LANSCOPE

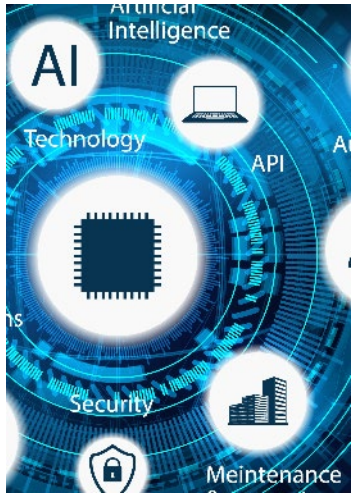
クラウド環境下で IT資産管理を 実現するポイント

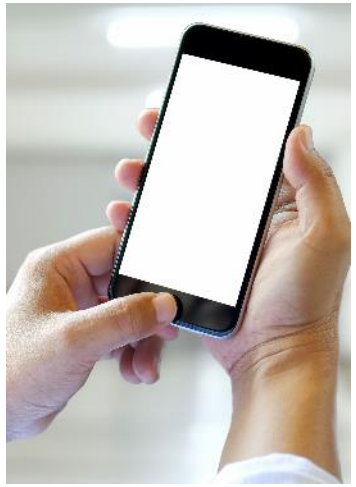
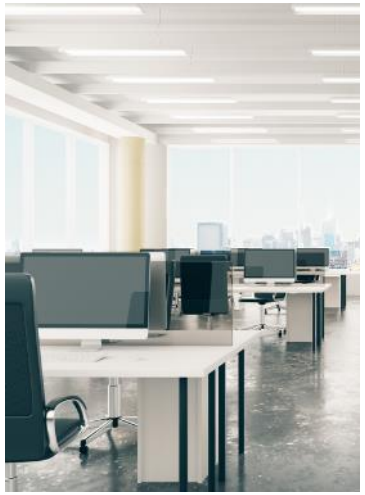
※本資料におけるLANSCOPEとは、明記がない限りLANSCOPEオンプレミス版の事を指します

エンドポイントにおけるIT資産管理・セキュリティ・効率化のためのソフトウェアを開発しています

SYNCPIT　LANSCOPE cloud　LANSCOPE on-premises　CPMS

自動化	モバイル管理	IT資産管理	操作ログ管理	情報漏えい対策	外部脅威対策
バックオフィス自動化 FAQ・定型通知	位置情報管理 盗難・紛失対策	パソコン情報収集 アプリ管理・配布	PC操作を記録 アラート通知	デバイス制御 Webフィルタ	標的型攻撃対策 ランサムウェア対策




LANSCOPEのポイント

1. 豊富なクラウド環境導入実績

L クラウド基盤対応により場所や時間にとらわれない運用

2.クラウドの特性を生かしたグローバル対応

L 世界中のどこからでも、クライアントにインストールするだけ

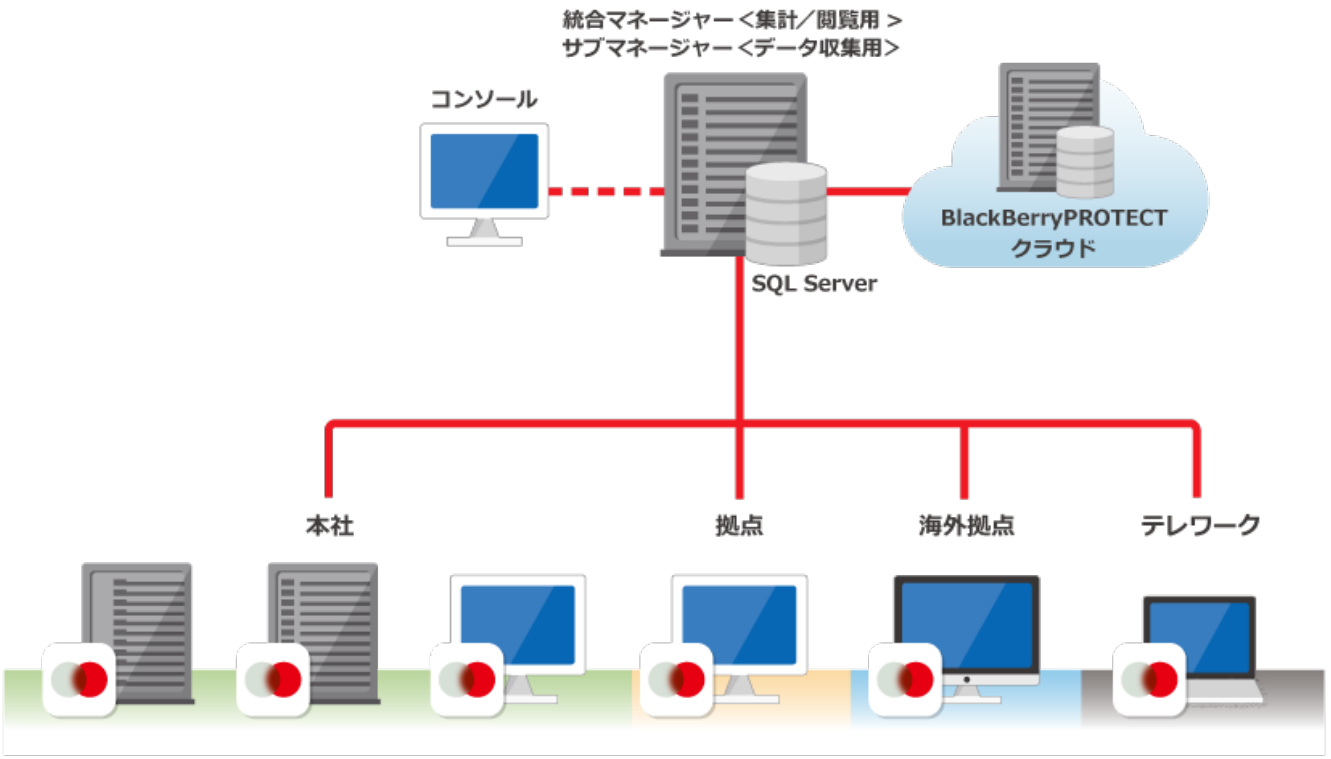
3. Windows10／レガシーOS一元管理

L XP/2003　すべての機能でサポートしています

4.選べる機能・選べる購入パターン

L 必要な範囲に合わせて購入できる

クラウド基盤に対応！通信の暗号化によりVPN接続を必須とせず インターネット経由で安全にPCを管理できます



クラウド基盤対応

LANSCOPEは各種クラウド基盤に対応しています

IIJ GIO
aws
NTT Communications
Enterprise Cloud
NIFCLOUD ニフクラ
vmware
Microsoft Azure

