

導入に必要な環境 *100台環境、標準バックの場合

統合マネージャー／サブマネージャー

- OS
Windows Server 2012、Windows Server 2012 R2、
Windows Server 2016、Windows Server 2019
- CPU
2.0GHz以上
- メモリ
4GB以上 *SQL Server 2019を利用する場合はメモリが8GB以上が必要です。
- HDD空き容量
200GB以上
- データベース
SQL Server 2012、SQL Server 2014、SQL Server2017、SQL Server2019
- Webコンソール(ブラウザ)
Internet Explorer 11 以上
Google Chrome 69 以上
Mozilla Firefox 62 以上

Catエージェント

- | | |
|--|---|
| [Windows] | [Mac] |
| ●OS
Windows XP
Windows Vista
Windows 7
Windows 8
Windows 8.1
Windows 10
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019 | ●OS
OS X Mavericks
OS X Yosemite
OS X El Capitan
macOS Sierra
macOS High Sierra
macOS Mojave
macOS Catalina
macOS Big Sur |

BlackBerry エージェント

- | | |
|--|---|
| [Windows] | [Mac] |
| ●OS
Windows XP SP3
Windows Vista
Windows 7
Windows 8
Windows 8.1
Windows 10
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019 | ●OS
OS X Mavericks
OS X Yosemite
OS X El Capitan
macOS Sierra
macOS High Sierra
macOS Mojave
macOS Catalina
macOS Big Sur |

*マネージャーのハードウェア環境は、クライアント数100台までの推奨環境です。管理する台数や収集するログにより推奨環境が異なります。
*マネージャーサーバーは、同一OS内に他システムと共存させることも可能ですが、専用ハードウェアをご用意いただくことを推奨しています。
共存させる場合、問題発生時の切り分けなど、サーバーの分離をお願いする場合があります。
*データベースは本製品に付属の製品、もしくはお持ちのMicrosoft SQL Serverライセンスが利用できます。
*500台以上をクラウド環境で管理する場合、本製品に付属のSQL Server(Standard Edition)は利用できません。
*Webコンソールの一部コンテンツの表示には、Silverlight5以降のインストールが必要です。
*エージェントの動作環境 (CPU、メモリ、HDD空き容量) はOSの推奨システム要件を満たしてください。
同居ソフトウェアの使用状況により必要となるシステム要件が変更になる場合があります。
*クライアントエージェント (MR) は日本語／英語／中国語 (簡体字) の海外OSに対応しています。
*Mac OS X Mountain Lion以前の管理には、LanScope Cat Ver.9.0のクライアントエージェントを利用する必要があります。
*対応OSについての詳細は、弊社Webサイト公開のOS対応表をご覧ください。
*Apple M1チップ搭載の端末については、Ver.9.3.3.3 (MacMR A9320) から対応しています。
*マルウェア対策ライセンスについての詳細はお問い合わせください。
*Apple M1チップ搭載の端末については、Ver.9.3.3.3 (MacMR A9320) から対応しております。
*SQL Server 2019をご検討の場合お問い合わせください。

●お問い合わせは当社へ

●開発／販売

エムオーテックス株式会社

本 社 〒532-0011 大阪市淀川区西中島 5-12-12 エムオーテックス新大阪ビル TEL：06-6308-8980
東京本部 〒108-0075 東京都港区港南 1-2-70 品川シーズンテラス 5F TEL：03-5460-1371
名古屋支店 〒460-0003 名古屋市中区錦 1-11-11 名古屋インターシティ 3F TEL：052-253-7346
九州営業所 〒812-0011 福岡市博多区博多駅前 1-15-20 NMF 博多駅前ビル 2F TEL：092-419-2390

TEL：0120-968995 受付時間 9:30-12:00、13:00-17:30 (月～金曜日)
※携帯電話／PHSからは06-6308-8981をご利用ください。

E-mail: sales@motex.co.jp
URL: www.motex.co.jp

- 本カタログは、2021年6月現在の内容となります。
最新の情報および制限事項詳細は弊社Webサイトをご確認ください。
- 本カタログは予告なく変更することがあります。
画面／パッケージ等は実際の物とは異なることがありますので、予めご了承ください。
- エムオーテックス／MOTEX、Secure Productivityは、エムオーテックス株式会社の登録商標です。
- Hangouts ChatはGoogle LLCの商標です。
- その他、カタログに記載の会社名、ブランド、製品、ロゴなどは、各社の商標または登録商標です。

市場シェア

NO.1

富士キメラ総研 2020 ネットワークセキュリティビジネス
調査総覧「IT資産管理ツール」2019年度

LANSCOPE
on-premises

ウイルス対策も情報漏洩対策もこの1本で



MOTEX

“Secure Productivity”

安全と生産性の追求

統合エンドポイント管理で

複雑化するITマネジメントをシンプルに、より効率的に。

サイバー攻撃、内部不正のリスクから組織を守り

IT活用による組織の生産性を高めます。

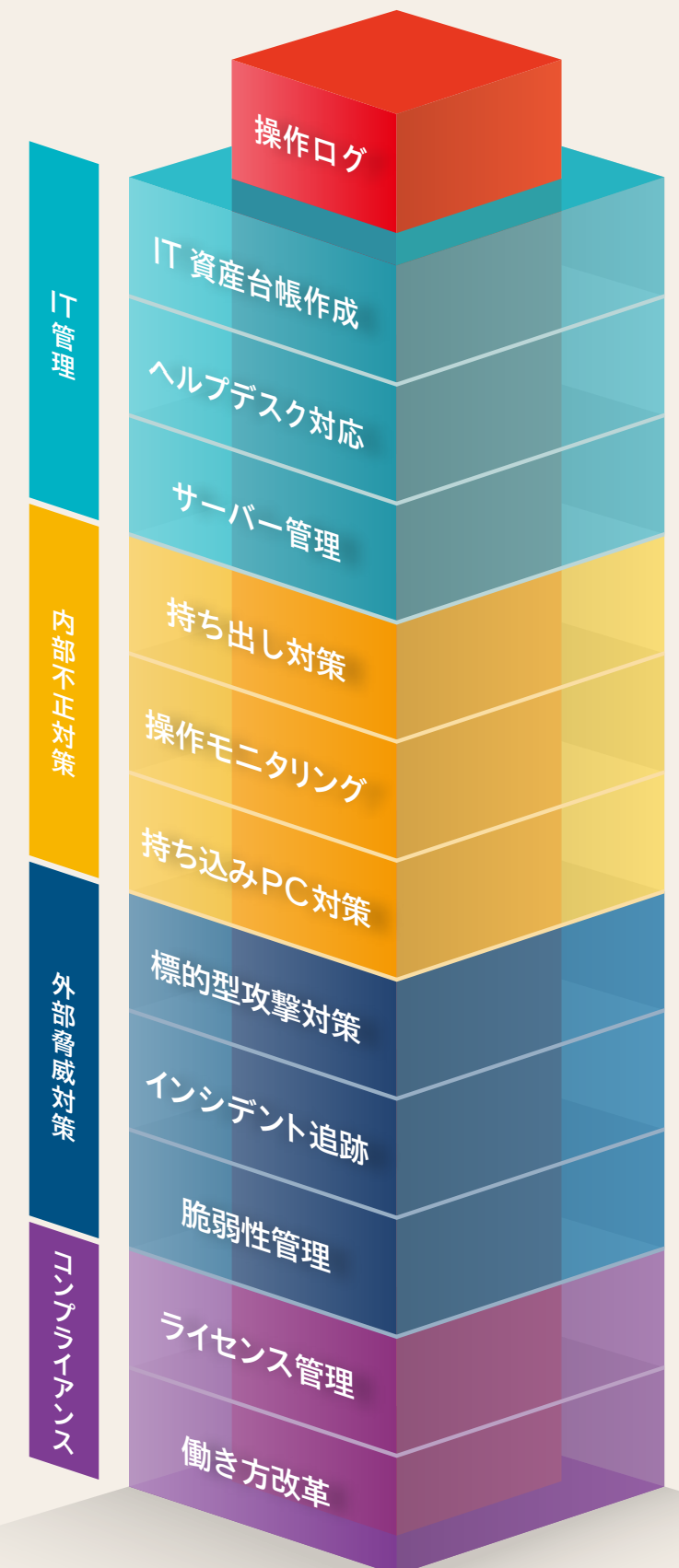


組織の生産性を高め、同時に大切な情報資産を守るためには、「エンドポイント」を管理することが重要です。

なぜなら、IT資産管理／内部不正対策／外部脅威対策のすべてと密接に関係し、最もリスクにさらされているものは「エンドポイント」であるからです。

しかし、それらの管理には複数のツールを組み合わせる必要があり、その運用はますます複雑化しています。

「統合エンドポイント管理」
LANSCOPEは、これらを統合管理することで、シンプルで効率的なITマネジメントを実現します。



LANSCOPEの信頼と実績

シェア No.1、
10,000以上のユーザー様に
ご導入いただいています。

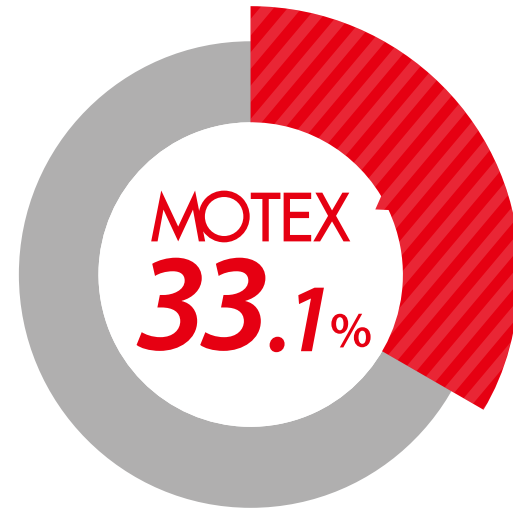
市場シェア No.1

富士キメラ総研 2020 ネットワークセキュリティビジネス調査総覧
「IT 資産管理ツール・2019 年度」



ITreview Leader 獲得

アイテッククラウド社が運営する法人向け IT 製品・SaaS のレビュー
サイト ITreview で、IT 資産管理・ログ管理の 2 部門で Leader
を獲得。



継続利用率 93%

ご購入いただいたお客様のうち、93%の
方に継続してご利用いただいています。
この数字はお客様満足度の証です。

2018年10月現在

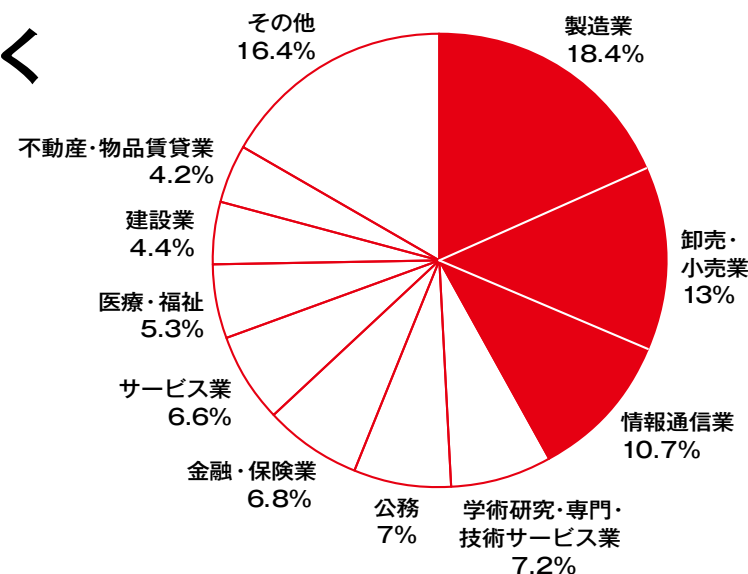
規模を問わず、
すべての業種で幅広く
利用されています。

金融機関の3分の1

上場企業の4社に1社が導入

■ 上場企業導入数

東証一部	東証二部	マザーズ	JASDAQ
636社	97社	56社	139社



2017年8月現在

お客様の課題に合わせた

LANSCOPE 活用シーン

case 1

情報漏えい対策

「改正個人情報保護法」に対応。安全管理措置における
「技術的安全管理措置」をエンドポイントで対策できます。

▶ P.5

case 2

標的型サイバー攻撃対策

既知・未知のマルウェアを 99%以上防御。
さらに流入経路の特定から対策まで可能になります。

▶ P.6

case 3

「働き方改革」を支援

働き方改革への対応は、見える化が重要です。
“人”の操作を把握し実態に基づいた取り組みを支援します。

▶ P.7

case 4

Windows アップデート対応

アプリの互換性確認・更新プログラムへの対応など、
Windows10 の企業導入・運用を支援します。

▶ P.8

case 5

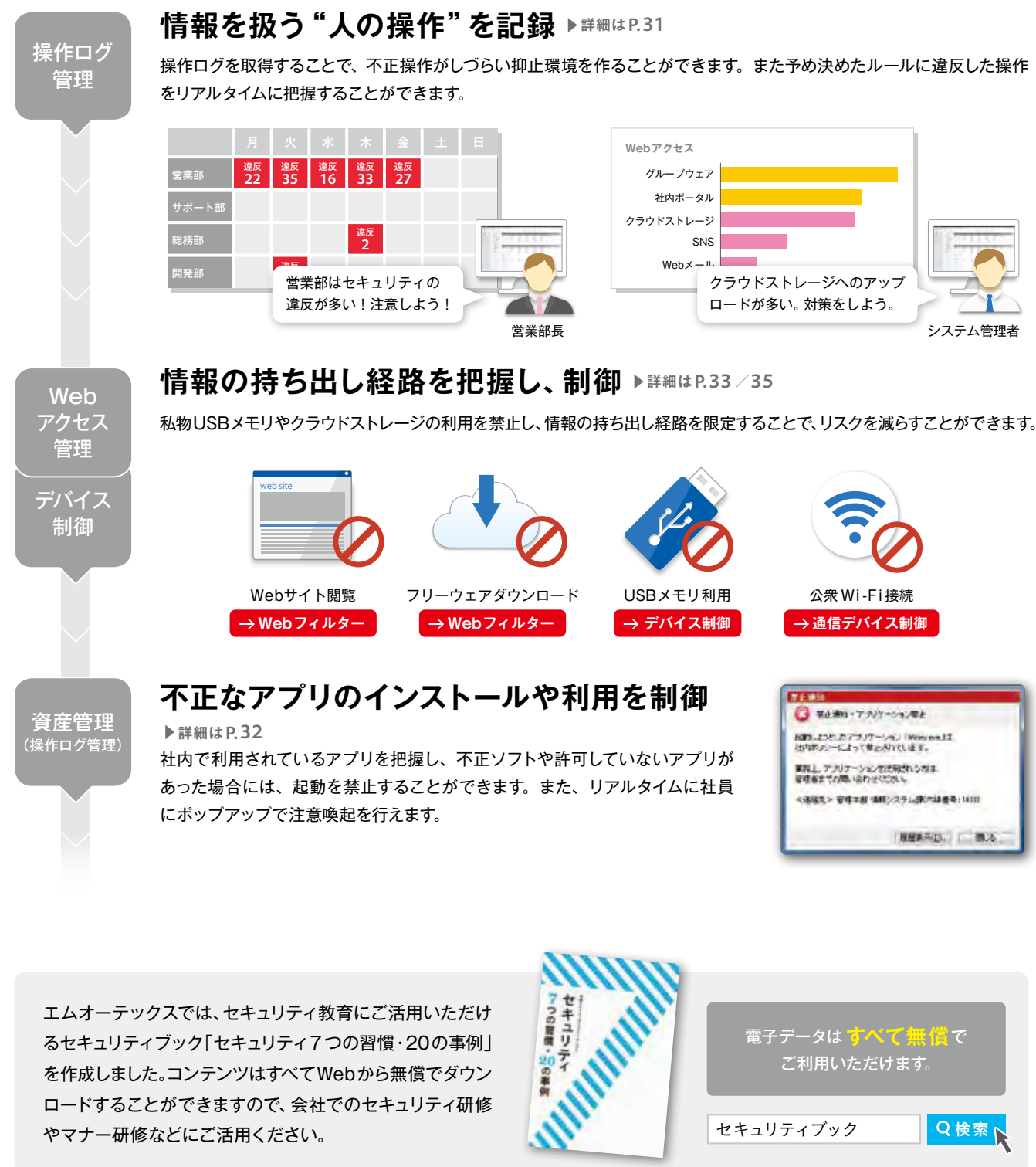
IT 資産管理・ヘルプデスク対応

ハードウェア・ソフトウェアの情報を自動収集し棚卸を支援。
PC 環境のメンテナンスとヘルプデスク対応に活用できます。

▶ P.9

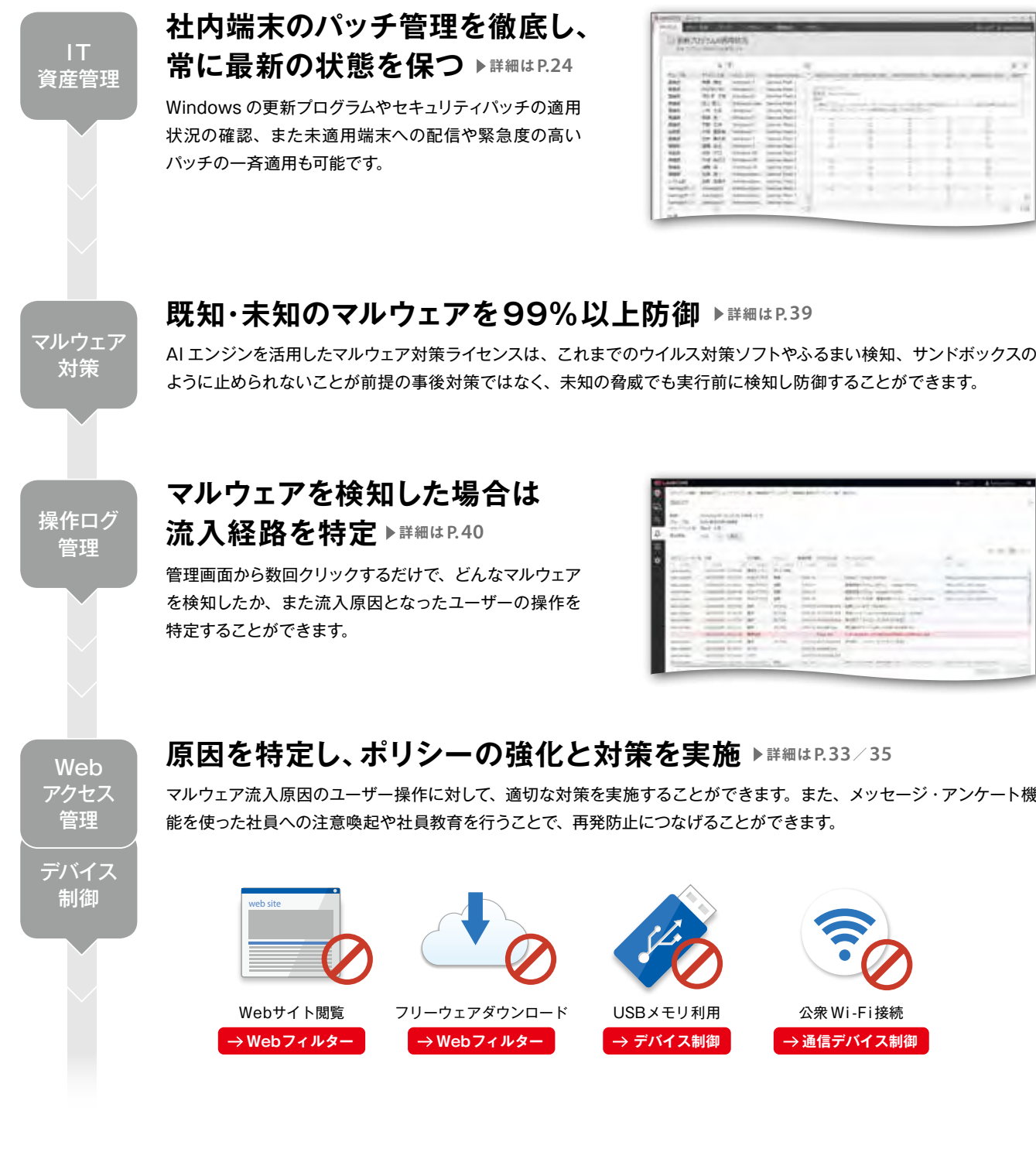
改正個人情報保護法における 「技術的安全管理措置」をエンドポイントで対策。

2017年に全面施行された改正個人情報保護法により、取り扱う個人情報の数が5,000件以下の事業者（小規模取扱事業者）を含み、一部を除くすべての事業者が個人情報取扱事業者として改正法の適用を受けることになり、その対応が求められています。



既知・未知のマルウェアを99%以上防御。 さらに流入経路の特定から対策までが可能。

1日に誕生するマルウェアは100万個ともいわれており、従来のアンチウイルスだけで脅威から組織を守ることは難しくなっています。BlackBerry Protect®と機能連携することで猛威を振るうサイバー攻撃から大切な情報／人を守ります。



働き方改革への対応は、見える化が重要です。 “人”の操作を把握し実態に基づいた取り組みを支援。

働き方改革の第一歩は「現状把握」です。今の働き方を把握した上で、負荷の偏りを発見し分散したり、オフィス以外での業務実態を知り最適な対応を行うことでリモートワークを推進することができます。

操作ログ管理

“人の PC 操作”を記録 ▶詳細は P.31

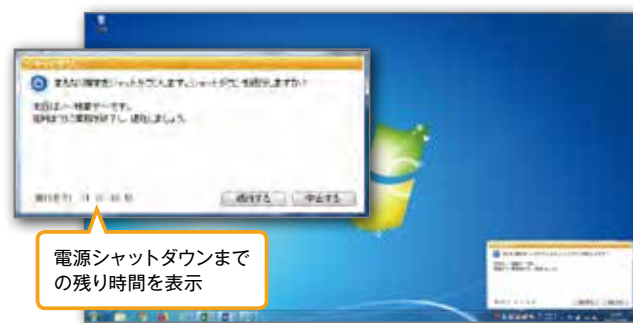
社内はもちろん、社外やネットワーク非接続環境の PC でも「誰が」「いつ」「どのくらいの時間」「何をしたか」をログとして取得できるので、業務実態を把握できます。



電源／省電力管理

電源管理で、定時退社を促進 ▶詳細は P.22

ノー残業デーなど、指定した時刻に端末上にメッセージを表示、また強制的にシャットダウンを行うことができます。クライアント単位で定期電源設定を一時的に解除することも可能です。



レポート

各種レポートを業務管理に活用 ▶詳細は P.47



業務時間外に操作されたパソコン台数を一目で把握できます。



業務時間外に操作されたパソコンの一覧と、残業申請を突合することで、サービス残業を把握できます。

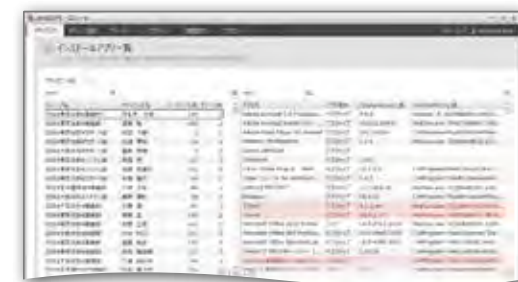
Windows10 のアップデート状況の確認、配信。 BitLocker の暗号化キーを一元管理。

マイクロソフト社はWindows10 からOSの永続的なアップデートのため WaaS (Windows as a Service) という考えを取り入れ、OS のサポート期間は各アップデートから18ヶ月または 30ヶ月となり企業は計画的なバージョンアップが必要となります。

IT 資産管理

Windows10 導入に向けた事前準備。現在の利用状況を把握、アプリの互換性を確認

利用中のアプリの中にはWindows 10 との互換性がないものやパッチ適応が必要な場合があります。事前に利用が多いアプリを把握することで、導入前に対策を打てます。



IT 資産管理

年2回の機能更新プログラム (FU)への対応

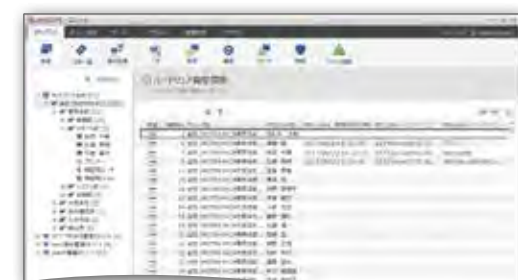
OSのアップデートに合わせて、利用中のアプリもバージョンアップが必要になります。ファイル配布機能を使えば、一斉にアップデートを適用できます。



IT 資産管理

ドライブ暗号化機能をさらに活用

Windows 10 ではドライブ暗号化機能であるBitLocker が標準で搭載されました。LANSCOPE ではBitLocker による暗号化の状況確認、回復キーの収集が行えます。



LANSCOPEのWindows 10 対応ポリシー

MOTEX は、Windows 10 環境でも安心してご利用いただくため、Windows 10 のアップデートに対して以下3つのポリシーを表明しています。

- 機能更新プログラムのリリース後、3ヶ月を目処に対応バージョンをリリース
- バージョンアップはクライアントのみ(マネージャーのバージョンアップ不要)
- LANSCOPE の各バージョンリリースから2年間、対策プログラムを提供

ハードウェア・ソフトウェアの情報を自動収集し棚卸を支援。 PC環境のメンテナンスとヘルプデスク対応に活用できます。

IT資産の棚卸を行うと、ハード・ソフトウェアの数や利用状況を可視化できます。その結果、正確なライセンス管理ができ、未稼働分のソフトウェアのライセンスに係るコスト削減、ソフトウェアを最新状態に保てるため、セキュリティ面でも効果が期待できます。

IT
資産管理

ソフトウェア
資産管理

ファイル
配布

REMO-
CON

ハードウェア資産情報を自動収集し、常に正確な情報を把握 ▶詳細はP.23

コンピュータ名、IPアドレスの情報など50種類以上を自動取得。WindowsとMacの混在環境でも一元管理を実現します。

ソフトウェア情報を自動取得し、不審なファイルやアプリがないかを確認 ▶詳細はP.26

ライセンスの過不足や利用状況を把握し、必要な対策が打てます。またバージョン情報はアプリの脆弱性管理に活用できます。

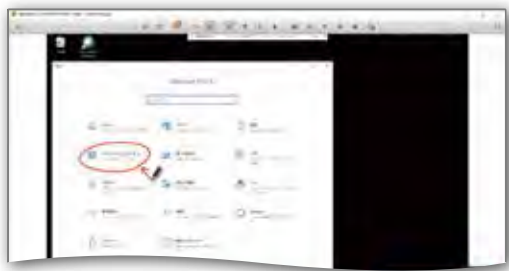
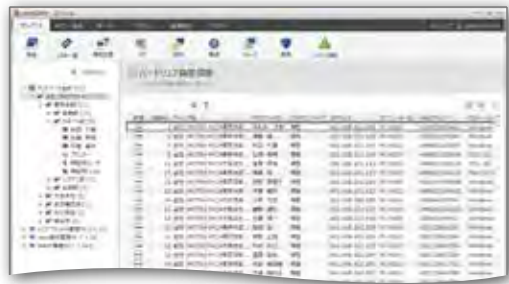
アプリを自動インストールし、クライアント環境を標準化 ▶詳細はP.27

特定アプリのインストール有無を条件に、指定アプリの自動インストールができます。複数ファイルを組み合わせた配布物の作成、配布スケジュールなど柔軟な配布設定ができます。

リモート操作でヘルプデスクやメンテナンスの効率化を実現 ▶詳細はP.44

遠隔地にあるサーバーやPC、スマホへの「リモート操作」「画面共有」やWeb会議によりヘルプデスク業務を効率化します。

※ REMO-CON の購入が必要です



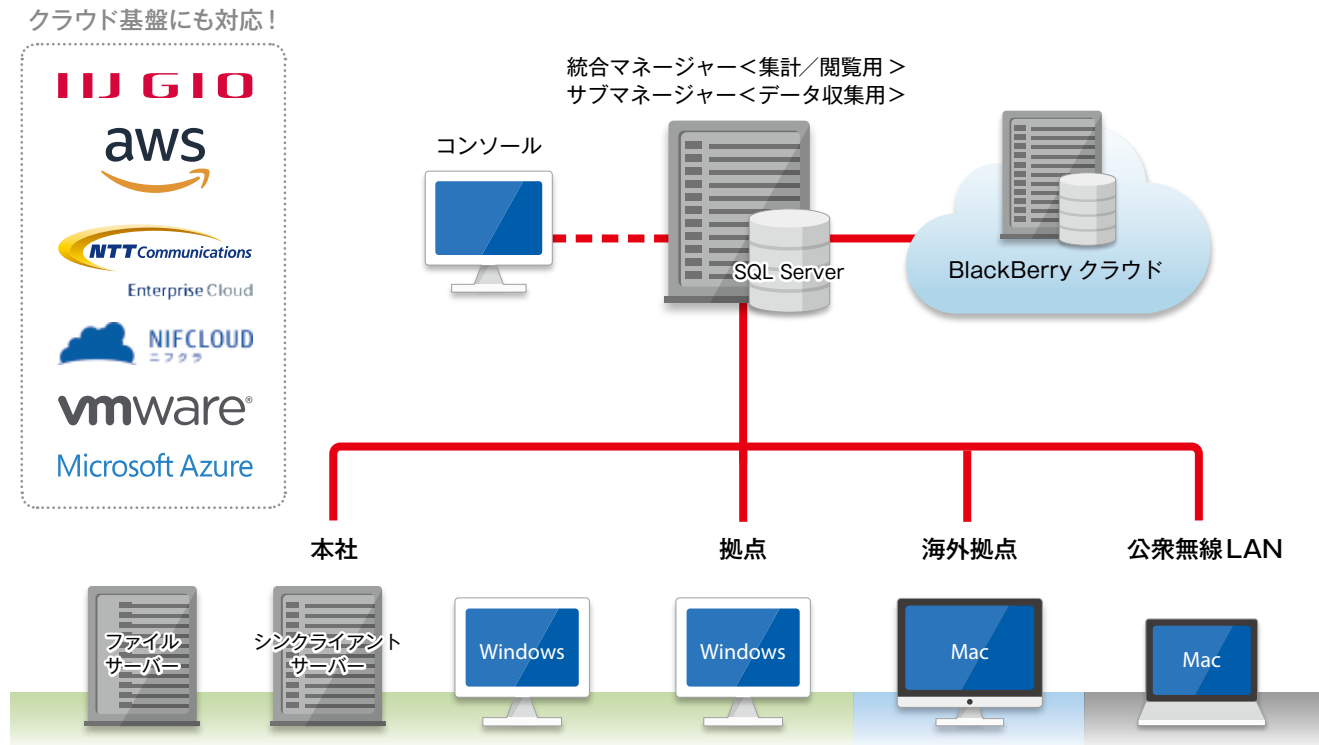
マネージャーライセンス(必須)	Webコンソール	ダッシュボード／レポート		組織の弱い部分を監視し、問題点の自動抽出から対策までをワンストップで実現します。グループ別、日付別など様々な切り口でログを集計／グラフ化できます。
		アラーム管理		ルール違反の有無をグループ単位／人単位で把握できます。各種ログを複数条件で組み合わせ、より重要度の高い1つのアラームとして通知できます。
		ログ検索／ファイル追跡		様々な条件で5年分のログを検索。抽出した特定ファイルの流出経路を追跡できます。
		資産情報の閲覧		コンピュータ名、IPアドレスなどのハードウェア情報、インストールされているソフトウェアの情報などを一覧で確認できます。
標準バック	ネットワーク検知	持ち込みPC検知		持ち込みPCなどの不正接続を検知し、リアルタイムに通知します。
		SNMP機器管理／死活監視		SNMP対応機器の情報を収集。稼働状況を確認し、死活監視ができます。
	IT資産管理	ハードウェア管理		コンピュータ名、IPアドレスなどの資産情報を自動取得。プリンター／周辺機器などを、任意で資産登録して管理できます。
		ソフトウェア管理		ソフトウェアのインストール情報を自動取得／集計し、許可／不許可を分類できます。
		アプリ稼働ログ管理／制御		アプリの稼働情報を取得し、未使用アプリを把握。不正アプリは禁止もできます。
		USB管理		接続されたUSBデバイスを自動検出し、台帳作成や未使用期間の確認ができます。
		電源／省電力管理		指定時刻にPC電源の強制OFFや、PC省電力設定の一括変更ができます。
		メッセージ・アンケート		管理者からユーザーに対して、メッセージ・アンケートを送信できます。
		ソフトウェア資産管理 (SAM)		ソフトウェア辞書を活用し、SAMに必要な台帳を作成。ライセンス違反を把握できます。また、アップグレード、ダウングレードなどの契約情報も管理できます。
		更新プログラム配布／脆弱性対策		サービスパック、更新プログラムの適用状況の把握。未適用PCに配布できます。
		アプリ配布／自動インストール		アプリの一括配布／インストールができます。また、インストール手順を録画することで、スクリプトを自動生成できます。
		Microsoft Defender連携		検知状況の集中管理・検知情報の管理者メール通知などMicrosoft Defenderの運用管理における課題を解決します。
バック1000	操作ログ管理	アプリ稼働ログ管理／制御		アプリの稼働情報を取得し、未使用アプリを把握。不正アプリは禁止もできます。
		操作ログ管理		PC上での画面閲覧（ウィンドウタイトル）やファイル操作を記録できます。
		プリントログ管理		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。
		アプリ通信ログ管理		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。
		通信デバイスログ管理		Wi-Fi／Bluetooth／赤外線／有線の接続を把握し、管理外の接続を検知できます。
	Webアクセス管理	動怠ログ管理		各クライアントの動怠情報（業務開始時間、業務終了時間、残業時間など）を閲覧できます。
		Webアクセス管理		Webサイトの閲覧や書き込み、Webメールやクラウドストレージへのアップロード／ダウンロード操作を記録します。また、不正サイトや操作の禁止もできます。
		Webアクセス制御／ホワイトリスト		不正サイトや操作の禁止もできます。またキーワードを指定し、特定のWebサイトのみ閲覧可能にできます。
		クライアントWebフィルタリング (オプション)		フィルタリングデータベースを用い、カテゴリからWebの閲覧を一括制御できます。
		デバイス制御		CD／DVD、フロッピー、USBメモリなどのデバイス種別単位で制御します。PCごとに禁止／許可／読み取り専用／一時許可／一時読み取り専用の設定ができます。
プレミアムバック	デバイス制御	個体識別管理		個別デバイスごとに禁止／許可／読み取り専用／一時許可／一時読み取り専用の設定ができます。
		接続USB管理		社内で利用したUSBデバイスを一覧で確認。未使用期間や最終使用者を把握できます。
		デバイス責任者設定		管理者以外に、登録したデバイスの利用を許可できる責任者を設定できます。責任者は自分のPCから許可／読み取り専用／一時許可／一時読み取り専用の設定ができます。
		通信デバイス制御		Wi-Fi／Bluetooth／赤外線通信への接続を制御できます。
		メール管理 (クライアント型) ▶P.37		Microsoft Outlookからの送信メールの内容や添付ファイルを記録できます。
	アプリID監査	ID監査ログ管理		システムへのログイン情報を記録し、なりすましなど不正なID使用を把握できます。
		特権ユーザー管理		特権ユーザーによるIDの作成、権限変更などの操作を記録できます。
		マルウェア検知		AIエンジンにより、未知の脅威をリアルタイムに発見できます。
		マルウェア隔離		検知した脅威ファイルをポリシーに応じて隔離できます。
		原因追跡 (操作ログ管理)		インシデント発生前後の操作を確認できます。
REMO-CON	サーバー監視	ファイルサーバーアクセスログ管理		WindowsやNetAppへのアクセスを記録し、権限のないアクセスを把握できます。
		ファイルサーバー容量管理		フォルダー容量を監視。設定したしきい値を超えると、管理者にメール通知できます。
		ドメインログオン・ログオフ管理		Active Directoryサーバーを監視し、ドメインへのログオン・ログオフを記録できます。
	不正PC遮断	持ち込みPC遮断		持ち込みPCなど、セキュリティリスクのあるPC接続を遮断できます。
		リモートアクセス (ワンタイム型／常駐型)		PCやサーバーに対し、管理者からリモートで画面を操作できます。
	REMO-CON	Web会議		Web上の会議で資料や画像の共有、音声&ビデオチャットができます。

