LanScope Cat

統合型エンドポイントマネジメント

Version 9.1

13年連続
市場シェア
NO.1

富士キメラ総研 2005～2017 ネットワークセキュリティビジネス
調査総覧「IT資産/PC構成管理ツール、2016年度」

導入に必要な環境 ＊100台環境、標準パックの場合

統合マネージャー／サブマネージャー

- **OS**
  Windows Server 2008、Windows Server 2008 R2、
  Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
- **CPU**
  2.0GHz 以上
- **メモリ**
  4GB以上
- **HDD空き容量**
  200GB以上
- **データベース**
  SQL Server 2008、SQL Server 2008 R2、
  SQL Server 2012、SQL Server 2014
- **Webコンソール（ブラウザー）**
  Internet Explorer 10～11
  Google Chrome Ver.43.0.2357～
  Mozilla Firefox Ver.38.0.5～

エージェント

[Windows]

- **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

[Mac]

- **OS**
  Mac OS X Tiger v10.4.11 以降
  Mac OS X Snow Leopard
  OS X Lion
  OS X Mountain Lion
  OS X Mavericks
  OS X Yosemite
  OS X El Capitan
  macOS Sierra
  macOS High Sierra

＊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。
＊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。

●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

●お問い合わせは当社へ

2018.7 発行

MOTEX
Secure Productivity

“Secure Productivity”

安全と生産性の追求

統合型エンドポイントマネジメントで
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。

LanScope Cat

リスク低減

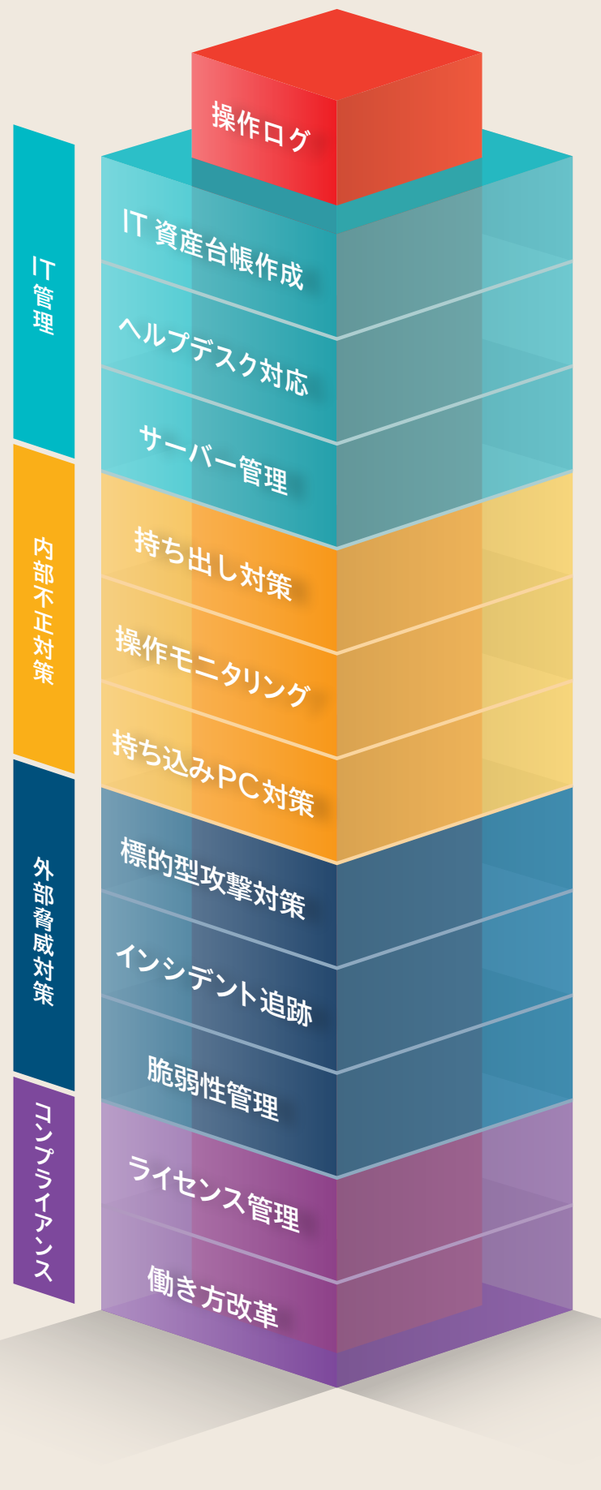
生産性向上

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。

「統合型エンドポイントマネジメント」LanScope Cat 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。

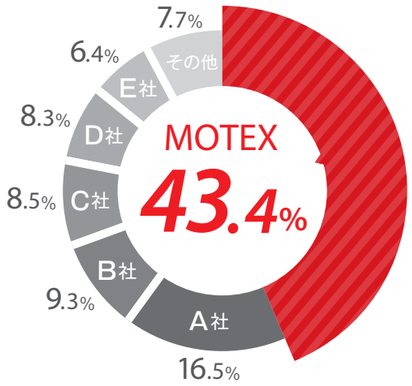


LanScope シリーズの信頼と実績

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 43.4% 13年連続 No.1

富士キメラ総研 2005～2017 ネットワークセキュリティビジネス調査総覧「IT資産／PC構成管理ツール・2016年度」



顧客満足度調査 No.1

中小企業向けセキュリティアワード 2015
「今後も利用し続けたいIT資産管理製品　第1位」
「誰かにすすめたいIT資産管理製品　第1位」

パートナー満足度調査 No.1

日経コンピュータ
パートナー満足度調査 2015
「統合運用管理ソフト（クライアント系）部門」

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。

2017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

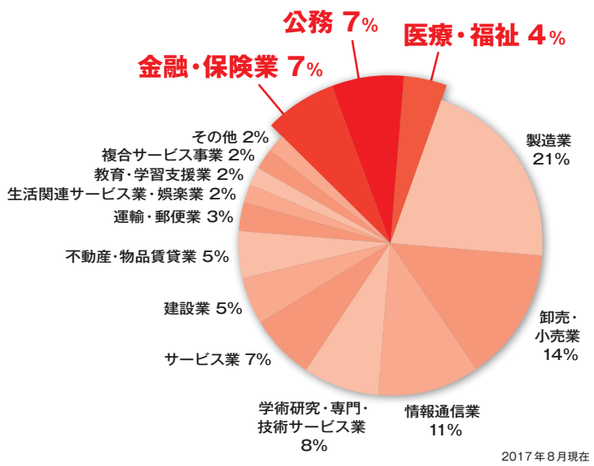
東証一部	東証二部	マザーズ	JASDAQ
530社	108社	44社	147社

■ 認証取得企業数

Pマーク取得企業…1,147社

ISO27001/ISMS取得企業…540社

官公庁導入数	病院／医療導入数	金融／保険導入数
459機関	284機関	499ヶ所



2017年8月現在

機能一覧

V バーチャルキャット（SBC方式シンクライアント管理）対応　Mac Mac 端末管理対応
バーチャルキャット／Mac 端末管理には専用ライセンスの購入が必要です。

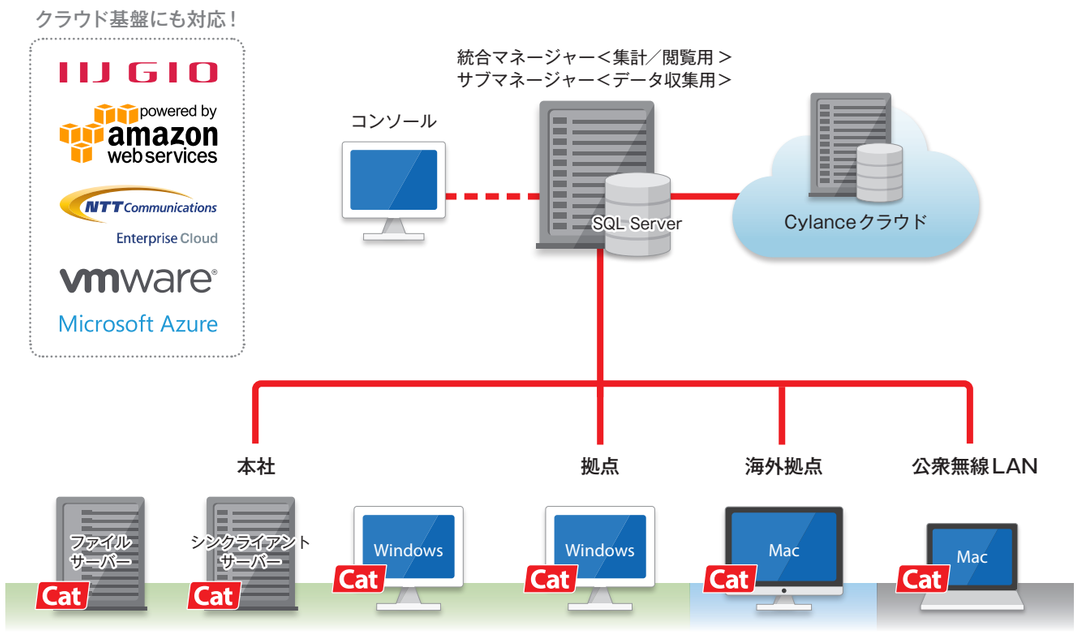
マネージャーライセンス（必須）	スカウトキャット	Webコンソール P.19-24 P.47-54	アラーム管理	ルール違反の有無をグループ単位／人単位で把握できます。
			カスタムアラーム	各種ログを複数条件で組み合わせ、より重要度の高い1つのアラームとして通知できます。
			サマリー	セキュリティを数値で把握できます。
			ログ検索／ファイル追跡	様々な条件で5年分のログを検索。抽出した特定ファイルの流出経路を追跡できます。
			レポート	グループ別、日付別など様々な切り口でログを集計／グラフ化できます。
		ネットワーク検知 P.25	持ち込みPC検知	持ち込みPCなどの不正接続を検知し、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。
		リモートコントロール（vPro）	インテル vProテクノロジー対応	インテル vProテクノロジー対応PCへのBIOS設定／電源ON／OFFなどのリモート操作ができます。
標準パック／パック1000／プレミアムパック	アセットキャット	IT資産管理 P.26-28	ハードウェア管理 Mac	コンピューター名、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 Mac	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。
			アプリ稼働管理／制御 Mac	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 Mac	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） P.29-30	ソフトウェア辞書 ソフトウェア資産管理台帳 Mac	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。
		ファイル配布 P.31-32	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。
	ログキャット	操作ログ管理 P.33-34	アプリ稼働管理／制御 V Mac	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 V Mac	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 V Mac	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。
			プリントイメージ（オプション）	プリントログから印刷イメージを表示できます。
			アプリ通信ログ	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。
	ウェブキャット	Webアクセス管理 P.35-36	Webアクセス管理／制御 V Mac	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。
			ホワイトリスト V	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。
	デバイスキャット	デバイス制御 P.37-38	デバイス制御 Mac	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。
			個体識別管理 Mac	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 Mac	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。
	メールキャット	メール管理（クライアント型） P.39	メール送信ログ管理	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。
	IDキャット	アプリID監査 P.40	ID監査ログ管理 V	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 V	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。
	プロテクトキャット	マルウェア対策 P.41-44	マルウェア検知 Mac	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 Mac	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） Mac	インシデント発生前後の操作を確認できます。
	サーバーキャット	サーバー監視 P.45	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。
	遮断キャット	不正PC遮断 P.25	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。
	リモコンキャット	リモートコントロール（ISL Online） P.46	リモートアクセス（ワンタイム型／常駐型） Mac	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。
			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。
	An	スマートデバイス管理 P.55	資産管理／行動管理／活用分析／セキュリティ	iOS／Android／Windows／macOS端末の資産情報や位置情報の自動収集、アプリ活用／Web閲覧の状況を記録できます。リスクのある端末を確認して、リモートロック／ワイプができます。
	An F	紛失／盗難対策 P.56	パスワードポリシー／リモートロック／ワイプ	遠隔で端末画面のロックやデータの初期化、パスワードの設定ルールを一括で設定／配布できます。
	Guard	メール管理（ゲートウェイ型） P.57	送信メールログ管理／制御	メールゲートウェイサーバーで送信メールの内容を記録します。機密ファイルの添付など違反メールは送信を禁止し、送信者と管理者にメールで通知できます。

