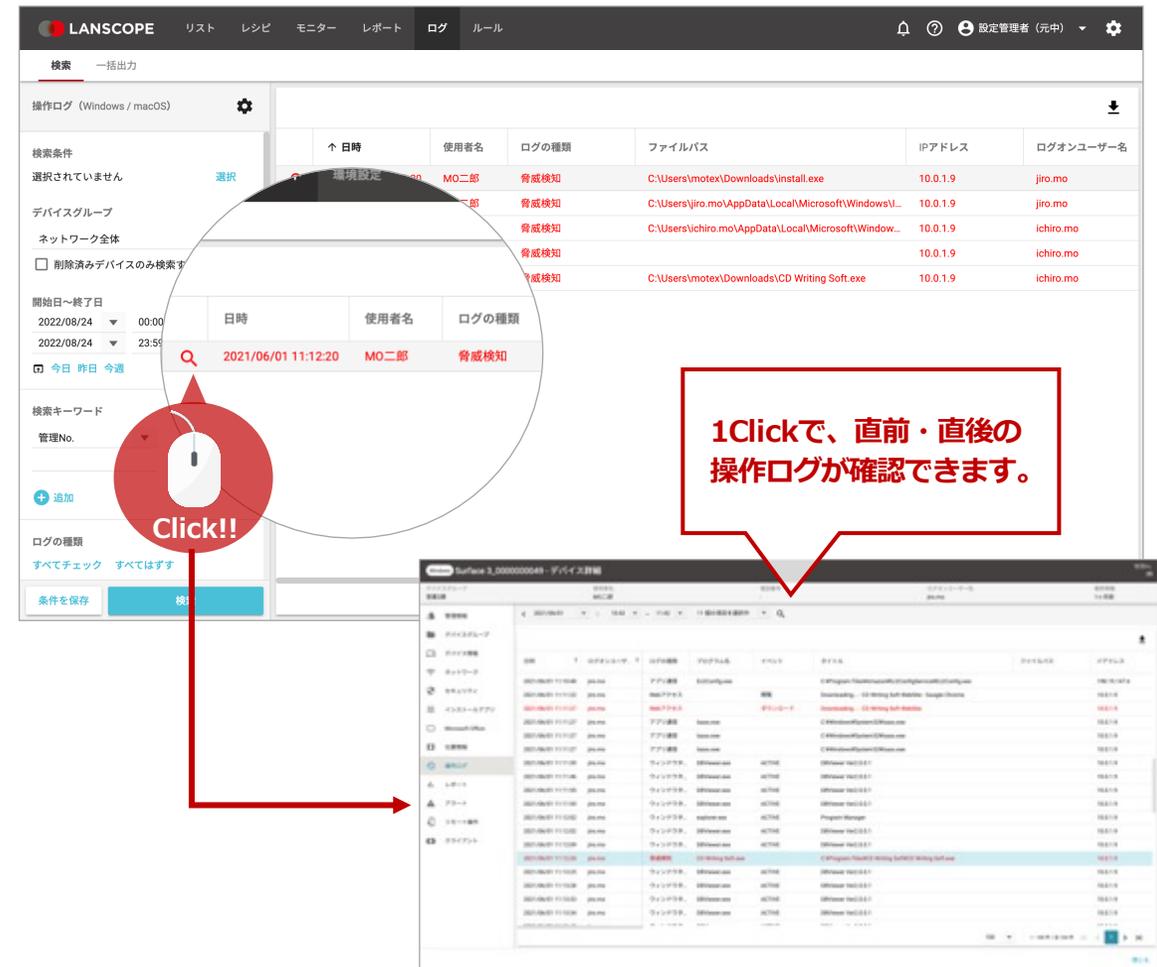
PC への負荷が小さく
快適なパフォーマンス
を發揮

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！

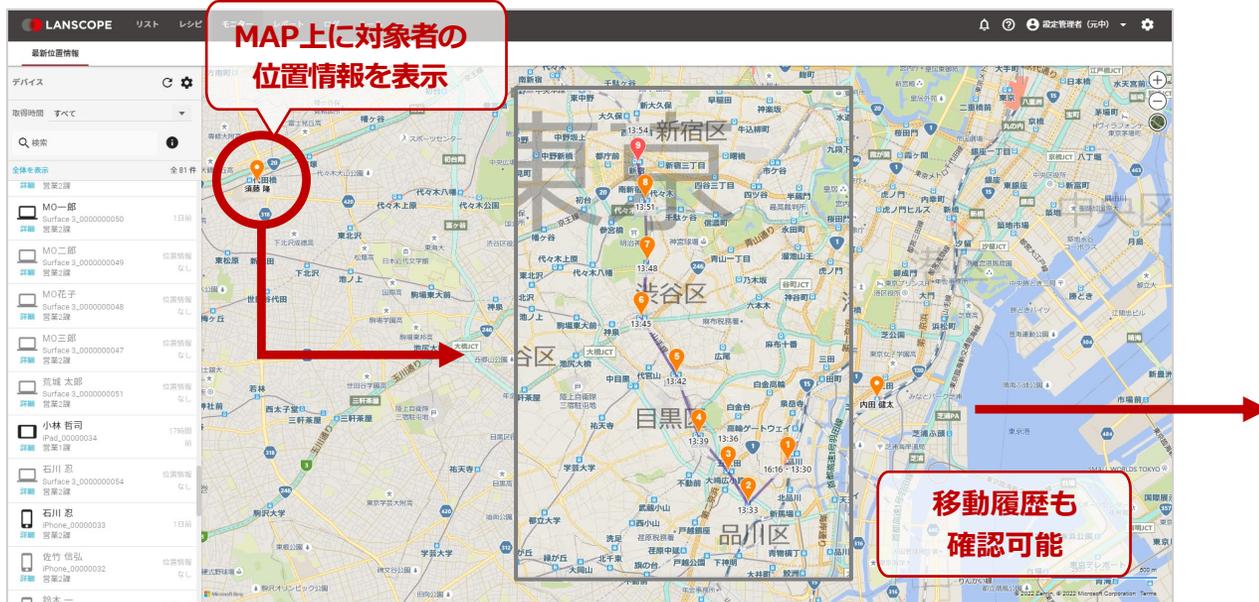
卸売・小売業

職員数 140名 対象OS

管理台数 80台 Windows iOS **Android** macOS

— 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。



一 利用者に依存しがち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が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。

パスワードポリシー

設定する

パスワードの最小文字数*

9文字

単純値 (aaaa、1234 など)

禁止する

英字と数字

必須にする

英数字以外の文字の最小文字数

設定する

最小文字数*

4文字

パスワードの有効期間

設定する

有効期間 (日) (1 ~ 730 日)*

90

以前使用したパスワードの再使用

禁止する

再使用禁止回数*

2回

パスワード入力連続失敗によるデバイス初期化

初期化する

連続失敗回数*

5回

パスワードの文字数や有効期間の設定が可能

この設定を有効にすることで、オフライン時でもワイプが実行されます。Wi-Fi モデルのデバイスにも有効！

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
パスワ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ワ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

管理台数 120台

Windows iOS **Android** macOS

— 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。

Storeカテゴリやアプリ名でも検索可能！

アプリ	管理アプリ	インストール台数	デベロッパー	カテゴリ	アプリケーションID
2ちゃんねるまとめサイトビ...		3台	Trysail Inc.	仕事効率化	com.mt2
Evernote		18台	Evernote	仕事効率化	com.evernote.iPhone.Evernote
FastEver XL - 素早く...		7台	rakko entertainment	仕事効率化	com.rakkoentertainment.Fas...
GNews leader		8台	LeadingWin Co.Ltd	仕事効率化	jp.co.leadingwin
LockMail		3台	Canned Bananas LLC	仕事	com.cannedbananas.lockno...
ガイガ カウンタ...		1台	Image Insight, Inc.	仕事	com.dosiapp.RadiationDosi...
チャットワーク		1台	ChatWork Inc.	仕事	com.chatwork
メモリースター(Memory B...		7台	AIO Toolbox Inc.	仕事効率化	imobile.memorybooster.full