・バック1000 は1001ライセンス以上のご購入はできません。また、バーチャルライセンスとMac 端末管理は含まれません。・アプリ稼働管理／制御は、IT資産管理ライセンス／操作ログ管理ライセンス両方に含まれています。・アプリ制御とWebアクセス制御はMac 端末管理非対応です。・Webコンソールは導入機能の取得情報に基づきレポートを表示します。・バーチャルライセンスは、シンクライアントサーバーごとかつ、利用ユーザー数分のライセンスの購入が必要です。・クライアントWebフィルタリングは専用ライセンスの購入が必要です。・マルウェア対策ライセンスの最小購入ライセンスは100です。

システム構成

システムの負荷分散により、安定して快適に、操作／データ閲覧ができます。

※1,000台環境の構成です。ただし、Windows 端末管理台数にかかわらず、1サーバーで管理できる Mac 端末は500台までです。



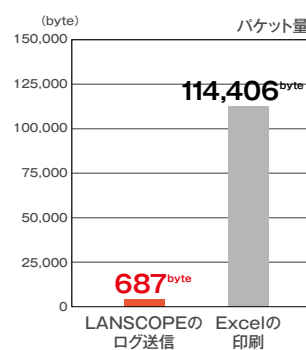
※保有するライセンスによって、以下のエージェントをインストールする必要があります。
クライアントエージェント (Windows用 / Mac用)、検知エージェント、サーバーエージェント (Windows用 / NetApp用)
BlackBerry Protect エージェント、Web フィルタリングのクライアント、ISLOnline のクライアント

品質・性能

ネットワーク負荷の軽さ

ログ送信時のネットワーク負荷は、Excel A4ドキュメントを1枚印刷した時の160分の1です。ネットワークアナライザを開発していた技術があるから実現できた圧倒的な性能です。

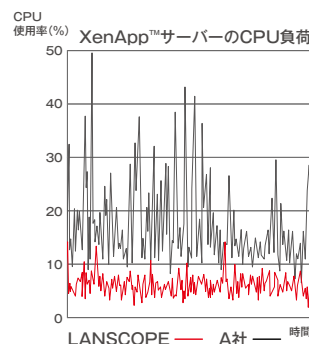
<計測内容>
通信パケット量



クライアント負荷の軽さ

他社製品の常駐エージェントと比べて、XenApp™サーバーに40ユーザーがアクセスした時のCPU負荷を3分の1に抑えています。

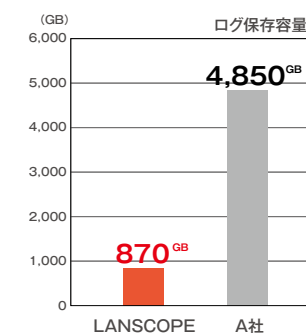
<計測内容>
40ユーザーアクセス時のXenApp™サーバー負荷



ログの保存容量の少なさ

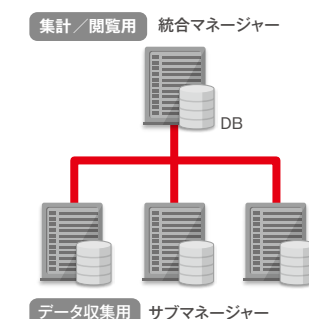
人が操作した内容を判別する仕組みで、必要ない大量のシステムログなどをフィルタします。他社製品の約5分の1までログ保存容量を抑え、HDDを圧迫しません。

<計測内容>
1,000台の操作ログ5年分



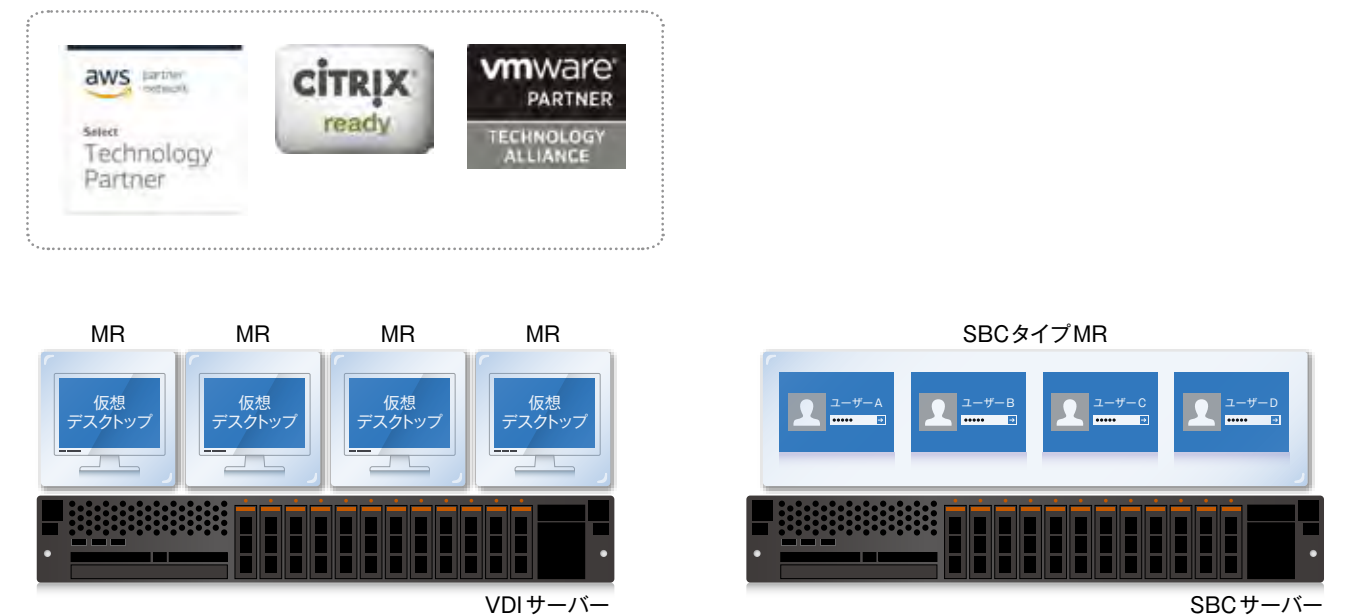
システムの負荷分散

サーバーを集計／閲覧用とデータ収集用に分けることでシステムの負荷を分散しています。大規模環境でも運用可能な構成で、4万台のPCを管理している実績があります。



シンククライアント対応

シンククライアント環境の操作状況を取得し業務状況を見える化します。



VDI方式

仮想デスクトップごとにクライアントエージェント (MR) をインストールして、Windows 端末と同様の管理ができます。Amazon WorkSpaces、Citrix XenDesktop、VMware Horizon / Horizon Air、VirtualPCenter に正式対応しています。

※通常のクライアントライセンスが必要です。

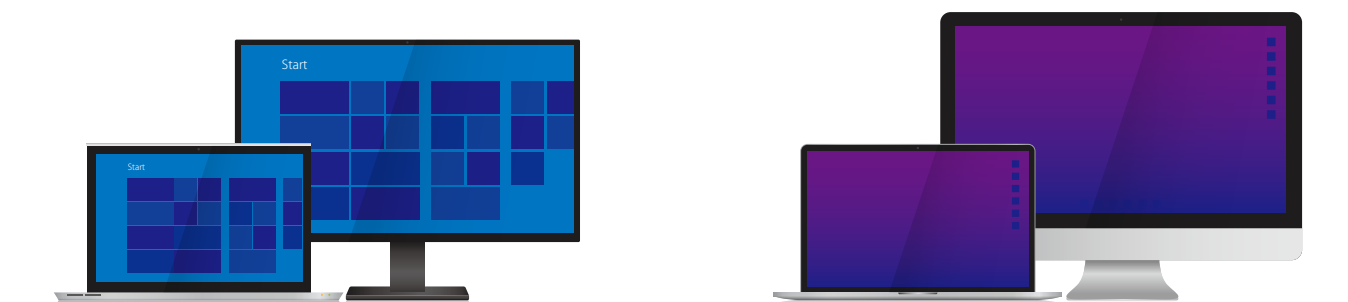
SBC方式

SBCサーバーにクライアントエージェント (SBCタイプMR) をインストールして、ログオンユーザーごとに操作ログ管理、Webアクセス管理、アプリID監査ができます。VMware Horizon RDSH、Citrix XenApp、Remote Desktop Services に正式対応しています。

※バーチャルライセンスが必要です。

グローバル対応

国内はもちろん海外拠点のWindows 端末やMac 端末もまとめて管理できます。管理コンソールの英語表示切り替えにも対応しています。



Windows (Unicode対応)

Windows 端末の資産管理、操作ログ管理、Webアクセス管理、デバイス制御、メール管理、アプリID監査ができます。Unicodeに対応しており、日本語以外に英語／中国語 (簡体字) のOSも正式にサポートしています。

Mac (Unicode対応)

Mac 端末の資産管理、操作ログ管理、Webアクセス管理、デバイス制御ができます。Mac 端末管理の独自機能として、モリサワフォントなどのフォント管理機能を実装しています。

ダッシュボード

Windows サポート状況やパッチの適用状況を可視化。 脆弱性の自動抽出から対策までワンストップで実現します。

サイバーセキュリティの最も基本的なことは、端末の環境を最新に保ち、攻撃者が利用する穴(脆弱性)を未然に防ぐことです。WannaCry などの大きなサイバー事件でも Windows のセキュリティパッチを適用していれば感染を防ぐことができました。



ダッシュボード

ダッシュボードでは、組織に存在する端末の中で、最新の状態に保たれていない脆弱な端末を自動で抽出しカードに表示します。カードの詳細には適用すべきパッチの情報を含んでいるため、専門的な知識がなくても、必要な対策を実施できます。対策情報は MOTEX から更新されるので、毎日ダッシュボードを確認するだけで、社内の脆弱な端末の発見・対策を実現します。

OS 分布状況

XP などサポート期限切れ OS の台数を把握

Windows (サーバー) パッチ適用状況

XP などサポート期限切れ OS の台数を把握

Windows (クライアント) パッチ適用状況

WindowsOS の月例累積パッチ適用状況の把握

アプリケーション パッチ適用状況

脆弱性が狙われやすい各種アプリの
パッチ未適用台数を把握

Windows OS 緊急パッチの適用状況

緊急配信されたパッチの未適用台数

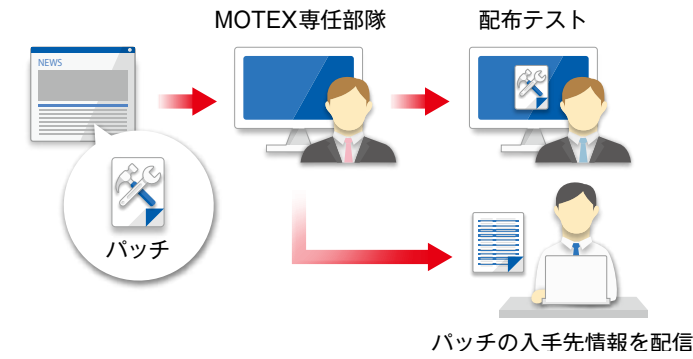
脆弱性情報配信サービス

365 日脆弱性情報を確認・検証

専任部隊が土日／祝日問わず、毎日脆弱性情報を確認します。脆弱性情報が見つかった場合は、パッチを入手し配布テストを行います。

ダッシュボードに自動配信

脆弱性情報の有無をお客様の環境に自動配信します。脆弱性情報があった場合には、脆弱性情報と併せてパッチの入手先情報を配信します。



ダッシュボードの運用イメージ

従来の対策手順

1 STEP
脆弱性情報の入手

2 STEP
該当端末の把握

3 STEP
対策パッチの入手

4 STEP
対象端末に配布

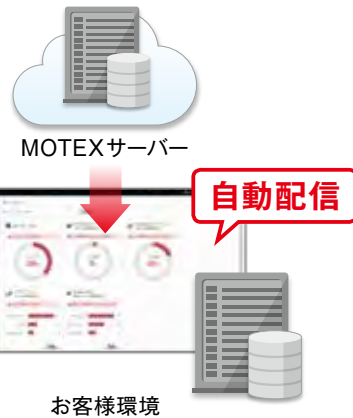
**LANSCOPE ダッシュボードなら
従来の1～3STEPを自動化**

脆弱性情報・更新プログラム情報を MOTEX から配信。
配信された最新情報は、自動でダッシュボードに表示されます。

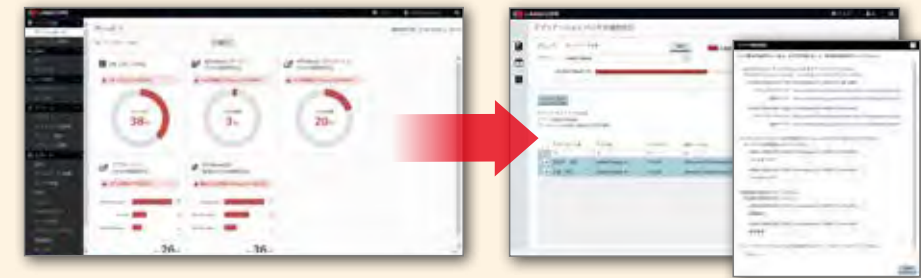
1 脆弱性情報の入手

2 該当端末の把握

3 対策パッチ情報の
入手・配布テスト



1 STEP カードを確認し、パッチを入手して配布。
1日がかりの作業を、**15分**に短縮できます。



ダッシュボードのカードに緊急対応が必要な
端末が何台あるかが表示されるので、クリック
して詳細を確認。

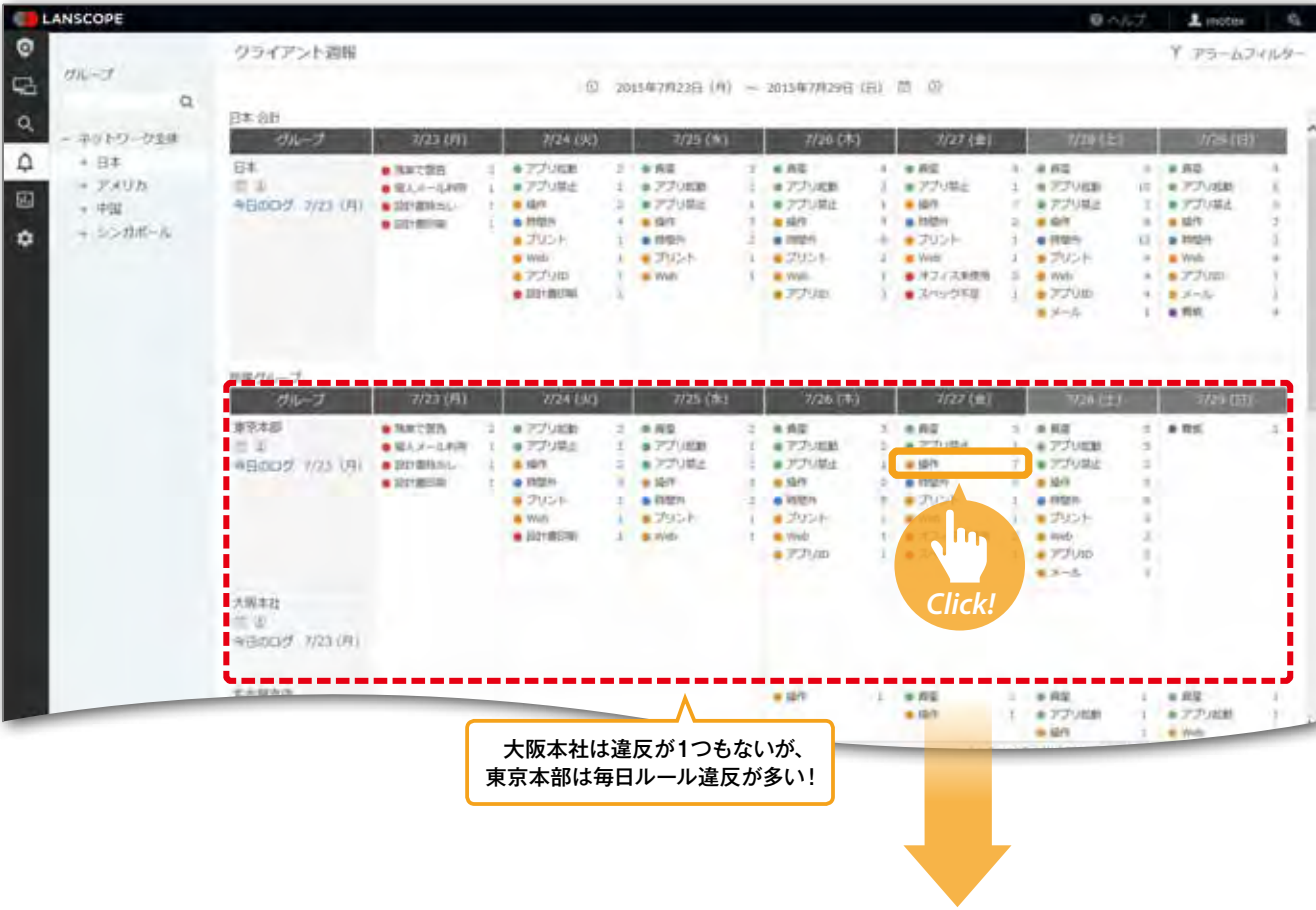
詳細画面から対策が必要な2台を選択し、
リンククリックでパッチをダウンロードし、
「パッチ配信」で配布を行って対策完了。

アラーム管理

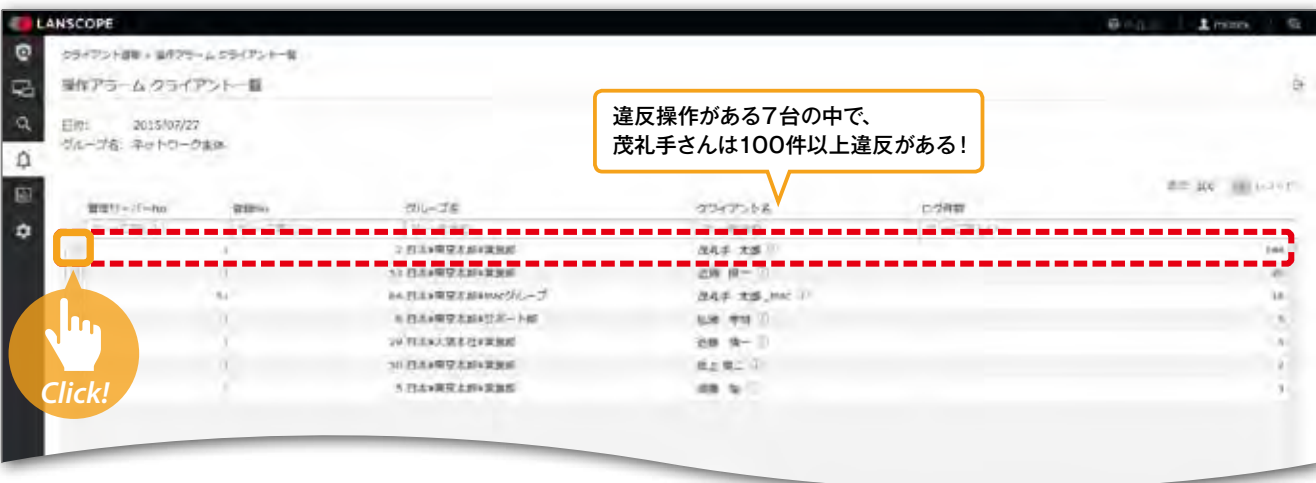
Webブラウザで、簡単にルール違反の有無をチェック。
誰がどんな違反をしたか、クリックするだけで確認できます。

「現状把握→分析→問題発見」までを自動でレポートするので、一般社員から経営者まで同じ判断基準で、問題の対策に集中できます。また、現場に即した運用を実現するために、必要なレポートを必要な人にだけ見せて管理を分散できます。

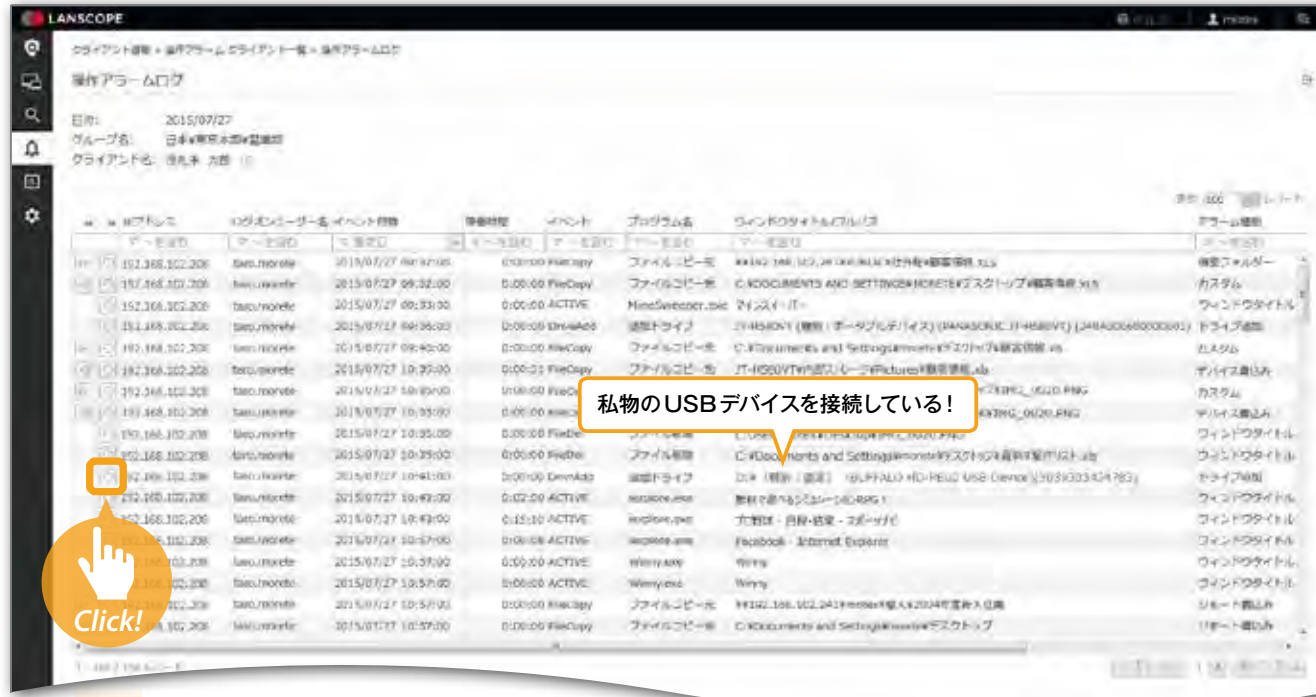
Step1 カレンダー上で、どんなルール違反が何台のPCにあったかを把握できます



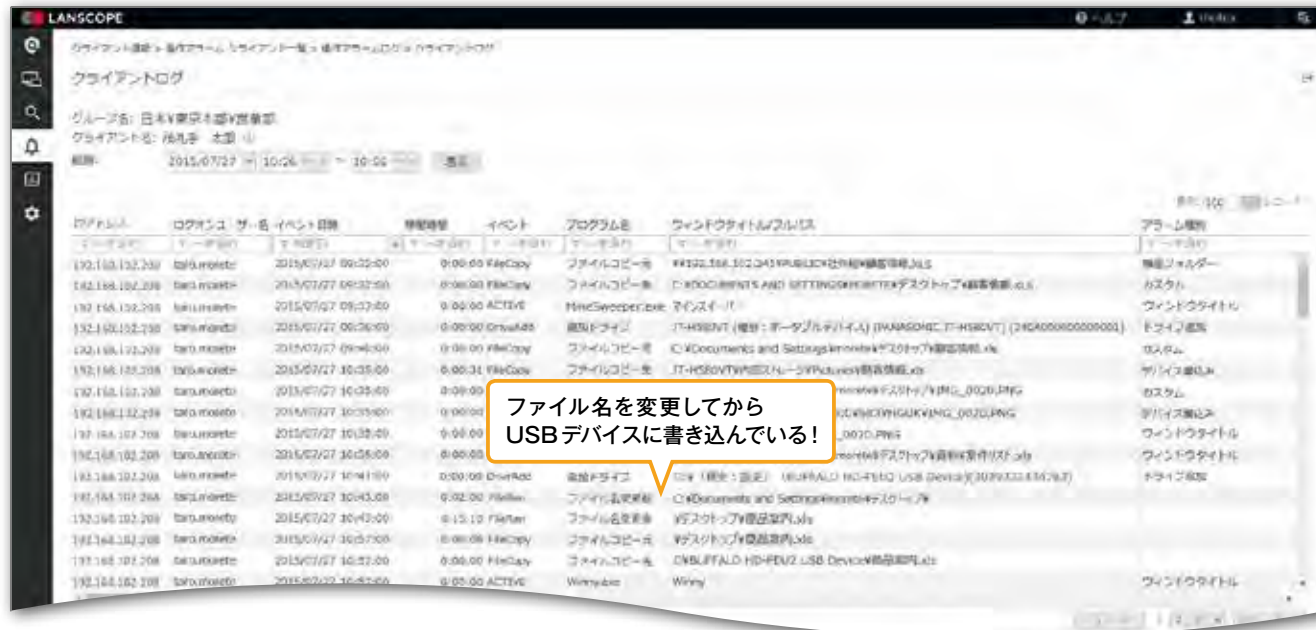
Step2 ルール違反が、どのPCで何件あったかを把握できます



Step3 ルール違反の詳細を、ログで確認できます



Step4 ルール違反があったログの前後15分間のログが確認できます



User's Voice

カレンダー形式がポイント！1日ごとのアラームだけを抽出、問題操作の有無を一目で把握。

今までは大量のログからキーワードを一つ一つ検索していたので、見ようとしても膨大な時間がかかり、取りっぱなしの状態になっていました。LANSCOPEのWebコンソールでは、カレンダーから問題操作をクリックして見ていくだけ。手間がかからないので毎日運用できています。

アラーム管理

カスタムアラーム

問題を知らせるアラーム一覧

セキュリティリスクのある操作や資産情報の変更など、決めたルール(ポリシー) に違反した場合、カレンダー上にアイコンで表示し、管理者や違反者の上司など必要な人にメールで通知できます。

カテゴリ	アラーム	ポリシー	項目	禁止
環境	資産	資産ポリシー	IP アドレスの重複 / 変更	－
			コンピューター名変更	－
			NIC / SCSI / モデムの変更	－
			DMI ハードウェア情報の変更	－
			CPU / メモリサイズの変更	－
			MAC アドレスの変更	－
			日時の変更	－
			リース切れ	－
			新規アプリのインストール	－
			HDD 容量不足	－
	アプリ起動	アプリ稼働ポリシー	新規アプリの起動	－
			禁止アプリの起動 / 名前変更	○
	アプリ禁止	アプリ禁止ポリシー	レジストリの変更 (禁止設定時)	○
			アプリのインストール (禁止設定時)	○
			システム構成の変更 (禁止設定時)	○
	通信デバイス	通信デバイスポリシー	不許可通信デバイスの接続	○
効率	時間外	操作ポリシー	業務時間外の操作	－
		サーバー監視ポリシー		－
		アプリID 監査ポリシー		－

カテゴリ	アラーム	ポリシー	項目	禁止	
行動	操作	操作ポリシー	機密フォルダーの操作	－	
			CSVの出力	－	
			USBメモリなどの外部メディアへの書き込み	－	
			リモート PC への書き込み	－	
			ローカル共有フォルダーの作成または書き込み	－	
			ドライブの追加	－	
			ウィンドウタイトルアラームに抵触	－	
			メールの添付	－	
	プリント	プリントポリシー	指定した条件に抵触するファイルの操作	－	
			印刷枚数の超過	－	
	Web	Web アクセス ポリシー	キーワードに抵触したドキュメントの印刷	－	
			指定したキーワード／ URL に抵触	○	
	ファイル操作	サーバー監視 ポリシー	アップロード／ダウンロード	○	
			Web への書き込み／ Webメールの送信	○	
			サーバーファイルの削除／アクセスの失敗	－	
			サーバー接続の失敗	－	
不正接続	不正 PC 検知 ポリシー	ネットワークへの不正な接続	－		
		ネットワークへの不正な接続を禁止	○		
		アプリ ID 監査	アプリ ID 監査 ポリシー	アプリの ID の作成／削除	－
				不許可設定した PC での操作	－
メール送信	メールポリシー	操作回数アラームに抵触	－		
		キーワードに抵触したメールの送信	－		
脅威	脅威	－	マルウェアの検知	－	
カスタム	カスタム	カスタムアラーム	カスタムアラームで指定した条件に 抵触する操作	○	