•パック1000は1001ライセンス以上のご購入はできません。また、バーチャルキャットとMac端末管理は含まれません。•アプリ稼働管理／制御は、アセットキャット／ログキャット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。•バーチャルキャットは、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フィルタリングとプリントイメージは専用ライセンスの購入が必要です。•プロテクトキャット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。



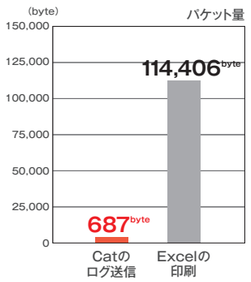
※保有するライセンスによって、以下のエージェントをインストールする必要があります。
クライアントエージェント（Windows用／Mac用）、検知エージェント、サーバーエージェント（Windows用／NetApp用）
CylancePROTECT エージェント、プリントイメージのクライアント、Webフィルタリングのクライアント、ISLOnline のクライアント

品質・性能

ネットワーク負荷の軽さ

Catの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。

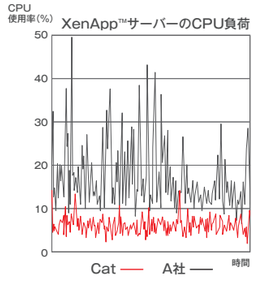
＜計測内容＞
通信パケット量



クライアント負荷の軽さ

Catは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。

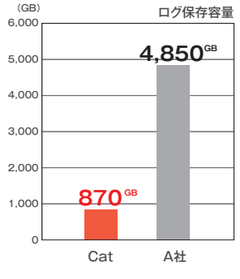
＜計測内容＞
40ユーザーアクセス時の
XenApp™ サーバー負荷



ログの保存容量の少なさ

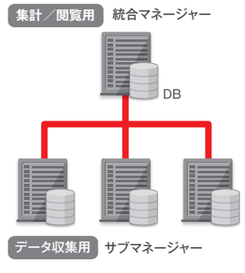
Catは人が操作した内容を判別する仕組みで、必要ない大量のシステムログなどをフィルタします。他社製品の約5分の1までログ保存容量を抑え、HDDを圧迫しません。

＜計測内容＞
1,000台の操作ログ5年分



システムの負荷分散

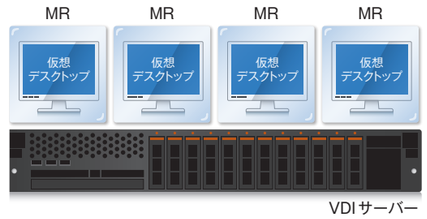
Catは、サーバーを集計／閲覧用とデータ収集用に分けることでシステムの負荷を分散しています。大規模環境でも運用可能な構成で、4万台のPCを管理している実績があります。



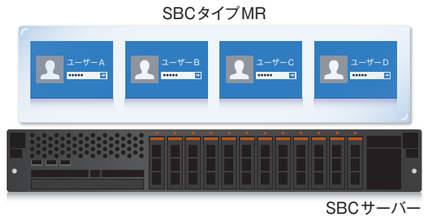
クラウド／マルチデバイス／グローバル対応

シンクライアント LanScope Cat

新たなワークスタイルにも対応、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、VirtualPCCenter 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。
※バーチャルキャットライセンスが必要です。

グローバル対応 LanScope Cat

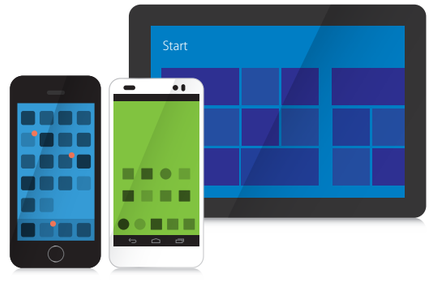
国内はもちろん海外拠点のWindows端末やMac端末もまとめて管理できます。

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。

スマートデバイス LanScope An

紛失／盗難対策から現在位置や移動履歴まで管理できます。



iOS
iPhone や iPad の資産管理、位置情報管理、紛失／盗難対策、構成プロファイル管理ができます。

Android
Android 端末の資産管理、位置情報管理、紛失／盗難対策に加え、独自機能の操作ログ管理では、アプリ利用、Web 閲覧、電話発着信、設定変更のログを収集します。

Windows
Windows タブレットの資産管理、位置情報管理、紛失／盗難対策ができます。

LanScope Cat は、IT資産管理から 統合型エンドポイントマネジメントへ。

LanScope Cat は 1996 年の誕生以来、ITの進歩と共に成長し続けてきました。

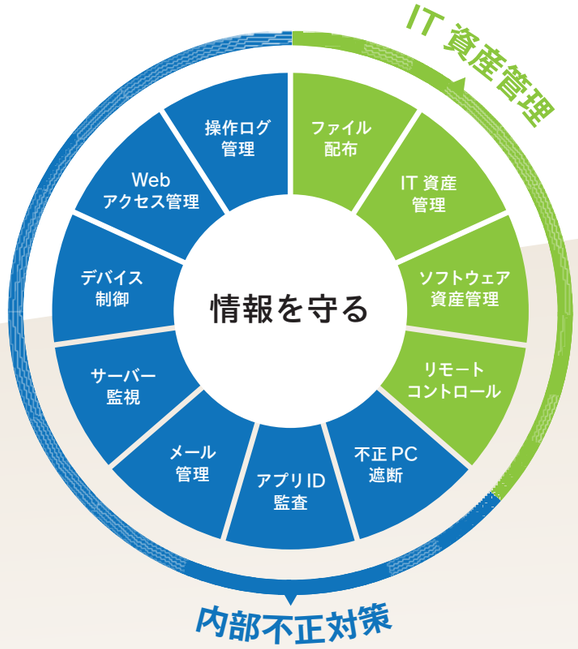
ハードウェアやソフトウェア自体が高価であった1990年代には、それらを管理するための資産管理として。
IT活用がさらに活発化する中、2000年からは、組織にとって重要な資産となる個人情報の保護のため。
そして2016年、高度化／深刻化するサイバー脅威に対応すべく新たに「外部脅威対策」の分野に機能拡張し、
『IT資産管理』から『統合型エンドポイントマネジメント』へと進化しました。

1990年~

お客様を取り巻く環境の変化

・高価なハード／ソフトの資産管理
・PC／ネットワークトラブルとの闘い
・Windows 95 の発売

2000年~



お客様を取り巻く環境の変化

・個人情報保護法の施行（2005年）
・日本版 SOX 法の施行（2008年）
・リーマン・ショック後のコスト削減

2016年~

お客様を取り巻く環境の変化

・標的型攻撃やランサムウェアなどサイバー脅威の深刻化
・クラウドサービス利用の本格化、シャドーITの脅威
・働き方改革を発端に、多様化する働く環境、制度の変化

Ver.9.0 新機能

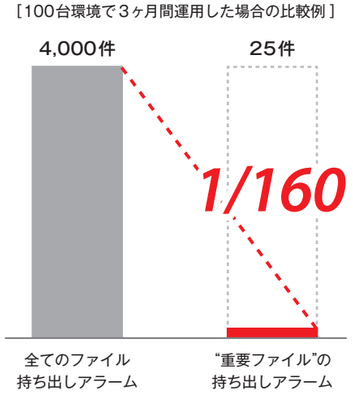
LanScope Cat Ver.9.0「ログ活用」を徹底　的に見直した新機能：カスタムアラーム

見るべきログの量が激減します ※当社調べ

情報漏えいをはじめとした内部不正は、社内ルールに違反する操作をアラームに設定することで発見できます。しかし、多忙な管理者にとって日々のアラームを確認するにはログ量が多く時間がかかることが課題でした。

そこで、LanScope Cat Ver.9.0では、新たに「カスタムアラーム」機能を搭載しました。

カスタムアラームでは、複数の行動を組み合わせてアラーム判定を行うため、管理者が本当に知るべき違反操作のみをアラームとして抽出することができます。これにより、日々の運用の効率化を実現します。



新機能1 カスタムアラーム機能

カスタムアラームは用途/目的にあわせて活用できるテンプレートをご用意。管理者一人一人に合わせた運用を実現します。
テンプレートはセキュリティ対策だけでなく、労務管理・業務効率向上など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

重要ファイルの持ち出しだけを察知
ファイルサーバーの重要ファイルを、「外部デバイス」「メール」「Webアップロード」「印刷」で持ち出した場合にアラームとします。

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。

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。

サーバーファイルの印刷を察知
指定のファイルサーバー上のファイルを印刷した場合にアラームとします。

社外での印刷を察知
指定のプリンター以外で印刷を行った場合にアラームとします。

データの出力を察知（CSV／PDF）
業務システムやWebアプリからのCSV／PDFファイルの出力をアラームとします。

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。

低スペックPCの利用を把握
PCのスペックが低く、アプリが固まり業務影響が出ている端末をアラームとします。

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。

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。

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。

常用アプリの終了を注意
セキュリティツールなど常に動作すべきアプリが終了した場合にアラームとします。

デスクトップへのファイル配置を注意
クリーンデスクトップのためにデスクトップにファイルを置くとアラームとします。

大容量ファイルのコピーを注意
サーバーにアップされたファイルサイズの合計が指定値以上の場合にアラームとします。

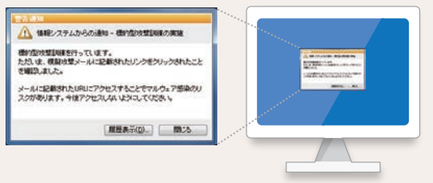
私用デバイスの接続を注意
会社指定のデバイス以外をPCに挿したらアラームとします。

非圧縮ファイルの持ち出しを注意
デバイスにファイルを書き出す際に圧縮ファイルでない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。

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。

例えば…標的型攻撃訓練のテンプレートを使うと、ユーザーが訓練メールの中のURLをクリックしたり添付ファイルを開いてしまった場合、このようなポップアップを出すことができます。



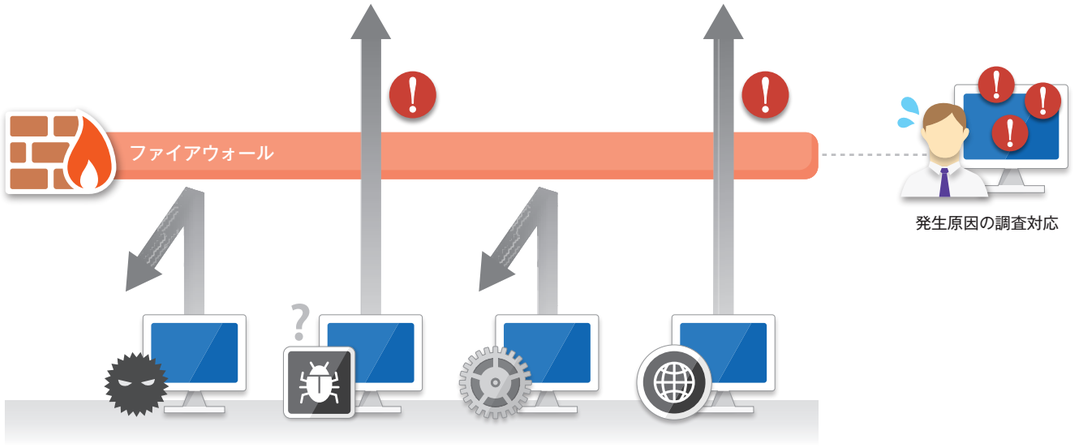
カスタムアラームのテンプレートはお客様の声をいただきながら随時追加を予定しています。