世界中のどこからでもインストールするだけ！グローバルな管理体制がLANSCOPEで実現します

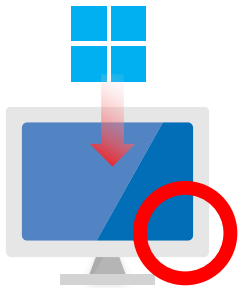
1．管理画面の日本語／英語表示切替・・・管理する国（管理者）に合わせて切り替えができます

2．グローバル時差対応・・・・・・・・・

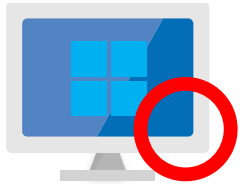
3．海外拠点にある PC も一元管理可能・・インターネットが接続できれば情報取得が可能です

LANSCOPEはWindows XP も対応！全機能をお使いいただけます

Windows10

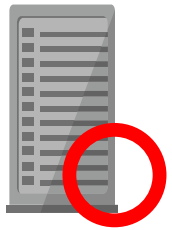


WSUSが無くても
アップデートコントロールが可能



検証後にアップデートするなど
アップデートのコントロール

レガシーOS



Windows Server
2003

Windows 7

Windows XP

4．選べる機能・選べる購入パターン

今、必要な機能だけを選んで導入できるので、コストを抑えて導入できます

パッケージ	機　能	
	マネージャーライセンス	レポート／ダッシュボード／アラーム管理／ネットワーク検知
標準パック	IT 資産管理	IT資産管理/SAM／ファイル配布・パッチ適用／Microsoft Defender連携 ※
パック1000	操作ログ管理	アプリ稼働管理・制御／操作ログ・印刷ログ管理
プレミアムパック	Webアクセス管理	Webアクセスログ管理／Webアクセス制御/フィルタ
	デバイス制御	デバイス禁止・読込許可／USB責任者設定
	メール管理	メール送信ログ管理
	アプリID監査	ID使用ログ・特権管理
	マルウェア対策	マルウェア検知･隔離／原因追求
	サーバー監視	サーバーアクセスログ管理／サーバー容量管理
	不正PC遮断	持ち込みPC遮断
	リモートコントロール（REMO-CON）	リモートアクセス／Web会議

選べる購入方法

初めてご購入される方は、マネージャーライセンスが必須

●お得なパックを選ぶ!!

例１　マネージャーライセンス ＋ パック1000

例２　マネージャーライセンス ＋ パック1000 ＋ マルウェア対策

●必要な機能を選ぶ!!

例３　マネージャーライセンス ＋ 操作ログ管理 ＋ デバイス制御

※Microsoft Defender連携機能は次のいずれかのライセンスを保有さている場合に使用可能です（IT資産管理・操作ログ管理・Webアクセス管理・デバイス制御・アプリID監査・メール管理）

企業における様々なセキュリティ脅威に対してLANSCOPEで幅広く対策することができます

	順位	組織	昨年順位
外部	1位	ランサムウェアによる被害	5位
外部	2位	標的型攻撃による機密情報の窃取	1位
外部	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
外部	4位	サプライチェーンの弱点を悪用した攻撃	4位
外部	5位	ビジネスメール詐欺による金銭被害	3位
	6位	内部不正による情報漏えい	2位
	7位	予期せぬIT基盤の障害に伴う業務停止	6位
外部	8位	インターネット上のサービスへの不正ログイン	16位
	9位	不注意による情報漏えい等の被害	7位
外部	10位	脆弱性対策情報の公開に伴う悪用増加	14位

IT 資産管理	IT資産管理/SAM／ファイル配布/パッチ適用／Microsoft Defender連携
操作ログ管理	アプリ稼働管理/制御／操作ログ・印刷ログ管理
Webアクセス管理	Webアクセスログ管理／Webアクセス制御/フィルタ
デバイス制御	デバイス禁止/読込許可／USB責任者設定
メール管理	メール送信ログ管理
アプリID監査	ID使用ログ/特権管理
マルウェア対策	マルウェア検知･隔離／原因追求
サーバー監視	サーバーアクセスログ管理／サーバー容量管理
不正PC遮断	持ち込みPC遮断
リモートコントロール（REMO-CON）	リモートアクセス／Web会議

※IPA「情報セキュリティ１０大脅威２０２１」

基盤と合わせて月額・年額も選択可能！イニシャルコストを抑えて必要な範囲から始められます

よくある課題

契約形態がバラバラ・・・

クラウド基盤

月額／年額

×

ツール

ライセンス+保守

LASCOPEなら

基盤もツールも使用料ライセンスで

クラウド基盤

月額／年額

×

ツール

月額／年額

導入事例

※本事例は取材当時の内容となっております。旧プロダクト名称の場合がありますのでご了承ください

LanScope	→	LANSCOPE
LanScope Cat	→	LANSCOPE
Cylance	→	BlackBerry Protect
プロテクトキャット	→	LANSCOPEのマルウェア対策機能