Microsoft Outlook		5台	Microsoft Coporation	仕事効率化	com.microsoft.Office.Outlook
LINE WORKS		5台	Works Mobile Corps.	ビジネス	com.nhncorp.worksone
Google マップ - 乗換案内 & ...		1台	Google LLC	ナビゲーション	com.google.Maps
乗換案内		6台	Jorudan Co.,Ltd.	ナビゲーション	jp.co.jorudan.NorikaeAnnai
Pokémon GO		6台	Niantic, Inc.	ゲーム	com.nianticlabs.pokemongo
100万人のための麻雀		2台	UNBALANCE Corporation	ゲーム	jp.co.unbalance.android.mj1...

ゲームアプリが2台インストールされている！

Click!!

そのデバイスにインストールされているアプリも1Clickで確認可能！

iOS iPhone_00000027 - デバイス詳細

取得日時: 2017/12/07 18:42:23

アプリ名	バージョン	管理アプリ	デベロッパー	カテゴリ	アプリケーションID	アプリサイズ
Evernote	10.5.1		Evernote	仕事効率化	com.evernote.iPhone.Evernote	0Bytes
2ちゃんねるまと...			Trysail Inc.	仕事効率化	com.mt2	0Bytes
FastEver XL - 素...			rakko entertainm...	仕事効率化	com.rakkoentertainment.Fas...	0Bytes
AIO Toolboxスタ...			AIO Toolbox Inc.	仕事効率化	imobile.memorybooster.full	0Bytes
GNewsReader			LeadingWin Co.Ltd	仕事効率化	jp.co.leadingwin	0Bytes
LINE WORKS			Works Mobile Co...	ビジネス	com.nhncorp.worksone	0Bytes
乗換案内			Jorudan Co.,Ltd.	ナビゲーション	jp.co.jorudan.NorikaeAnnai	0Bytes
Pokémon GO	1.167.1		Niantic, Inc.	ゲーム	com.nianticlabs.pokemongo	0Bytes
100万人のための...			UNBALANCE Cor...	ゲーム	jp.co.unbalance.android.mj1...	0Bytes
Drive Safe Text S...			Cosey Managem...		appinventor.ai_a4ayush.SMS...	0Bytes
私の車を見つけ...			Presselite		appinventor.ai_hejia_blavitt.FL...	0Bytes
Graffiti Pro for iOS			ACCESS CO.,LTD.		com.access_company.graffit...	0Bytes
WidgetPad			Calcium Ion Ltd.		com.calciumion.swipecad.ad...	0Bytes
Handbook			Infoteria Corpora...		com.infoteria.handbook	0Bytes