Ver.9.0
新機能

LanScope Cat は、さらに激化する外部か らの攻撃に対応するための機能を強化。

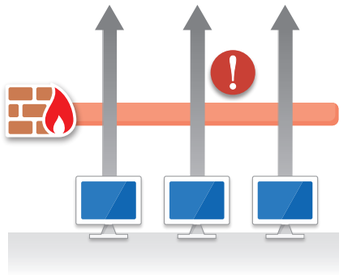
課題：日々発生する不審な通信アラート運用に対する課題

ファイアウォールなどの境界防御製品から日々届けられるアラートの中でも、組織内から外に向けて行われた通信のアラートは、マルウェアによる通信の可能性があるため、調査が必要になります。
しかし、発生するアラートに対して「なぜ」そのアラートが発生したのか、どんな対策を行えばよいのかを追究することは、スキル的にも、時間的にも難しいのが現状です。

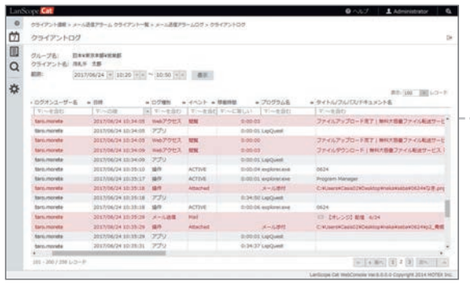


解決：違反操作が行われたエンドポイントで原因を発見

境界防御のファイアウォールの情報とエンドポイントを管理するLanScope Catの操作ログを組み合わせることで、これまで追究が難しかった問題の発生原因を特定することが可能になります。



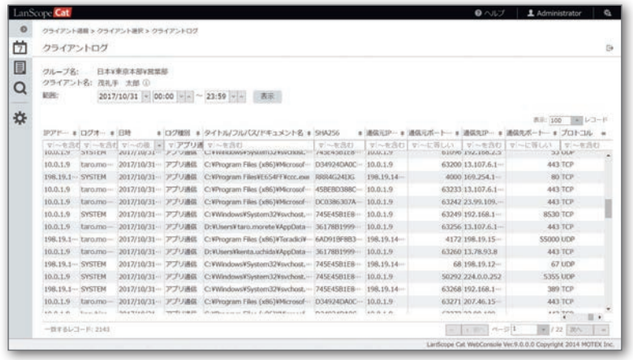
ファイアウォールによる検知
- IP アドレス情報（通信元／先）
- ポート番号（通信元／先）
- ログオンユーザー
- アラートの内容



Webコンソールのクライアントログ画面で
ファイアウォール製品のアラート情報から
問題の発生原因を追究

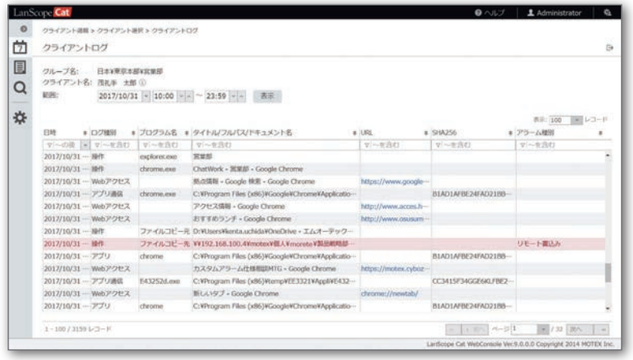
新機能2 不審なプロセスを発見「アプリ通信ログ」

ファイアウォール等の製品で検知した通信元 IP アドレス、通信元ポート情報から、不審な通信を行っているプロセス（アプリ）を特定。
アプリ名やハッシュ情報から不審なアプリの解析を行うことができます。



新機能3 リアルタイムにすべてのログを一括確認

インシデント発生時は素早い調査、対応が必要となります。Ver.9.0では調査する端末のログをリアルタイムに表示、すべてのログを1つの画面で確認することで、原因追究時間を削減します。



新機能4 SIEM製品など、外部ツールとの連携

LanScope Catのログを Syslog 形式で出力することで、SIEM 製品や BI ツールとの連携が可能になります。
エンドポイントの操作ログと各企業にある様々なデータと組み合せることで、より広範囲のログ管理が可能になります。

※ SIEM 製品のイメージです。

Ver.9.0
新機能

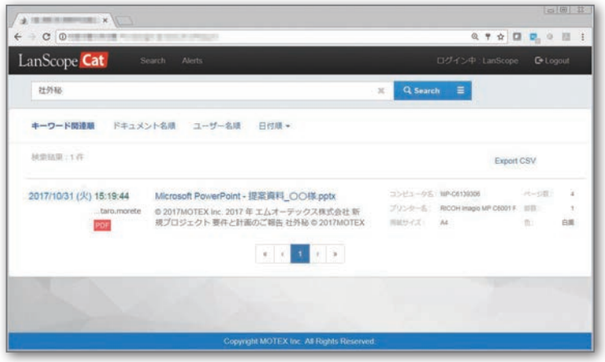
内部情報漏えい対策、働き方改革の対応など　今の課題を解決する機能を提供し続けます。

新機能5 印刷内容を全て保存「プリントイメージ」 オプション

プリントイメージ取得
印刷ログに、実際に印刷されたファイルのイメージを追加、どんな情報が印刷されたのか中身を見て判断できます。

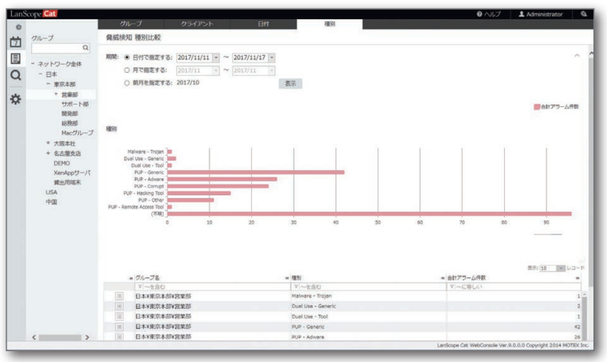
メーカーを問わない マルチベンダー対応
社内で複数メーカーのプリンターを利用している場合でも、メーカーや機種を問わずに印刷情報の取得が可能です。

印刷ファイルの中身を全文検索
印刷されたファイル名だけでなくファイルの中身も含めて文字での検索が行えます。機密ファイル印刷の発見などが行えます。



新機能6 検知／隔離したマルウェアの傾向を分析

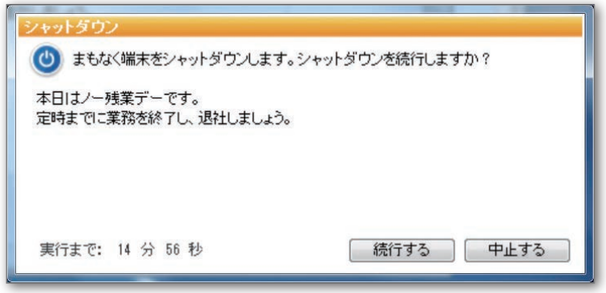
グループ、クライアント、検知日、種別比較の脅威検知レポート
様々な視点で脅威を分析することで脅威流入の傾向がつかめます。種別比較では脅威の重要度順に集計値が表示されます。



新機能7 電源管理強化で残業時間抑制

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。



Ver.9.0／Ver.9.1 新機能一覧

ITマネジメント	Webコンソール	アラームログの一括表示：選択したグループの全アラームログを一括で表示	全般
		ログ表示権限の改良：表示権限をアラーム件数のみ、アラームログのみ、すべてのログの３段階から設定可能	
		今日のログ：データ更新前のログも閲覧可能に	アセットキャット ログキャット Webキャット
		各種ログの一括表示：クライアントログ画面で、１台のクライアントの各種ログを横断して表示	
		各種アラームからの周辺ログ：アラーム前後にどのような操作をしていたかを追跡	
	ポリシー	ポリシーの即時適用：クライアントが定期的にマネージャーに通信し、設定をダウンロード	全般
	資産管理	最新の資産情報：資産情報を定期的にデータ更新し、最新の資産情報を閲覧可能に	アセットキャット
		電源操作時のメッセージ設定：指定した電源操作が行われる前に、任意の通知メッセージを設定可能に	
		端末使用者の表示：Web コンソールのクライアント週報と、ハードウェア資産情報で、端末使用者のフルネームとログオンユーザー名を表示	
		固定列の指定：横スクロールをしても常に表示する列を指定可能に	
		一括 CSV エクスポートにグルーピングアプリを追加： 複数のバージョンや表記が異なるアプリをまとめて表現できるグルーピングアプリを指定可能に	
内部不正対策	ログ管理	カスタムアラーム：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	アセットキャット ログキャット Webキャット
		SIEM 製品への Syslog 転送：SIEM 製品にリアルタイムにログを転送	全般
		クライアントに保存されたログの難読化：端末使用者がログを確認できないように難読化	
		プリントイメージ：プリントログから印刷イメージを表示（オプション）	ログキャット
		デバイス名の記録：ファイル操作ログで、どのデバイスに対して行った操作かを記録	
	デバイス制御	デバイス情報の表示改良：フレンドリーネーム／デバイスクラス／制御区分を表示	デバイスキャット
外部脅威対策	ログ管理	脅威検知レポート：任意のグループ、クライアントの検知数集計／日付ごとの検知数の推移／マルウェア種類別の検知数集計	プロテクトキャット
		DisconnectedModeの把握： CylancePROTECTエージェントが、インターネット非接続端末のためのDisconnectedModeで動作しているか否かを表示	
		セキュリティインシデントの原因調査： UTM／次世代 FW から得た IP アドレスやログオンユーザー名から端末を特定し、各種ログを一括で閲覧可能に	アセットキャット ログキャット Webキャット
		アプリ通信ログ：データ送信を行うプロセスの取得。UTM ／次世代 FW のインシデントの原因調査を可能に	ログキャット
		ハッシュ値／ファイルパスの取得：アプリ稼働ログ、アプリ禁止ログのハッシュ値とファイルパスを取得	アセットキャット ログキャット
環境対応	OS	サーバー監視：NetApp ONTAP 9.2 に対応	サーバーキャット
		(Ver.9.1) Windows Server 2016 WSUS に対応	アセットキャット
		(Ver.9.1) Firefox のプライベートブラウジングモード使用時における、閲覧ログの URL を取得、アップロード・ダウンロード・書込みログを取得	Webキャット
性能改良	表示速度改善	(Ver.9.1) 統合コンソールにおけるツリーの描画性能を改善	全般
		(Ver.9.1) 統合コンソールにおける各種データの表示速度を改善	
	排他制御緩和	(Ver.9.1) アカウント同時実行制御を緩和。同時利用の利便性を向上	
	ガイドタブ	(Ver.9.1) アクションメニューにガイドタブを追加、関連サイトへの遷移が可能	
	画面ヘルプ	(Ver.9.1) 現在開いている画面に絞り込んだヘルプ画面を表示	

LanScope Cat は、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。

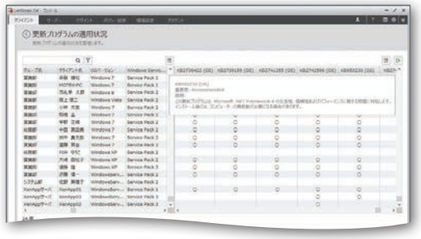
1日に誕生するマルウェアは100万個ともいわれており、従来のアンチウイルスだけで脅威から組織を守ることは難しくなっています。LanScope CatはCylancePROTECT®を組み込み、これまでの機能と組み合わせることで猛威を振るうサイバー攻撃から大切な情報／人を守ります。