パターンファイル脱却と操作ログとの統合で運用負担を軽減

ネットワーク分離など自治体特有の環境に対応できるプロテクトキャット

山梨県庁 様

業種	公務	職員数	約3,600名

ネットワーク分離によって顕在化したパターンファイルの弊害

パターンファイルを用いたアンチウイルスソフトとふるまい検知ソリューションを個別に導入し、未知のマルウェア対策にも対応していた。

しかし配信ファイルが徐々に大きくなり、ネットワーク面のストレスが発生。さらに庁内の**「ネットワーク分離」に関する取り組み**により、これまでのように**インターネット経由でのパターンファイル更新が簡単にできなくなり**、運用面での課題を抱えていた。

シグネチャレスの恩恵ネットワークおよび運用負担の軽減

アップデートは半年から1年に1回ほど数理モデルの更新が発生しますが、**半年前の数理モデルでも最新のマルウェアに対応可能**な実績があり、**ネットワーク分離環境にもマッチ。**日々の管理工数が激減しました。

これまでグレーな検知を行った際、判定で悩ましい場面もあったが、**検知ファイルの検知理由なども表示されるため、判断しやすく**運用の精度が高まっている。以前のツールほど**過検知も少なく**、管理工数が削減できている。

Cylance×LanScope Catで原因特定の迅速化にも貢献

プロテクトキャットでは、Cylanceの技術を搭載しながらPCの操作ログまでが取得可能。**該当端末の特定や原因究明も含めて1つのソリューション内でかなりの部分を完結**させることができ、運用工数を削減しながら、インシデント対応が可能に。

以前であればログ解析まで含めた原因特定に**30分から1時間程度必要だったが、今は数クリック**で必要な情報にたどり着けている。

VDIによるテレワーク環境整備に
効果的なエンドポイント管理、強化を実現

auフィナンシャルサービス株式会社 様

従業員数 102名　　業種 金融・保険業

VDIによるテレワーク導入に伴い エンドポイント管理強化が課題

多様な働き方を実現するため、デスクトップ仮想化（VDI）を用いたテレワークの仕組みの整備を進めていたが、課題となったのが、エンドポイント管理のためのIT資産管理ツールである。

当時、利用していたツールはAWSのサポートが非対応で、操作ログの保存期間が短く、アプリ配信機能がないという課題がありました。加えてテレワーク時のセキュリティ対策も行いたかったです。

月に30～40時間のパッチ適用業務が 約4分の1に削減

主導インストールが、一斉配信できる仕組みが整ったことで、運用負荷を大幅作戦できました。課題だった出社頻度の少ない社員に対してもバックグラウンドで配信できるため、スムーズに業務が継続できるようになりました。

運用負荷軽減の効果は、月数十件、1件の配信で約1時間から2時間かかっていた作業が軽減され、月30～40時間が10時間程度に削減されています。

障害発生時や労務管理に活躍！ログの 保存期間の長さが安心

過去に遡ってPCの操作ログを追跡できるため、たとえば「特定のファイルがなくなった」などの状況に対しても、誰が、いつ、ファイルにアクセスしたかがすぐに確認でき、対応できるようになりました。

テレワークにおける労務管理の観点からPC操作のログを確認し、長時間労働対策がしたいと問い合わせが社内各所からあり、幅広い活用ができています。

最新状態にするサイクルをたった約3ヵ月で確立！IT資産の可視化が工数・コスト減へ

IT資産管理機能・ダッシュボード活用

株式会社ディー・エヌ・エー（DeNA）様

従業員数 2,475名　　業種 サービス業

Win10端末の脆弱性対策が課題 使い易さとユーザサポートが決め手

業務用のWindows端末のOS脆弱性管理の課題解決のため、IT資産管理ツール導入の検討を開始。

IT資産管理製品としてシェアNo.1であるという安心感に加え、ユーザーサポートの手厚さや、分かりやすいUIが選定ポイントとなり、LANSCOPEに決めました。

端末管理の可視化と省力化が高評価 アップデート漏れが一目で分かる

アップデートは管理者が連絡し、社員が自主的にアップデートする運用です。忘れたり失敗した場合、WSUSでは把握する事が難しい状況でした。LANSCOPEを利用する事で失敗端末を可視化が実現し、3,300台のWindows端末のほぼすべてを最新バージョンに統一することが3~4ヵ月の短期間で実現できました。

内製台帳からIT資産台帳へ IT資産の可視化により大幅コスト減

内製の資産管理システムデータと、LANSCOPEの情報が連携することで、資産情報と所有者情報が即座に紐づけることができました。

それにより使われていない端末やソフトウェア資産の可視化が実現。リース費用・ライセンス費用の最適化が実現し、トータルでのコストダウンにもつながっています。

問題の可視化と改善で残業時間10%削減！ ISO27001更新とセキュリティ強化で 信頼される体制作り

株式会社テリロジー様

従業員数 117名　　業種 サービス業

ISO27001更新と取引先から 信頼されるセキュリティ体制作り

導入の目的は2点です。1点目はISO27001の更新、2点目はセキュリティを強化してお客様に信頼と安心感をもっていただく社内体制を作るためにLANSCOPEを導入しました。
取引先から情報セキュリティの管理状況を確認されることがあり、万が一の際に追跡が可能な操作ログ取得や有害なファイル共有ソフトなどのインストール実態把握の必要性を感じていました。

導入後約5ヶ月で、 月平均約10%の残業時間を削減

残業がここ数年増える傾向があり、課題だと考えていましたが、その現状が可視化できていなかったために「なぜ」「どこが問題か」といった事が分からず、対応が困難な状況でした。
LanScope導入後は何が問題なのか、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。

資産管理の工数を大幅削減 ライセンス管理を効率化

手動での資産管理では情報がリアルタイムに更新できず、工数が1週間近くかかっていました。

今ではソフトウェアライセンスの管理やHotfixの適用状況、インストールソフトウェアの最新の状況が、LANSCOPEで自動取得できるので管理工数の削減につながっています。ライセンスの無駄も省けるのではと期待しています。