— 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



Android Enterprise

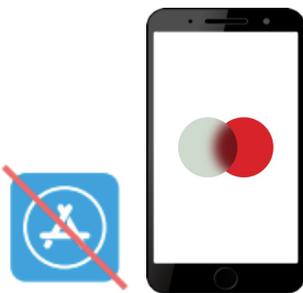


連携

エンドポイントマネージャー



App Store を
禁止していても
管理可能



配信

許可したアプリ
のみPlay ストア
に表示



配信

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最低限の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	デバイス種類、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。	<input type="checkbox"/>
1.2	購入日、リース期限、資産管理No.、利用権、保管場所などの情報管理している。	<input type="checkbox"/>
1.3	Apple ID や Google ID をデバイスに付帯している場合、誰がどのApple ID を利用しているか管理している。	<input type="checkbox"/>
1.4	デバイスの修理状況を記録し、定期的に更新を行っている。	<input type="checkbox"/>
1.5	各種ソフトウェアのライセンスを台帳等で管理し、ライセンス満期が近いを確認している。	<input type="checkbox"/>
1.6	USBメモリなどの外部を介している記録メディアを台帳等で管理している。	<input type="checkbox"/>
1.7	不要なアプリケーションインストールや削除を定期的に行っている。	<input type="checkbox"/>
1.8	シャットダウンのため、管理外のPCの社内ネットワーク接続を切断、制限している。	<input type="checkbox"/>
1.9	遠隔地に存在するデバイスでトラブルが発生した場合は、リモートコントロールを実施することができる。	<input type="checkbox"/>
2 情報漏洩対策		
2.1	情報セキュリティに関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に従事員に教育・周知している。	<input type="checkbox"/>
2.2	機密データ等の情報漏洩の懸念を行っている。	<input type="checkbox"/>
2.3	機密の漏洩記録として、操作ログを取得している。	<input type="checkbox"/>
2.4	OSint や 匿名化し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。	<input type="checkbox"/>
2.5	画像、音声などの写真、音声は圧縮し、高画質で共有することができる。	<input type="checkbox"/>
2.6	情報の持ち出しについて、会社許可した記録メディアやオンラインストレージ以外を使用できないように制限している。	<input type="checkbox"/>
2.7	機密データを保管するファイル名のアクセスを制限している。	<input type="checkbox"/>
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外部サービスのダウンロード）を把握している。	<input type="checkbox"/>
2.9	漏洩条件があった場合に、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。	<input type="checkbox"/>
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。	<input type="checkbox"/>
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。	<input type="checkbox"/>
3.3	ブラウザについて、最新のバージョンを適用している。	<input type="checkbox"/>
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更新している。	<input type="checkbox"/>
3.5	設定が変更できない Web サイトを利用できないように制限している。	<input type="checkbox"/>
3.6	ウイルス対策ソフトについて、悪意あるファイルの検出状況やマルウェアの検出状況を一覧管理している。	<input type="checkbox"/>
3.7	Free Web 版のアドウェアやアドウェアの検出を行っている。	<input type="checkbox"/>
3.8	NGAV (Next Generation Antivirus) に応答づけられるような、より高度なウイルス対策ソフトを導入している。	<input type="checkbox"/>
3.9	EDRソリューション等で、なぜ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。	<input type="checkbox"/>
4 盗難・紛失対策		
4.1	SIM が盗み取られたかデバイスを検知し、すぐに把握することができる。	<input type="checkbox"/>
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。	<input type="checkbox"/>
4.3	パスワードは数語（1234,1111など）ではなく、強度のある複雑かつパスワードが設定されるように制限している。	<input type="checkbox"/>
4.4	設定したパスワードは定期的に変更している。	<input type="checkbox"/>
4.5	設定したパスワードを、第三者に教えないよう教育・周知している。	<input type="checkbox"/>
4.6	紛失した場合に備えて、デバイスの現在の場所や移動履歴を確認できる。	<input type="checkbox"/>
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。	<input type="checkbox"/>
4.8	紛失した場合に備えて、遠隔でリモートロック・ワイプ後の検出状況を行うことができる。	<input type="checkbox"/>
4.9	BitLocker、FileVault 等でハードディスクを暗号化している。また、実行された暗号キーを適切に管理している。	<input type="checkbox"/>

情報セキュリティ36項目チェックシート



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

60日間無料で体験できます！

体験版を利用したお客様の7割が製品版をご導入いただいています



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。

MOTEX

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

ご購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

・記載の会社名および製品名・サービス名は、各社の商標または登録商標です。

・MOTEX はエムオーテックス株式会社の略称です。