LanScope Cat で対策

IT 資産管理

社内端末のパッチ管理を徹底し、常に最新の状態を保つ ▶詳細はP.28

Windows の更新プログラムやセキュリティパッチの適用状況の確認、また未適用端末への配信や緊急度の高いパッチの一斉適用も可能です。



マルウェア対策

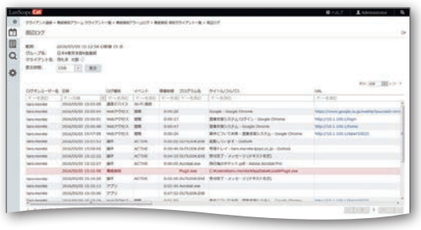
既知未知のマルウェアを99%以上防御 ▶詳細はP.41

AI エンジンを活用したプロテクトキャットは、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。

操作ログ管理

マルウェアを検知した場合は流入経路を特定 ▶詳細はP.42

管理画面から数回クリックするだけで、どんなマルウェアを検知したか、また流入原因となったユーザーの操作を特定することができます。



Web アクセス管理

デバイス制御

原因を特定し、ポリシーの強化と対策を実施 ▶詳細はP.35／37

マルウェア流入原因のユーザー操作に対して、適切な対策を実施することができます。また、メッセージ・アンケート機能を使った社員への注意喚起や社員教育を行うことで、再発防止につなげることができます。

Webサイト閲覧
→ Webフィルター

フリーウェアダウンロード
→ Webフィルター

USBメモリ利用
→ デバイス制御

公衆 Wi-Fi 接続
→ 通信デバイス制御

2020年1月のWindows７延長サポート終了に向けたWindows10の企業導入、運用を支援します。

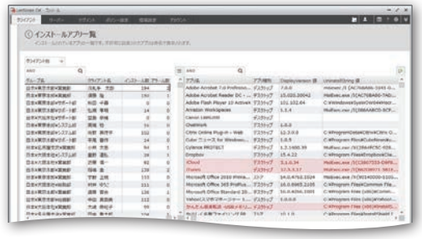
マイクロソフト社は Windows 10 から OS の永続的なアップデートを行うために、WaaS（Windows as a Service）という考えを取り入れています。これにより、OS のサポート期間は各アップデートから18カ月となり企業は計画的なバージョンアップが必要となります。

LanScope Cat で対策

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

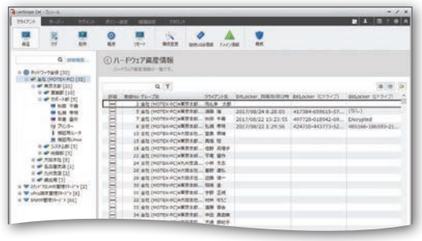
年２回のSemi-Annual Channelへの対応

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 Cat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 CatのWindows 10対応ポリシー

Windows 10 の企業展開スピードに合わせて、LanScope Cat も Windows 10 の各アップデートに対応したバージョンをリリースします。検証用に先行配信される、Windows 10 の Semi-Annual Channel（Targeted）リリース後、3 カ月をめどに LanScope Cat の対応バージョンをリリース。Windows 10 の先行配信 4 カ月後にリリースされる、Windows 10 の正式配信である Semi-Annual Channel に間に合わせることで、Windows 10 でも安心してご利用いただけます。

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。

国をあげて取り組んでいる「働き方改革」。その対応が各企業に求められていますが、課題が多いのが現状です。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。

LanScope Cat で対策

操作ログ管理

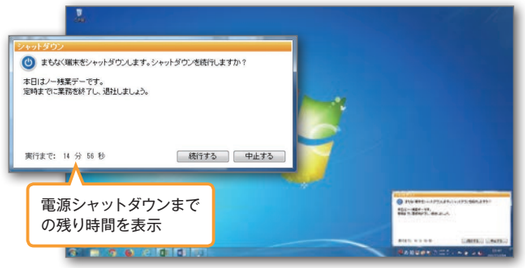
“人の PC 操作”を記録 ▶詳細はP.33

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.26

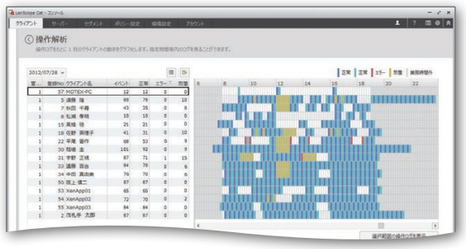
ノー残業デーなど、指定した時刻に端末上にメッセージを表示、また強制的にシャットダウンを行うことができます。



レポート

各種レポートを業務管理に活用 ▶詳細はP.49

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。

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。

2017年5月30日に全面施行された改正個人情報保護法。これまでは、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）は規制対象外でしたが、今回の改正により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。

LanScope Cat で対策

操作ログ管理

情報を扱う“人の操作”を記録 ▶詳細はP.33

操作ログを取得することで、不正操作がしづらい抑止環境を作ることができます。また予め決めたルールに違反した操作をリアルタイムに把握することができます。

Webアクセス管理 / デバイス制御

情報の持ち出し経路を把握し、制御 ▶詳細はP.35／37

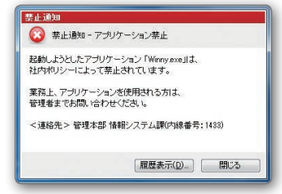
私物USBメモリやクラウドストレージの利用を禁止し、情報の持ち出し経路を限定することで、リスクを減らすことができます。

Webサイト閲覧 → Webフィルター
フリーウェアダウンロード → Webフィルター
USBメモリ利用 → デバイス制御
公衆 Wi-Fi 接続 → 通信デバイス制御

資産管理（操作ログ管理）

不正なアプリのインストールや利用を制御 ▶詳細はP.34

社内で利用されているアプリを把握し、不正ソフトや許可していないアプリがあった場合には、起動を禁止することができます。また、リアルタイムに社員にポップアップで注意喚起を行えます。



エムオーテックスでは、セキュリティ教育にご活用いただけるセキュリティブック「セキュリティ７つの習慣・20の事例」を作成しました。コンテンツはすべてWebから無償でダウンロードすることができますので、会社でのセキュリティ研修やマナー研修などにご活用ください。

電子データは **すべて無償** でご利用いただけます。

セキュリティブック 検索

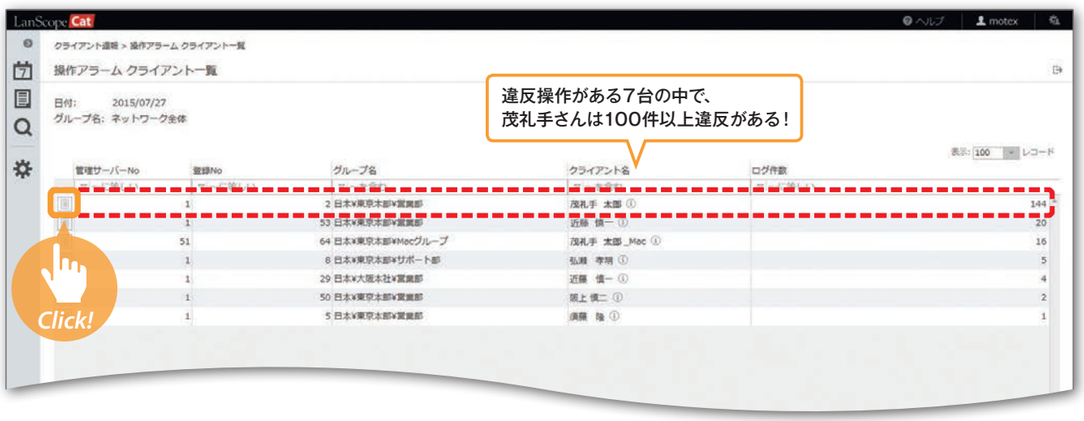
アラーム管理

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。

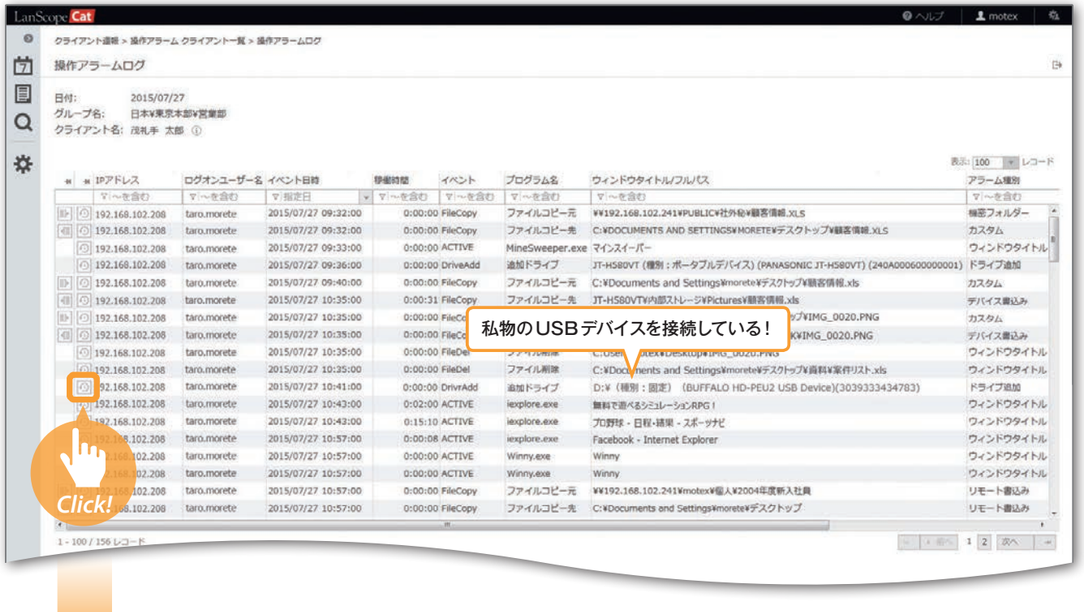
「現状把握→分析→問題発見」までを自動でレポートするので、一般社員から経営者まで同じ判断基準で、問題の対策に集中できます。また、現場に即した運用を実現するために、必要なレポートを必要な人にだけ見せて管理を分散できます。

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

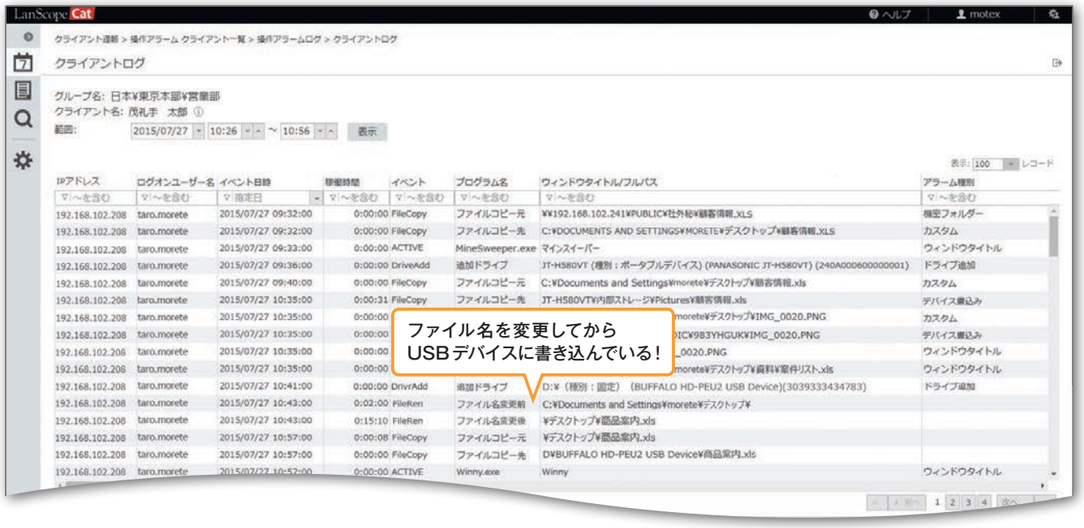
Step2 ルール違反が、どのPCで何件あったかを把握できます



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。Cat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

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	－
	アプリ禁止	アプリ禁止ポリシー	禁止アプリの起動／名前変更	○
			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	－
			指定した条件に抵触するファイルの操作	－
	プリント	プリントポリシー	印刷枚数の超過	－
			キーワードに抵触したドキュメントの印刷	－
	Web	Web アクセスポリシー	指定したキーワード／ URL に抵触	○
			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	○
	ファイル操作	サーバー監視ポリシー	サーバーファイルの削除／アクセスの失敗	－
	接続失敗		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	－
	不正接続失敗		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	－
			操作回数アラームに抵触	－
	メール送信	メールポリシー	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）	－	○	－	－
	標的型攻撃訓練（URL をクリック）	－	○	－	○
労務管理・業務効率向上	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