アラームをさらに絞り込むカスタムアラームのテンプレート

カスタムアラームでは、アラームに自由に条件を追加することができます。管理者が本当に知るべき違反操作のみを、一日数件程度のアラームで受け取ることができるので、日々の運用の効率化が実現できます。また、用途／目的に合わせて活用できるテンプレートもご用意しています。

目的	項目	ポリシー			
		アプリ稼働	操作	プリント	Web アクセス
情報漏えい対策	外部デバイス経由の重要ファイルの持ち出しだけを察知	－	○	－	－
	メール経由の重要ファイルの持ち出しだけを察知	－	○	－	－
	Web アップロード経由の重要ファイルの持ち出しだけを察知	－	○	－	○
	印刷経由の重要ファイルの持ち出しだけを察知	－	○	○	－
	大量のダウンロードを察知	－	－	－	○
	社外での印刷を察知	－	－	○	－
	私用デバイスへの持ち出しを察知	－	○	－	－
	サーバーファイルの印刷を察知	－	○	○	－
	CSV データの出力を察知	－	○	－	－
	PDF データの出力を察知	－	○	○	○
	外部デバイスへのデータ出力を察知	－	○	－	－
	標的型攻撃訓練 (添付ファイルを開封)	－	○	－	－
労務管理・業務効率向上	標的型攻撃訓練 (URL をクリック)	－	○	－	○
	常用サイトの非アクセスを通知	－	－	－	○
	アプリの非活用を把握	－	○	－	－
	低スペック PC の利用を把握	－	○	－	－
	残業時間超えを通知	－	○	－	－
ルール違反検知	フリーメールの利用を注意	－	－	－	○
	常用アプリの終了を注意	○	－	－	－
	大容量ファイルのコピーを注意	－	○	－	－
	非圧縮ファイルの持ち出しを注意	－	○	－	－
	業務時間外の Web 閲覧を注意	－	－	－	○
	デスクトップへのファイル配置を注意	－	○	－	－
	私用デバイスの接続を注意	－	○	－	－
	業務時間外の印刷を注意	－	－	○	－
	不許可 Web アプリの利用を注意	－	－	－	○

※カスタムアラームテンプレートの一部抜粋です

他にも色々なシーンに対応できるテンプレートをご用意しています。

情報漏えいにつながる操作だけをリアルタイムに察知

大量のダウンロードを察知 ブラウザで動く業務システム／クラウドサービスからの多数のダウンロードをアラームとします。		私用デバイスへの持ち出しを察知 会社指定のデバイス以外にファイルをコピーした場合にアラームとします。	
外部デバイスへのデータ出力を察知 (ファイル数／ファイルサイズ) 外部デバイスにコピーされたファイルの数や合計サイズが指定値を超えた場合にアラームとします。		標的型攻撃訓練 (添付ファイル／URL) 訓練用攻撃メールを開き、「添付ファイルを開いた」「本文に記載された URL をクリックした」ことをアラームとします。	

労務管理・業務効率向上につながる行動を促進

常用サイトの非アクセスを通知 指定時刻までにポータルサイトなど、特定のサイトへ一定回数アクセスを行わなければアラームとします。		残業時間超えを通知 定時後に一定時間PC操作をした場合にアラームとします。	
アプリの非活用を把握 有償アプリの利用時間が少ないことをアラームとします。		過剰な SNS 利用を抑制 SNS の閲覧時間が一定時間以上の場合にアラームとします。	

ルール違反をその瞬間に通知し事故を予防

フリーメールの利用を注意 Gmail や Outlook.com で社用アカウントではなく私用のアカウントを使ったメール送信のみをアラームとします。		業務時間外の Web 閲覧を注意 業務時間外に一定時間以上 Web サイトを閲覧した場合にアラームとします。	
不許可 Web アプリの利用を注意 許可していない SNS やオンラインストレージ、Web メールを一定時間もしくは一定回数以上閲覧した場合にアラームとします。		業務時間外の印刷を注意 業務時間外に印刷をした場合にアラームとします。	

カスタムアラームのテンプレートは、お客様の要望をもとに随時追加しています。
テンプレートは「LANSCOPE 保守契約ユーザー様専用サイト」からダウンロードできます。

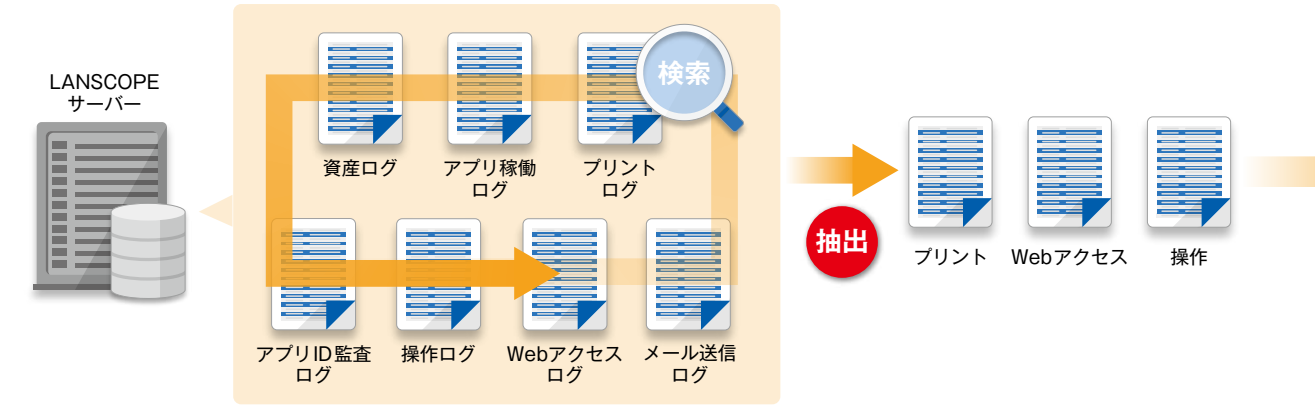
<https://tryweb2.motex.co.jp/support/login.php> (ログインには ID / PW が必要です)

LANSCOPE 保守サイト 検索

ログ検索

5年分のログから、様々な条件で特定のログを抽出できます。

ログの種類／対象の期間／グループなど、様々な切り口で横断的に検索し、目的のログを抽出できます。また、保存した複数パターンの検索条件をワンクリックで呼び出せるので、定期的なログ監査を効率的に行うことができます。



ログ検索

LANSCOPE クライアントログ検索

検索条件: 2015/07/01 ~ 2015/07/31

ログ種類: 資産, アプリ, 操作, プリント, Webアクセス, アプリID, メール送信

絞り込み: すべてを選択, 絞り込み

期間／対象／ログ種別を指定した上で、複数のキーワードを組み合わせた検索(AND条件/OR条件)での絞り込みと、条件の保存ができます。

ログ種別

- 資産: IP変更、新規アプリインストール、HDD容量不足など
- アプリ: 新規アプリ起動、特定アプリ起動、アプリ禁止など
- 操作: 業務時間外操作、ドライブ追加、機密フォルダなど
- プリント: 枚数、キーワード、正常ログ
- Webアクセス: 閲覧禁止、アップロード禁止、書き込み禁止など
- アプリID: 操作回数、不許可クライアント、不正ID作成など
- メール送信: 添付ファイル名、送信先、件名、正常ログ
- 通信デバイス: アラーム、禁止、正常ログ

検索結果

LANSCOPE クライアントログ検索

検索結果一覧

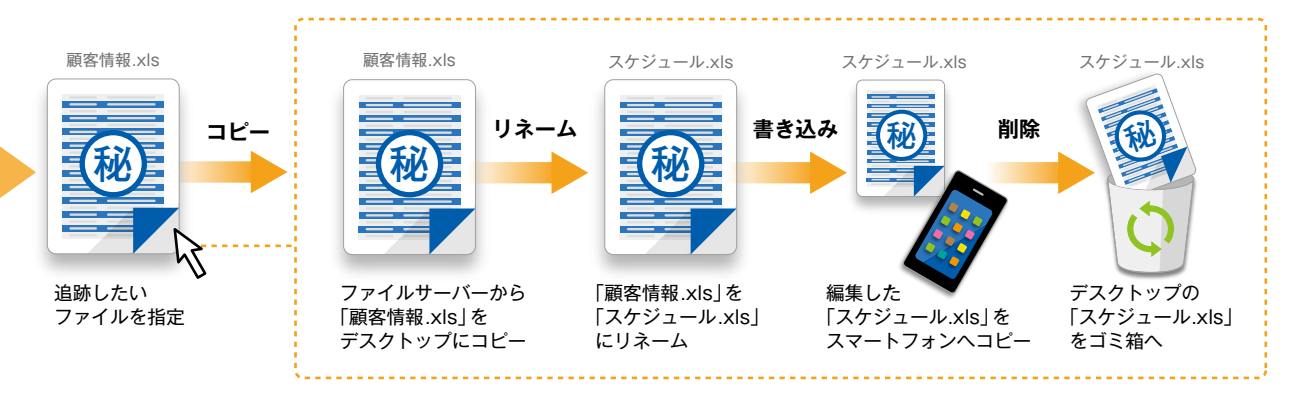
グループ名	クライアント名	ログオンユーザー名	日時	ログ種別	イベント	プログラム名	タイトル/ファイル名	ファイルサイズ (KB)	アラーム種別
1	101 日本電産本部	tanaka	2015/07/01 09:00:00	プリント			報告リスト [あーむ].xls		キーワード
2	101 日本電産本部	tanaka	2015/07/01 09:10:00	プリント			報告リスト [あーむ].xls		キーワード
3	101 日本電産本部	tanaka	2015/07/01 09:15:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	キーワード
4	101 日本電産本部	tanaka	2015/07/01 09:15:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	デバイス読み込み
5	101 日本電産本部	tanaka	2015/07/01 09:15:00	実行	FileDel	ファイル削除	Xperia ZW内部ストレージ\機密フォルダ\...		デバイス読み込み
6	101 日本電産本部	tanaka	2015/07/01 10:00:00	プリント			報告リスト [あーむ].xls		キーワード
7	101 日本電産本部	tanaka	2015/07/01 10:00:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	アップロードアラーム
8	101 日本電産本部	tanaka	2015/07/01 10:00:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	アップロードアラーム
9	101 日本電産本部	tanaka	2015/07/01 10:00:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	アップロードアラーム
10	101 日本電産本部	tanaka	2015/07/01 10:00:00	実行	FileCopy	ファイルコピー	C:\Documents and Settings\Tanaka\...	15,500	アップロードアラーム

各ログ項目のフィルター条件でログの絞り込みができます。また、①をクリックするとクライアントの資産情報を確認できます。

ファイル追跡

万が一の場合でも、ファイルの流出経路を追跡できます。

特定ファイルを、誰が、いつ、どのように操作したか、ネットワーク上のファイルの動きを追跡します。顧客情報がファイル名を変えられてデバイスで持ち出されたなど、流出の経路を把握し、前後にどのような操作をしていたかも確認できます。



ファイル追跡 (トレース)

LANSCOPE クライアントログ検索

ファイル追跡 (トレース)

検索条件: 2015/07/01 ~ 2015/07/31

ファイル操作履歴

日時	操作	ファイルパス	ログオンユーザー名	アラーム種別	UTC日時
2015/07/28 15:56:00	ファイルコピー	C:\Documents and Settings\Tanaka\デスクトップ\顧客情報.xls	tanaka	キーワード	2015/07/28 15:56:00
2015/07/28 16:01:00	ファイルコピー	C:\Documents and Settings\Tanaka\デスクトップ\スケジュール.xls	tanaka	キーワード	2015/07/28 16:01:00
2015/07/28 16:01:00	ファイルコピー	Xperia ZW内部ストレージ\机密フォルダ\スケジュール.xls	tanaka	アップロードアラーム	2015/07/28 16:01:00

ファイル操作 (コピー／移動／作成／削除／名前変更) をした際の、操作前／操作後の履歴をフルパスで取得することで、最終的にファイルがどこからどこに移動したのかを追跡できます。

周辺操作ログ

LANSCOPE クライアントログ検索

周辺操作ログ

検索条件: 2015/07/28 16:01:00 前後15分

周辺操作履歴

日時	操作	ファイルパス	ログオンユーザー名	アラーム種別	UTC日時
2015/07/28 15:56:00	ファイルコピー	C:\Documents and Settings\Tanaka\デスクトップ\顧客情報.xls	tanaka	キーワード	2015/07/28 15:56:00
2015/07/28 16:01:00	ファイルコピー	C:\Documents and Settings\Tanaka\デスクトップ\スケジュール.xls	tanaka	キーワード	2015/07/28 16:01:00
2015/07/28 16:01:00	ファイルコピー	Xperia ZW内部ストレージ\机密フォルダ\スケジュール.xls	tanaka	アップロードアラーム	2015/07/28 16:01:00

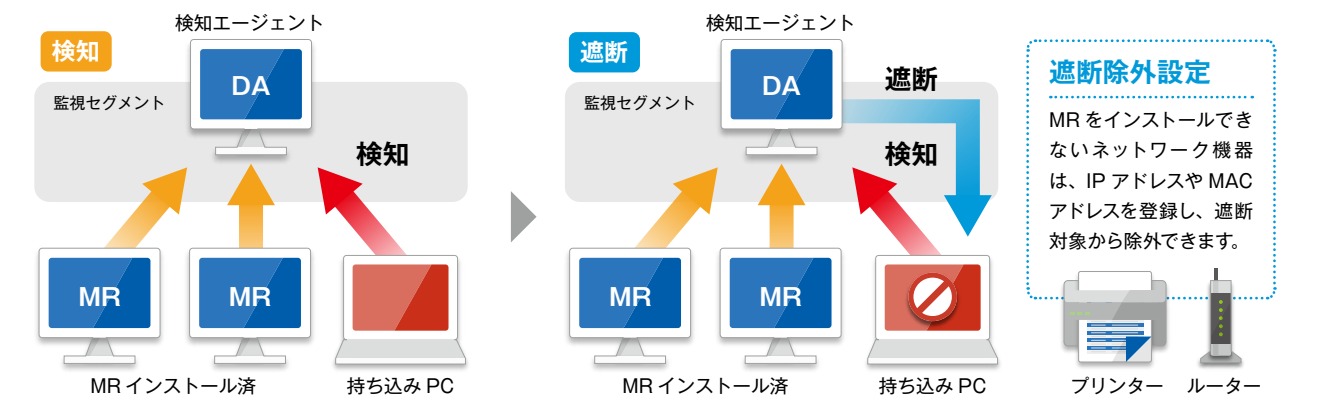
ワンクリックするだけで、前後15分間にどのような操作をしていたか確認できます。

ネットワーク検知不正PC遮断

電源／省電力管理

ネットワーク上の機器を検知し、不正な接続を遮断します。

社内にあるネットワーク機器を自動検知／情報収集し、管理対象とすべき IT 資産を把握できます(ネットワーク検知)。また、社員の持ち込み PC なども検知／遮断し、管理者に通知することで、ウイルス感染などの脅威からネットワークを守ります(不正 PC 遮断)。



ネットワーク機器検知／遮断

セグメントに検知用のエージェントをインストールし、ネットワーク機器の接続検知／情報収集ができます。また、管理対象外の不正な機器接続を検知／遮断できます。

LANSCOPEだけのゾーン管理

Aゾーン：LANSCOPE導入環境

LANSCOPEを導入している環境

Bゾーン：社内PC

会社に必要なネットワーク機器

Cゾーン：不正PC

LANSCOPE未導入環境

自動で許可

任意で許可

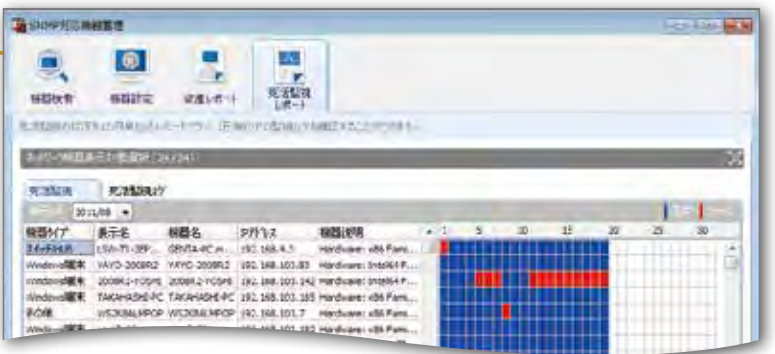
自動で遮断！



※遮断には別途不正PC遮断の購入が必要です。

SNMP対応機器検知／死活監視

SNMP 対応機器の情報を収集し、資産管理と死活監視ができます。プリンターやルーターなどの機器配置の最適化や新設時の検討に活用できます。



取得できる SNMP 機器

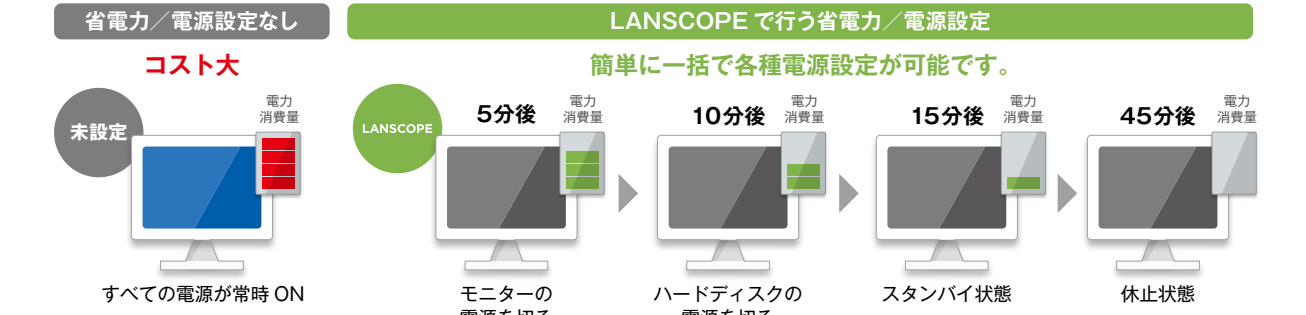
機器	取得可能な情報
共通	●機器タイプ ●MACアドレス ●IP アドレス ●機器名 ●機器説明
プリンター	●ペンダー ●型番 ●タイプ ●インク色数 ●インク色 ●最大用紙サイズ ●給紙トレイ数 ●累計印刷枚数 ●印刷枚数 ●状態 ●エラー状態
ルーター	●転送速度
スイッチ/Hub	●ポート数 ●転送速度
端末 (Windows /Linux /Mac)	●NIC 名 ●OS バージョン ●プラットフォーム ●メモリサイズ ●ドライブ数 ●メディアタイプ ●ドライブ ●全容量 ●空き容量 ●ソフトウェア情報

●SNMP (Simple Network Management Protocol) は、インターネット標準のネットワーク管理用プロトコルです。LANSCOPE は、マネージャーが管理対象のクライアントと通信して、MIB (Management Information Base) と呼ばれる一種のデータベースにアクセスすることにより管理を行います。●取得項目は、SNMP 対応機器の設定および MIB 情報に依存します。PC など事前に取得設定が必要な場合があります。

リモートでPCの電源を一括設定し、コストを削減できます。

PCを指定時刻に強制OFFし、利用時間のルールを徹底できます。また、Wake On LANを利用したりリモート電源ONや、無操作状態のPC、モニター、ハードディスクを指定時間経過後に電源OFFなど、無駄な電源コストを削減できます。

●Wake on LANによるリモート電源ONの利用は、マジックパケットがルータを超えられるように設定の変更が必要です。



電源設定

指定したクライアント端末に5種類の電源設定が適用できます。(電源ON、電源OFF、再起動、スリープ/スタンバイ、休止状態)

繰り返し期間を設定し、「毎日」「毎週の曜日」「時間帯」を指定して電源設定ができます。クライアント単位で、定期電源設定の一時的解除が可能に。解除期間中は、電源 ON、OFF、スリープ/スタンバイ、休止、すべての定期電源設定が解除されます。



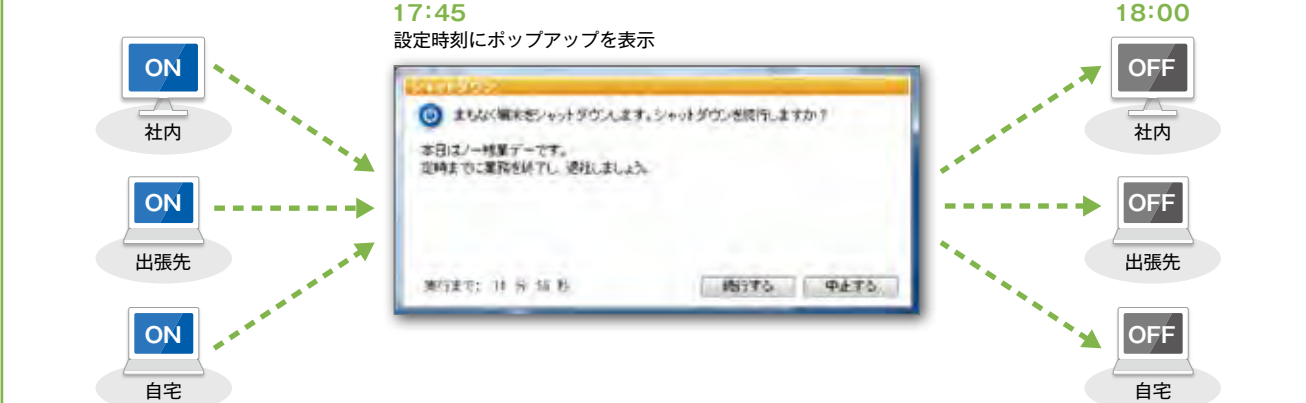
Pick Up New

編集可能なメッセージ

残業削減の意図や会社のルールなど管理者が自由に記載できます。

オフライン時でも実行

社内ネットワークにつながっていない場合でも指定の時刻が来た場合にシャットダウンを実施します。

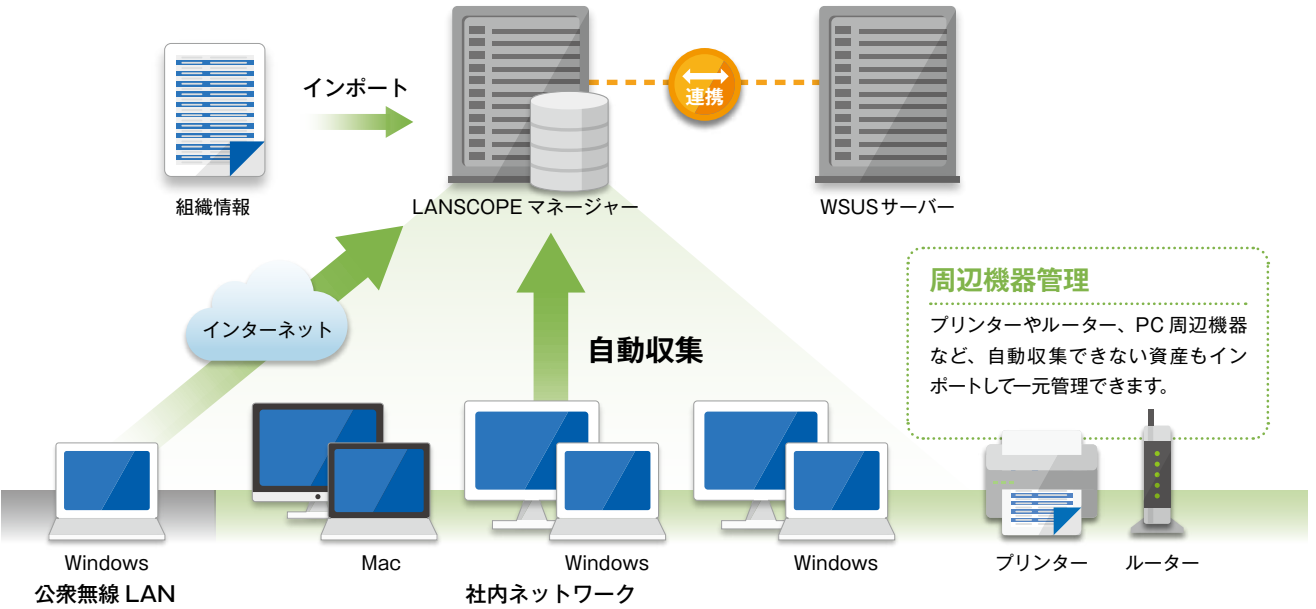


IT 資産管理

Mac Mac 端末管理対応 ※専用ライセンスの購入が必要です。

ハードウェア／ソフトウェアの情報を毎日更新し、
管理業務の手間をかけずに、適正な環境を保てます。

IT 資産情報を自動収集し、常に正確な情報を把握できます。また、変更履歴を残し、管理者にメールでお知らせします。既存の管理台帳のインポートや、世代ごとに台帳のエクスポートができます。



ハードウェア資産情報

コンピューター名、IPアドレスなど 50 種類以上のハードウェア情報と任意で設定したレジストリ情報を自動取得します。プリンター、周辺機器などを任意で登録して管理できます。また、様々な条件で検索し必要な情報が確認できます。

自動取得可能な項目				編集可能な項目			
●管理サーバー No.	●CPU タイプ	●NIC-A ~C	●プロセッサ数	●クライアント名	●導入形式 (リース等の選択)		
●登録 No.	●CPU クロック数	●モデム	●CPUコア数	●クライアントタイプ	●期限 (リース期間等)		
●フルネーム (表示名)	●メモリサイズ	●SCSI	●Office 365 プラットフォーム	●E-mail アドレス 1~3	●購入日	●資産 No.	
●ログオンユーザー名	●Windows Product ID	●サブネットマスク 1~3	●Office 365 チャネルタイプ	●導入日	●部署名 1~5	●外付けハードディスク	
●IP アドレス1~3	●ドライブ数	●DNS サーバー	●Office 365 バージョン	●機種名	●購入先	●CD-ROM	
●MAC アドレス	●セカンダリDNSサーバー1~3	●デフォルトゲートウェイ1~3	●Office 365 COMオブジェクト	●購入先	●導入責任者	●メモ欄	
●ドメイン名(ワークグループ名)	●IE バージョン	●BIOS バージョン	●ISL AlwaysOn バージョン	●導入金額	●任意項目 1~200		
●コンピューター名	●IEサービスパック	●BlackBerry Protect バージョン					
●ホスト名	●メディアタイプ 1~26						
●グループ No.	●ドライブ 1~26						
●登録日	●全容量 1~26						
●OS バージョン	●空容量 1~26						

その他 ESET, spol. s.r.o., シマンテック、トレンドマイクロ、マイクロソフト、マカフィーのアンチウイルス製品のパターンファイルのバージョンの情報が取得できます。
LANSCOPE クラウド版で収集した iOS / Android / Windows / macOS 端末の資産情報を定期的に自動インポートして、スマートデバイスも統合管理できます。

ソフトウェア情報を自動取得し、不審なファイルやアプリがないかを確認できます。

ソフトウェア管理

許可アプリと不許可アプリを分類し、アプリごと、PCごとにインストール状況を把握できます。また、PC内に存在するファイル (.exe、.dll、.sys など) の情報を取得します。バージョン情報はアプリの脆弱性管理に活用できます。

Mac 端末管理

Mac 端末内のモリサワフォントやアプリのインストール情報を取得し、ライセンスの過不足が管理できます。



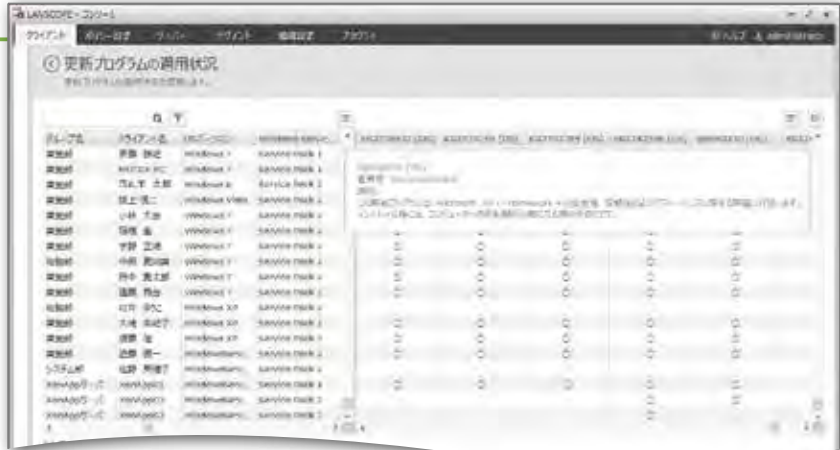
更新プログラムの適用状況を把握し、未適用端末に一齐配布・実行できます。 ※ Mac 端末管理非対応

更新プログラム管理 (脆弱性対策)

Windows 更新プログラムやセキュリティパッチの適用状況を視覚的に把握できます。未適用の PC を簡単に抽出し、必要な更新プログラムだけを一齐適用できます。

WSUS 連携

WSUS と連携し、Windows Update の自動更新 / 手動更新の設定を一括で変更できます。また、更新プログラムの説明や重要度などの属性情報を確認し、重要度の高い更新プログラムが未適用の端末を発見できます。

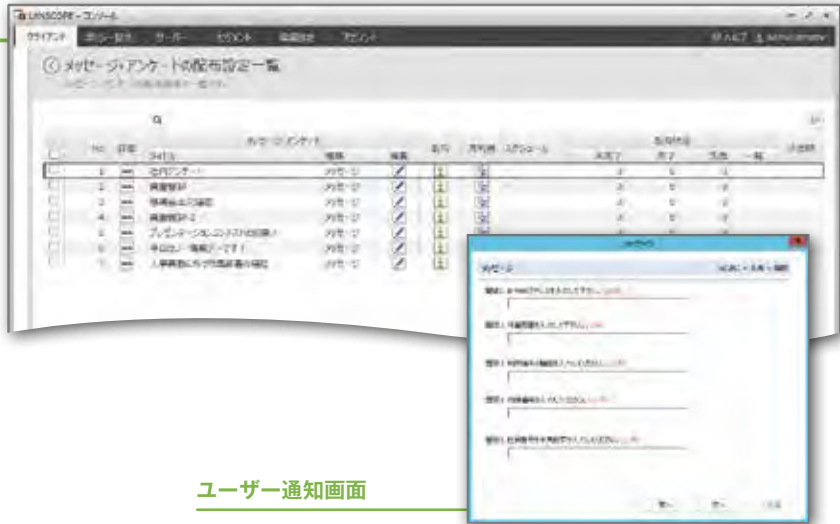


資産管理に必要な情報をユーザーに入力させて、収集できます。 ※ Mac 端末管理非対応

メッセージ・アンケート

管理者からユーザーに対して、自由記述やプルダウン形式でアンケートを送信できます。資産管理番号や管理部署など自動収集できない情報を収集し、回答結果を確認した上で資産台帳に反映できます。

通知タイミング	
●エージェントインストール時	
●ログオン時	
●ログオンユーザー変更時	
●IPアドレス変更時	
●特定アプリインストール時	
●即時	
●スケジュール設定時 (毎週水曜日の18時など)	
●PC利用者の任意のタイミング	



ユーザー通知画面

User's Voice

もう行かなくても大丈夫! 自席にしながら、一人で70拠点800台のPCを管理。

古いモニターの入れ替えを検討していたものの購入年月は控えておらず…LANSCOPEの導入前なら、70以上の営業所に訪問や電話、メールで確認していたところですが、アンケート機能をフル活用。入力形式を選択的に規制し、入力のバラつきなく台帳に反映できました。本当に楽になり助かっています。

ソフトウェア資産管理

Mac Mac 端末管理対応 ※専用ライセンスの購入が必要です。

契約情報とソフトウェア利用実態の突合を効率的に行い、ライセンス違反が起こらない管理体制をつくります。

ソフトウェア資産管理 (SAM) で必要な台帳の作成から更新までを支援します。ライセンスの契約情報と利用実態との突合から相違点の把握を行い、ライセンス違反が起こらない適切な運用サイクルを構築できます。