62拠点7,900台のPCセキュリティ対策を実現
顔が見える情報シスで現場の信頼と協力を獲得

パナソニックシステムネットワークス株式会社 様

従業員数	3,500名	業種	サービス業

グループ企業の推奨製品を導入
トラブルで１年以上運用できず

2011年当時、パナソニックではグローバルで使えることを条件とした他社製品が推奨・導入されていたが、インストールがうまくいかずブルースクリーンが発生。その度に業務が止まり職場は混乱していました。
情報システム部30名体制でインストールしましたが、1年以上経っても安定稼働しませんでした。

5,000台環境でトラブルなく展開
他製品とバッティングしない製品

懸念していたインストール時のブルースクリーン障害はなく、驚くほどスムーズに導入が進み、全国展開を無事に完了できました。

インストールは、管理ソフトをActive Directoryで一斉配布し、1ヶ月で全拠点5,000台に展開でき、PC負荷の軽い事に、非常に驚きました。

業務効率を落とすことなく
全国800本のUSBメモリを管理

USBメモリは読み取り専用の運用をしています。業務上必要なUSBメモリが接続されると、管理コンソールに情報が追加されるので確認・許可しています。
このデバイス責任者機能のおかげで現場の負担軽減につながり、拠点に散らばるUSBメモリを回収することなく、1ヶ月で800本ものデバイス登録が完了できました。

ご参考資料

LANSCOPEで実現するWindows10管理

LANSCOPEならWindows10の対応ポリシーが明確です。安心してお使いください

Windows 10では、年2回 機能更新プログラム（FU）がリリースされます。
これに伴い、当社ではWindows 10各バージョン（FU）におけるLanScope Catの対応について、方針（ポリシー）を制定いたしました。

Windows 10対応ポリシー

LanScope Catは、次のポリシーでWindows 10 各バージョン（FU）に対応いたします。

対応時期	Windows 10 各バージョン（FU）リリース後、3か月を目処に動作確認完了 または 対応バージョンのリリースを以って対応を表明いたします。 ※一部制限事項や注意事項が発生する場合があります。
対応内容	Window10の新しいFUに対する対応ポリシーは次のとおりです。 • マネージャーのバージョンアップをせずに MR の対策プログラム適用のみで新しいFUに対応できるようにしております。 • 新しいFUへの対策プログラムの提供は LanScope Cat マネージャー各バージョンのリリースから 2 年間です。
対応開始バージョン	LanScope Cat Ver.8.4.2.0 以降のMR
Long Term Servicing Channel（LTSC）について	POS端末や医療用機器など、ハードウェア固有のカスタマイズ・チューニングを行っている環境はサポートの対象外となります。

※本ポリシーは予告なく変更する場合がございます。

Windows 10のアップデートは2種類！LANSCOPEは両方に対応しています

機能更新プログラム（Feature Updates / FU）

OSのアップデートに相当しOS全体の機能強化・拡張を行う更新プログラムです。例えばスタートメニューやCortana、Edgeブラウザなどの機能追加・変更が含まれます。