サマリー

セキュリティを数値で把握し、何に対策が必要か判断できます。

「環境」「効率」「行動」のカテゴリごとに正常率が表示されます。また、グループ別やクライアント別のアラーム数ランキングを確認し、社内の状態と課題を一目で把握できます。

サマリー

正常率

取得したログとアラームの数から正常率を 3 つのカテゴリに分けて表示します。また、比較期間（前日、先週、先月）との変化が数値で表示されるので、対策の効果なども見ることができます。

カテゴリ	アラーム
環境	資産情報の変更や新規／禁止アプリの起動、通信デバイスの接続など、環境の変化を捉えることができます。
効率	深夜や早朝、土日の操作など、業務時間外の操作を把握することができます。
行動	重要な顧客データのコピーや印刷、不正サイトの閲覧やメール送信など、情報漏えいにつながる行動を把握することができます。

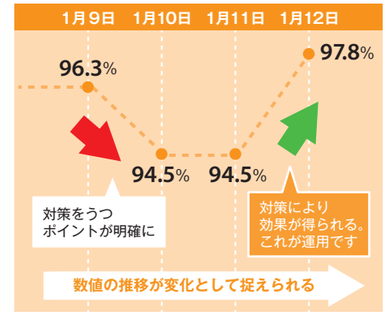
アラーム数グループランキング

アラームの多いグループのワースト 10 が表示されます。

アラーム数クライアントランキング

アラームの多いクライアントのワースト 10 が表示されます。

社長から一般社員まで“数値の変化”で対策の効果を実感できます。



User's Voice

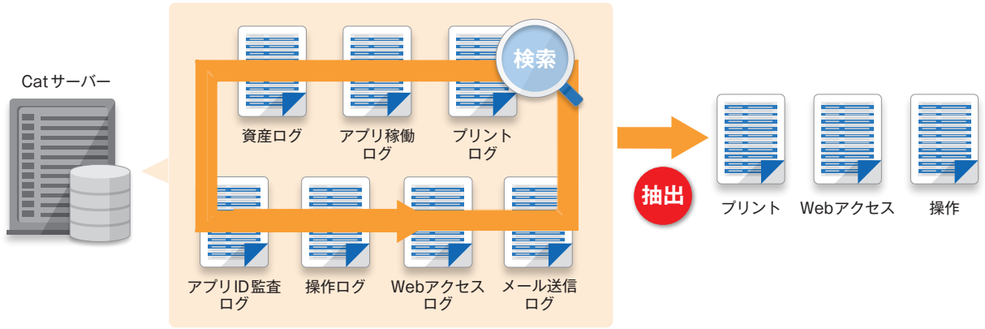
社長自ら毎朝 Web コンソールを確認！朝の 3 分で会社のセキュリティ状態が分かる。

Cat 導入前はセキュリティは難しいからとシステム管理者任せの状態でした。現在は、各本部の部長だけでなく社長も自ら Web コンソールを毎日確認することで同じ指標（数値）を見ながらセキュリティ対策ができるようになり、セキュリティレベルは大幅に UP しました。

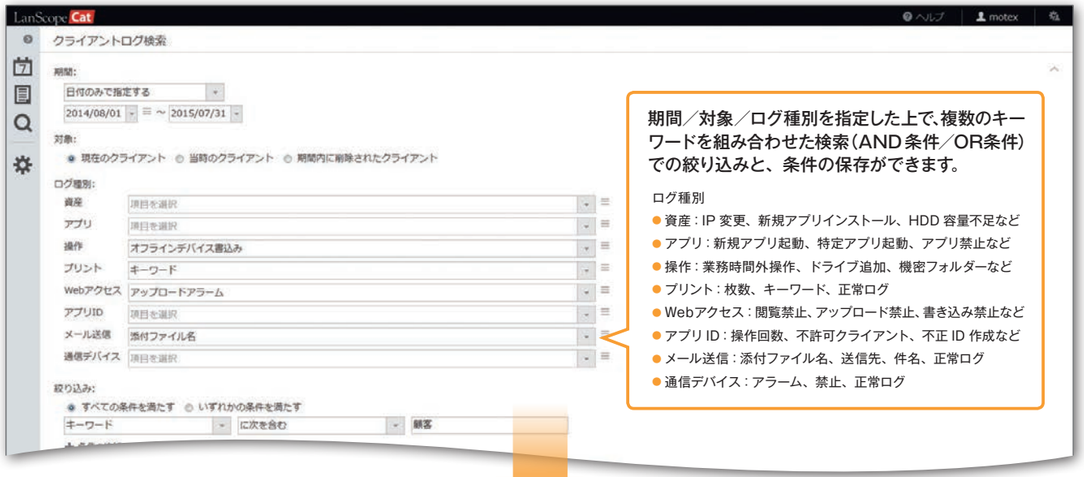
ログ検索

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

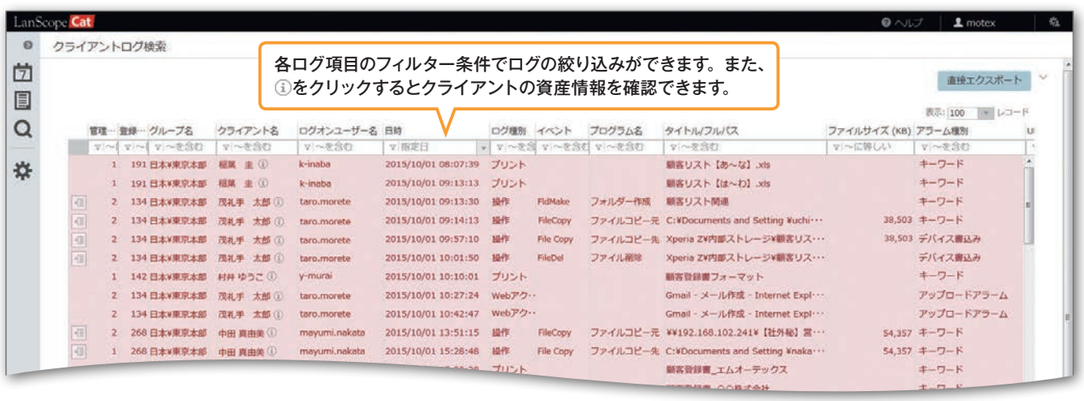


期間／対象／ログ種別を指定した上で、複数のキーワードを組み合わせた検索（AND条件／OR条件）での絞り込みと、条件の保存ができます。

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、機密フォルダーなど
- 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

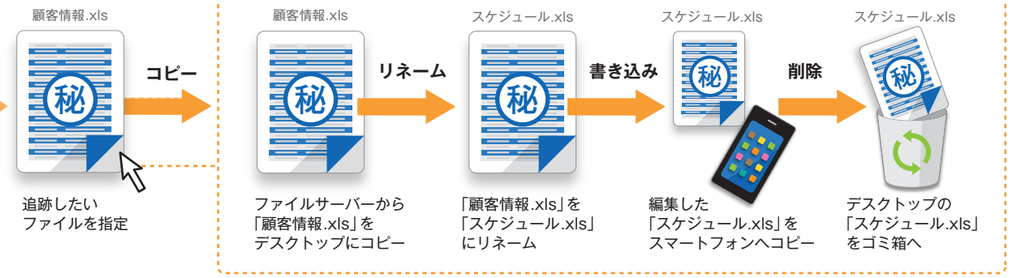


各ログ項目のフィルター条件でログの絞り込みができます。また、ⓘをクリックするとクライアントの資産情報を確認できます。

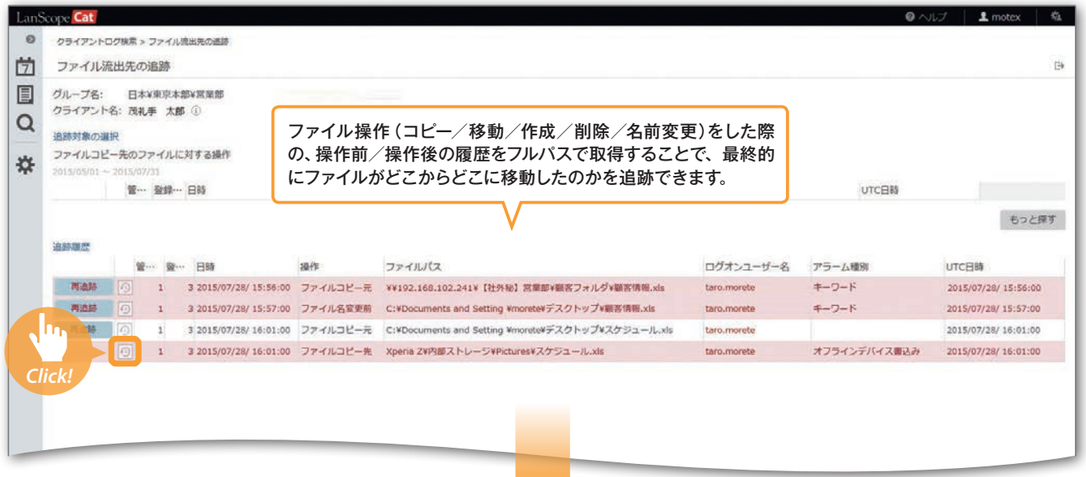
ファイル追跡

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更さ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。