1 現状把握

ハードウェア/ソフトウェアの情報を自動収集。



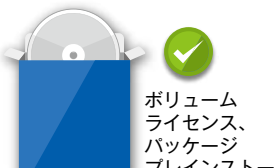
2 管理ソフト選定

ソフトウェア辞書で有償/無償を自動分類し、管理対象を選定。



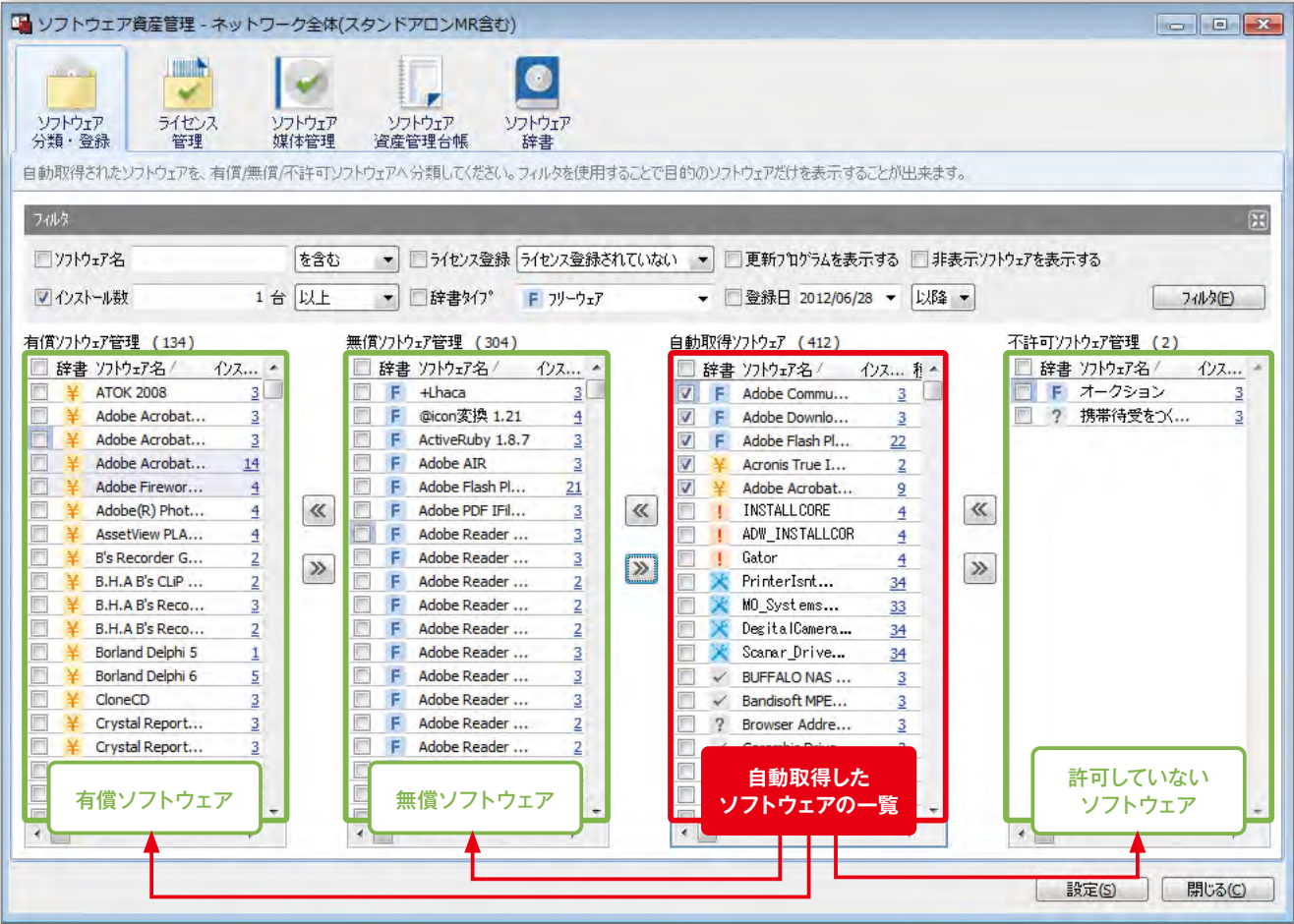
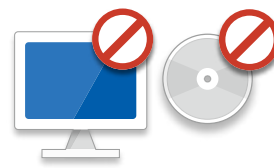
3 ライセンス登録

契約情報を登録。Microsoft Office のライセンス種別を自動判別。



4 過不足チェック

ライセンス過不足を確認し、不正使用 PC / ソフトウェアを自動抽出。



有償ソフトか無償ソフトか、SAMAC[※]ソフトウェア辞書と連携し自動判別できます。

インストールされているソフトウェアに辞書タイプを自動的に付与し、管理すべきソフトウェアの選定を支援します。

※ SAMAC：一般社団法人 IT 資産管理評価認定協会

辞書タイプ

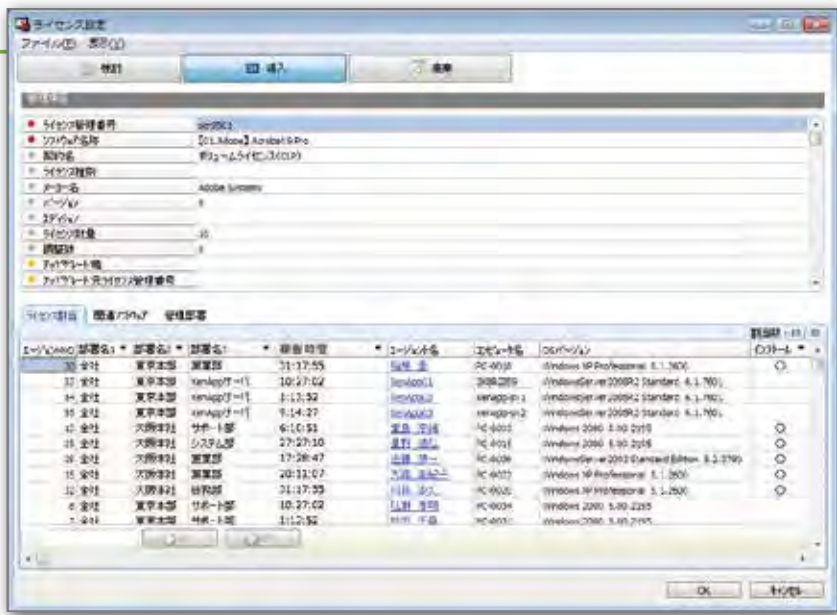
- 辞書未登録 (手動登録可能)
- 有償ソフトウェア (有料)
- 無償ソフトウェア (無料)
- 更新プログラム (セキュリティパッチ)
- アドウェア
- ドライバー/ユーティリティ
- その他

契約ごとに、管理に必要なライセンス情報を登録できます。

ライセンス設定

ライセンス数量や関連ソフトウェア、管理部署など必要な情報を登録します。また、Microsoft Office のライセンス種別 (ボリュームライセンス、パッケージ、ブレインストール) や SQL Server のエディション情報 (Express、Standard、Enterprise、Datacenter) を、自動で判別します。

SQL Server のライセンス管理に必要なハードウェアのプロセッサ数、CPU コア数の情報も自動収集し、ライセンスの過不足管理に活用できます。



ライセンスの過不足や利用状況を把握し、必要な対策が打てます。

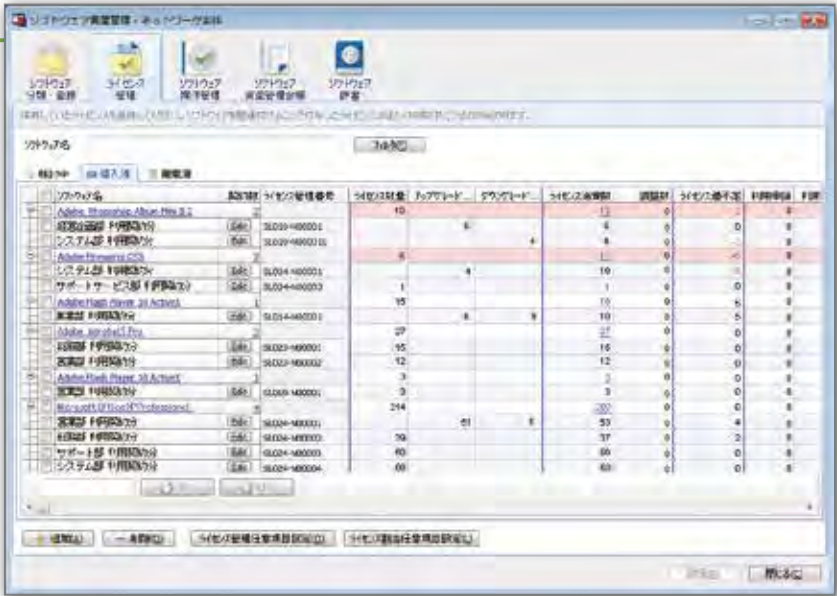
ライセンス管理

保有ライセンス数とインストール数の過不足確認や、アップグレード/ダウングレードの管理ができます。ライセンスの不正使用や、無駄なライセンスを発見し、適材適所にソフトウェアをインストールすることで、ライセンス割り当てを最適化できます。

SAMに使える5つの台帳

ソフトウェア資産管理に必要な5つの情報を台帳で管理できます。

- ユーザー情報
- ハードウェア情報
- ソフトウェア情報
- ライセンス管理
- ライセンス関連部材情報 (インストール媒体など)



Pick Up

専任のSAMコンサルタントがご支援します。

エムオーテックスは、日本マイクロソフト株式会社の SAM ゴールドパートナーとして 100 社以上の企業に対して SAM ソリューションの提供実績があります。メーカーからのライセンス調査対応、リスク診断や社員教育など、ツールだけでは解決できないお客様の課題に対し、専任の SAM コンサルタントが、お客様の立場に立ってサポートします。



User's Voice

たった2ヶ月で完了! ライセンス調査対応の作業工数を約80%削減。

メーカーから「ライセンス調査依頼」がきたのですが、拠点は40以上、PCは1,200台、ソフトウェアは130種類以上と、どこから手をつけていいのか分からない状況に。LANSCOPEを導入して「ライセンス過不足チェックサービス」を実施し、1年以上はかかる作業をたった2ヶ月で完了できました。

新機能

課題解決

機能詳細

レポート

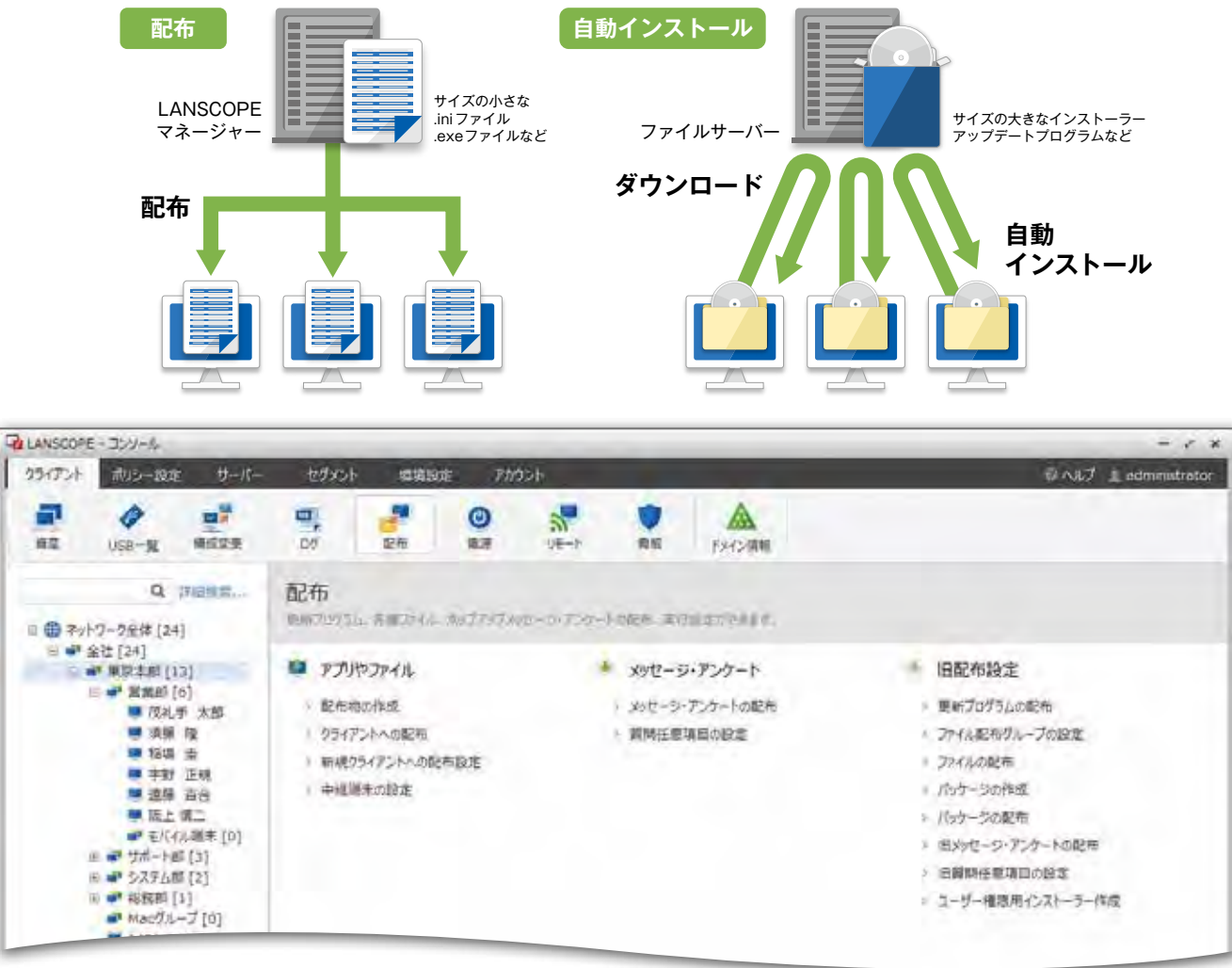
連携製品

制限事項

ファイル配布

ソフトウェアの配布／自動インストールを一括で行い、PCメンテナンス業務の効率アップが図れます。

複数のPCに対し一括で、アプリや更新プログラムの配布／自動インストールができます。サイレントインストール未対応のソフトウェアは、インストール操作を録画し、自動インストールを実現します。また、様々な条件を設定し配布効率を高められます。



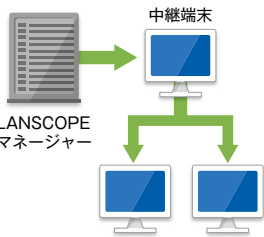
配布
アプリやファイル、更新プログラム、メッセージ・アンケートの配布／実行ができます。
また、配布物に応じた独自の配布グループ作成や、パラメーター付きの実行など、柔軟な設定ができます。

Pick Up

ネットワークに負荷をかけずに配布する仕組み

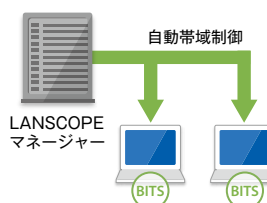
中継端末経由のアプリ配布

拠点間のネットワーク負荷を軽減するため、拠点にある中継端末（MR インストール端末）を経由して拠点内のPCへの一斉アプリ配布／インストールができます。



BITS (バックグラウンドインテリジェント転送サービス)

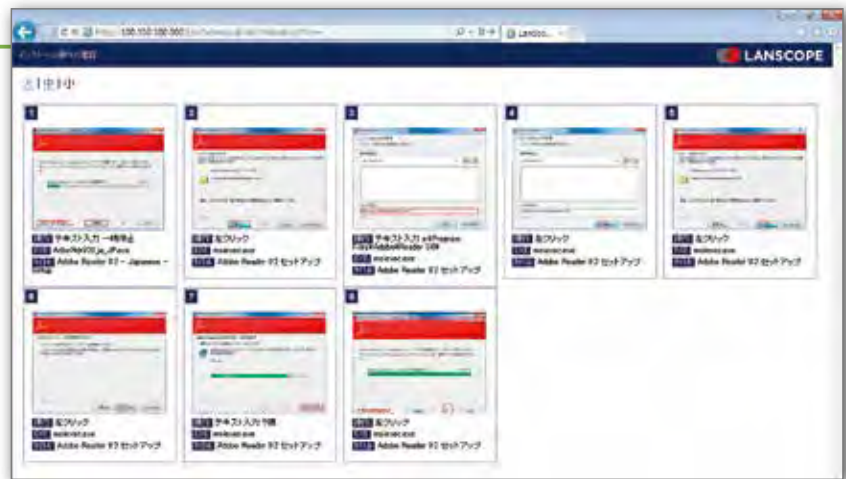
ネットワーク負荷をかけないように、自動的に帯域制御を行います。また、レジェウム機能により、ダウンロード中にPCがシャットダウンされても、次回起動時に前回の続きからダウンロードを再開できます。



インストール操作を録画するだけで、スクリプトファイルを自動で作成できます。

スクリプト自動作成ツール

専用ツールを使い、インストール操作を録画するだけで、自動インストール用のスクリプトファイルを作成できます。また、録画した操作手順を確認し、手順に間違いがないかをチェックできます。



新規導入PCにアプリを自動インストールし、クライアント環境を標準化できます。

新規クライアントへの配布設定

クライアントエージェントインストール後、特定アプリのインストール有無を条件に、指定アプリの自動インストールができます。また、複数ファイルを組み合わせた配布物の作成や配布スケジュール設定、帯域制御など柔軟な配布設定ができます。



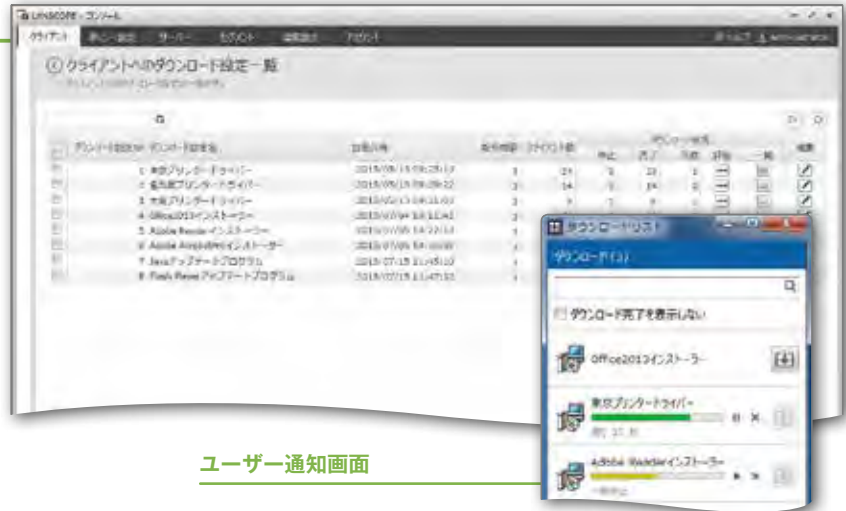
配布アプリ例

- Office のインストーラー
- Adobe Reader のインストーラー
- Java のアップデートプログラム
- Flash Player のアップデートプログラム

PC利用者が任意のタイミングで、ファイルをダウンロードできます。

クライアントへのダウンロード設定

管理者が設定したファイルやフォルダーを、PC利用者が任意のタイミングでダウンロード、実行できます。また、管理者はPC利用者がダウンロードを完了したか、失敗したかの確認ができます。



ユーザー通知画面

User's Voice

年間約900時間分の作業を短縮！日常的にPC350台のソフトウェアをアップデート。

LANSCOPEの導入前は、1台ずつソフトウェアのアップデートをしており、月に75時間、年間900時間もの工数がかかっていました。ファイル配布機能は、サイレントで完了できるので、ユーザー側に手間をかけず、こちらで配るファイルを設定するだけなので、大きな工数削減になっています。

新機能

課題解決

機能詳細

レポート

連携製品

制限事項

Microsoft Defender 連携

LANSCOPE × Microsoft Defender 連携で Microsoft Defender の運用管理における課題を解決します。

Microsoft Defender 運用管理における、検知状況の集中管理ができない・検知情報の管理者メール通知ができない・エンジン/パターンファイル更新状況の集中管理ができないといった課題を LANSCOPE と連携することで解決できます。



カレンダー形式でマルウェアの検知状況を確認
マルウェアを検知した端末が、いつ・どのくらいあったかをカレンダーで確認することができます。

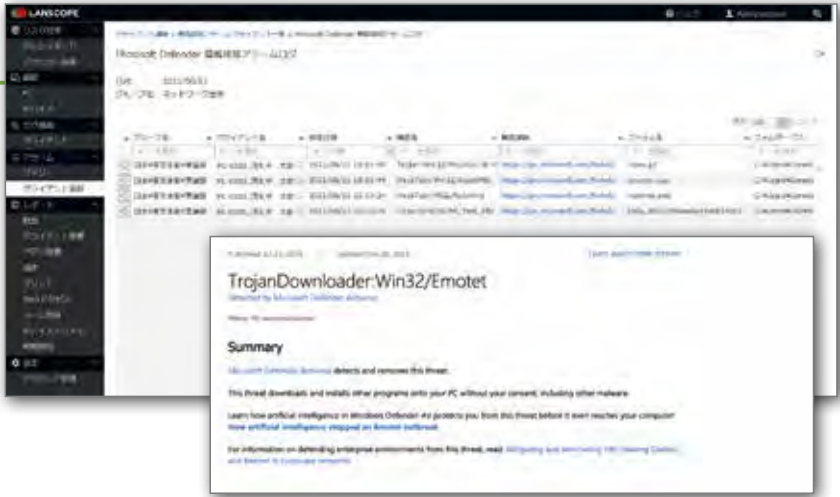
取得できる検知イベント

項目	取得可能な情報
脅威情報	検知したマルウェアの情報が掲載されているサイトの URL
ファイル名	検知したファイルの名前
検出元の場所	ローカル コンピューター/ネットワーク共有/インターネット/受信トラフィック/送信トラフィック/不明
検出の種類	ヒューリスティック/一般/コングリート/動的シグネチャ
カテゴリ	脅威やマルウェアの種類
重大度	低/中/高/重大

どの PC でどんなマルウェアを検知したのか詳細を確認できます。

Microsoft Defender
脅威検知アラームログ

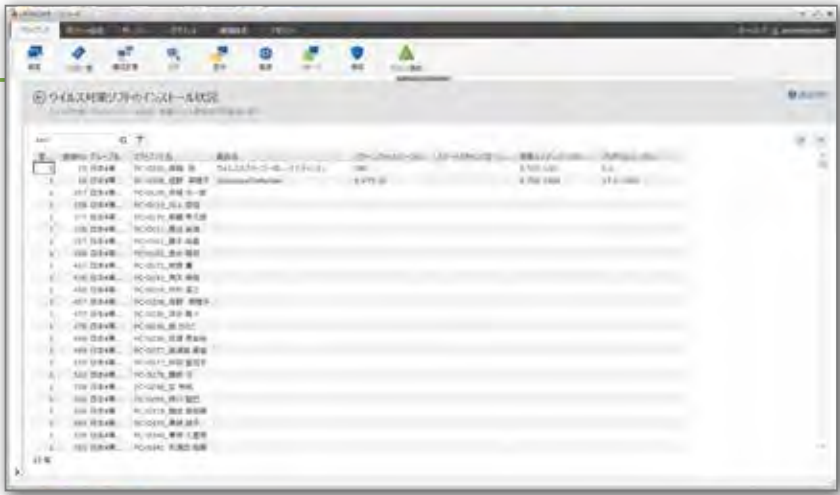
ログの一覧から脅威情報のリンクをクリックし、
脅威情報の詳細を確認することができます。



エンジン・パターンファイル更新状況の集中管理ができます。

ウイルス対策ソフトの
インストール状況

「パターンファイルバージョン」「検索エンジンバージョン」「プログラムバージョン」など、各 PC 情報を一覧で確認できます。



Pick Up

BlackBerry Protect との
同居による多層防御

脅威検知ログ取得設定

Microsoft Defender は、Windows10 端末に標準で搭載されているセキュリティ対策ソフトです。端末にほかのウイルス対策ソフトがインストールされている場合、通常は Microsoft Defender のリアルタイム保護機能は自動的に無効になりますが、BlackBerry Protect に設定を加えることで、Microsoft Defender と BlackBerry Protect を併用できます。



User's
Voice

クライアント週報を確認するだけ！ Microsoft Defender が検知した脅威が把握できる。

LANSCOPE と Microsoft Defender を連携させることで、マルウェア検知状況の集中管理ができるようになりました。また周辺ログを活用することで流入原因の調査も可能なので、より強固なセキュリティ対策ができるようになりました。

操作ログ管理

V バーチャルライセンス対応 Mac Mac 端末管理対応 ※専用ライセンスの購入が必要です。

PC 操作のログを管理し、業務効率を下げずに、セキュリティモラル向上や障害発生時の問題発見ができます。

アプリ稼働、印刷、ファイル操作、画面閲覧（ウィンドウタイトル）など PC の利用状況を記録します。違反操作があった場合は、ユーザーに警告表示しセキュリティモラル向上を促します。また、リアルタイムに管理者に通知し、重大な問題を未然に防ぎます。

シンクライアントサーバー

Windows Mac

PC 操作

アプリ稼働

USB 書き込み

Wi-Fi

印刷

ファイル操作

メール添付

Bluetooth

ある会社の茂礼手さんの PC 操作履歴の一例

15:55 案件リストを印刷

15:56 ファイルサーバーから「顧客リスト.xls」をコピー

15:56 「顧客リスト.xls」をデスクトップにコピー

15:57 「顧客リスト.xls」のファイル名を「商品案内.xls」に変更

16:00 スマートフォンを接続し「商品案内.xls」をコピー

16:07 人事給与システムにログインし、源泉徴収を一括出力

どの PC で

誰が

いつ

どのくらいの時間

何をしたら

グループ名	クライアント名	IPアドレス	ログオンユーザー名	イベント時刻	稼働時間	プログラム名	ウィンドウタイトル
Company # LA ...	Brown	192.168.10.2	J-Brown	15:53:00	0:01:06	explore.exe	Gmail - Compose message- Windows Internet Explorer
Company # LA ...	Brown	192.168.10.2	J-Brown	15:54:00	0:00:02	EXCEL.EXE	Microsoft Excel - Price list
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:54:00	0:01:06	EXCEL.EXE	Microsoft Excel - 案件リスト
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:55:00	0:00:03	EXCEL.EXE	印刷
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:56:00		ファイルコピー	※192.168.102.241【社外秘】営業部 #東京1課用 #顧客ファイル #顧客リスト.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:56:00		ファイルコピー	C:\Documents and Settings\morete\デスクトップ #顧客リスト.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:57:00		ファイル名変更	C:\Documents and Settings\morete\デスクトップ #顧客リスト.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	15:57:00		ファイル名変更	C:\Documents and Settings\morete\デスクトップ #商品案内.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		追加ドライ	Xperia Z (モデル: SGP-92E) (Sony SO-92E) (CB5A1P7433)
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		ファイルコピー	C:\Documents and Settings\morete\デスクトップ #商品案内.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		ファイルコピー	Xperia Z #内蔵ストレージ #顧客案内.xls
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		人事給与システム	人事給与システム - ログイン
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		年末調整 - 源泉徴収	年末調整 - 源泉徴収
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:06:00		帳簿一括出力	帳簿一括出力
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:07:00		ファイル作成	※192.168.102.241【社外秘】総務 #源泉徴収 #2014年源泉徴収第一報.pdf
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:07:00		ファイルコピー	※192.168.102.241【社外秘】総務 #源泉徴収 #2014年源泉徴収第一報.pdf
会社 #東京本部...	茂礼手 太郎	192.168.102...	taro.morete	16:07:00		ファイルコピー	C:\Documents and Settings\morete\デスクトップ #2014年源泉徴収第一報.pdf

操作ログ管理 「どの PC で」「誰が」「いつ」「どのくらいの時間」「どんな操作をしたか」を記録します。許可していない Free Wi-Fi への接続や顧客リストの USB メモリへの書き込みなど、違反操作があった場合、ユーザーに警告表示し不正操作を抑止します。

Pick Up New

違反操作が行われた
エンドポイントで原因を発見

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するので、境界防御のファイアウォールの情報をもとに LANSCOPE の操作ログを検索できます。これまで追及が難しかった、問題の発生原因の特定が可能です。

ファイアウォールによる検知

管理者
LANSCOPE 管理画面

検知した情報をもとに検索

利用者の特定

アプリの特定

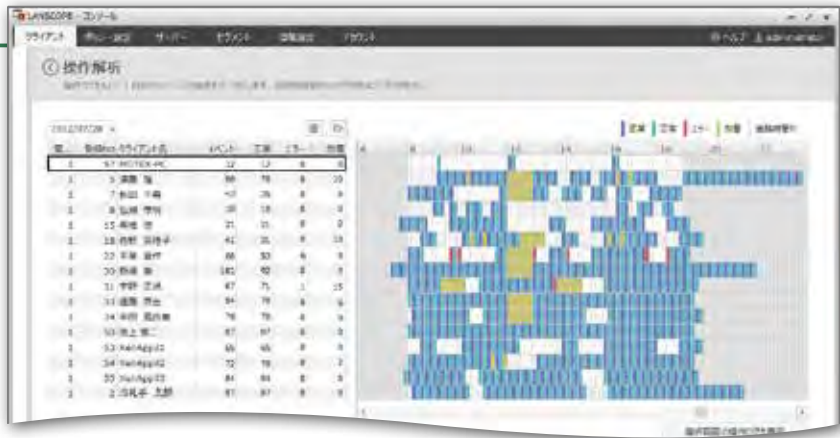
操作の把握

PC の利用状況を見える化し、残業の有無など業務状況をチェックできます。

操作解析

PC がどのような状態になっているのかグラフで視覚的に把握します。また、指定した PC / 時間帯の操作ログをワンクリックで確認できます。

- 青色 正常な稼働状態です。10 分間に 1 つでも操作が発生した場合は青、水色が交互に表示され、操作が発生しなければ青または水色を連続して表示します。
- 赤色 PC 上でエラーが検出され、通常のイベントを上回るか、同数の場合に赤色で表示します。
- 黄色 スクリーンセーバーが稼働すると黄色で表示します。
- 灰色 「業務時間」を設定すると、業務時間外部分を灰色で表示します。



印刷履歴を記録し、機密データの印刷や無駄な印刷を把握できます。

プリントログ管理

「どの PC で」「誰が」「いつ」「どのプリンターで」「何を」「何枚印刷したか」を記録します。無駄な印刷を把握し、コストの削減ができます。また特定のファイルが印刷された場合、ユーザーに警告し、不正な印刷を抑止します。

クライアント名	プリンター名	プリンターアドレス	印刷日時	印刷枚数	印刷ファイル名
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 15:53:00	1	C:\Documents and Settings\morete\デスクトップ #顧客リスト.xls
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 15:54:00	1	C:\Documents and Settings\morete\デスクトップ #顧客リスト.xls
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 15:56:00	1	C:\Documents and Settings\morete\デスクトップ #顧客リスト.xls
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 15:57:00	1	C:\Documents and Settings\morete\デスクトップ #商品案内.xls
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 16:06:00	1	C:\Documents and Settings\morete\デスクトップ #商品案内.xls
会社 #東京本部...	Canon iBP100	192.168.10.241	2012/07/27 16:07:00	1	C:\Documents and Settings\morete\デスクトップ #2014年源泉徴収第一報.pdf

●プリントログは Windows のシステムログから取得しています。

使われていない不要なライセンスの発見や、不正アプリの禁止ができます。 ※ Mac 端末管理非対応

アプリ稼働管理

「どの PC で」「誰が」「いつ」「どのアプリを使用したか」を記録します。アプリごとに稼働 PC 台数や稼働時間 / 回数を把握し、ライセンスを適材適所に配置することで、無駄なライセンスコストの削減ができます。

アプリ稼働禁止

業務に関係ないアプリや不正アプリの起動を禁止できます。特定のアプリを起動した場合、ユーザーに警告しゲームや情報漏えいにつながるアプリ起動を抑制できます。

アプリ稼働管理

ユーザー禁止通知画面

禁止通知 - 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「Microsoft Word」は、社内ポリシーによって禁止されています。
業務上、アプリケーションの使用は認められていないため、管理者までお問い合わせください。
<連絡先> 管理本部 情報システム課 (TEL: 03-XXXX-XXXX)



健康面からも非常によかった！業務の可視化で残業時間を10%削減。

ここ数年、増える傾向にあった残業時間。何が問題なのか残業時の操作ログから業務の現状を把握し、申請書などの管理体制もこの機会に改善することができました。導入してから5ヶ月で月平均10%の残業時間を削減でき、労務管理の面からも非常によかったと感じています。