リリースタイミング　1年に2回を予定されています。

サポート期間　リリースから18ヵ月間※

品質更新プログラム（Quality Updates / QU）

従来の更新プログラムに相当するものになります。セキュリティ対策の更新を中心に過去にリリースされた更新を含む“累積更新プログラム”としてリリースされます。

リリースタイミング　毎月1回提供されます。

（日本時間毎月第2水曜日）

※Enterprise エディション、Education エディションでは、リリース日から30か月サポートされるバージョンが存在します。

LANSCOPEで行うFU・QU管理

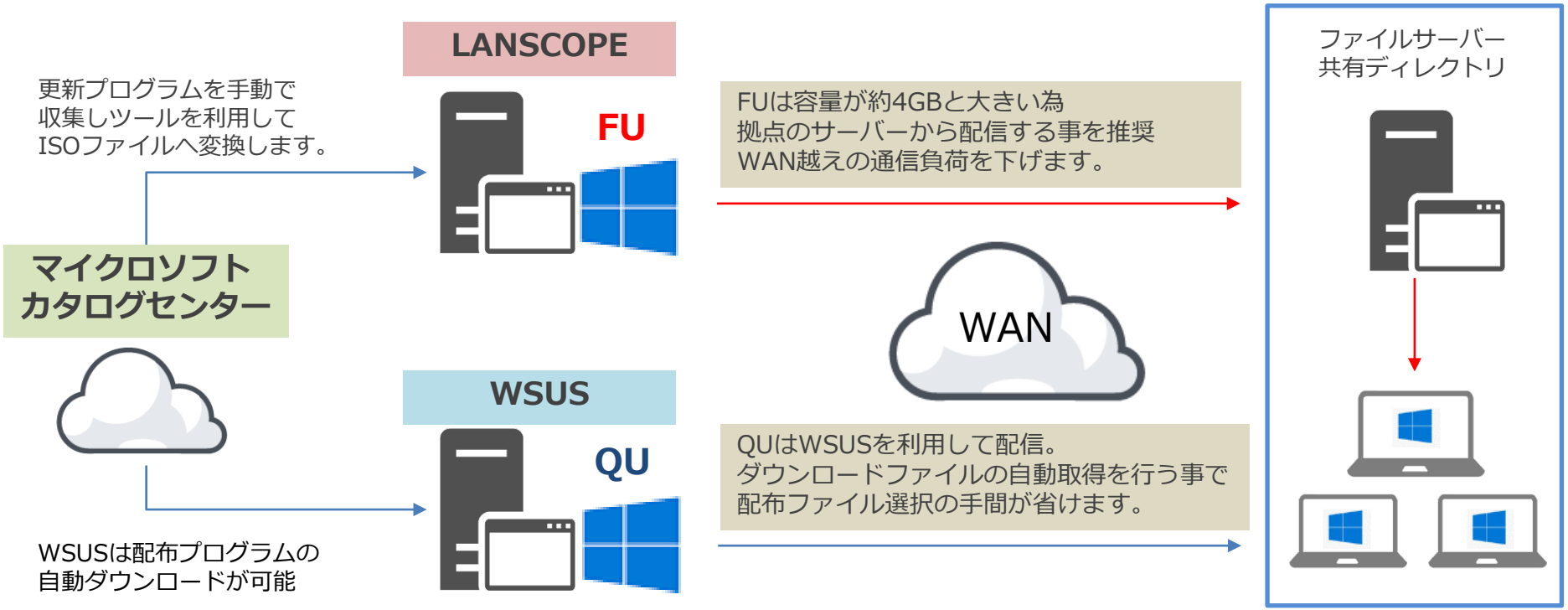
LANSCOPE×WSUS

WSUSとLANSCOPE（IT資産管理）の得意分野はそれぞれ異なるため管理に合わせて選択が必要です

	Windows Update For Business	WSUS (Windows Server Update Services)	IT資産管理ツール
概要	インターネット経由の自動更新サービス	Windows Server の更新プログラム管理機能	ファイル配布機能などのデータ配布・展開機能
費用	無償	無償	有償
サーバー	不要	WSUSサーバーが必要	管理用サーバーが必要
機能	更新プログラムの自動更新	更新プログラムの自動更新 更新プログラムの管理	更新プログラムの自動更新 更新プログラムの管理 資産管理,ログ管理など様々な情報収集
詳細	利用者が個別に適応する。 Windows 10 Pro エディション以上では、更新プログラムの受信タイミングを延期出来る機能を搭載。（WUfB）	管理者が更新プログラムを管理し配信を行う	LANSCOPEの場合、ファイル配布機能でFU,QUの配信を行う事ができ、WSUSとの連携も可能。マイクロソフト社製品以外のアップデートの配布も対応

【ポイント】
WSUSとLANSCOPEを組み合わせて活用することで、Windows10のアップデート管理がより便利になります。LANSCOPEは「更新プログラムの自動取得」の機能がない以外はWSUSと同等の機能を備えていますので、WSUSの利用が難しい場合には、LANSCOPEのみでWindows10アップデートが可能です

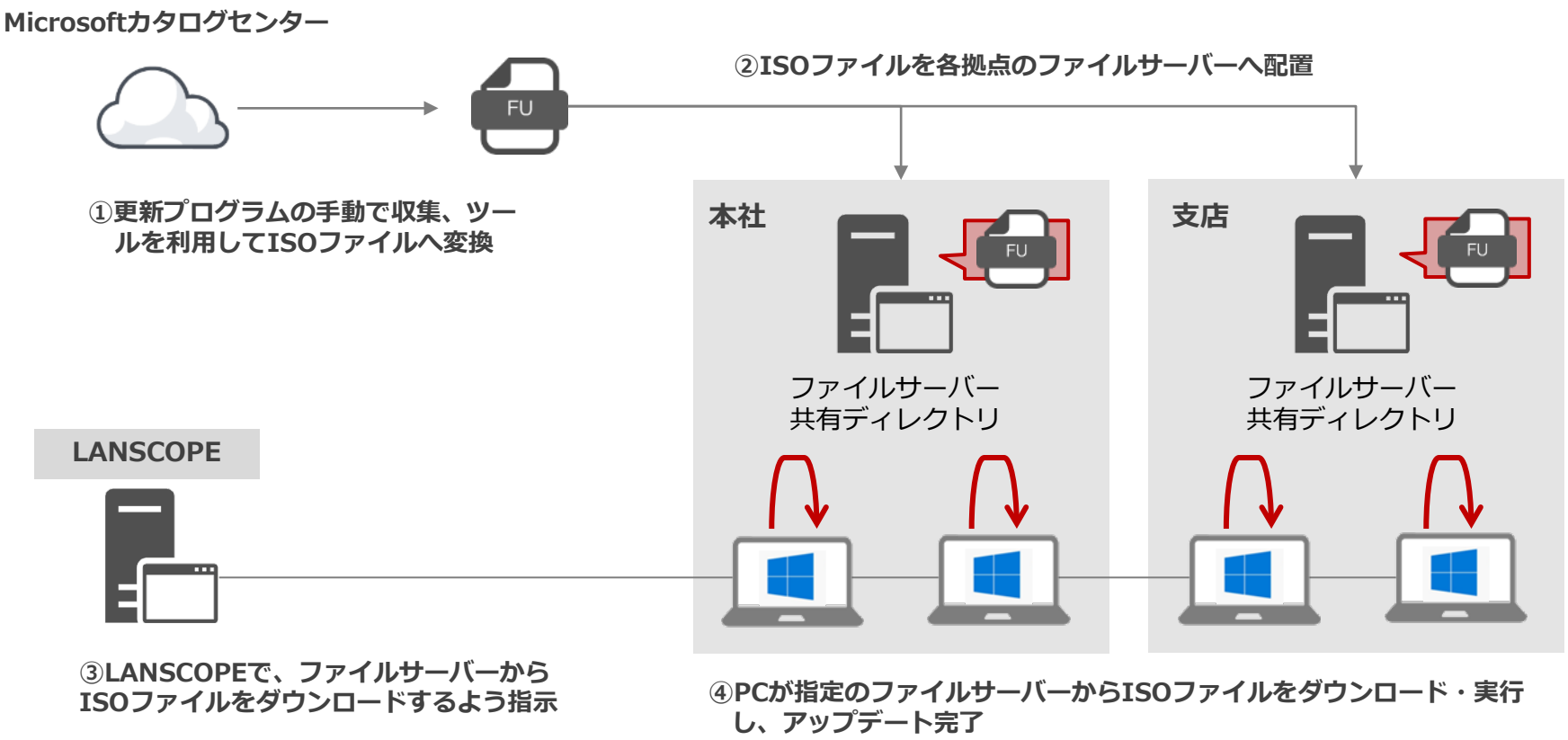
FU、QU配信のベストプラクティス案



プログラム	配信ツール	頻度	メリット
FU	LANSCOPE	年2回	約4GBとデータ量が大きく、ネットワーク負荷を考慮したい。 WAN越えをさせず拠点のサーバーから配信を行える。BITSを活用できる。 WSUSでも配信可能だが、回線帯域が有る本社などに絞って配信する。
QU	WSUS	月1回	情報の自動収集が出来る為、配信プログラムの確認手間が省ける。 更新頻度も高く、容量も1GB程度であり、WSUSで配信します。