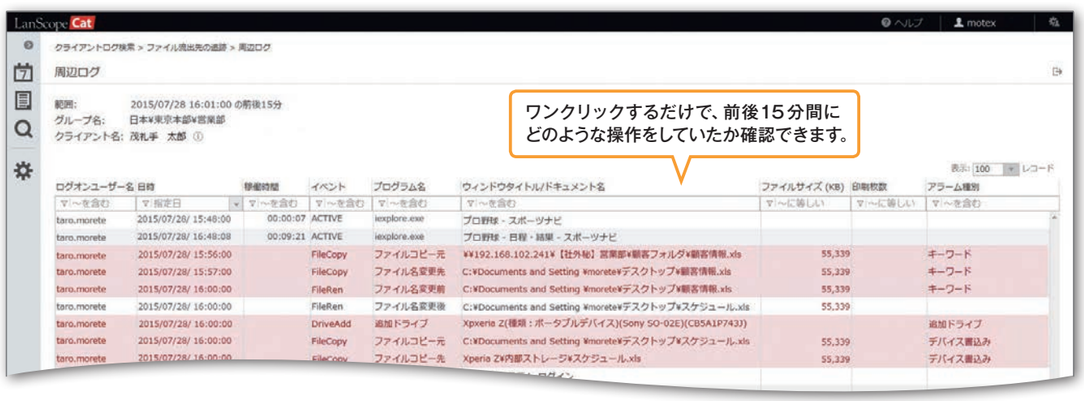


ファイル追跡（トレース）



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

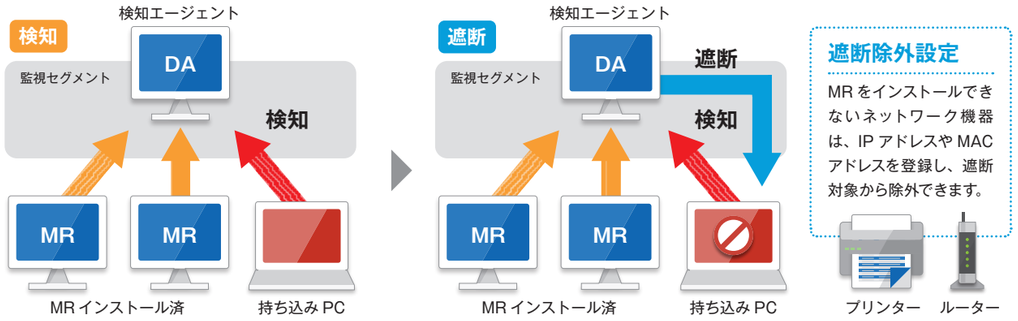


ワンクリックするだけで、前後15分間にどのような操作をしていたか確認できます。

ネットワーク検知　不正PC遮断

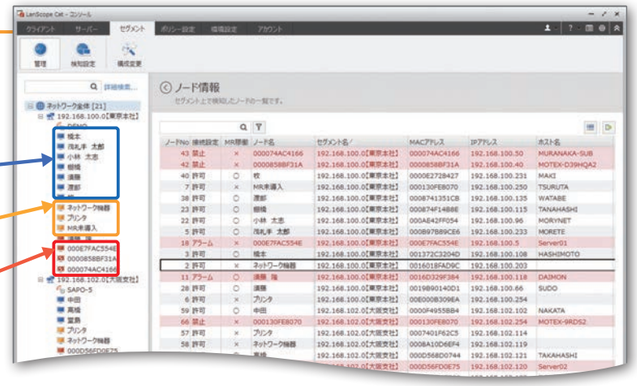
ネットワーク上の機器を検知し、不正な接続を遮断します。

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。



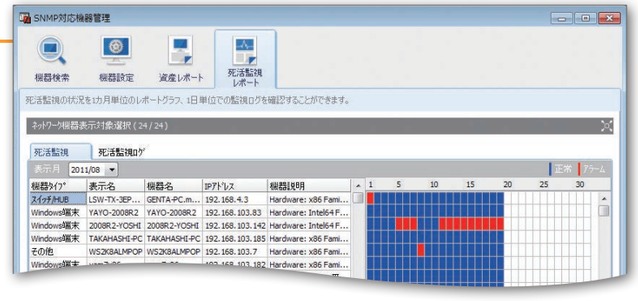
Catだけのゾーン管理

- **Aゾーン：Cat導入環境**（自動で許可）
  LanScope Catを導入している環境
- **Bゾーン：社内PC**（任意で許可）
  会社に必要なネットワーク機器
- **Cゾーン：不正PC**（自動で遮断！）
  LanScope Cat 未導入環境

※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

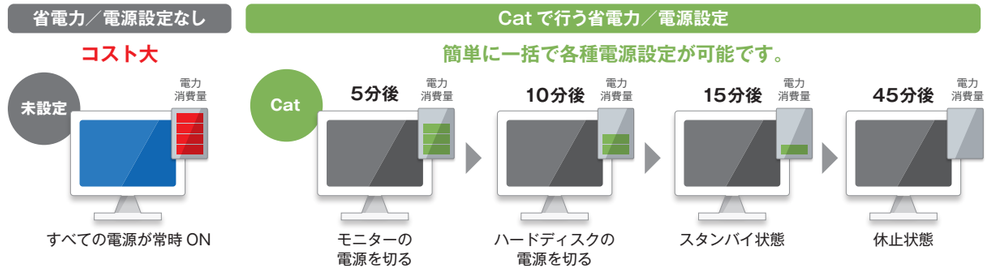
機器	取得可能な情報
共通	●機器タイプ ●MACアドレス ●IP アドレス ●機器名 ●機器説明
プリンター	●ベンダー ●型番 ●タイプ ●インク色数 ●インク色 ●最大用紙サイズ ●給紙トレー数 ●累計印刷枚数 ●印刷枚数 ●状態 ●エラー状態
ルーター	●転送速度
スイッチ／Hub	●ポート数 ●転送速度
端末（Windows／Linux／Mac）	●NIC 名 ●OS バージョン ●プラットフォーム ●メモリサイズ ●ドライブ数 ●メディアタイプ ●ドライブ ●全容量 ●空き容量 ●ソフトウェア情報

• 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。Cat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。

電源／省電力管理

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。

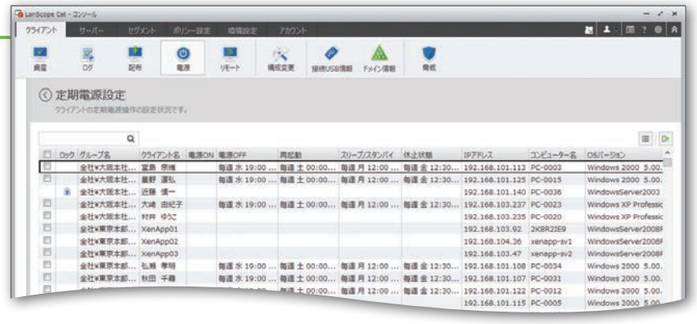
PCを指定時刻に強制OFFし、利用時間のルールを徹底できます。また、Wake On LANを利用したリモート電源ONや、無操作状態のPC、モニター、ハードディスクを指定時間経過後に電源OFFなど、無駄な電源コストを削減できます。



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。



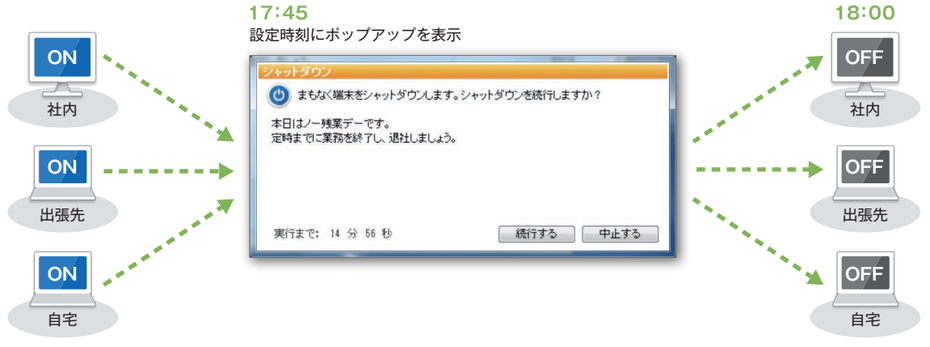
Pick Up New

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。

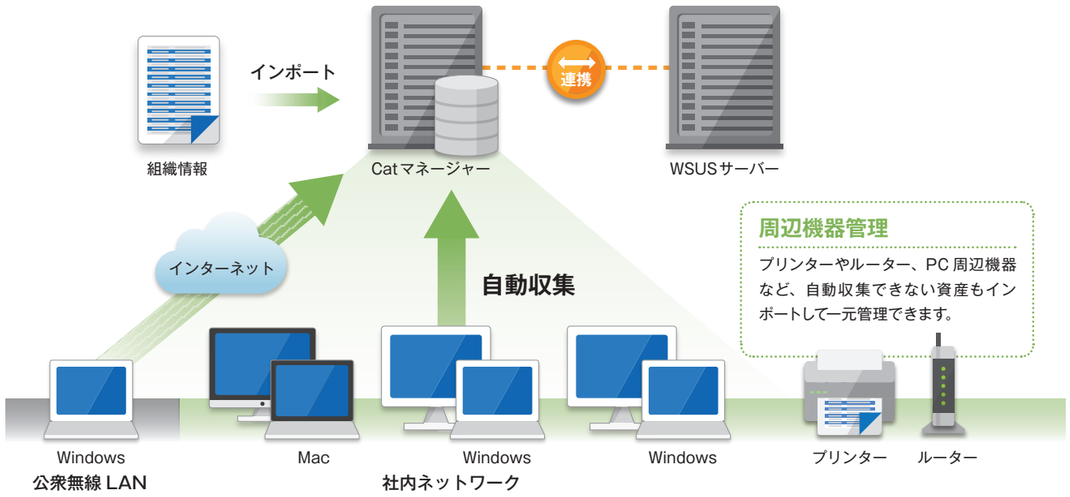


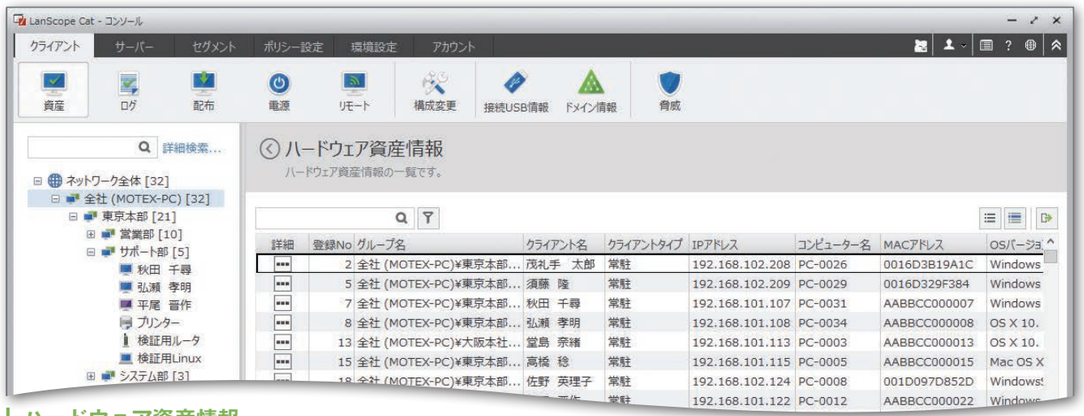
IT 資産管理

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			
● 管理サーバー No.	● 登録日	● メディアタイプ 1～26	● デフォルトゲートウェイ 1～3
● 登録 No.	● OS バージョン	● ドライブ 1～26	● BIOS バージョン
● フルネーム（表示名）	● CPU タイプ	● 全容量 1～26	● マシン名
● ログオンユーザー名	● CPU クロック数	● 空容量 1～26	● マシンベンダー
● IP アドレス 1～3	● メモリサイズ	● NIC-A ～C	● マシンシリアル
● MAC アドレス	● Windows Product ID	● モデム	● LAN 形式 1～3
● ドメイン名（ワークグループ名）	● ドライブ数	● SCSI	● プロセッサ数
● コンピューター名	● Windows サービスパック	● サブネットマスク 1～3	● CPUコア数
● ホスト名	● IE バージョン	● DNS サーバー	
● グループ No.	● IE サービスパック	● セカンダリDNS サーバー1～3	

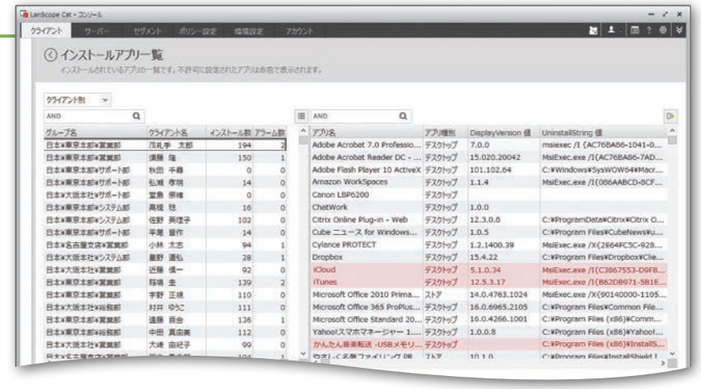
編集可能な項目	
● クライアント名	● 導入形式（リース等の選択）
● クライアントタイプ	● 期限（リース期間等）
● E-mail アドレス 1～3	● 購入日
● 導入日	● 資産 No.
● 部署名 1～5	● 外付けハードディスク
● 機種名	● CD-ROM
● 購入先	● MO ドライブ
● 導入責任者	● メモ欄
● 導入金額	● 任意項目 1～200

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 An 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。



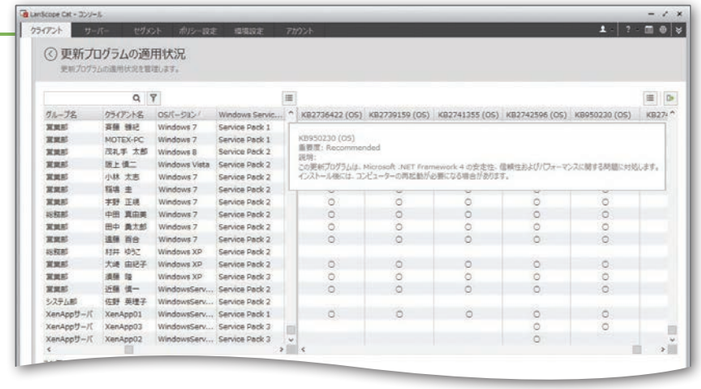
Mac端末管理

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、未適用端末に一斉配布・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斉適用できます。