Webアクセス管理

- V

バーチャルライセンス対応

※クライアントWebフィルタリングは未対応です。
- Mac

Mac 端末管理対応

※専用ライセンスの購入が必要です。
※ Web アクセス制御はMac 端末管理非対応

Webサイトの利用を監視し、不正サイトへのアクセスを制御。 信頼性の高いフィルタリングデータベースを採用しています。

Webサイトの閲覧記録、特定 Web サイトやカテゴリごとの閲覧制御ができます。ユーザーの適切な Web 利用を促進し、有害サイトへのアクセスを防ぎます。また、公衆ネットワークでの Web 利用も監視や制御ができます。

Step1

現状把握

インターネットの閲覧状況を把握

Step2

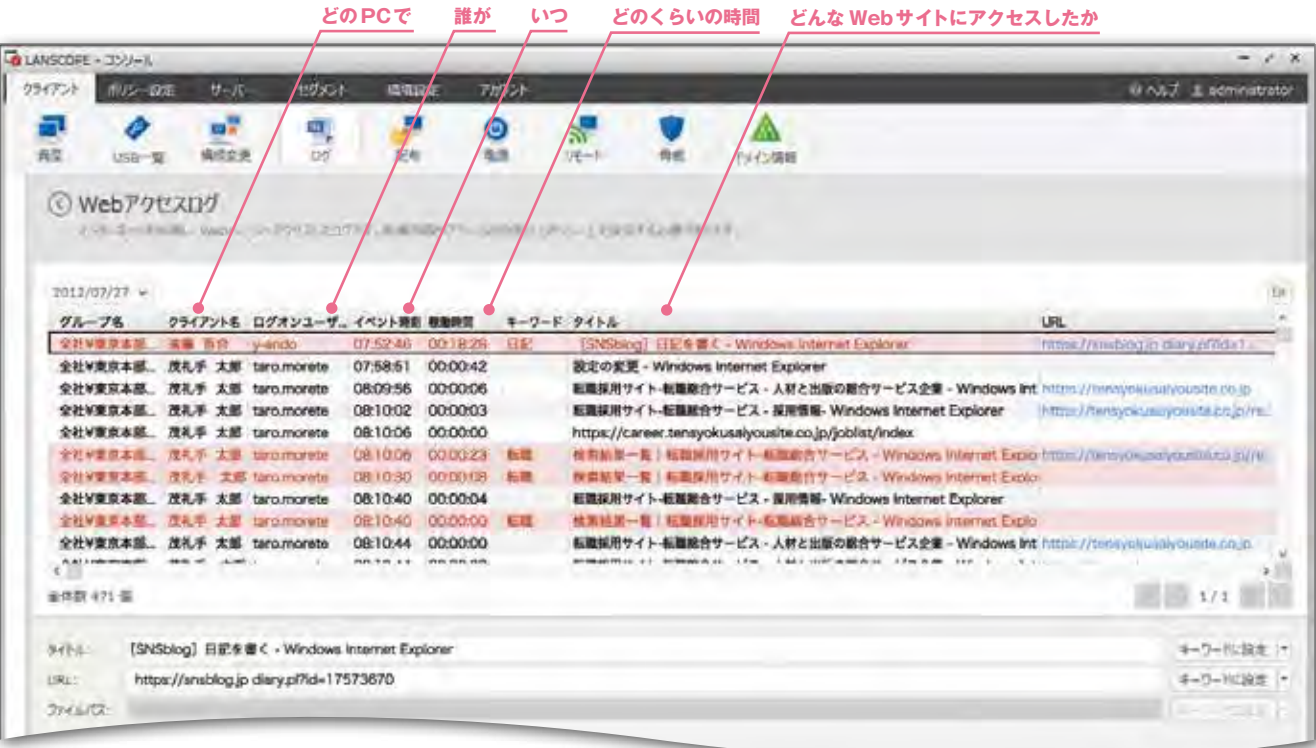
キーワード制御

キーワードを登録すると、不正サイトの閲覧を禁止

Step3

フィルタリングデータベース制御

指定したカテゴリに含まれるサイトを自動的に閲覧禁止



Web アクセス管理／制御
「どのPCで」「誰が」「いつ」「どのくらいの時間」「どんなWebサイトを閲覧したか」を記録します。
URLやウィンドウタイトルが設定したキーワードに抵触した場合、警告表示や閲覧禁止ができます。

業務に必要なWebサイトだけを閲覧可能にできます。

ホワイトリスト

キーワードを指定し、特定の Web サイトのみ閲覧可能にできます。
グループウェアやクラウドサービスなど業務に必要な Web サイトのみが利用できる環境をつくれます。

Webへのアップロード／ダウンロードや、Webメールの送信内容を確認できます。

クラウドストレージ／
Webメール利用ログ

クラウドストレージへのアップロード／ダウンロードのログを取得し、情報漏えい経路を監視できます。また、Webメールの送信内容として、送信元、送信先、件名、本文の内容を取得します。

対応サービス

クラウドストレージ

● Dropbox
● Google Workspace
● Microsoft 365

Webメール

● Gmail
● Outlook.com
● Outlook Web App

※アップロード、ダウンロード、Web書き込みログは、Webページの仕様により、正しく取得できない場合があります。

社内LANを経由しないインターネット環境でも、Webを安全に利用できます。

クライアントWebフィルタリング

エージェントをインストールし、クライアント側でWebフィルタリングができます。外出先やホテルの公衆無線LAN利用時など、社内LANを経由しないインターネット環境においても安全なWeb利用ができます。

Web フィルタリングカテゴリ		
● 不法	● ショッピング	● スポーツ
● 主張	● コミュニケーション	● 旅行
● アダルト	● ダウンロード	● 趣味
● セキュリティ・ プロキシ	● 職探し	● 宗教
● 出会い	● グロテスク	● 政治活動・政党
● 金融	● 話題	● 広告
● キャンブル	● 成人嗜好	● 未承諾広告
● ゲーム	● オカルト	● ニュース
	● ライフスタイル	

※ 全148カテゴリ

Pick Up

業界No.1フィルタリングデータベース採用！
通信キャリアをはじめ、様々な企業が採用しているネットスターの
フィルタリングデータベースを利用しています。

Webフィルタリングデータベース登録数

43億コンテンツ以上

(2019年2月28日現在)

国内Webセキュリティ市場
ベンダー別売上額／シェア※
※出典：IDC Japan, 2018年7月「国内情報セキュリティ製品市場シェア, 2017年：外部脅威対策および内部脅威対策」

User's Voice

深夜の不審なWebアクセスをキャッチ！情報漏えいを未然に防止できました。

LANSCOPEを導入して7年間で2回、それぞれ、深夜の大量のWebアクセスと大量印刷をLANSCOPEで発見。何を行ったのか確認し、情報漏えい対策を実施できました。今では、この経験を活かして社内啓発がしっかりできていますので大丈夫ですが、LANSCOPEは何かがあったときの保険のような存在です。

33

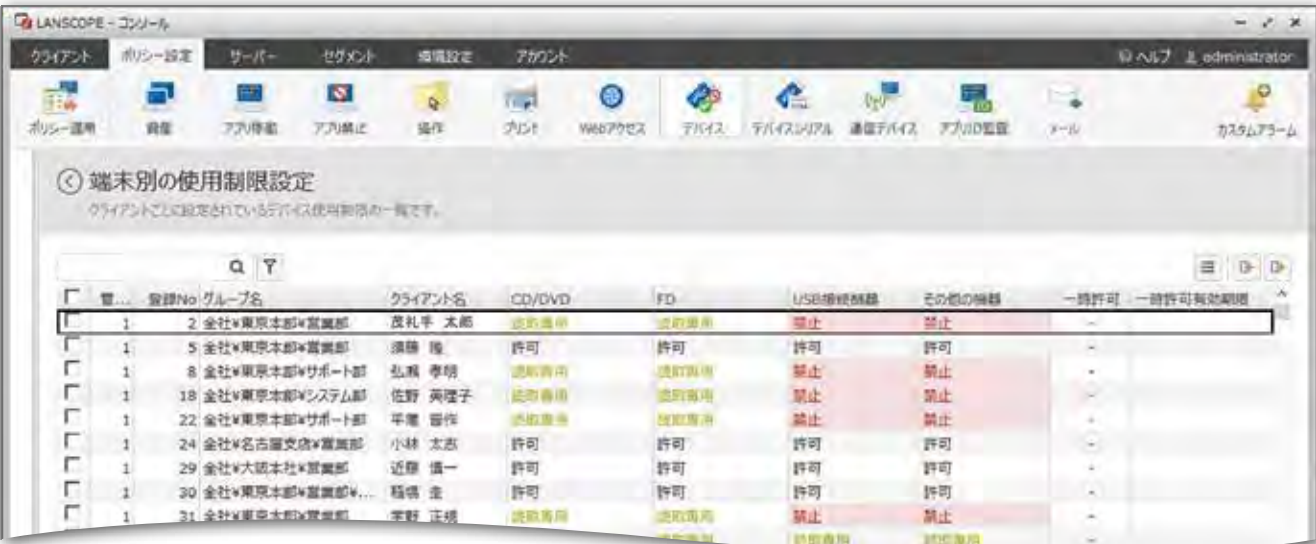
34

デバイス制御

Mac Mac 端末管理対応 ※専用ライセンスの購入が必要です。

USBメモリやCD、スマートデバイスなどのデバイス利用を制御し、重要な機密データの情報漏えいを防止できます。

社内のデバイスを一元管理し、利用を制御できます。禁止デバイスが接続されると、ユーザーに禁止通知し、不正利用を抑制できます。また、PCやデバイスごとの詳細な条件で限定的にデバイス利用を許可し、現場に即した運用が可能です。



端末別の使用制限設定
CD/DVD、USBメモリなどのデバイス種別単位で使用を制限／禁止できます。またPCごとに読み書き禁止／書き込みのみ禁止など、柔軟に設定できます。
・CD/DVD または FD の「禁止（外付け）」を選択した場合、USB 接続機器・その他の機器も「禁止」設定となります。
・スタンドアロン端末用にデバイス制御設定を適用したインストーラーを作成できます。

暗号化 USBメモリなど、特定のデバイスだけを利用許可できます。

許可または読み取り専用にする管理デバイスの設定

デバイス製品名（フレンドリーネーム）を指定しての利用許可、ベンダー ID とプロダクト ID の組み合わせ、シリアルナンバー単位の個体識別で指定して特定のデバイスを許可または読み取り専用ができ、その他のデバイスの使用を制御できます。

個体識別による許可設定強化

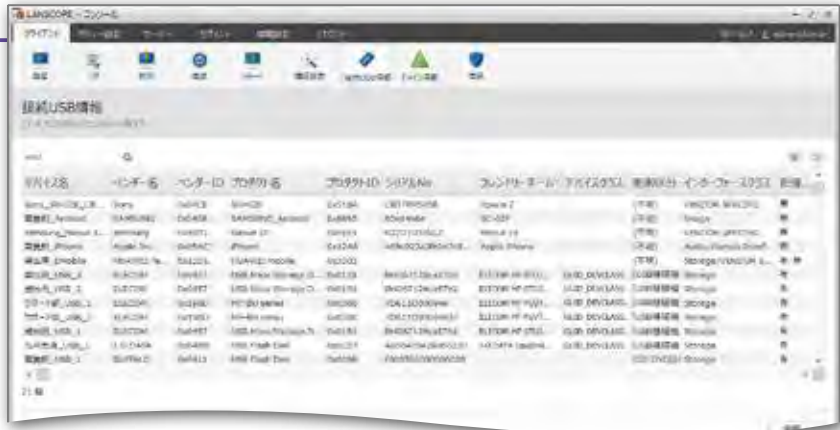
SD カードなど個体を識別する番号のないデバイスに対しても個別に許可／読み取り専用／一時許可／一時読み取り専用の設定が可能です。



ネットワーク上のPCに接続されたUSBメモリを一覧で表示し、管理できます。

接続 USB 情報

管理 PC に接続された USB を一覧で表示し、許可している USB か制御している USB かを把握できます。また、ユーザーや資産管理番号など管理に必要な情報を入力できます。



管理デバイスの利用許可ができる責任者を複数設定できます。 ※ Mac 端末管理非対応

デバイス責任者設定

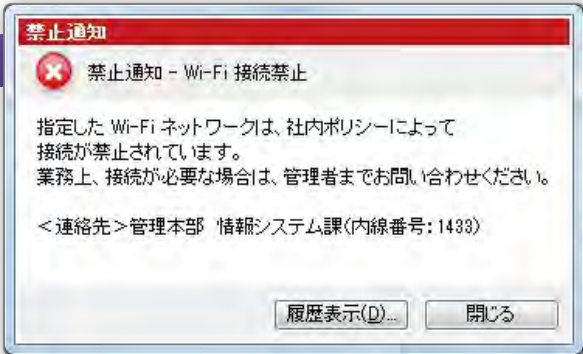
管理者以外に、登録したデバイスの利用を許可できる責任者を設定できます。責任者は自分の PC から登録しているデバイスに対して、コンソールの設定に従う／許可／一時許可／読み取り専用／一時読み取り専用をリアルタイムに変更できます。



Pick Up

通信デバイスの接続禁止／ホワイトリスト設定

Wi-Fi、Bluetooth、赤外線通信の接続を禁止し、ユーザーにポップアップ通知できます。また、SSID や BSSID 指定での特定 Wi-Fi 接続のみの許可や、デバイスの種類／MAC アドレスごとの Bluetooth の接続許可など、運用に即して柔軟に設定できます。



User's Voice

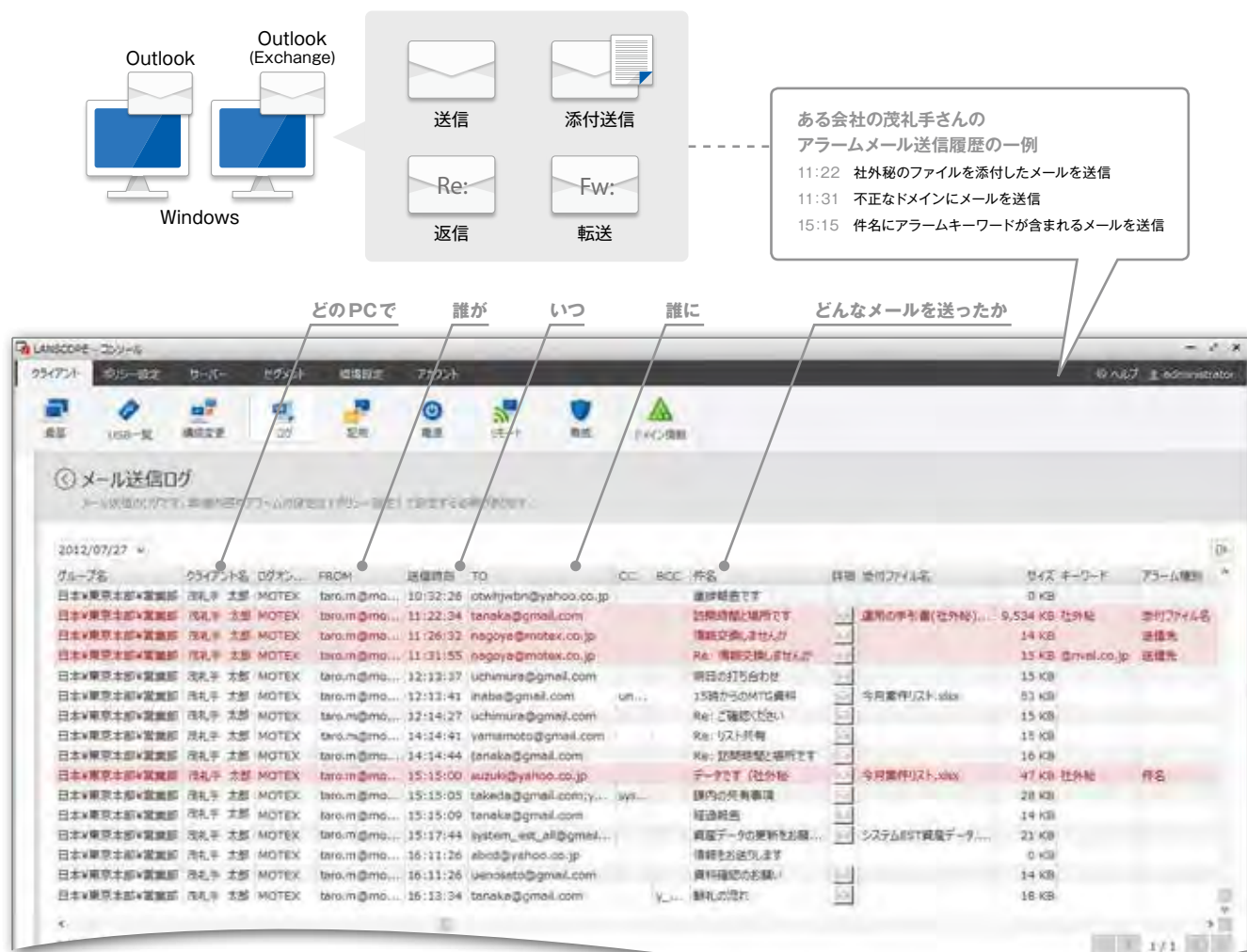
紛失／盗難は一つありません！私物 USB メモリの利用も完全シャットアウト。

センシティブな情報を大量に扱うため、情報漏えいを想像するだけで不眠症になりそうでしたが、LANSCOPEのおかげで、PCやUSBメモリを「一台も紛失・盗難されていない」ことを毎月チェックできるように。また、事前登録したもののだけ許可して私物利用をシャットアウト。これでぐっすり安眠できます。

メール管理 クライアント型

メール送信を適切に管理し、情報漏えいリスクを低減できます。

Exchange 環境など、Outlook から送信したメールの内容をクライアント側で記録します。機密ファイルの添付など違反メールが送られると、送信者に警告を表示します。不正なメール送信を抑止し、ユーザーのセキュリティモラルを向上させます。

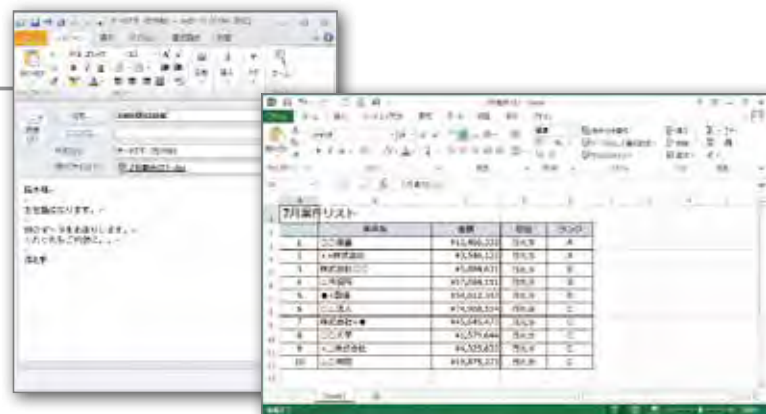


メール送信ログ管理

「どのPCで」「誰が」「いつ」「誰に」「どんなメールを送ったか」を記録します。送信メールの送信先 (TO、CC、BCC) / 件名 / 添付ファイル名が設定したキーワードに抵触した場合、ユーザーへの警告と管理者へのメール通知ができます。

メールファイル

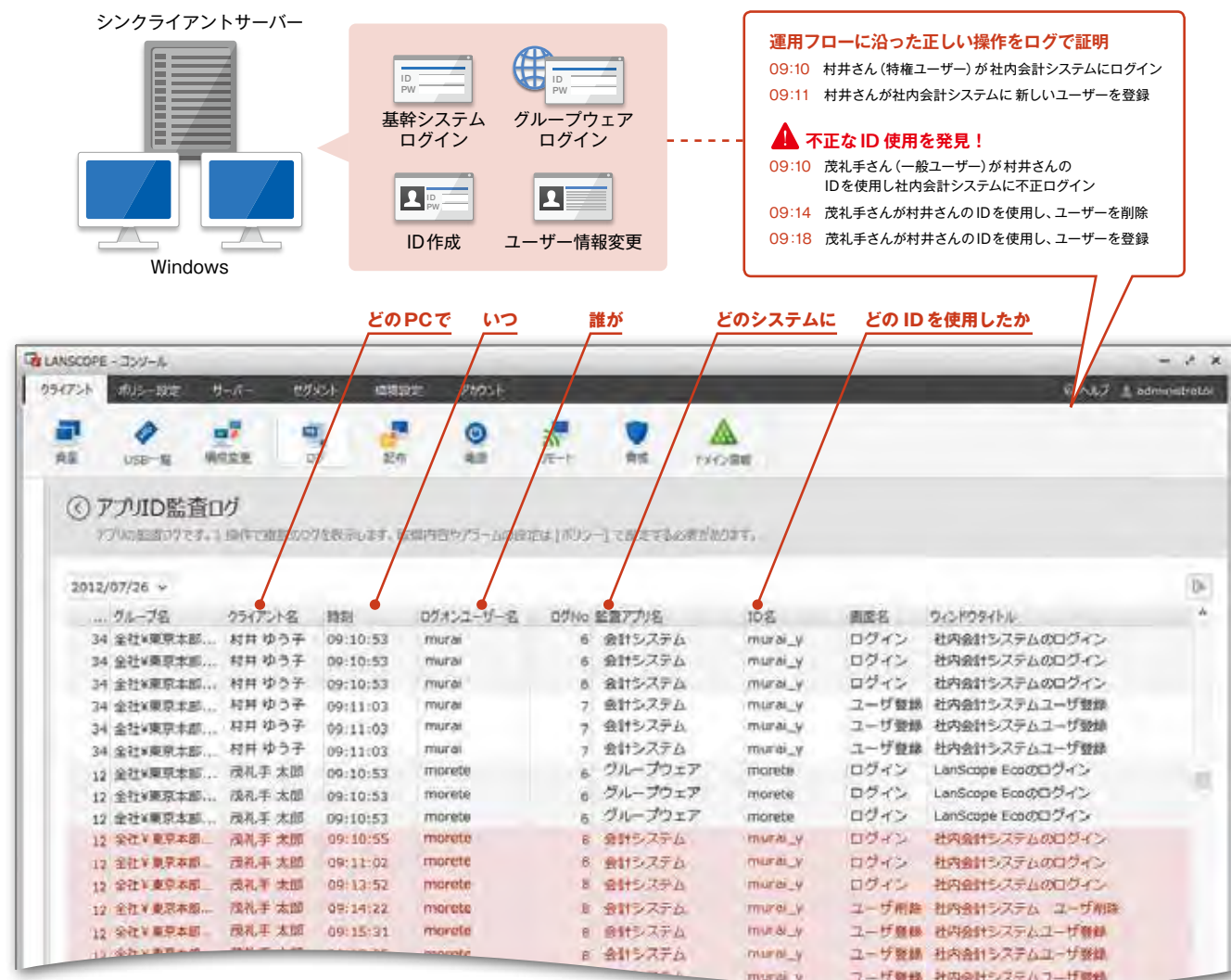
メールファイルをログからワンクリックで呼び出し、メールの本文や添付ファイルの確認ができます。



アプリID 監査 バーチャルライセンス対応 ※専用ライセンスの購入が必要です。

システムのID利用を把握し、監査対策に活用できます。

指定したアプリや Web 内の入力ボックスへの書き込み内容を記録します。ログインや ID 作成、変更などの操作を一元管理できます。また、なりすましや未使用 ID などを発見し、コンプライアンス違反につながる操作を抑止できます。



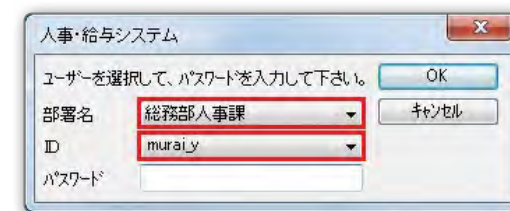
ID 監査ログ管理

「どの PC で」「いつ」「誰が」「どのシステムに」「どの ID を使用したか」を記録します。
なりすましや退職者の ID 使用など、許可されていない ID の使用が把握できます。

Pick Up

システムのログインID取得と不正ログイン発見

システムのログイン画面上のID入力ボックスへの入力内容を、OK ボタンクリック時に取得できます。マイナンバーを管理している人事／給与システムなどシステムへのログイン実績を確認し、業務時間外のログインや不許可端末からのログインをリアルタイムに管理者にメール通知します。また、各IDの最終利用日を一覧で確認し、長期間ログインしていない未使用IDを発見できます。



システムへのログイン状況と不正利用を把握し、社内セキュリティ対策をさらに強化。

グループウェアや CRM、業務システムなどの各システムに対し「どのPCで」「いつ」「誰が」「どのIDでログインしたか」を収集し、不正なログインがないかを監視しています。人や日時などの条件でログ検索し、複数システムにまたがった利用状況確認ができるようになったのは大きな成果です。

マルウェア対策

Mac Mac 端末管理対応 ※専用ライセンスの購入は必要ありません。

既知／未知のマルウェアを検知／隔離し、流入経路を追跡。原因となるユーザー操作に対策することで再発を防ぎます。

マルウェアを検知し、トロイの木馬・ランサムウェアなどの種別やリスクの高さを判断します。検知前後の操作ログから特定のWebサイト閲覧・標的型メールの開封など、流入原因を確認し、Webサイトのフィルター強化や社員教育により再発を防止できます。



ダッシュボード
実行／自動実行されている脅威の数、隔離した脅威の数、BlackBerry 社のみが発見した脅威数の合計値と24時間以内の件数が確認できます。検知したマルウェアを、危険／異常／隔離済みで分類しレポートします。管理者はマルウェアの詳細内容を確認した上で、許可するか、隔離するかを選択できます。また、マルウェア検知状況を脅威／ゾーン（任意で設定した端末のグループ）／端末に分けて確認し、どこにセキュリティリスクがあるかを把握できます。

マルウェア／エクスプロイト対策機能

ファイルアクション	危険なファイル、異常なファイルをAIが検知し自動隔離することでマルウェアの実行を防ぎます。また、検出したファイルをクラウドにアップロードし、詳細な分析を行い、危険性を判定するための情報をフィードバックします。
メモリアクション	OSのメモリ上で稼働中のプロセスを監視し、脆弱性の悪用やメモリ上で動作するほかのプロセスを利用した攻撃／権限昇格を検知し、攻撃が成功する前にブロックします。
スクリプト制御	Office 製品のマクロ実行や PowerShell や VBScript、JScript などのスクリプト実行の検知やブロックを行います。

Step1 カレンダーで脅威の有無を確認。

Step2 どのPCで何件の脅威があったかを確認。

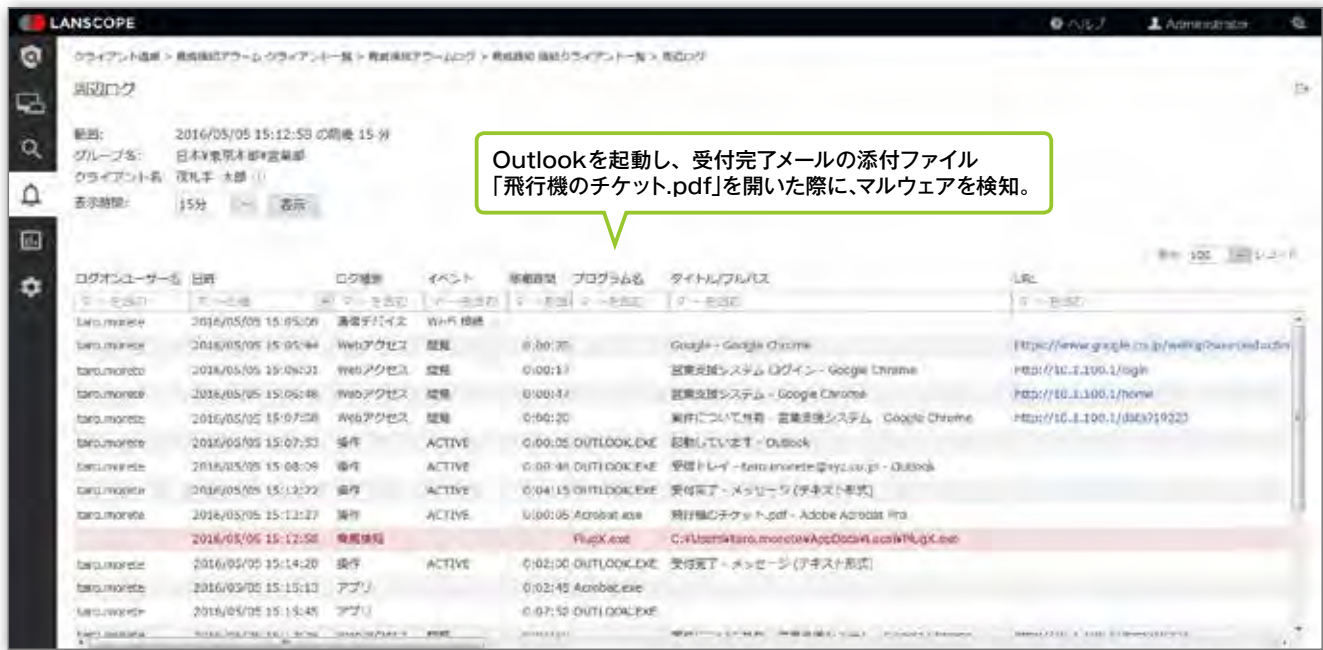


Step3 どんなマルウェアを検知したかを確認。

Step4 同じマルウェアを検知したPCの確認。



Step5 マルウェアの流入原因となるユーザー操作を追跡・確認し、再発を防止。



※別途操作ログ管理の購入が必要です。

User's Voice

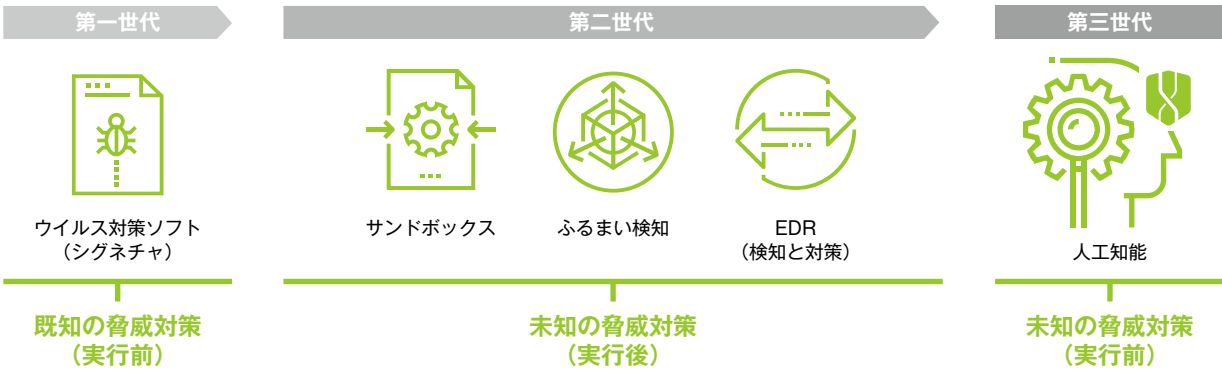
事後対策の限界により事前対策へ方針転換！未知のマルウェアも感染前に隔離。

セキュリティ対策は行っていたが、マルウェア検知後の対応業務が増える一方で、対応工数やコストに見合った効果が見えない状態に…そんな中、人工知能で感染前に防御するコンセプトに興味を持ち、自社環境250台で評価を開始。既に侵入していたマルウェアを複数検知／隔離できたのを確認し導入を決めました。

マルウェア対策ライセンス Powerd by BlackBerry Protect

特長① AIエンジンを活用したAIアンチウイルス

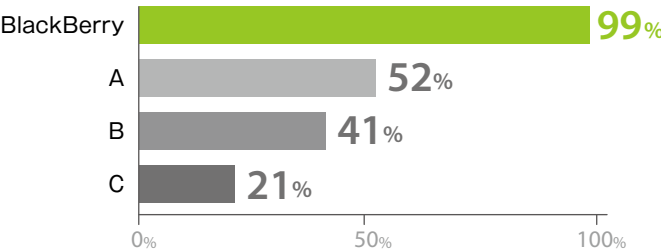
マルウェア対策ライセンスはAIエンジンを活用。これまでのウイルス対策ソフトやふるまい検知、サンドボックスのように止められないことが前提の事後対策ではなく、未知の脅威でも実行前に検知し防御することができます。