LANSCOPEのファイル機能を利用することで、拠点のファイルサーバー経由で配信できます

本社の他に拠点が複数ある。本社のWSUS1台では拠点にFUを配信するとトラフィックが問題となる。
WSUSを階層構造にするのがベストではあるが、**WSUS専用サーバーを拠点数分用意するのが難しい**。

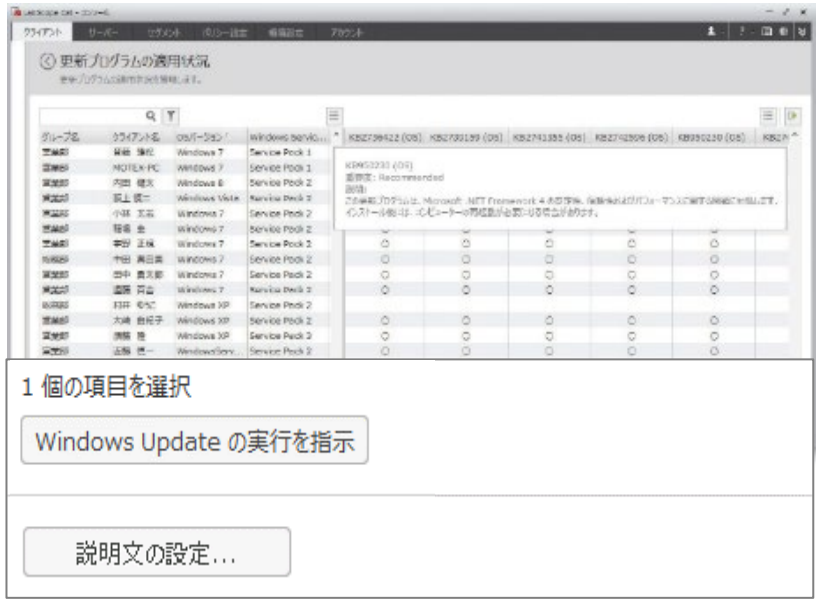


WSUSで一斉配布後、失敗した端末に対して管理者からPUSHで配信を指示することができない

配信が失敗した端末に対してLANSCOPEの機能で今すぐWSUSサーバーを参照するよう指示が可能。
対象についても1台単位に指定ができるため、対象を柔軟に調整できる。