WSUS連携

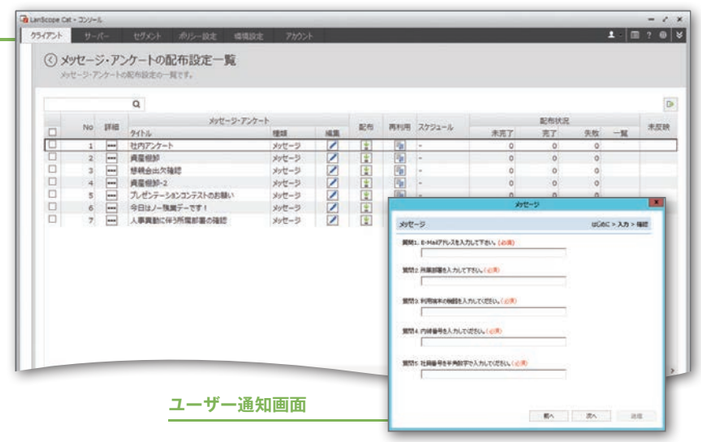
WSUSと連携し、Windows Updateの自動更新／手動更新の設定を一括で変更できます。また、更新プログラムの説明や重要度などの属性情報を確認し、重要度の高い更新プログラムが未適用の端末を発見できます。

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



User's Voice

もう行かなくても大丈夫！自席にいながら、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…Cat 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。入力形式を選択式に規制し、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

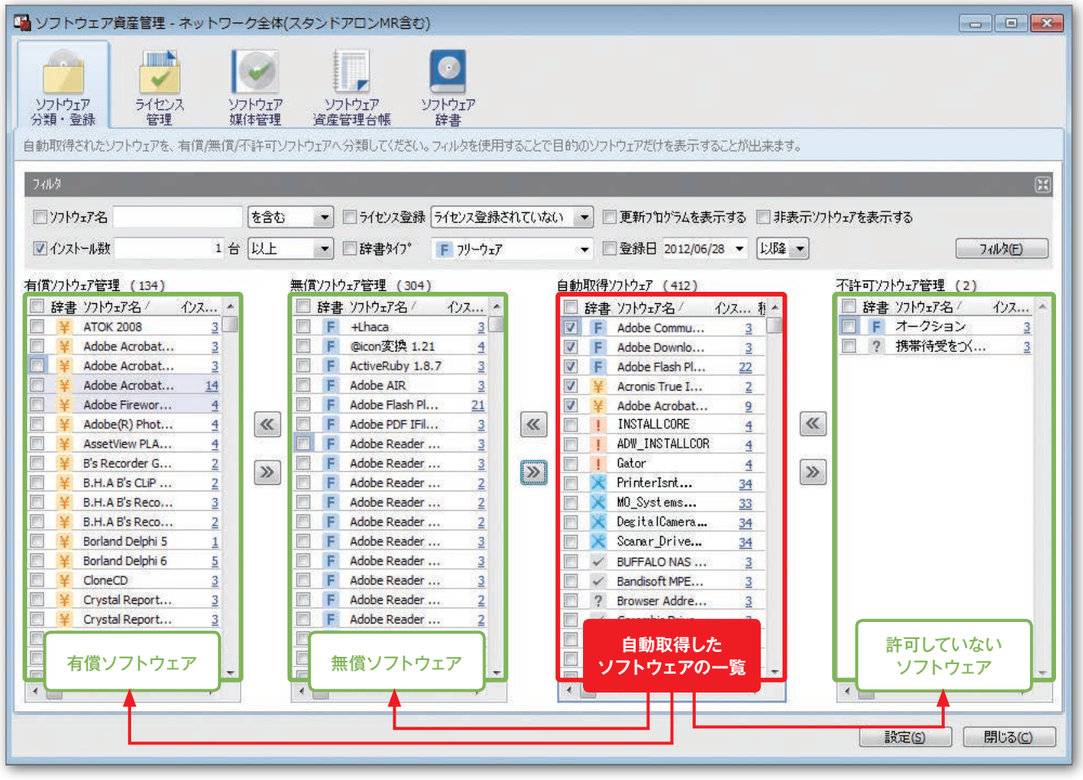
ソフトウェア辞書で有償／無償を自動分類し、管理対象を選定。

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

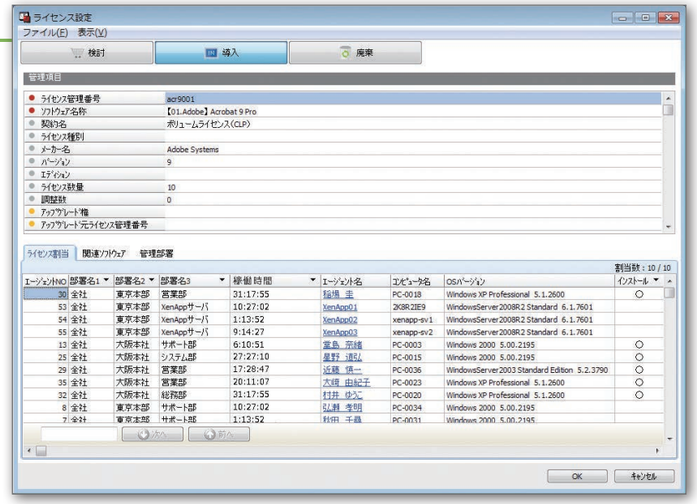
- ? 辞書未登録（手動登録可能）
- ¥ 有償ソフトウェア（有料）
- F 無償ソフトウェア（無料）
- 更新プログラム（セキュリティパッチ）
- ! アドウェア
- ドライバー／ユーティリティ
- その他

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、プレインストール）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ー数、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。

Microsoft Partner
Gold Software Asset Management

User's Voice

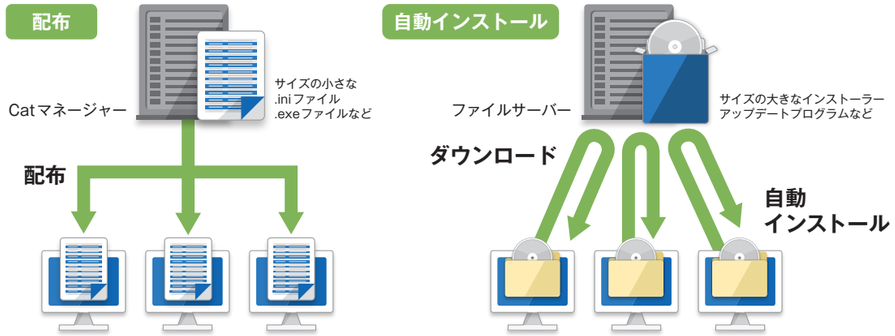
たった２ヶ月で完了！ライセンス調査対応の作業工数を約80%削減。

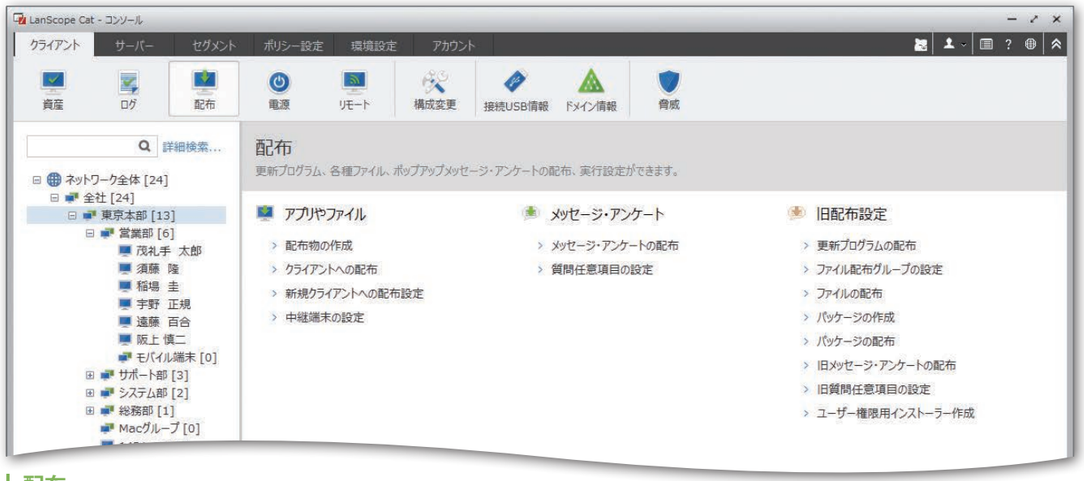
メーカーから「ライセンス調査依頼」がきたのですが、拠点は 40 以上、PC は 1,200 台、ソフトウェアは 130 種類以上と、どこから手をつけていいのか分からない状況に。Cat を導入して「ライセンス過不足チェックサービス」を実施し、1年以上はかかる作業をたった２ヶ月で完了できました。

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

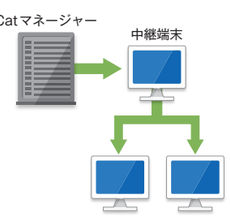
アプリやファイル、更新プログラム、メッセージ・アンケートの配布／実行ができます。
また、配布物に応じた独自の配布グループ作成や、パラメーター付きの実行など、柔軟な設定ができます。

Pick Up

ネットワークに負荷をかけずに配布する仕組み

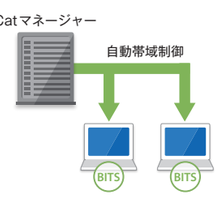
中継端末経由のアプリ配布

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）

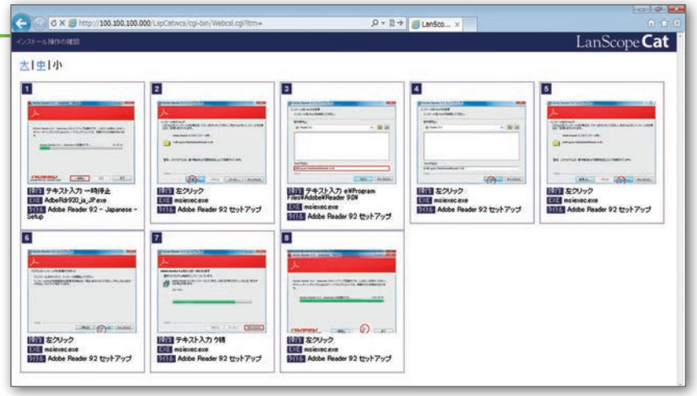
ネットワーク負荷をかけないように、自動的に帯域制御を行います。また、レジューム機能により、ダウンロード中にPCがシャットダウンされても、次回起動時に前回の続きからダウンロードを再開できます。