特長② マルウェア検知率99%以上※を実証

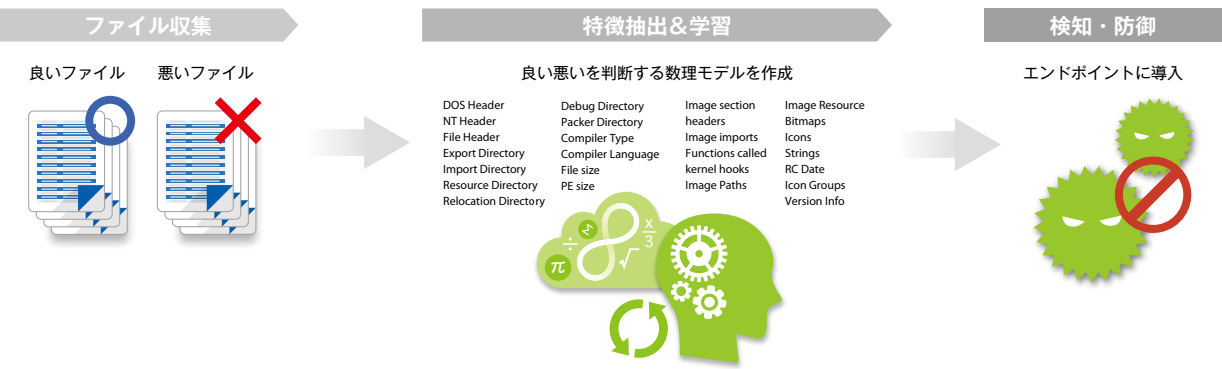
全米75都市でアンビリバーブルツアー開催。

- 都度、24時間以内に入手した最新のマルウェア100個とその亜種の合計200個が対象
- BlackBerryとアンチウイルス3製品のマルウェア検知結果を累計2,100人以上の観客が目撃
- 2017年5月に発生したWannaCryを当日に防御 (2015年のバージョン)



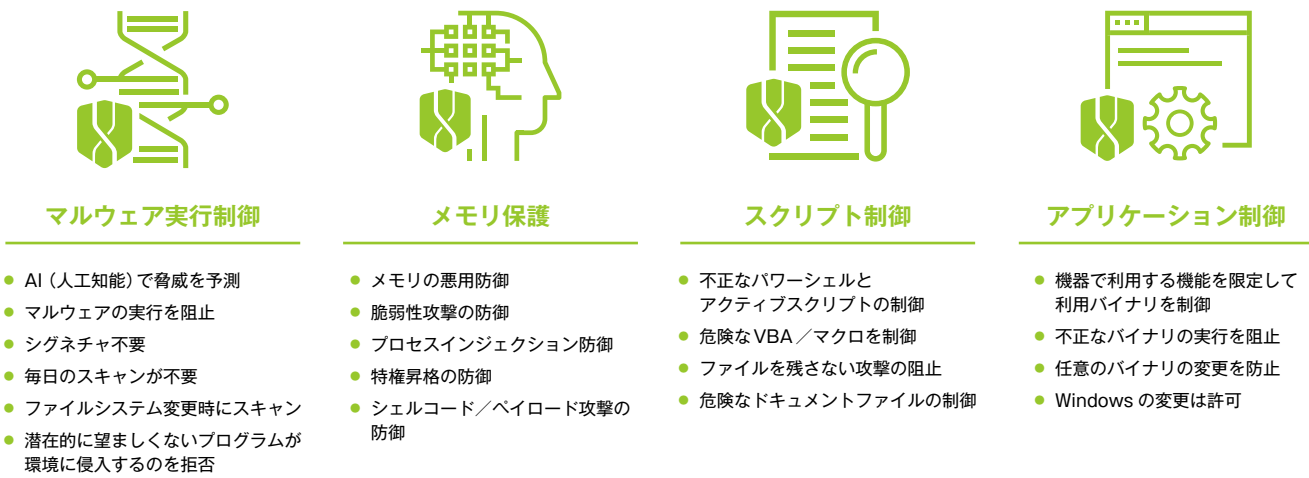
特長③ “ファイルの要素”から人工知能が予測防御

クラウドにあるAIに10億のファイルを学習させ、各ファイルから最大700万の特徴を抽出。マルウェアが正常ファイルかを判断する数理モデルを作成し、エンドポイントに導入します。



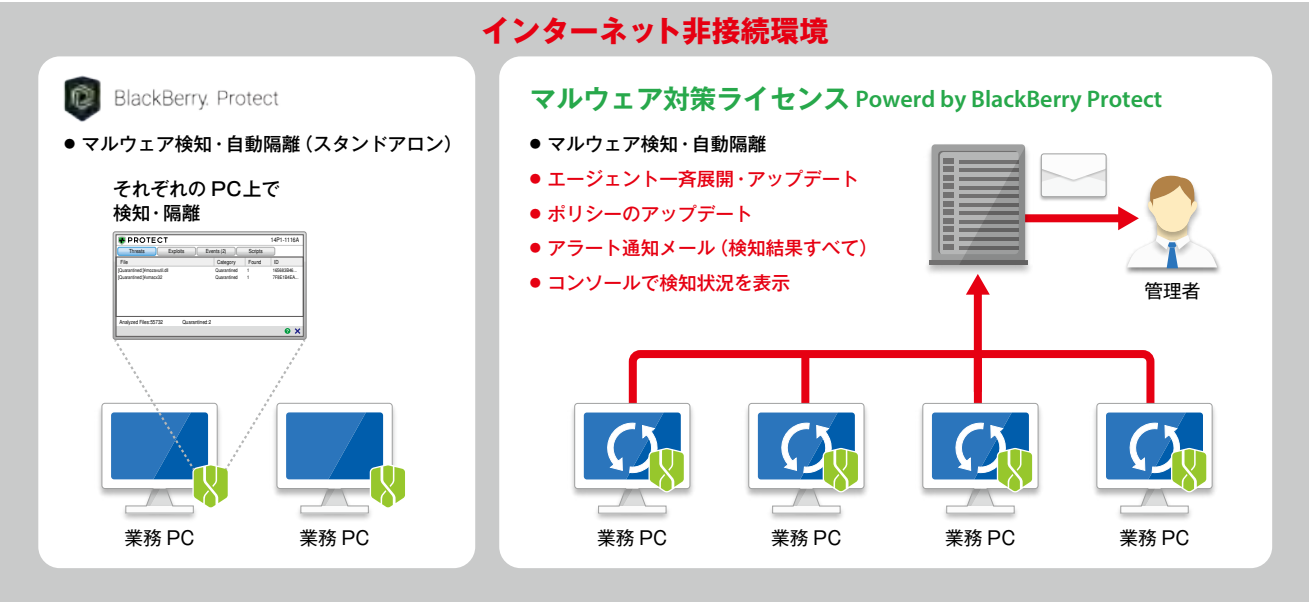
特長④ 実行前防御を実現する4つのプロテクション機能

AIを使った「マルウェア実行制御」以外に、メモリの悪用・脆弱性攻撃の防御、マクロやスクリプトを使った侵入制御、クローズド環境における特定アプリ以外の起動制御ができる機能を搭載しています。



特長⑤ インターネット非接続環境下においても管理が可能

インターネットに繋がらない環境でもLANSCOPEのマネージャーにすべての情報を集め、レポートで検知状況の確認やアラートメールによる通知を行います。またエージェントの配布やポリシーのアップデートが可能です。



Pick Up

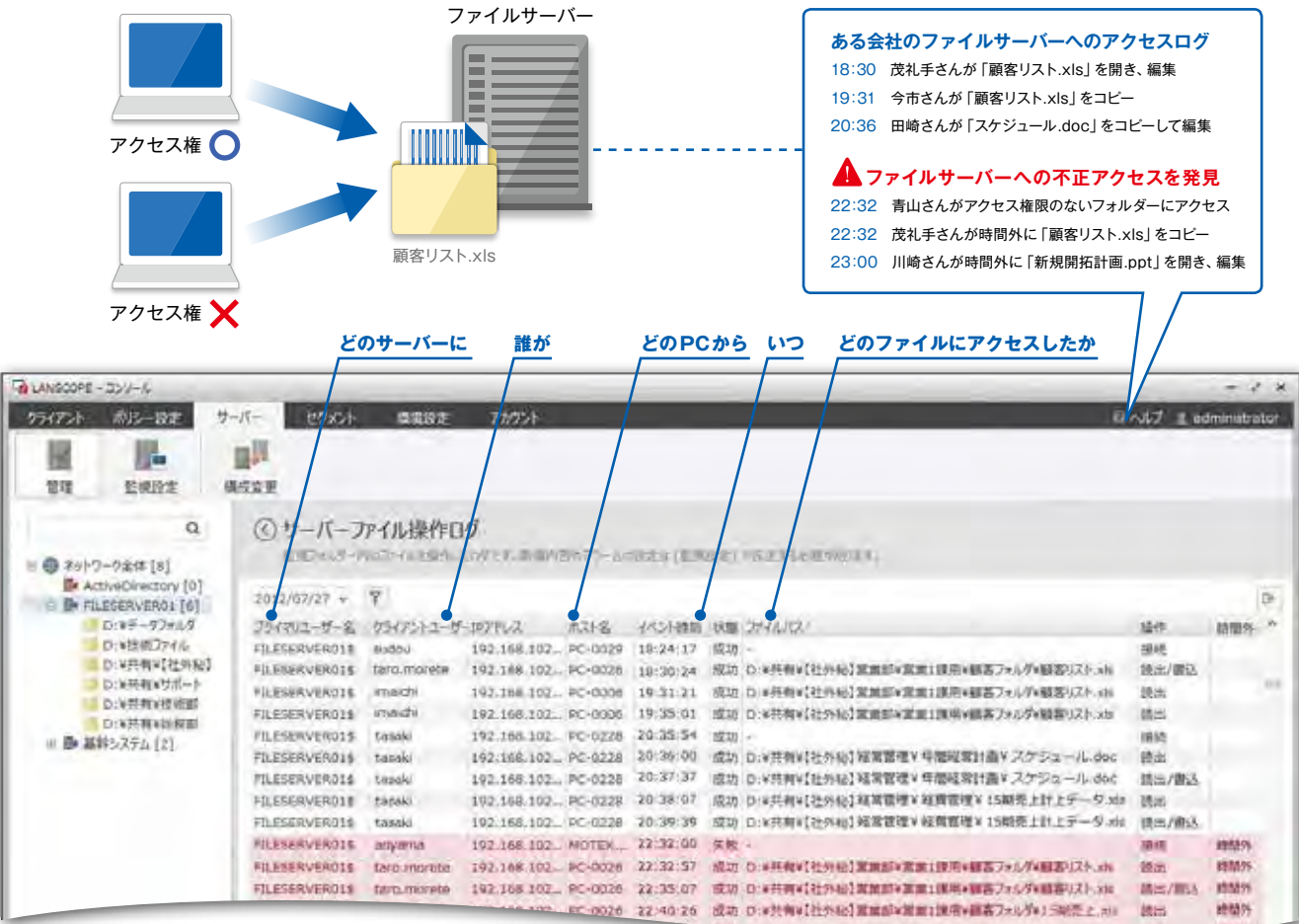
業界最高峰のAIアンチウイルス BlackBerry Protect

未知のマルウェアに対応できるAIアンチウイルスBlackBerry Protectと、パターンマッチング型のMicrosoft Defenderの組み合わせによる多層防御で、強固なセキュリティを実現できます。BlackBerry ProtectとMicrosoft Defenderは併用が可能です。

サーバー監視

ファイルサーバーを監視し、セキュリティ監査に活用できます。

Windows や NetApp のファイルサーバーへのアクセスや、Active Directory へのログオン状況を把握できます。権限を持たないユーザーからの不正アクセスも記録可能なため、権限設定の見直しやセキュリティ監査時の証拠として活用できます。



サーバーアクセスログ

「どのファイルサーバーに」「誰が」「どの PC から」「いつ」「どのファイルにアクセスしたか」を記録します。ファイルの読み出し、書き込み、削除、名前変更、EXE の実行を記録し、ファイルサーバーへの不正なアクセスを把握できます。

サーバーアクセスログの詳細

- 【削除】ファイルの削除／移動
- 【読出】ファイルのコピー／貼り付け、ファイルのプロパティを見る、ファイルを開く、エクスプローラーでファイルのポップアップメニューを見る
- 【読出／書込】ファイルを編集する
- 【書込】アプリケーションからファイルを開く／ファイルの上書きコピー（既存ファイル名と同一ファイルを上書きする）
- 【名前変更】ファイル名の変更
- 【実行】EXE の実行



ドメインログオン・ログオフ管理

「どのドメインに」「誰が」「どの PC から」「いつ」「ログオン・ログオフしたのか」を記録します。社内ネットワークへの参加状況の把握や勤怠管理にも活用できます。



ファイルサーバー容量管理

管理対象のフォルダー容量を監視します。設定した容量のしきい値を超過すると管理者にメール通知されるので、容量不足を未然に防ぐことができます。

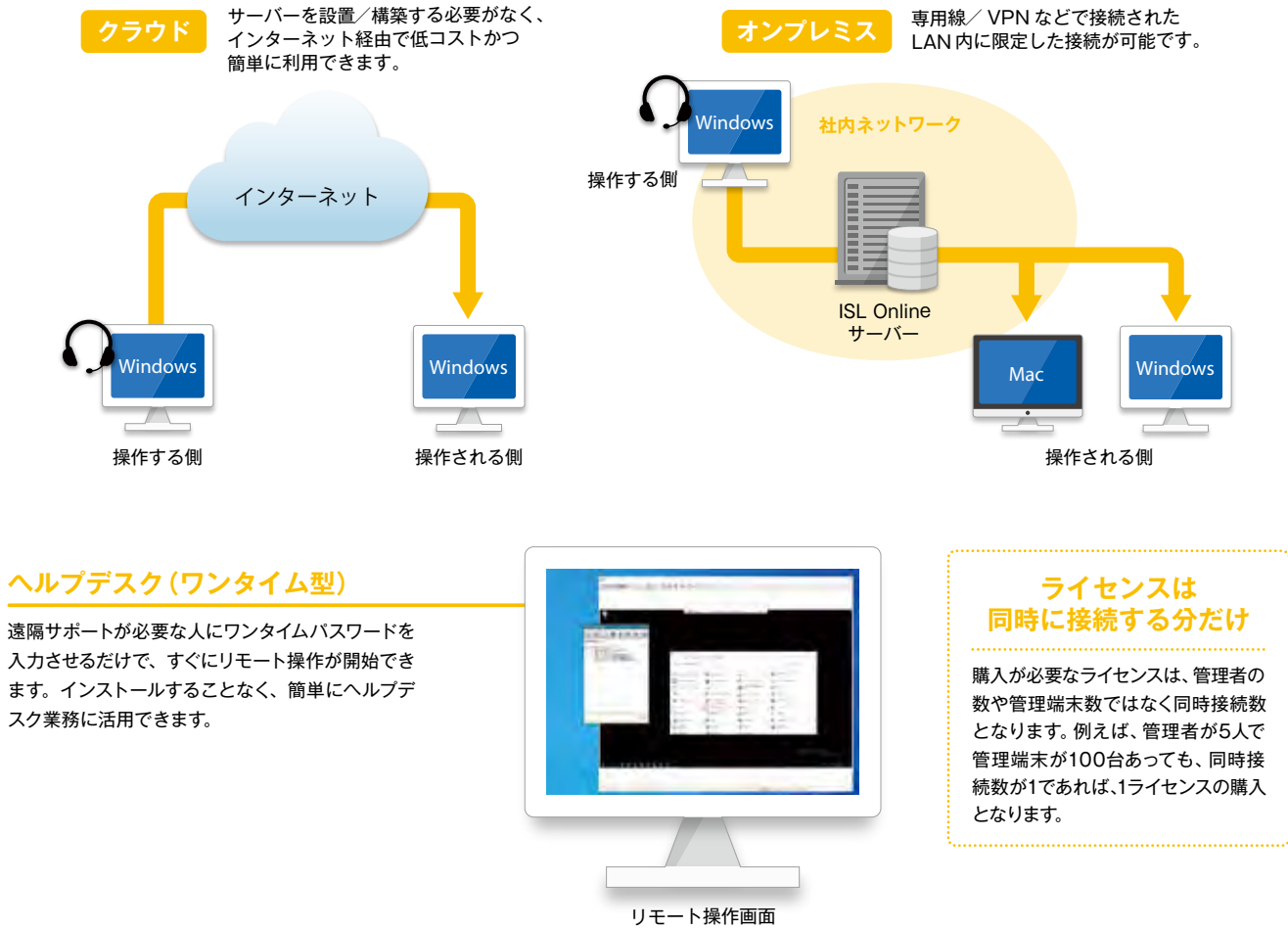
•接続先のサーバーが Windows XP の場合、接続ログ、ファイル操作ログの IP アドレスが空白になります。•切断時のログは IP アドレス、コンピュータ名が空白になります。•NetApp 環境ではサーバーアクセスログのみ取得します。

REMO-CON

Mac Mac 端末管理対応 ※専用ライセンスの購入は必要ありません。

リモート操作でヘルプデスクやメンテナンスの効率化を実現します。

REMO-CON powered by ISL Online は、LANSCOPE と連携して遠隔地にあるサーバーや PC、スマホへの「リモート操作」「画面共有」を実現する企業向けのリモートコントロールツールです。



新機能

課題解決

機能詳細

レポート

連携製品

制限事項

設定と運用、両方の使いやすさを追求したインターフェース

システム管理者の効率を重視した設定用のコンソール

組織のメンテナンスやポリシーの設定、アプリの配布などシステム管理者の日々の運用を集約。3ステップの統一された操作で、迷うことなく目的の画面にたどり着けます。対象のPCを直観的に把握できるツリー、大量の情報から知りたいことをすぐに検索できるフォームなど、かゆいところに手が届く工夫を詰め込みました。

目的ナビ

この画面で何をやるのか、目的を分かりやすく説明します。

チュートリアル

初めてお使いの方も安心、設定の完了まで一緒に案内します。

便利なリンク

マニュアル、Webコンソール、保守サイトをすぐに呼び出すことができます。

ハードウェア資産情報

クライアント名	登録グループ名	詳細	クライアントタイプ	IPアドレス	コンピュータ名	MACアドレス	OSバージョン
田中 太郎	2 会社 (MOTEX-PC) 東京本部...	...	...	192.168.102.208	PC-0026	001603B19A1C	Windows
...	...	...	...	...	...	...	...

列の固定

列を固定し、Excelライクに閲覧できます。

検索／フィルター

主要な画面で検索／フィルターが使えます。AND/OR 検索も対応しています。

使う人に合わせた「専用コンソール」を作れます。

対象のグループと使える機能を限定して、必要な人に必要な機能だけを持たせた専用のコンソールを設定できます。専用のコンソールでは、その人に必要のない選択肢を出さないで、迷わず使えます。また、分散管理を正しく行っていることを証明するために、管理コンソールへのログイン・ログオフや閲覧内容、設定内容の履歴を保存できます。

システム管理者のコンソール

拠点の担当者専用コンソール

組織全体での運用を実現するWebコンソール

インストール不要、ブラウザからセキュリティ状況が把握できる運用画面です。カレンダー形式でその日発生したアラームの有無を一目で確認、組織内で発生したアラームをリアルタイムに把握し対処を実施。充実したレポートで分析や報告を支援します。

レポート

一目で状況が分かるレポート。リストでフィルターをした結果もすぐに反映されます。

Excel データ出力

ワンクリックで、グラフと表数値のExcel形式で出力できます。

検索／フィルター

すべての項目で、フィルターや検索ができます。

列の固定

列を固定し、Excelライクに閲覧できます。

閲覧情報の表示レベルを選んで、拠点ごとに運用できます。

「ルール違反の数値のみ」「ルール違反のアラームログの内容まで」「すべてのログを閲覧可能」の3段階の表示レベルを選択できます。「ログの中身は見せたくないが、ルール違反が何台あったかだけは拠点の担当者に把握してほしい」「違反したログは見せたいが、それ以外のログはシステム管理者にも見せたくない」といった、かゆいところに手が届く設定ができます。権限を分散して管理し、システム管理者に運用負担が偏らない「全社で取り組むセキュリティ」を実現できます。



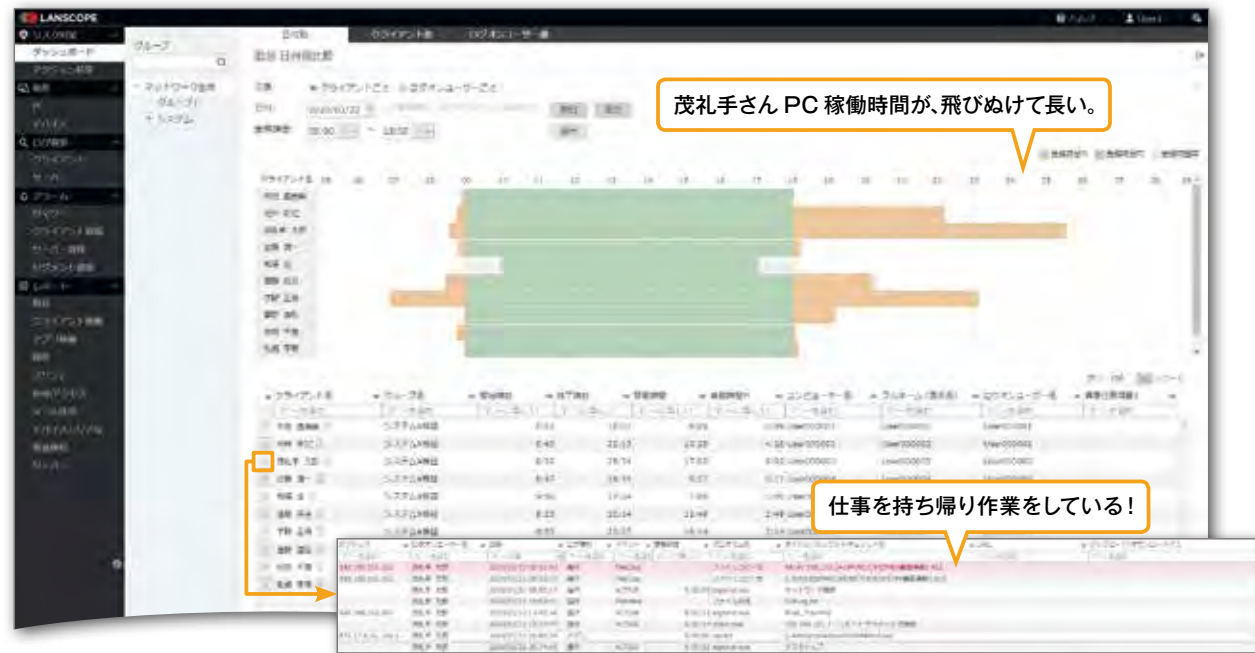
レポート - Webコンソール

PCやアプリの稼働状況を確認し、残業／コストを削減できます。

PCの稼働状況を確認することで、勤務状況や残業の把握、未稼働PCの発見／最適配置によるコスト削減ができます。
また、アプリの稼働状況を確認することで、無駄なライセンスの発見や危険なアプリの稼働状況の把握ができます。

勤怠 日付別比較

操作ログ管理

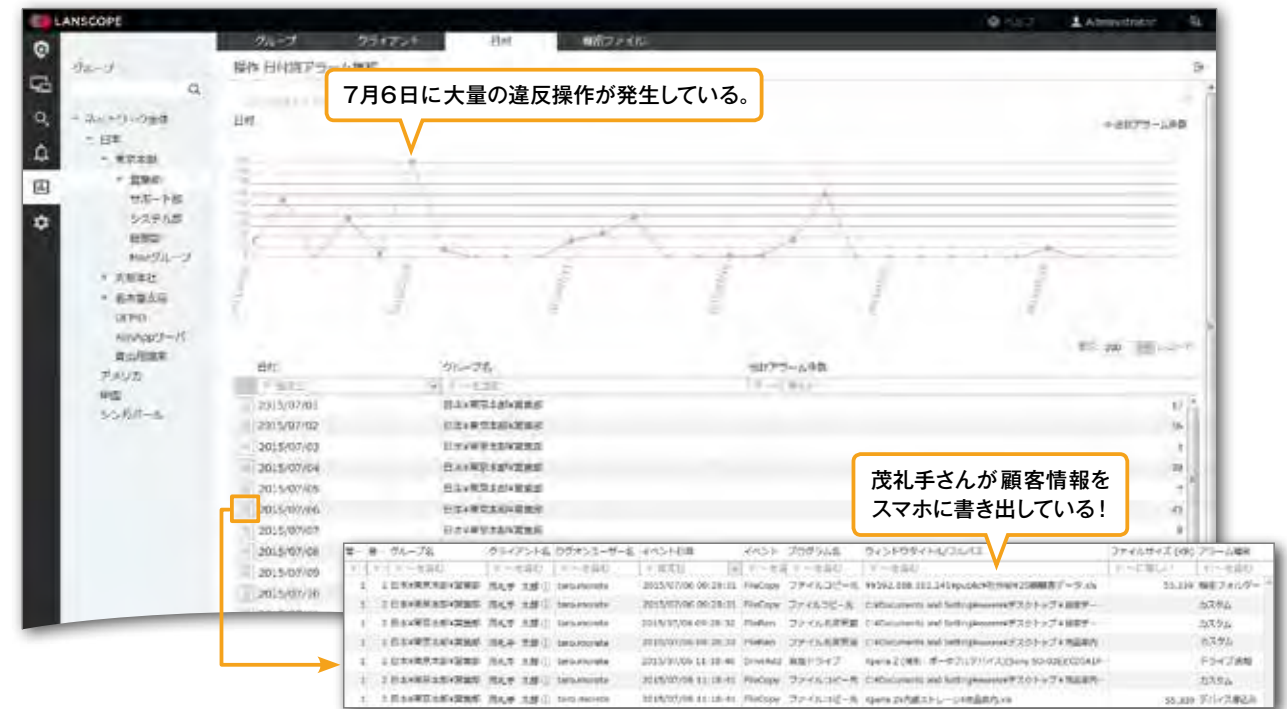


USB書き出しや印刷による情報漏えいリスクを把握できます。

機密フォルダー内のファイル操作や、USBメモリ／スマートフォンへの書き出しなど、情報漏えいリスクのある操作を把握できます。また、デバイス単位に書き出した内容を確認することで、重要情報の持ち出しを把握できます。

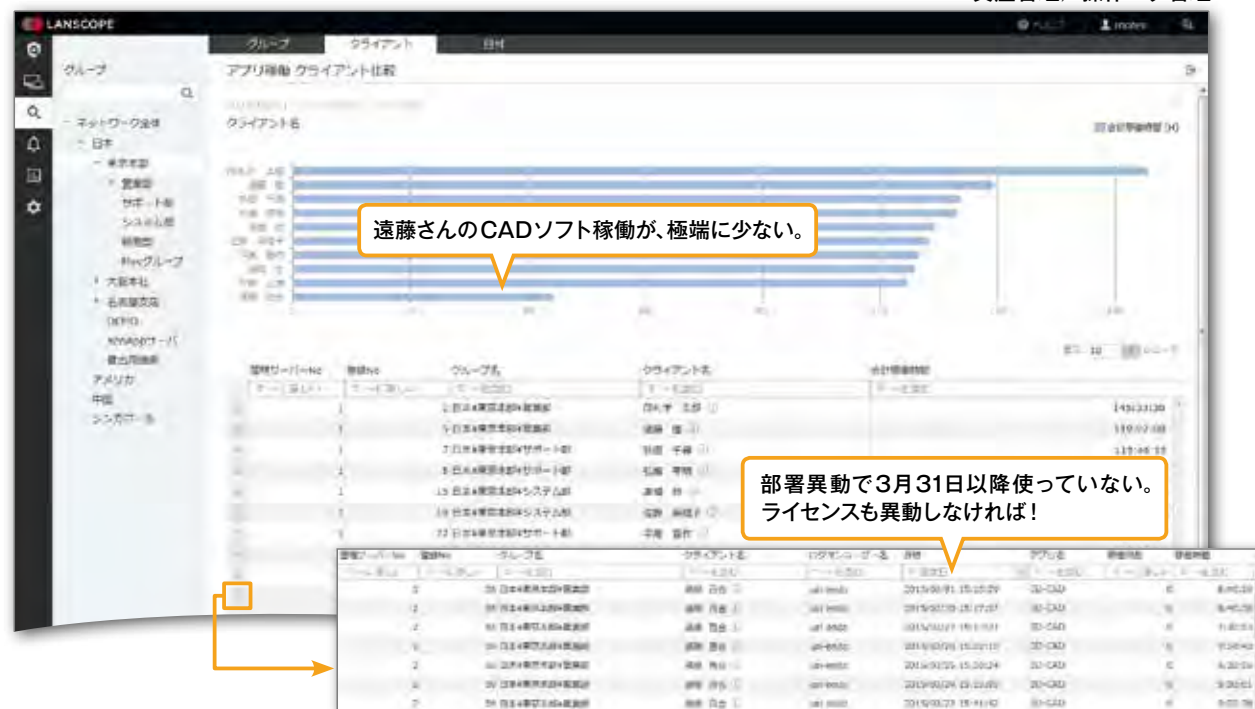
操作 日付別アラーム推移

操作ログ管理



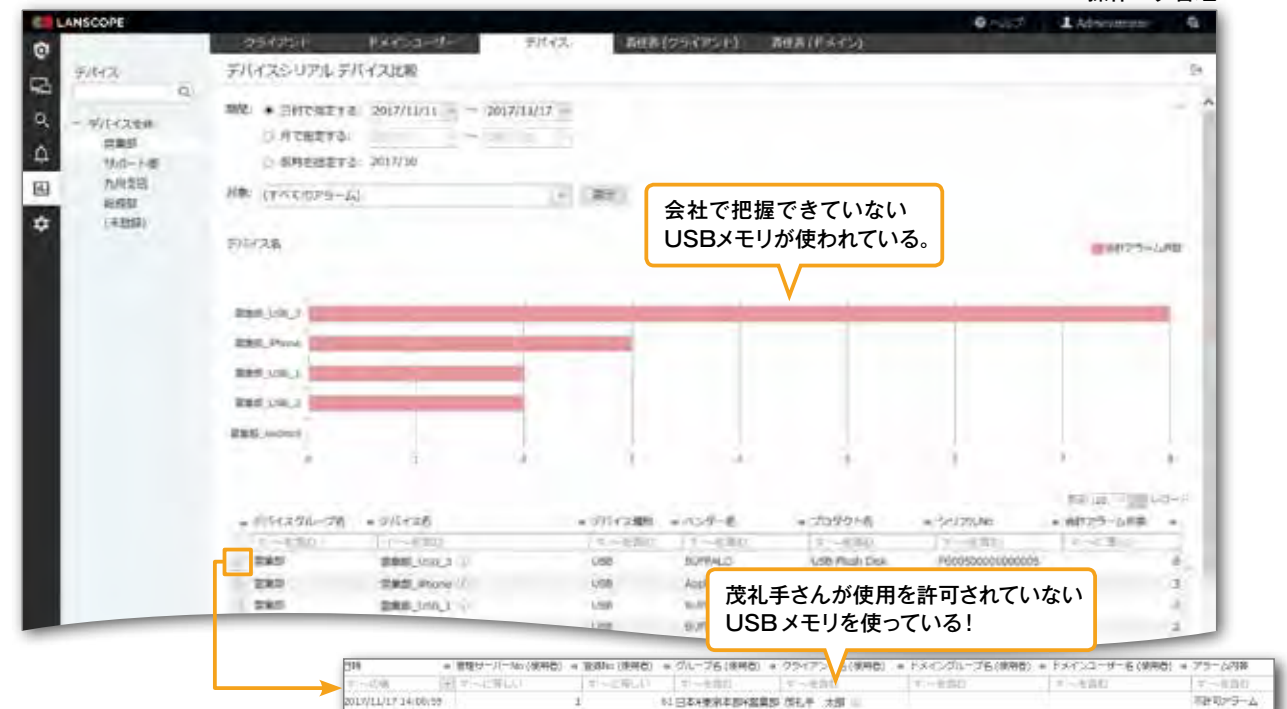
アプリ稼働 クライアント比較

IT 資産管理／操作ログ管理



デバイスシリアル デバイス比較

操作ログ管理



新機能

課題解決

機能詳細

レポート

連携製品

制限事項

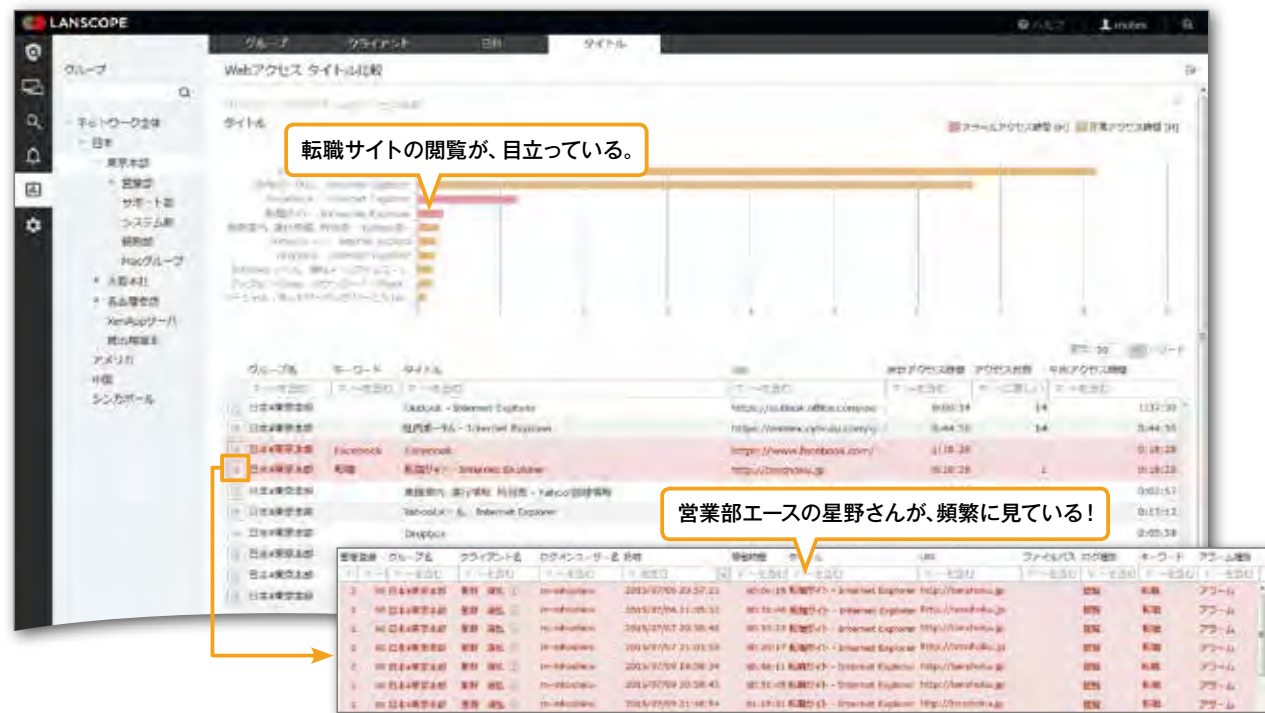
レポート – Webコンソール –

Webやメールが適切に活用されているか、分析できます。

社内ポータル利用頻度や業務外のWeb閲覧状況などを把握し、適切にWebが活用されているか分析できます。
また、競合会社やフリーメールへの送信／ファイル添付の状況から、適切なコミュニケーションが取れているか確認できます。