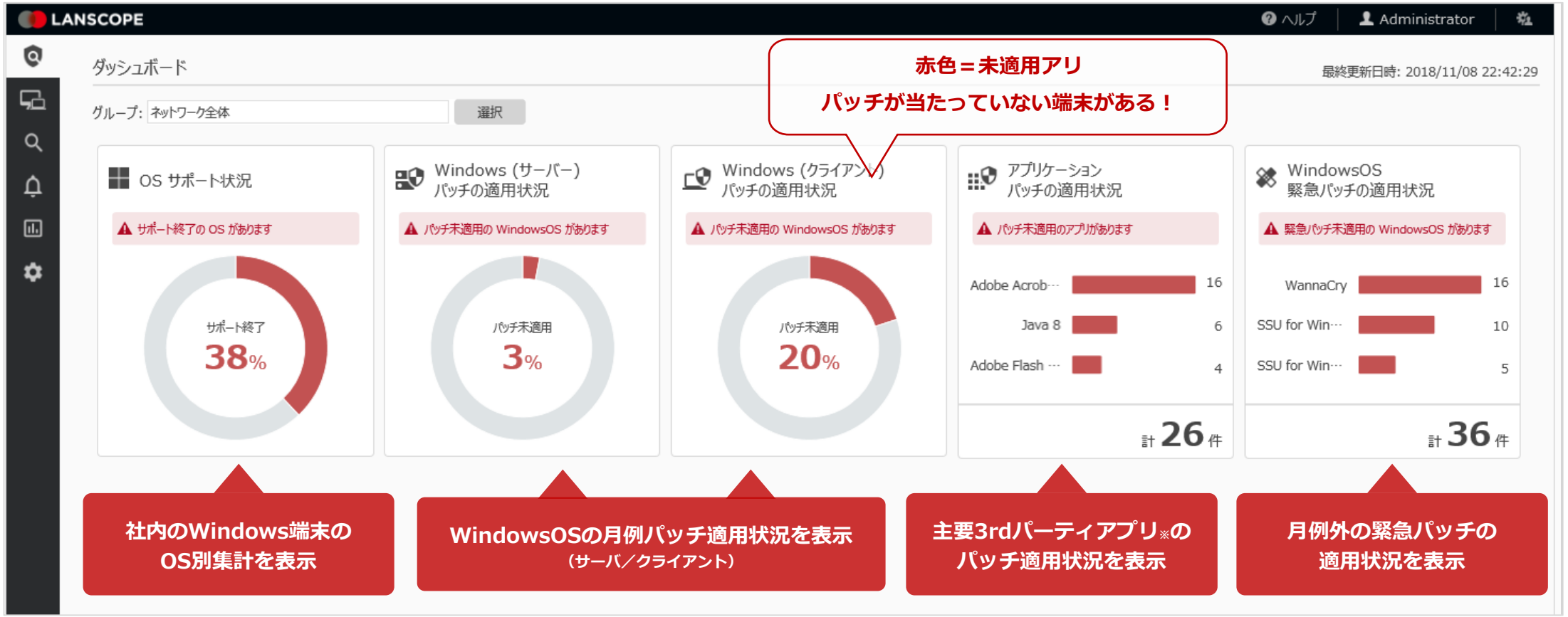
接続先設定
接続するWSUSサーバのURLを指定できます

Windows Updateの実行を指示
LANSCOPEの管理画面から端末を選択し指示できます



最新の状態になっているかどうかを一目で把握！対策すべき脆弱性の可視化～対策までを支援

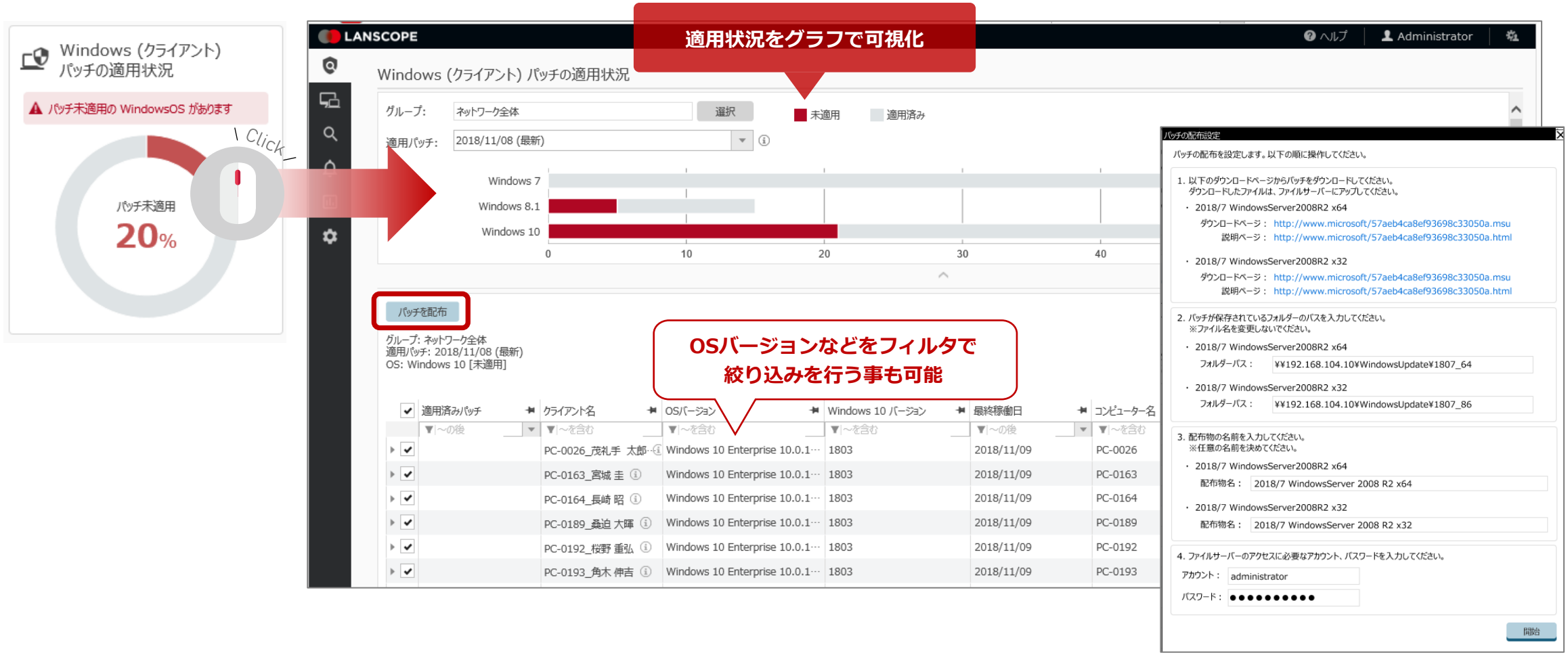
最新の状態でない＝脆弱性がある場合は赤色で表示されるので対策の必要有無をカンタンに判断できます