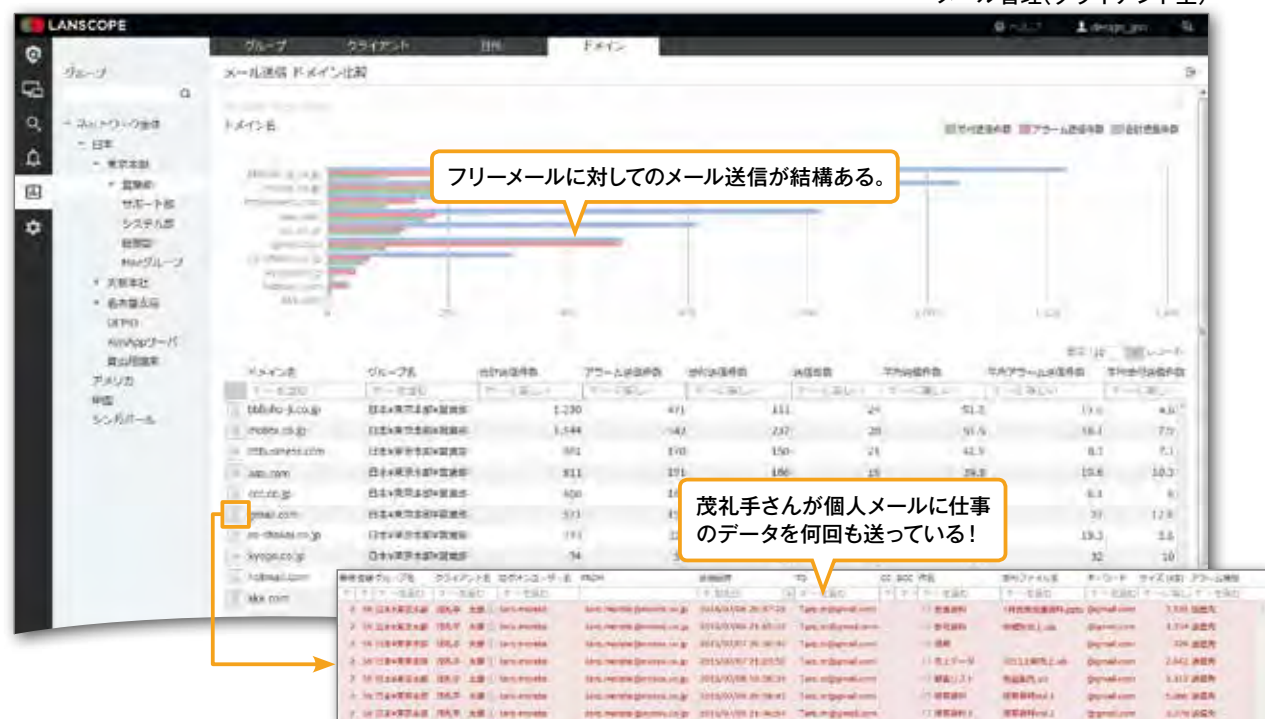
Webアクセス タイトル比較

Webアクセス管理



メール送信 ドメイン比較

メール管理(クライアント型)

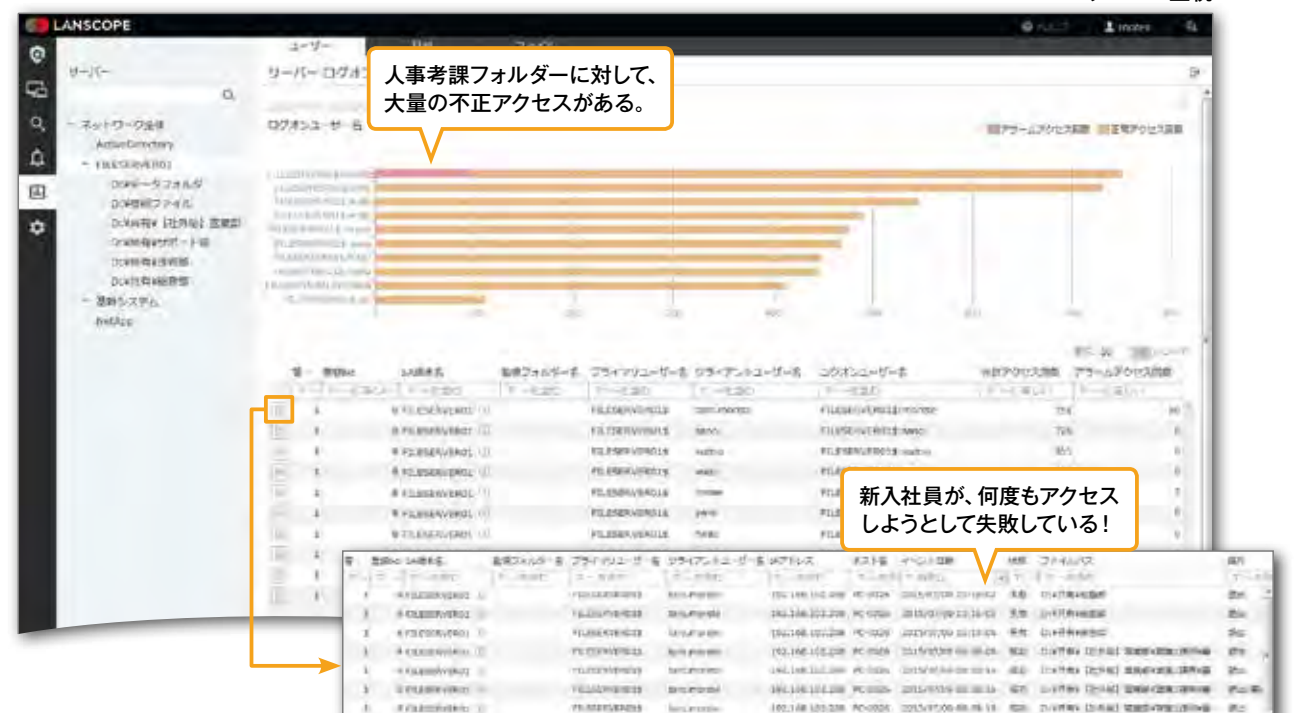


サーバーやネットワークへの不正なアクセスを発見できます。

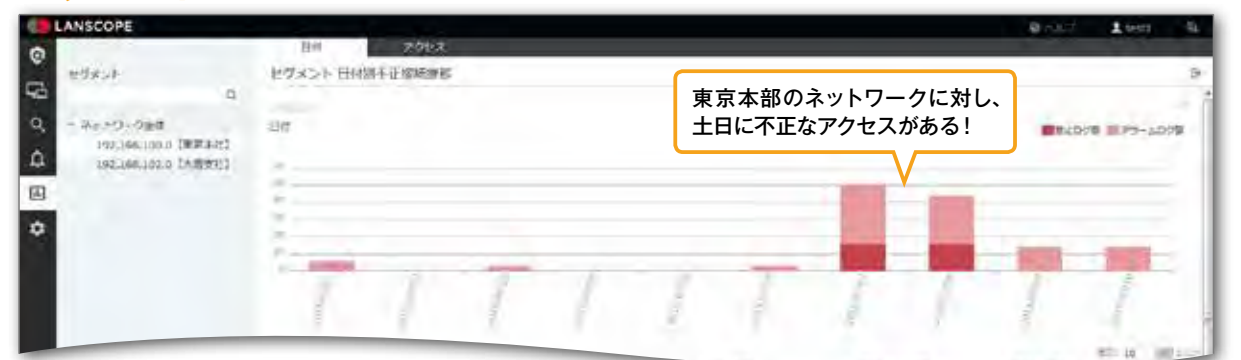
ファイルサーバー上の機密情報に対して、権限のない不正アクセスの有無やユーザーごとのアクセス状況を把握できます。
また、社内ネットワークへの機器接続状況をセグメント単位で確認し、管理外の不正な機器接続がないかを発見できます。

サーバー ログオンユーザー比較

サーバー監視



セグメント 日付別不正接続推移



Pick Up

レポートごとに自由度の高いデータ抽出が簡単にできます。

レポートフィルター

レポートの表示項目すべてに対し、様々な条件でフィルターをかけることができます。Webのレポートで、イントラネット以外のアクセス状況を確認するなど、柔軟なデータ抽出ができます。

Excel データ出力

ワンクリックで、グラフと表数値のデータを連動させた形でExcel出力できます。出力したExcelデータを自由に加工して、高度なデータ検索／抽出ができます。

新機能

課題解決

機能詳細

レポート

連携製品

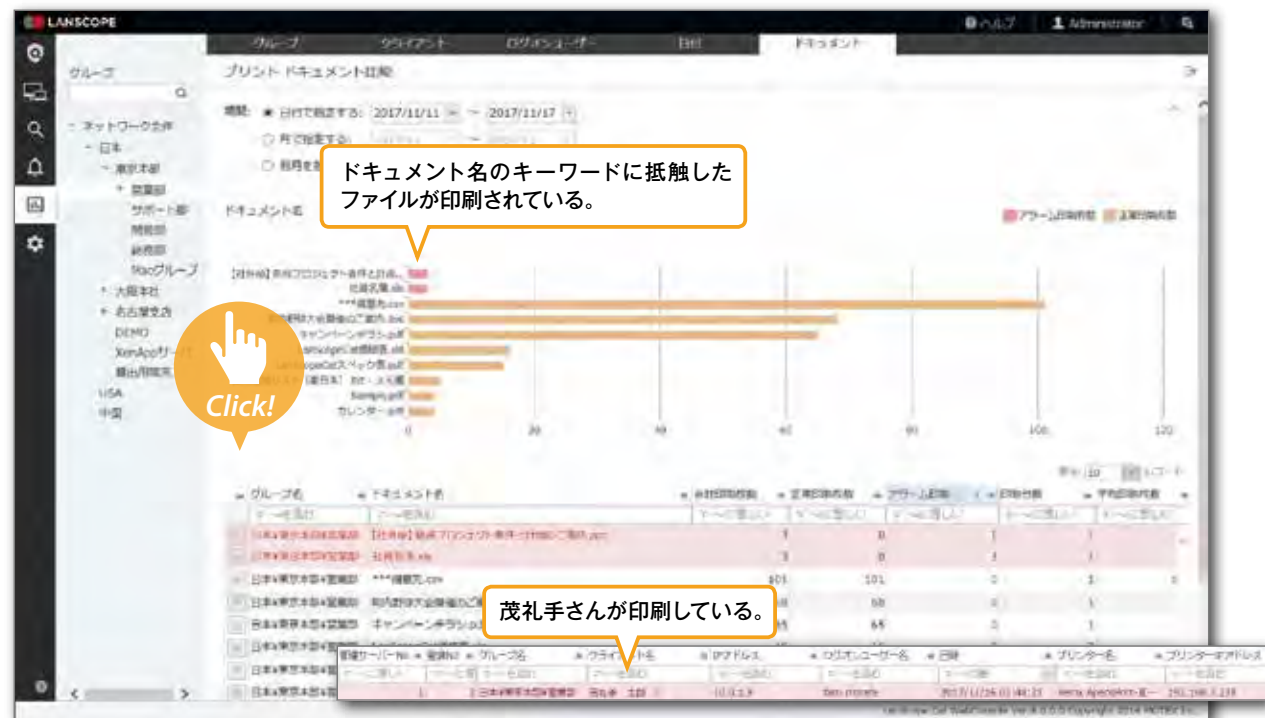
制限事項

レポート – Webコンソール

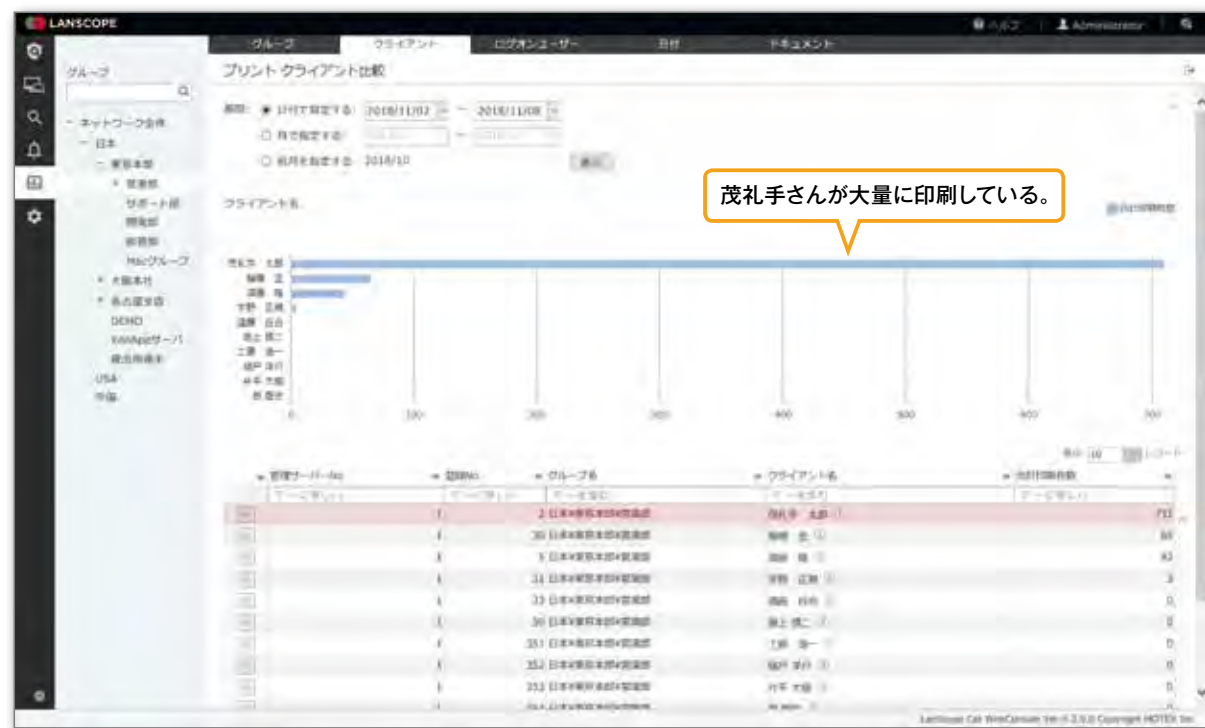
印刷による情報漏えいリスクを把握できます。

ファイル名だけではなく実際の印刷物のイメージを確認できるので、ファイル名が変更されていても、情報漏えいにつながる印刷を発見できます。また、業務に関係ない書類の大量印刷を把握でき、社員の指導に活用できます。

プリント ドキュメント比較



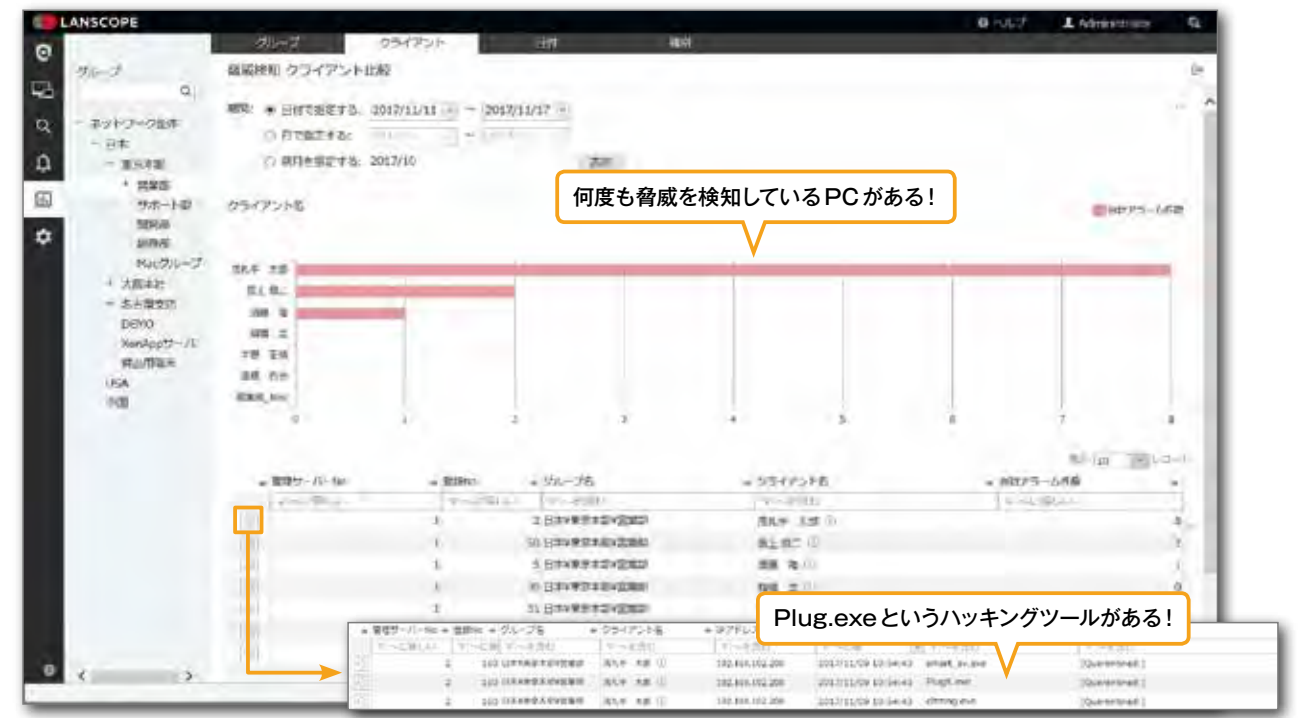
プリント クライアント比較



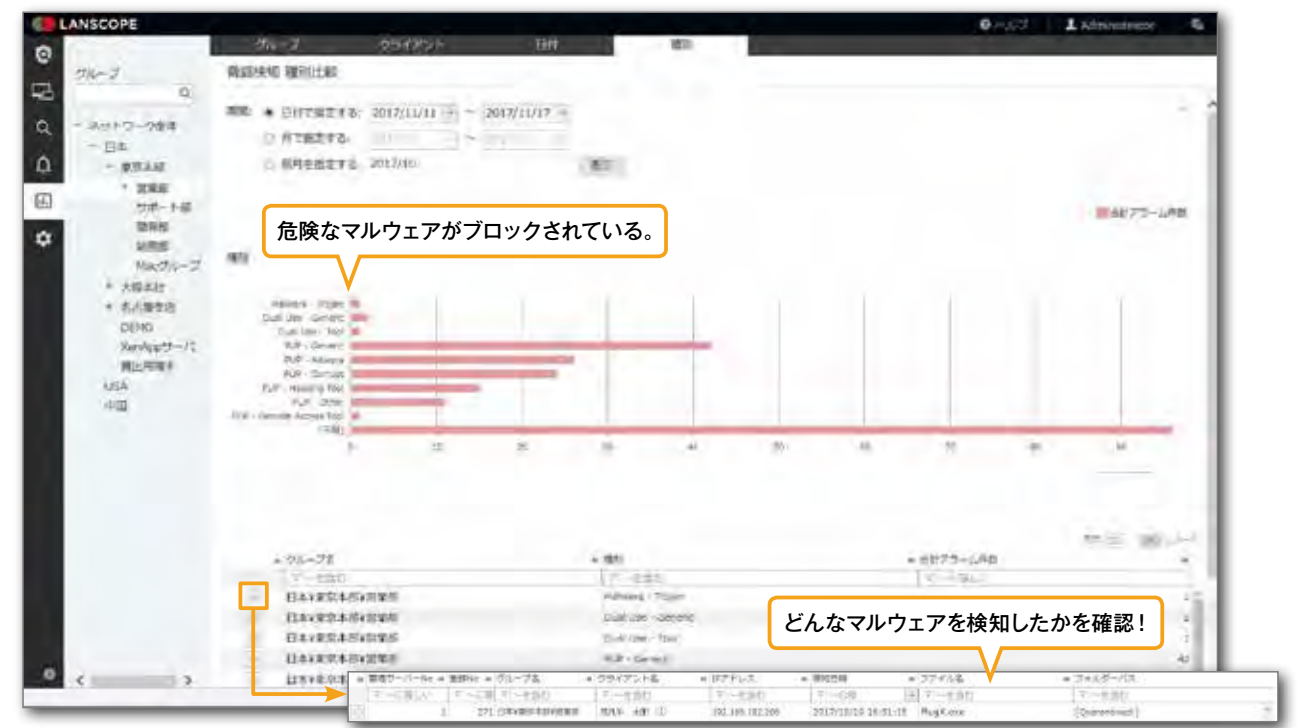
検知した脅威を種別やクライアント別にレポートします。

どのような脅威が、どのPCで発生したのかを分析できます。種別比較では、危険度の高い脅威順に集計値が表示され、周辺ログを確認することで、原因の追及と対策に役立ちます。

脅威検知 クライアント比較



脅威検知 種別比較



制限事項／注意事項

動作環境	
ネットワーク	管理コンソール、マネージャー、管理クライアント端末間で LANSCOPE が使用する TCP/IP、UDP による通信が行える必要があります。環境によりネットワーク機器、ファイアウォール等で LANSCOPE が使用するポートの開放が必要な場合があります。
	IPv6 には対応していません。
全般	マネージャーサーバー、管理クライアント端末は、OS の推奨システム要件を満たしてください。また、同居ソフトウェアの使用状況により、必要となるシステム要件が変更になる場合があります。
	LANSCOPE プログラムと SQL Server のインストールフォルダーはウイルス対策ソフトのリアルタイムスキャンの対象から除外してください。
サーバー	マネージャーサーバーは専用サーバーをご用意いただく必要があります。他のシステム等と同居する場合、問題発生時に対処として他システムとの別立てをご依頼する場合があります。
	マネージャーサーバーはパフォーマンス向上のため64bitOS環境を推奨しています。
	クライアント端末台数とご利用機能構成によって必要なマネージャーサーバー台数、サーバースペックが異なります。また、必要な HDD 容量はご利用環境により、メーカー推奨値と異なる場合があります。
	クライアント端末が 1,000 台以下の場合はサーバー 1 台、1,000 台を超える場合は、統合マネージャーサーバーとサブマネージャーサーバーを分けて構築する必要があります。サブマネージャーサーバーは、2,500 台ごとに1台必要です。
	1 台の Mac 管理サブマネージャーで、管理する Mac クライアント端末は 500 台以下を推奨しています。Mac クライアント端末が 500 台を超える場合は、Mac 管理サブマネージャーを複数台用意してください。Mac 管理サブマネージャーは Windows 管理サーバーと同居可能です。
	マネージャーを仮想サーバーに構築する場合は、1つの仮想 OS に対して単独の物理ディスクの割り当てを推奨しています。I/O 処理のパフォーマンスに影響するため、できるだけ I/O 処理が分散されるように構成してください。
	データ量や表示する項目により表示に時間がかかる場合があります。
	マネージャーをクラウド環境に構築しパブリック回線経由でクライアント端末を管理する場合、ポリシーの適用はクライアント端末起動時に行われます。ポリシー配信機能を利用する場合は、VPN を構築してください。
	マネージャーサーバーを長期間停止していた場合など、マネージャーサーバーが管理クライアント端末から大量のログを一齐受信すると、サーバーの負荷が高くなり、正常に動作しなくなることがあります。マネージャーサーバーの停止時間は最小限に抑えてください。
	マネージャーサーバーにはサマータイムを適用できません。
データベース	SQL Server Express Edition は、1 データベースの容量 10GB が上限のため、管理クライアント台数は 500 台以下が目安です。端末のご利用状況により SQL Server Standard Edition の購入が必要となる場合があります。
	クラウド環境にマネージャーを導入する場合、本製品に付属の SQL Server Standard Edition はマイクロソフトのライセンスポリシー上、利用できません。別途ライセンスを購入するか、SQL Server 付きのイメージをご利用ください。導入する環境が不明な場合などは別途お問い合わせください。
	SQL Server Standard Edition ご利用時には、安定稼働のため SQL Server の最大メモリ使用量の上限を、サーバーメモリの 1/2 程度に設定する必要があります。
	LANSCOPE のデータベースとして使用する SQL Server は、Windows のドメインコントローラーとの同居を推奨していません。
クライアント	エージェントをクライアント端末に導入する場合、動作するためのメモリ容量が必要となります。同居しているアプリケーションによっては、端末の動作が遅くなる場合があります。
	エージェントのインストールは管理者権限で行う必要があります。
	Windows 7 の Windows XP モードを管理する場合、XP モード管理用にクライアントライセンスが必要です。また、接続方法により Push ポリシー配信、配布機能、不正 PC 検知／遮断の一部機能が利用できません。
	スタンドアロン端末には、専用のエージェントを導入してください。取得できる情報は、資産情報、アプリ稼働ログ、操作ログ、プリントログです。
	資産情報や操作ログに Unicode3.1 以降の文字が含まれる場合、「?」や「・」と表示される場合があります。
	Windows XP、Windows Server 2003 では Windows の標準サービスである「Terminal Services」が有効である必要があります。
	Windows の日付の書式設定は、西暦もしくは和暦に対応しています。他の暦の場合はログ取得できない場合があります。

IT 資産管理	
SNMP 機器管理	SNMP 機器管理機能は、SNMPv2 で管理できる機器が対象となります。
	SNMP 機器の検索や死活監視を行うには、マネージャーサーバーから各機器へ通信可能である必要があります。
	SNMP 機器情報は、機器に格納されている文字のエンコード情報を取得しています。取得できない場合、文字化けして表示される場合があります。
電源・省電力管理	電源操作機能のリモート電源 ON 機能を利用するには vPro 端末を利用するか、Wake on LAN の設定が必要です。別拠点のクライアントに対し設定を行う場合、ルーターの ARP テーブルに設定対象クライアントのデータが保持されていることが条件となります。ルーターの ARP テーブルが削除される時間の間隔は使用している機器により異なります。各メーカーにお問い合わせください。
	電源操作機能による、シャットダウンや再起動の指定は、端末がログオンもしくはログオフ状態であることが条件です。
ハードウェア資産管理	電源操作機能による、Windows Server 2008 以降のサーバーに対してのシャットダウンの指定は、管理者権限でのログオン、もしくはログオフ状態であることが条件です。
	古い端末など DMI に準拠しない機種ではマシンスリアル、ベンダー名、BIOS 情報などの資産情報が取得できない場合があります。
アプリ管理・ソフトウェア資産管理	Windows XP にドメインユーザーでログオンしたとき、ハードウェア資産情報の「フルネーム (表示名)」が取得できません。
	アプリケーションによっては、アプリケーション管理、ソフトウェア資産管理で取得されない場合があります。
	ソフトウェア資産管理機能の有償／無償の判別は自動取得したソフトウェア名とソフトウェア辞書に登録されているソフトウェア名を関連づけることにより判別しています。そのため、同じソフトウェア名で有償版と無償版が提供されているソフトウェアについては正しく判別できない場合があります。
更新プログラム管理	ライセンス種別は GUID をもとに判別しています。ソフトウェアやインストール方法により正しく判別されない場合があります。
	更新プログラム情報の取得は Windows、Internet Explorer の更新プログラム、サービスパックが対象です。Office の更新プログラムは取得しません。
MS Office 管理	MS Office 管理機能は、以下の製品に対応しています。 Microsoft Office 2000 Premium ／ Professional ／ Standard ／ Personal Microsoft Office XP Professional Special Edition ／ Professional ／ Standard ／ Personal Microsoft Office 2003 Professional ／ Standard ／ Personal ／ Professional Enterprise Edition Microsoft Office 2007 Professional ／ Professional Plus ／ Standard ／ Personal ／ Enterprise ／ Ultimate Microsoft Office 2010 Professional ／ Professional Plus ／ Standard ／ Personal ／ Home and Business Microsoft Office 2013 Professional ／ Professional Plus ／ Standard ／ Personal ／ Home and Business Microsoft Office 2016 Professional ／ Professional Plus ／ Standard ／ Personal ／ Home and Business Microsoft Office 2019 Professional ／ Professional Plus ／ Standard ／ Personal ／ Home and Business
ファイル情報管理	ファイル情報は、管理クライアント端末のハードディスク内のファイルを検索し取得します。クライアント環境により端末起動後に負荷が高くなる場合があります。
ドメイン情報管理	ドメイン情報の取得は対象ドメインのすべての情報を取得します。登録されているユーザー数によっては取得に時間がかかる場合があります。
ファイル配布	イメージスクリプトでは、以下のようなインストーラーは実行できません。配布前に検証を行ってください。 ・インストーラーの画面タイトルが、イメージスクリプトを作成時と変化するもの ・インストーラーの実行するプログラム名称が毎回変更になるもの ・インストール中にネットワーク通信を必要とするもの ・インストーラーの入力欄に IE コンポーネントが使用されているもの ・実行端末により表示される画面が異なるもの など
メッセージ・アンケート	メッセージ・アンケート機能は即時通知した場合、対象クライアントに対し順次設定が通知されます。通信状況や設定台数により時間差が生じる場合があります。
ON/OFF ログ	ON/OFF イベントログは 1 日の中で最初の ON と最後の OFF の時刻を取得します。
	ON/OFF イベントログは端末の電源 ON と電源 OFF の時刻を取得します。ログオン・ログオフログは OS にログオンおよび、ログオフした時刻を取得します。電源 OFF のログ、ログオフログについては端末終了時にログが取得できない場合があります。その際は翌日の端末起動時に時刻を補正します。
	クラウド／NAT 環境に LANSCOPE マネージャーを構築した場合、一部の電源管理機能が利用できません。
	モダスタンバイがサポートされた Windows10 端末で、「休止」「復帰」のログが挙がらない場合があります。