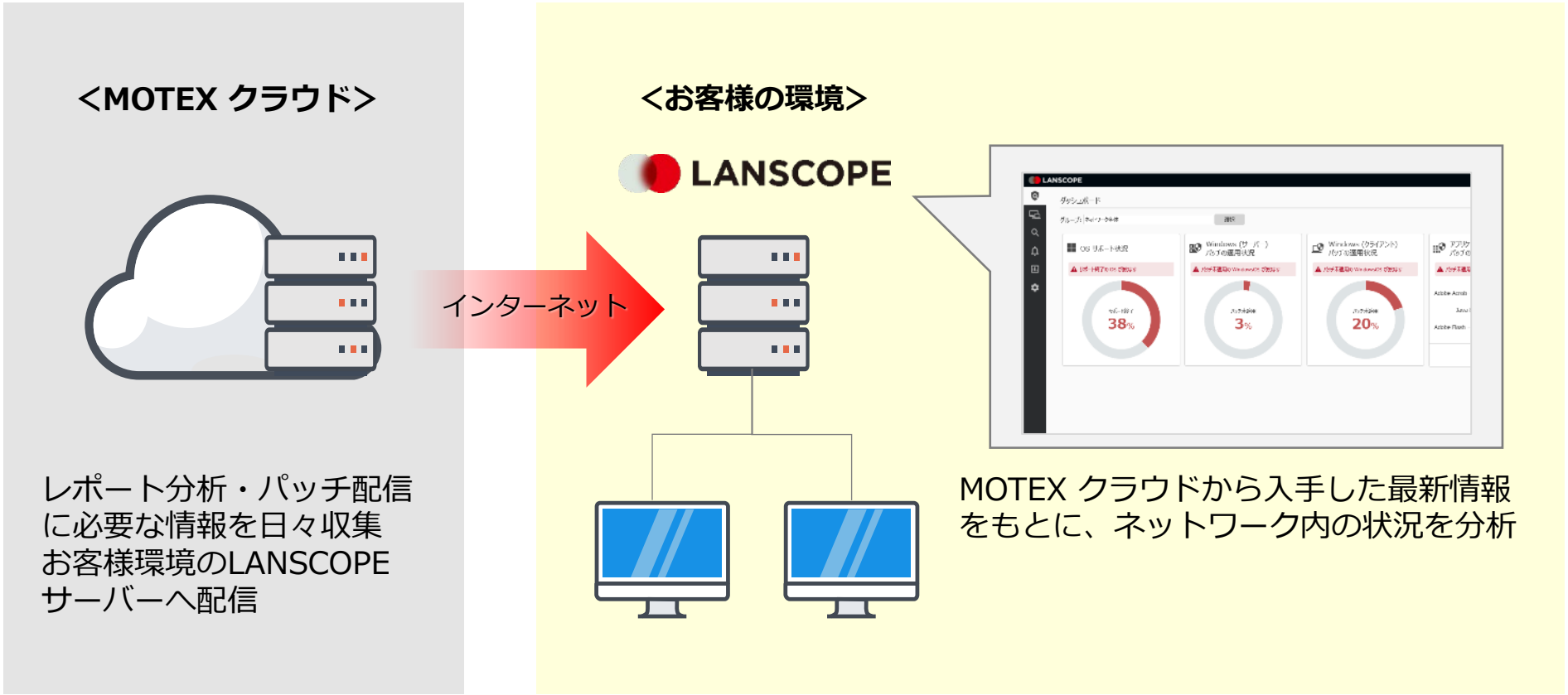
※ Adobe Reader DC (Continuous) (Adobe Reader旧バージョンも抽出は可能)
Adobe Flash Player (ActiveX, NPAPI)
Java Runtime Environment (8 以下)

パッチの適用情報をグラフ化！未適用者を絞り込みパッチ配布までをワンストップで行えます

パッチ適用情報をOS毎にグラフ化、パッチ別に確認することも可能です



「ダッシュボード」での分析・パッチ配信に必要な情報は全てMOTEXから提供します



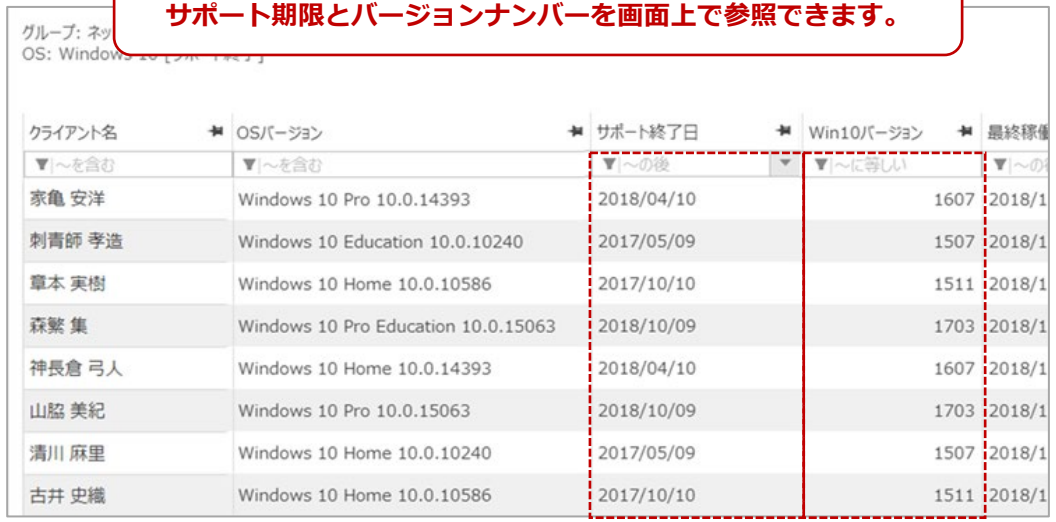
【参考】MOTEXクラウドから提供する情報の一例とその活用イメージ

レポート分析に必要な情報

＜Windows＞
- 最新のバージョン・緊急パッチのリリース状況
- OSビルド番号ごとのバージョンナンバー/名称
- OSバージョン・エディションごとのサポート期限

＜業務ソフトウェア＞
- 最新のバージョン・緊急パッチのリリース状況
- バージョンごとのサポート終了期限

Windows 10 のOSバージョン・エディションごとの
サポート期限とバージョンナンバーを画面上で参照できます。



クライアント名	OSバージョン	サポート終了日	Win10バージョン	最終稼働
家亀 安洋	Windows 10 Pro 10.0.14393	2018/04/10	1607	2018/1
刺青師 孝造	Windows 10 Education 10.0.10240	2017/05/09	1507	2018/1
章本 実樹	Windows 10 Home 10.0.10586	2017/10/10	1511	2018/1
森繁 集	Windows 10 Pro Education 10.0.15063	2018/10/09	1703	2018/1
神長倉 弓人	Windows 10 Home 10.0.14393	2018/04/10	1607	2018/1
山脇 美紀	Windows 10 Pro 10.0.15063	2018/10/09	1703	2018/1
清川 麻里	Windows 10 Home 10.0.10240	2017/05/09	1507	2018/1
古井 史織	Windows 10 Home 10.0.10586	2017/10/10	1511	2018/1

▲「OS分布状況」の詳細画面

パッチ配信に必要な情報

ダウンロードURL、説明ページURL／サイレントインストールのパラメータ

配信対象のパッチ・更新プログラムの詳細説明、
ダウンロードページのURLを参照できます。
リンクをクリックするだけで必要なファイルを
ダウンロードできます。

▲「パッチの配布設定」画面

https://www.lanscope.jp/cat/