アプリ制御	
アプリ制御	禁止対象となるのは 32bit、64bit のアプリケーションです。
	アプリ禁止は EXE ファイルの名前で禁止します。ファイル名が変更されると禁止されません。名前変更禁止設定を合わせて設定してください。
	Windows XP ではアプリ稼働ログ／アプリ禁止ログ／アプリ通信ログのハッシュ値が取得できません。またハッシュ値によるアプリ禁止もできません。

制限事項／注意事項

操作ログ管理	
ファイル操作ログ	ファイル操作ログはエクスプローラーを使用したファイル操作を取得します。アプリケーション経由のファイル操作など、ログが取得できない場合があります。
	OSからの通知順序や通知の有無により取得したログとユーザー操作に差異が発生する場合があります。
	ドライブ追加ログは機器により機種名が取得できない場合があります。
	ドライブ追加、ドライブ削除、メディア挿入ログは Windows にログオンした状態での操作が対象となります。
	デバイス禁止設定されているクライアントではドライブ追加、ドライブ削除、メディア挿入ログが取得されない場合があります。
	メール添付ログは操作方法によりログやファイルサイズが取得できない場合があります。
	CD 書き込みログは Windows 標準のライティング機能を用いて書き込んだ場合を取得対象としています。
	サーバー OSはコマンドプロンプトによるファイル操作ログの取得対象外です。
	コマンドプロンプトによるファイル操作でファイルサイズの取得対象となるのはローカルディスクに対する操作です。
	ファイル閲覧ログは、ファイルを開いたときに取得されますが、それ以降のタイミングでも取得されることがあります。
プリントログ	ファイル閲覧ログは、OS の「最近使った項目」の情報をを用いて取得しています。そのためファイルを開いても「最近使った項目」に情報があがらないファイルについてはファイル閲覧ログは取得されません。
	Windows 8、8.1、10 ではドキュメント名が「ドキュメントの印刷」と表示されます。OS の設定*によりドキュメント名は取得可能です。 ※ Windows 10 Home Edition ではプリントログのドキュメント名が取得できません。
	プリンターの環境によりプリンター IP アドレスが取得できない場合があります。
	プリントログの印刷枚数は、OS のプリントイベントログから取得しています。そのためプリンターや印刷するアプリケーションによっては正しい枚数を取得できない場合があります。 また集約や両面印刷などの設定による枚数もアプリケーションによって差異が発生する場合があります。
	プリンターサーバーを利用している場合、プリンターサーバーにクライアントエージェントをインストールしてログを取得します。
ログオン・ログオフログ	印刷イメージを取得するソフトウェアと同居していた場合、1 回の印刷でプリントログが 2 件取得される場合があります。
	リモートデスクトップ接続 / 切断やユーザー切り替えなどの操作によっては、OS としてはログオン・ログオフに当たらない場合でも、ログオンログ・ログオフログを取得する場合があります。

Webアクセス管理	
Webアクセスログ	Web アクセス管理機能は Internet Explorer／Google Chrome／Mozilla Firefox／Microsoft Edge に対応しています。 Web フィルタリング機能は Internet Explorer 6.0 SP3／7.0／8.0／9.0／10.0／11.0、Firefox 21.0／ESR 17 に対応しています。
	禁止設定はブラウザにより対応範囲が異なります。 【Windows 7 以上のクライアント OS、Windows Server 2012 以上のサーバー OS】 タイトル／URL：対応ブラウザ全て 書き込み：Internet Explorer (Windows 10 は除く) ※アップロード／ダウンロードは禁止できません。 【Windows 7 未満のクライアント OS、Windows Server 2012 未満のサーバー OS】 タイトル／URL：対応ブラウザ全て アップロード／ダウンロード／書き込み：Internet Explorer ※サイトにより禁止が有効にならない場合があります。
	URL、アップロード、ダウンロード、Web 書き込みログは、Web ページの仕様やアクセスタイミングにより、正しく取得できない場合があります。
	Microsoft 365、Google Workspace、Dropbox では、ログは取得されますが、アップロード禁止、ダウンロード禁止、Web 書き込み禁止を設定しても禁止は有効になりません。アラームの設定を行ってください。
	Outlook.com や Outlook on the web、Gmail の送信メールにて、一部情報が取得されなかったり、実際の情報とは違う情報になる場合があります。
	Google Chrome をシークレットモードやゲストモード、Windows8 モードで起動した場合は、ログ取得対象外です。 【Windows 7 以上のクライアント OS、Windows Server 2012 以上のサーバー OS】・Web 閲覧ログの URL 情報 ・Web 書き込みログ 【Windows 7 未満のクライアント OS、Windows Server 2012 未満のサーバー OS】 ・Web 閲覧ログの URL 情報 ・アップロードログ／ダウンロードログ／ Web 書き込みログ
	Microsoft 365 の Outlook on the web のメール暗号化機能の (S/MIME) には対応していません。
	アップロード中に別のタブに表示を切り替えると、ログのタイトルと URL が切り替えた後のサイトのタイトルと URL になる場合があります。
	ブラウザや Web サービスの仕様変更により一部のログが取得されなくなる場合があります。
	Internet Explorer を管理者権限で実行した場合、次のログが取得できません。 【Windows 7 以上のクライアント OS、Windows Server 2012 以上のサーバー OS】 Web 書き込みログが取得できません。 【Windows 7 未満のクライアント OS、Windows Server 2012 未満のサーバー OS】 アップロードログ／ Web 書き込みログが取得できません。
	Google Chrome／Microsoft Edgeでウィンドウに名前を付ける機能を利用したウィンドウでは、閲覧ログ/ダウンロードログ/アップロードログを取得できません。
	Google Chrome／Microsoft Edgeでサイトをアプリとしてインストールした場合、そのアプリでの閲覧ログ/ダウンロードログ/アップロードログを取得できません。
Web フィルタリング	Web フィルタリング機能は全アプリケーションの通信に干渉するため、少数の端末で動作確認をいただいたうえで展開してください。
	Webフィルタリング用のエージェントをインストールする端末では、DNSによる名前解決ができる必要があります。また、Windows Installer 3.0以上が必要です。
	Web フィルタリングは Windows OS に対応しています。
	プロキシ導入環境において、プロキシ認証を実施している場合、フィルタリングエージェントの通信をプロキシ側で認証除外に設定する必要があります。
	Web フィルタリング機能は Internet Explorer 6.0 SP3／7.0／8.0／9.0／10.0／11.0、Firefox 21.0／ESR 17 に対応しています。

デバイス制御	
デバイス制御	クライアントの負荷状況、インストール済みのソフトウェア等によりデバイスの認識や制御に時間がかかる場合があります。
	物理的には単一の機器でも Windows の OS 上では複数の機器として認識されるものがあります。 これらの機器をデバイスポリシーで制御するには、対応する機器分類のすべてに対して制御設定を行う必要があります。
	機器により許可登録するために複数の設定が必要な場合があります。 ・暗号化機能付き USB メモリの暗号化領域 ・iTunes など特定のソフトウェアをインストールすることで OS 上での認識が変更される機器 ・OS、Hotfix の適応状態、USB スロットにより認識が異なる機器
	OS の内部認識が、デバイスの外見とは異なる場合があります。この場合、内部認識に応じた設定を行ってください。 ・指紋認証機器や暗号化機能を搭載した USB メモリなどが、CD/DVD と認識される ・モジュールベ이의 CD/DVD など
	複数のカードスロットを搭載しているカードリーダーの一部のスロット（ドライブ）を許可設定した場合、同一機器のすべてのスロットが許可されます。
	内蔵の CD/DVD、FD を禁止設定した場合、キーワードやシリアル No. での許可設定は対象外となります。
	Windows XP でポータブルデバイスの読み取り専用設定およびログ取得を行うには、Service Pack2 以上かつ Windows Media Player Version11 以上をインストールする必要があります。
	読み取り専用設定していても iTunes などのアプリケーション経由でデバイスへの書き込みが行える場合があります。 アプリ禁止機能で該当アプリケーションを禁止設定してください。
	Windows 8 の 32bitOS では機器により内蔵 SD カードが禁止されない場合があります。
	電源 OFF の状態で端末に初めて接続する機器は、OS を再起動するまで制御の対象とならない場合があります。
デバイスシリアル 管理	デバイス禁止設定で、「記憶領域をもつデバイスのみ」を禁止する設定にした場合、Windows XP、Windows Server 2003 では iPhone が禁止されません。
	「USB 接続機器」を読み取り専用にした状態で、操作手順によっては、SD などメモリーカードがシリアル許可されない場合があります。
通信デバイス制御	デバイスシリアル管理機能をご利用いただくためには VID、PID、シリアル No. の情報を取得した後、管理画面上でデバイスの登録が必要です。
	機器によりシリアル No. が取得できない場合があります。その場合はシリアル No. を利用しての各種設定は行えません。
	内蔵 WiMAX アダプターを介した接続は有線接続として扱われるため、Wi-Fi 接続の禁止対象になりません。
	スマートフォンなどを USB で接続してテザリングを行う場合、有線接続として扱われるため、Wi-Fi 接続での禁止はされません。
	Windows XP または Windows Vista SP1 以前の OS では、バスキーを必要としない Bluetooth 機器の接続は取得できません。
	マイクロソフト以外のサードパーティ製の Bluetooth 機器は禁止されない場合があります。

メール管理	
メール送信 ログ管理	メール送信ログは Outlook2007／2010／2013／2016／2019 に対応しています。
	Microsoft Outlook にアドインを登録してログを取得します。アドインを解除するとログが取得されません。
	Microsoft Outlook の複数のバージョンがインストールされている場合はログ取得の対象外です。
	「本文」「添付ファイル」を取得する場合はマネージャーサーバーのディスク容量の確保が必要となります。

制限事項／注意事項

アプリ ID 監査	
ID 監査ログ	アプリケーションの画面や Web サイトのページの構成によっては、ID 監査ログが取得できない場合があります。導入前に、本機能の評価ツールを使って事前の評価を推奨します。
	ログ取得用の設定ファイルを作成した端末と、ログ取得対象の端末で、OS やアプリケーションの画面構成が異なる場合、ログが取得されない場合があります。
	Web アプリで対応しているブラウザは Internet Explorer です。
	管理者権限に昇格して起動されたアプリケーションのログは取得対象外です。

マルウェア対策	
動作環境	マルウェア対策エージェント（BlackBerry Protect エージェント）の対応 OS は、クライアントエージェント（MR）の動作 OS に準拠しますが、XP SP3 未満、OS X Mavericks 未満の OS は未対応です。また XP、2003 については KB968730 の適用が必須です。
	マルウェア対策エージェント（BlackBerry Protect エージェント）をインストールするには、「.Net FrameWork3.5(SP1)」以上が必要です。
	マルウェア対策エージェント（BlackBerry Protect エージェント）をネットワークに接続しないスタンドアロン端末で利用する場合、対応 OS は Windows のみとなります。
	アンチウイルスソフトと同居する場合、端末の動作に影響する可能性があります。そのため、アンチウイルスソフトの設定で特定のフォルダーを除外する必要があります。
	マルウェア対策機能は各ソフトウェアのバージョンおよび環境等の違いにより端末の動作に影響を及ぼす場合があります。導入前に、事前の評価を推奨いたします。
	サードパーティ製のメモリ監視をする製品と同居した場合は、MemoryProtection 機能をご利用いただけません。
	VDI 環境下を導入する場合、メモリアクション機能およびスクリプト制御機能を使用すると動作に影響する場合があります。導入前に動作検証が必須です。
	1 台の端末で脅威検知が 1000 を超えると、それ以降、脅威検知アラームログは取得されません。隔離設定をしている場合、隔離は行われます。
	外部ネットワークに接続できない環境では、脅威ログの種別が表示されません。
	脅威検知された圧縮ファイル内に日本語フォルダーが含まれる場合、脅威 Web コンソール「脅威検知アラームログ」の表示でそのフォルダーが文字化けします。
マルウェア検知	脅威検知の日時は、検知情報をサーバーで受信した際のサーバーの日時となります。そのため、脅威検知されたログから周辺操作ログを閲覧した際、脅威検知された時刻周辺のログが表示されないことがあります。その際は、Web コンソールのログ検索で操作ログをご確認ください。
	同一端末で同じ脅威を別の時間で検知した場合、タイミングによって脅威の状態が更新されない場合があります。
Syslog 転送	エージェントの OS が Mac、もしくは、クライアントエージェントが Ver.8.4.0.0 未満の PC で取得された脅威検知ログは、Syslog として転送されません。

不正 PC 遮断	
不正 PC 検知	イーサネットコンバーター環境では遮断が有効にならない場合があります。
	機器によってホスト名を取得できない場合があります。
	1 つのセグメントで管理できるノード数は上限 1,000 ノードを目安としてください。
	IP アドレス体系がクラス B など 1 セグメントで多数のノードが稼働している環境では検知に時間がかかる場合があります。
	遮断対象の機器がプリンターなどの場合、ARP 要求が送信されず遮断に時間がかかることがあります。また、環境によって遮断されない場合があります。
	無線 LAN のアクセスポイントに検知エージェントが無線接続している場合、遮断が行えません。
	端末／機器により遮断が行えない場合があります。 ・HP 製の端末（HP-DX2000MT、d530） ・ICMP リダイレクト機能付きの機器を使用している場合 ・ウイルス対策ソフトなどにより ARP スプーフィング機能を利用している端末

リモートコントロール	
ISLリ モコン	ネットワーク環境により操作開始までに時間がかかる場合があります。
	ネットワーク環境やプロキシの構成により接続できない場合があります。

Mac 管理	
資産管理	ソフトウェアの「メーカー名」の情報は取得しません。
アプリ稼働管理	アプリケーションバージョン管理で「バージョン」「メーカー名」は取得しません。
操作ログ管理	HDD のフォーマットタイプで「大文字／小文字を区別する」を選択していないことがログ取得の条件です。
	操作ログ、アプリケーション稼働ログ、Web アクセスログで稼働時間は取得しません。
	操作解析画面でエラー操作とスクリーンセーバーの解析グラフは表示されません。
	Mac 端末の操作ログ管理では以下の機能は取得対象外です。 ・CD/DVD 書き込みログ ・メール添付ログ
プリントログ	Mac 端末のプリントログは CUPS という印刷システムでログを取得します。CUPS を使用しているプリントシステムがログ取得の条件です。
	Mac 端末のプリントログでは「印刷枚数」「プリンター IP アドレス」は取得しません。
	Mac 端末のシステム日付を未来に変更した場合、プリントログが正常に取得できないことがあります。
Webアクセスログ	Mac 端末の Web アクセスログはブラウザの履歴を残す設定が必要です。
デバイス制御	Mac 端末のデバイス読み取り専用設定は除外登録の設定ができません。禁止設定については PID、VID による除外登録が可能です。
	制御対象となるのは OS がストレージ機器として認識される機器です。
	Mac 端末でのデバイス禁止／読み取り専用設定は、アプリケーション経由での書き込み操作は制御されません。
	Active Directory に参加している Mac 端末では読み取り専用設定は有効になりません。
	セキュリティ USB メモリにはパスワードロック解除をすると OS に SD カードと認識されるものがあります。この場合、許可設定をしても許可されません。

サーバー監視	
サーバーファイル操作ログ	サーバーファイル操作ログは、Windows のセキュリティログから取得しています。そのため OS の内部的な処理に沿った内容となるため、実際のユーザー操作とは差異が発生する場合があります。
	監査対象とするフォルダーのドライブにドライブ文字が設定されていることが条件です。
	サーバー接続／切断ログの切断時のログでは、IP アドレス、ホスト名は取得されません。
	NetApp 用エージェントは、Data ONTAP 7.3 ～ 9.3 に対応しています。
	NetApp 用エージェントは複数の NetApp サーバーを監視することができません。vFiler で構成している場合、vFiler で構成している IP アドレスの数分のライセンスと導入するためのサーバーが必要です。
	Windows の AD 環境、NetApp のワークグループ環境ではクライアントの操作ログとサーバーファイル操作ログを連携する機能は使用できません。
ドメインログオン・ログオフログ	NetApp clustered Data ONTAP では、サーバー接続／切断ログは取得されません。
	ドメインログオン・ログオフログは、クライアント端末がドメインコントローラーサーバーにアクセスできた場合に取得します。キャッシュログオンされた場合はログが取得されません。

Webコンソール	
ダッシュボード	ダッシュボードの OS 分布カードにおいて、LTSC 版ではサポート期限が正しく判定されません。LTSC 版としてはサポート中であってもサポート期限切れと判定されます。

仮想環境	
動作環境	仮想サーバー製品は以下の製品に対応しています。環境によって一部動作しない機能があります。 VMware：ESX、ESXi、Microsoft：Hyper-V、Microsoft Azure、Amazon：Amazon EC2、NTT Communications Enterprise Cloud
	仮想デスクトップ製品は以下の製品に対応しています。環境によって一部動作しない機能があります。 【VDI 方式】 VMware：Horizon、Horizon Air、Citrix：XenDesktop4.0 ～ 7.18、Virtual Desktops 7 1808 ～ 1912、NEC：VirtualPCCenter4.1、Amazon：Amazon Workspaces、Microsoft：Windows Virtual Desktop (Windows 7／10 (シングルセッション)) 【SBC 方式】 VMware：Horizon6.2/7.0 ～ 7.6 RDSH、Citrix：XenDesktop4.0 ～ 7.18、Virtual Desktops 7 1808 ～ 1912、XenApp5.0 ～ 7.18、Virtual Apps 7 1808 ～ 1912、Microsoft：Remote Desktop Service (Windows Server 2008 R2／2012／2012R2／2016／2019)、Microsoft：Windows Virtual Desktop (Windows 10 (マルチセッション))／Windows Server 2012 R2／2016／2019)
	SBC 方式での 1 サーバーあたりの同時接続台数は 50 ユーザーを上限としてご利用ください。
	エージェントがインストールされたマスタイメージを更新した後、動作仕様により各ログの 1 件目のログは取得されません。ただし 1 件目のログはシステムの動作やスタート画面に該当することが多く、運用への影響は軽微です。
	ファイル配布 仮想デスクトップ環境に対し配布したファイルを実行した際「対話型サービスダイアログの検出」が表示される場合があります。そのダイアログで「メッセージを表示する」を選択するとセッションが切断されます。
操作ログ管理	SBC 方式で取得する操作ログはプログラム名が統一して取得されます (XenApp の場合、稼働プロセスが Wfica32.exe で取得されます)。
アプリ制御	仮想デスクトップ環境では、フォルダーリダイレクト設定などによりファイル操作ログが取得できない場合があります。
Webフィルタリング	仮想デスクトップ環境では、製品、接続方式により一部機能でポップアップ通知が表示されない場合があります。
デバイス制御	Web フィルタリングは、仮想デスクトップ環境には対応していません。
	VMWare Horizon View でデバイス制御を使用する場合は 5.2 以降をご利用ください。

制限事項／注意事項 ー他社製品利用時の回避事項ー

アルプス システム インテグレーション株式会社 「InterSafe IRM」	
全般	【現象】 LANSCOPE MR と InterSafe IRM が同居している場合、以下の現象が発生する場合があります。 ・Firefox / Chrome などのブラウザが利用できない ・32bitOS では、BSOD（ブルースクリーン）が発生する ・リモートデスクトップが利用できない
	【回避方法】 LANSCOPE 側で以下のポリシー設定を解除することで回避できます。 ・操作ポリシー 「コマンドプロンプトによるファイル操作を取得する」 「Outlook メールへのファイル添付ログを取得する」 「ポータブルデバイスのファイル操作を取得する」 ・Web アクセスポリシー 「Web アクセスログを取得する」 ・デバイスポリシー CD/DVD と FD の「外付け」の禁止、または読み取り専用の設定 USB 接続機器、その他の機器の禁止、または読み取り専用の設定 または、InterSafe IRM の例外設定を行うことで回避できる場合があります。 アルプス システム インテグレーション株式会社サポートまでお問い合わせください。

イーディーコントライブ株式会社 「Traventy 3」	
全般	【現象】 コピーガード機能を有効にしている場合に、以下の現象が発生します。 ・MR から読み取り違反のエラーダイアログが表示される ・エクスプローラーが起動しなくなる ・ファイルの右クリックでエクスプローラーが終了する
	【回避方法】 Traventy 3 側でコピーガード機能を無効にすることで回避できます。

カシオ計算機株式会社 「CASIO IT-300」	
全般	【現象】 PDA 機器（携帯端末）を接続ユニットにセットしても組み込みアプリケーションが自動起動しない場合があります。 またアプリケーションからのデータ転送に通常よりも時間がかかる場合があります。
	【回避方法】 該当のデータ通信カードの情報を取得しないように LANSCOPE 側でフィルターすることで回避可能です。データベースへフィルターする情報を登録するためのツールを用意しております。弊社サポートセンター（ https://www.lanscope.jp/cat/faq/support/ ）までお問い合わせください。

株式会社東芝 「東芝デバイスアクセスコントロール V3」	
デバイス制御	【現象】 LANSCOPE のデバイス制御の読み取り専用設定をしている MR と、東芝デバイスアクセスコントロール V3 が同居している場合、以下の現象が発生する場合があります。 ・CD ドライブのランプが点滅する ・内蔵 CD ドライブ、USB メモリが禁止される ・マイコンピュータの CD ドライブアイコンの表示がされない
	【回避方法】 以下のいずれかを行うことで回避できます。 ・LANSCOPE のデバイス読み取り専用設定を解除する ・東芝デバイスアクセスコントロール V3 をアンインストールする

日本マイクロソフト株式会社 「URLScan2.5、IIS URLScan Tool2.0」	
Web コンソール	【現象】 Web コンソールで CSV 出力ボタンを押すと、「404 エラー」が表示され出力に失敗します。
	【回避方法】 （システムドライブ）: \windows\system32\inet_srv\urlscan\urlscan.ini をテキストで開き、「URLScan2.5」の場合は 17 行目、「IIS URLScan Tool2.0」の場合は 7 行目の「AllowDotInPath」の値を「0」から「1」に編集し上書き保存してください。その後、IIS のサービス（IIS Admin Service）を再起動してください。

日本マイクロソフト株式会社 「Microsoft SharePoint」	
その他	【現象】 MR 端末で Microsoft SharePoint のエクスプローラービューを利用した場合に、IIS サーバーの IIS ログ件数が増加する場合があります。
	【回避方法】 回避方法はあります。

ハンドリームネット株式会社 「SubGate」	
不正 PC 遮断	【現象】 MAC 詐称（ARP スプーフィング）対策機能を使用している端末は、不正 PC 検知機能の禁止設定を行っていても禁止が有効になりません。
	【回避方法】 SubGate 側で MDS の除外設定に「禁止用擬似 MAC アドレス（000000000001）」を登録することで禁止が有効になります。

株式会社シマンテック 「Symantec Endpoint Protection」	
不正 PC 遮断	【現象】 MAC 詐称（ARP スプーフィング）対策機能を使用している端末は、不正 PC 検知機能の禁止設定を行っていても禁止が有効になりません。
	【回避方法】 Symantec Endpoint Protection 側で MAC 詐称対策機能を無効にすることで、不正 PC 検知機能の禁止が有効になります。

株式会社日立ソリューションズ 「秘文」	
デバイス制御	【現象】※本制限事項は、LANSCOPE Ver.8.4.2.0 以上のクライアントエージェントを適用することで解消します。 Windows7 において LANSCOPE のデバイス制御の読み取り専用設定をしている MR と、秘文が同居している場合、以下の現象が発生する場合があります。 ・CD/DVD ドライブやデバイス通信機器が正常に認識されない ・内蔵 CD ドライブ、USB メモリが禁止される ・端末の CPU 負荷が高くなる
	【回避方法】 以下のいずれかを行うことで回避できます。 ・LANSCOPE のデバイス読み取り専用設定を解除する ・秘文をアンインストールする

日本ヒューレット・パッカード株式会社 「HP LoadRunner 9.0 / 9.5」	
Web アクセス管理	【現象】 Web コンテンツを対象にした操作内容を記録中に、記録対象の Internet Explorer が終了します。
	【回避方法】 LANSCOPE の Web アクセスログを取得しない設定にすることで回避ができます。

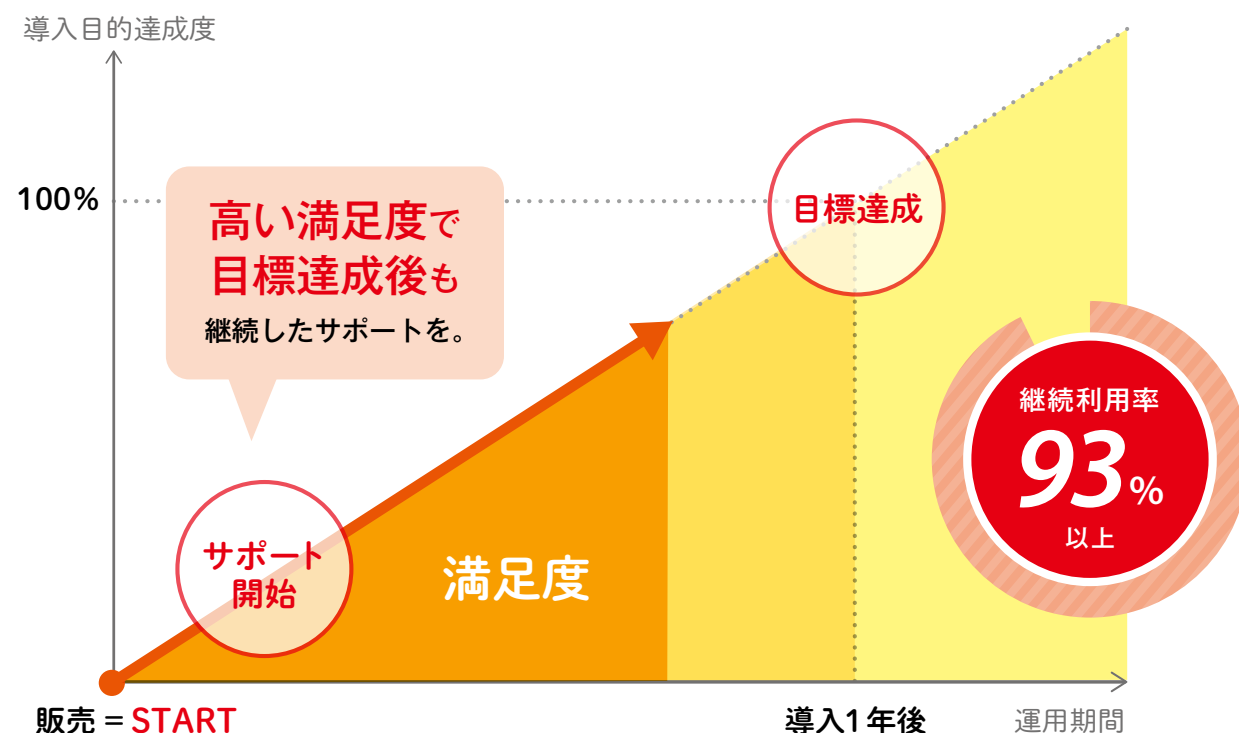
日本電気株式会社 「InfoCage FileShell」	
全般	【現象】 LANSCOPE MR と、InfoCage FileShell が同居している場合、ネットワーク上のストレージに新しく作成したファイルを暗号化できない現象が発生する場合があります。 ・InfoCage FileShell の発生バージョン V2.1 の場合：V2.1.0.35 以前 V3.0 の場合：V3.0.262.4183 以前
	【回避方法】 LANSCOPE 側で以下のポリシー設定を解除することで回避できます。 ・操作ポリシー 「コマンドプロンプトによるファイル操作を取得する」 「Outlook メールへのファイル添付ログを取得する」 「ポータブルデバイスのファイル操作を取得する」 ・Web アクセスポリシー 「Web アクセスログを取得する」 ・デバイスポリシー CD/DVD と FD の「外付け」の禁止、または読み取り専用の設定 USB 接続機器、その他の機器の禁止、または読み取り専用の設定 または、InfoCage FileShell のパッチを適用することで回避できる場合があります。 日本電気株式会社サポート（ https://www.support.nec.co.jp/ ）までお問い合わせください。

富士通株式会社 「Interstage Charset Manager」	
操作ログ	【現象】 LANSCOPE のファイル操作ログを取得する設定をしている 32bitOS の MR と、Interstage Charset Manager が同居している場合、Interstage Charset Manager が応答なしになる場合があります。
	【回避方法】 Interstage Charset Manager の「更新通知」メッセージを送る設定を、SendMessage でなく PostMessage に変更することで回避できます。

2021年6月25日時点の情報です。最新情報はWebサイトをご確認ください。

安心と充実のサポート体制

MOTEXはご購入いただいたお客様には、製品が持っている機能を最大限に活用してもらいたいと考えています。MOTEX独自のPUSH型サポートで、ご購入いただいたその日からお客様をしっかりとサポートすることがMOTEXの使命です。



導入サポート

オンサイトサポート ※有償

LANSCOPEの構築から運用に必要な設定などを、MOTEXのスタッフが現地に伺い実施します。

ハンズオンセミナー

企業が行うべき管理／対策のポイントをLANSCOPEの機能や事例をまじえてご紹介するハンズオン(実機操作)形式のセミナーです。



運用サービス

ログ活用支援サービス ※有償

現状のヒアリング及びLANSCOPEのログ分析を行い、MOTEXに蓄積したノウハウから規定・運用・設定変更に関する改善事項をご提案するサービスです。

インシデント マネジメント サービス ※有償

マルウェア対策ライセンスで検知したインシデントを、LANSCOPEで収集した情報をもとに、速やかに解析しリスクをご報告するサービスです。



運用サポート

▶ LANSCOPE PORTALを通じて最新の情報をお届けします。

LANSCOPE PORTAL

保守契約ユーザー様専用サイト

LANSCOPE PORTALは、LANSCOPEシリーズをご利用いただいているお客様専用のサポートサイトです。最新プログラムや運用の為の各種資料、MOTEXからの最新情報やよくあるご質問(FAQ)の閲覧、製品の基礎から活用方法までが簡単にわかる「猫ナビ」がご利用できます。

猫ナビ

LANSCOPEで「こんなことしたい」を実現するための手順をナビゲート。初めての方でもカンタンに活用していただけます。



よくあるご質問

LANSCOPEの「わからない」を解決！お客様から寄せられるご質問をもとに、随時更新しています。



トレーニングセミナー オンライン

大好評のトレーニングセミナーがインターネットで全国どこからでも受講できます。



MY LANSCOPE

お客様登録情報や購入機能／ライセンス数を確認、また登録変更などの各種お申し込みをいただけます。



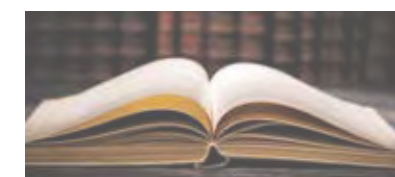
最新バージョン プログラム

メジャーバージョンアップを含む、最新プログラムを無償でお使いいただけます。



ソフトウェア辞書提供

SAMACソフトウェア辞書を無償でご提供します。ソフトウェア資産管理の効率をアップさせます。



▶ 専任のスタッフが運用フォローを行う充実のサポートもご用意しています。

定期フォローサービス

ご購入後、定期的にフォロー担当者からお電話またはメールをさせていただきます。お客様の導入目的を実現するため、定期的にフォロー担当者から電話またはメールでご連絡いたします。

引き継ぎフォローサービス

LANSCOPEのご担当者の変更／追加された場合、運用ガイドのご提供、お電話やメールでの運用支援を行います。



ヘルプデスクサポート

LANSCOPEをご利用いただいている中で発生した疑問や質問に対して、電話やメールによるサポート対応を行っています。

リモートサポート

お客様のPC画面を閲覧またはリモートコントロール(遠隔操作)し、操作案内やトラブル解決を行います。

トレーニングセミナー

LANSCOPEの導入から運用までのカリキュラムを実施するセミナーです。

ユーザー会／アワード招待

定期的にユーザー様同士の交流および情報交換の場をご提供します。

wizLANSCOPE 最新情報提供

ネットワークセキュリティの旬な情報やLANSCOPEの最新情報、MOTEXの今をご紹介します。

wiz LANSCOPE