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。

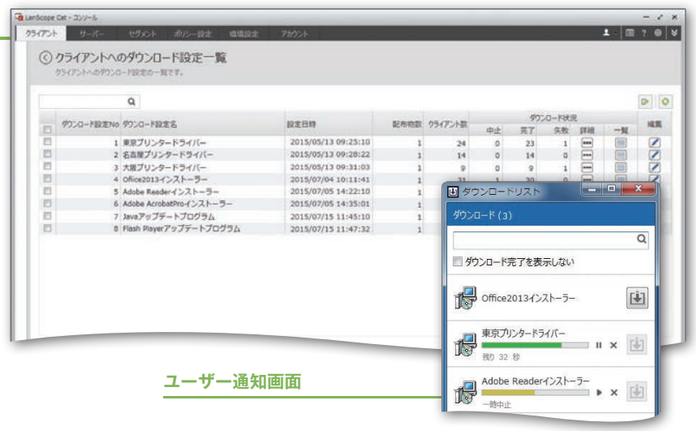
配布アプリ例

- 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。

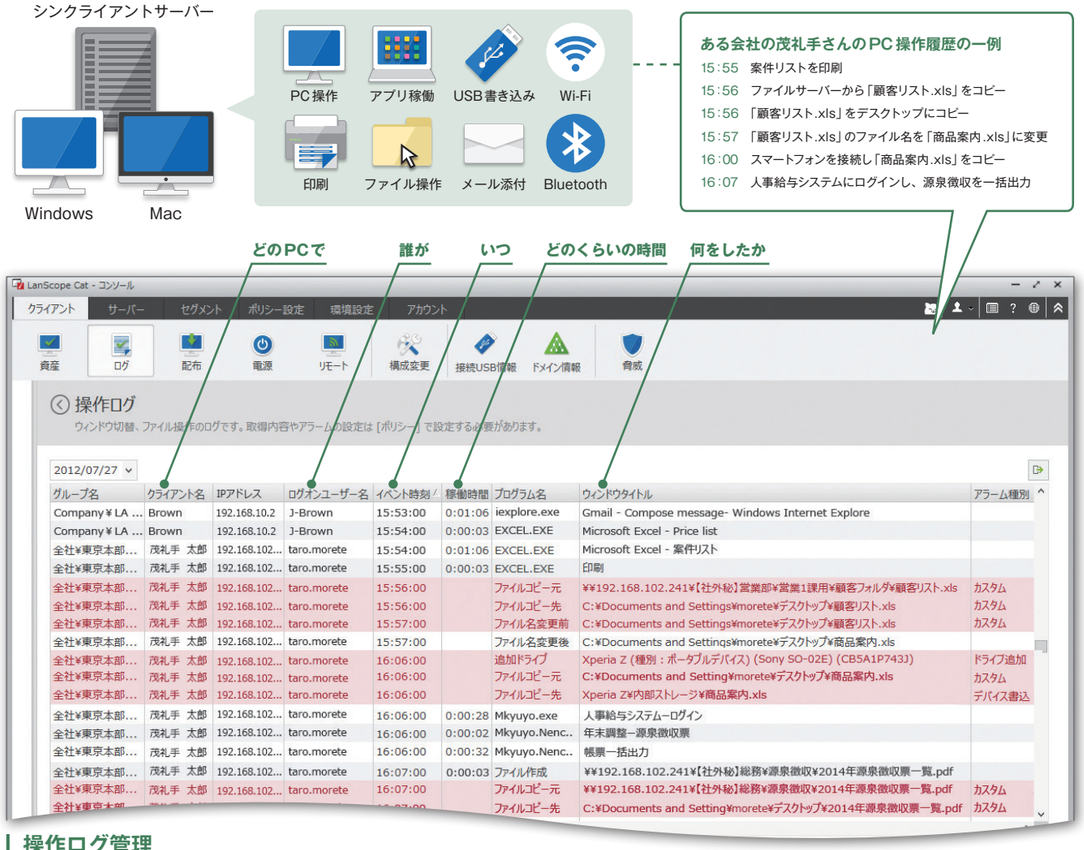
Catの導入前は、1台ずつソフトウェアのアップデートをしており、月に75時間、年間900時間もの工数がかかっていました。ファイル配布機能は、サイレントで完了できるので、ユーザー側に手間をかけず、こちらも配るファイルを設定するだけなので、大きな工数削減になっています。

操作ログ管理

V バーチャルキャット対応　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。



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 Cat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。

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。

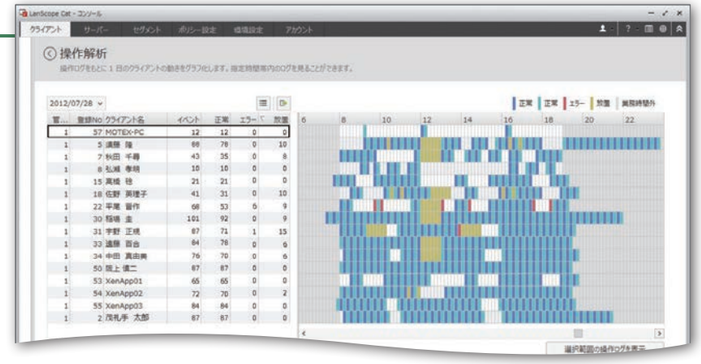
青色 正常な稼働状態です。10分間に1つでも操作が発生した場合は青、水色が交互に表示され、操作が発生しなければ青または水色を連続して表示します。

水色

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。



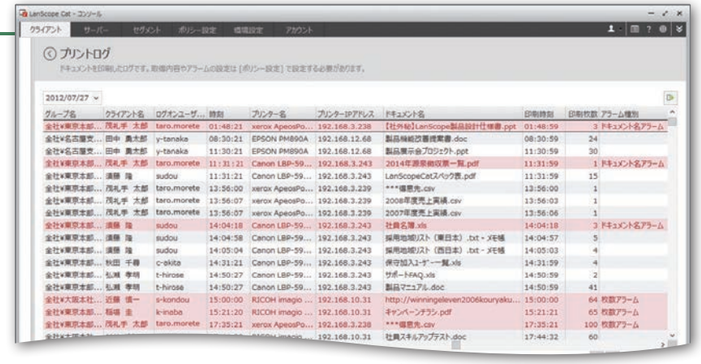
印刷履歴を記録し、機密データの印刷や無駄な印刷を把握できます。

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。

New プリントイメージ（オプション）

実際に印刷されたファイルの中身を確認することができます。また、ファイル名だけでなくファイルの中身も含めて検索が行えます。



・プリントログはWindowsのシステムログから取得しています。
・プリントイメージは専用ライセンスの購入が必要です。

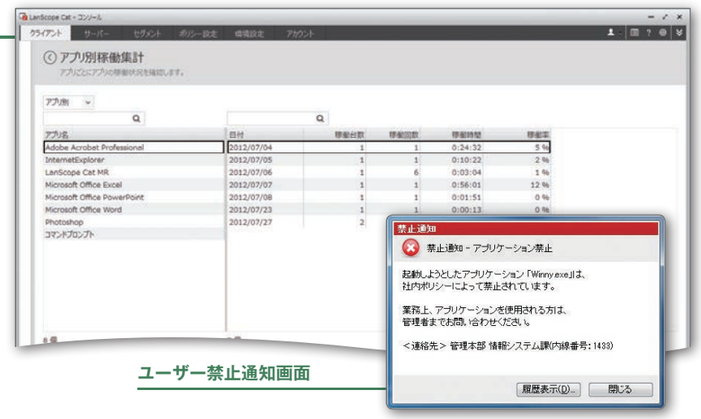
使われていない不要なライセンスの発見や、不正アプリの禁止ができます。 ※Mac端末管理非対応

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。



ユーザー禁止通知画面

User's Voice

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

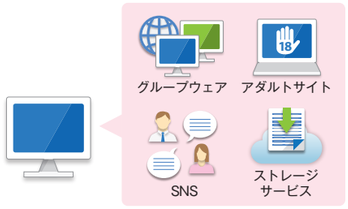
V バーチャルキャット対応
※クライアントWebフィルタリングは未対応です。

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

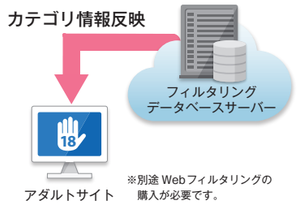


インターネットの閲覧状況を把握

Step2 キーワード制御

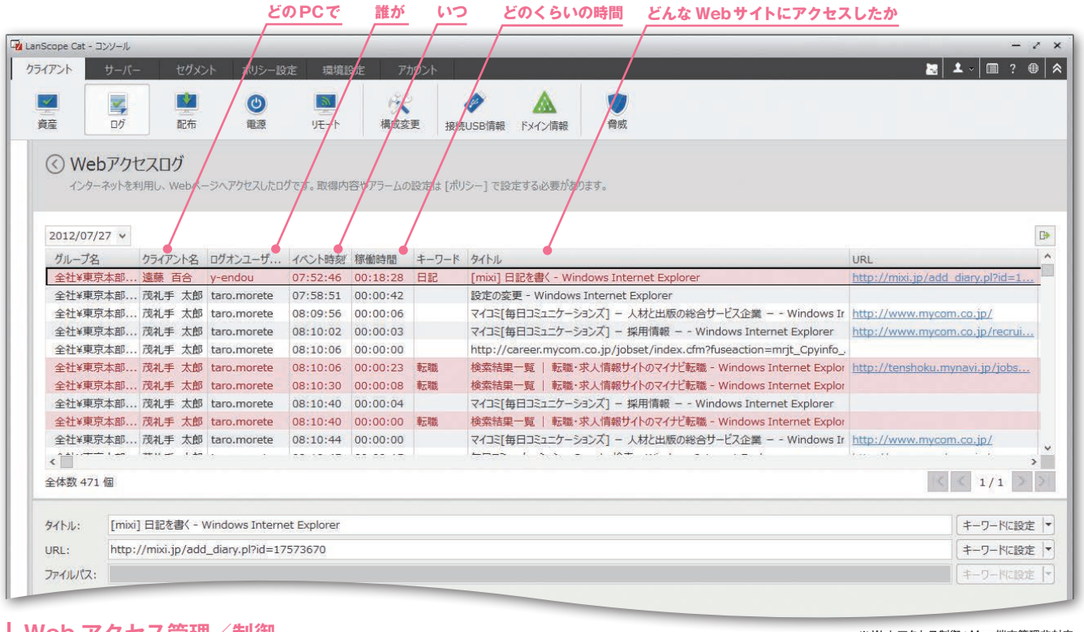
キーワードを登録すると、
不正サイトの閲覧を禁止

Step3 フィルタリングデータベース制御



※別途Webフィルタリングの購入が必要です。

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アクセス制御：Mac端末管理非対応

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。

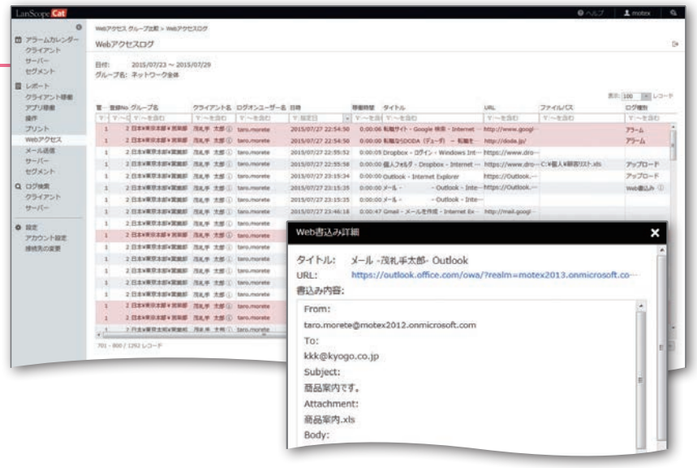
クラウドストレージ／Webメール利用ログ

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
- G Suite
- Office365

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
	グロテスク	政治活動・政党
出会い	話題	広告
金融	成人嗜好	未承諾広告
ギャンブル	オカルト	ニュース
ゲーム	ライフスタイル	

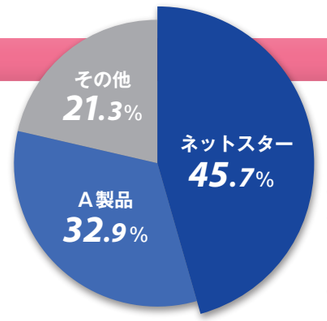
※別途Webフィルタリングの購入が必要です。
※Mac端末管理非対応

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
31億2191万コンテンツ
（2017年10月16日現在）



Webフィルタリングツール
市場占有率（2015年度）※

※出典：富士キメラ総研「2016 ネットワークセキュリティビジネス調査総覧」
（OEM製品［トレンドマイクロ社 InterScan WebManager など］を含む）

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。

Cat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Cat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るので大丈夫ですが、Catは何かがあったときの保険のような存在です。

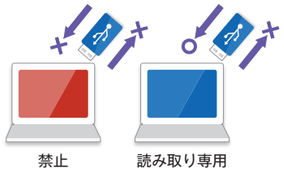
デバイス制御

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。

Step1 基本設定

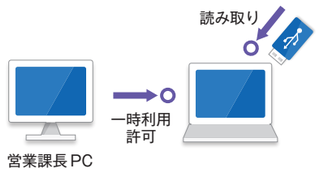


端末ごとに禁止／制限を設定

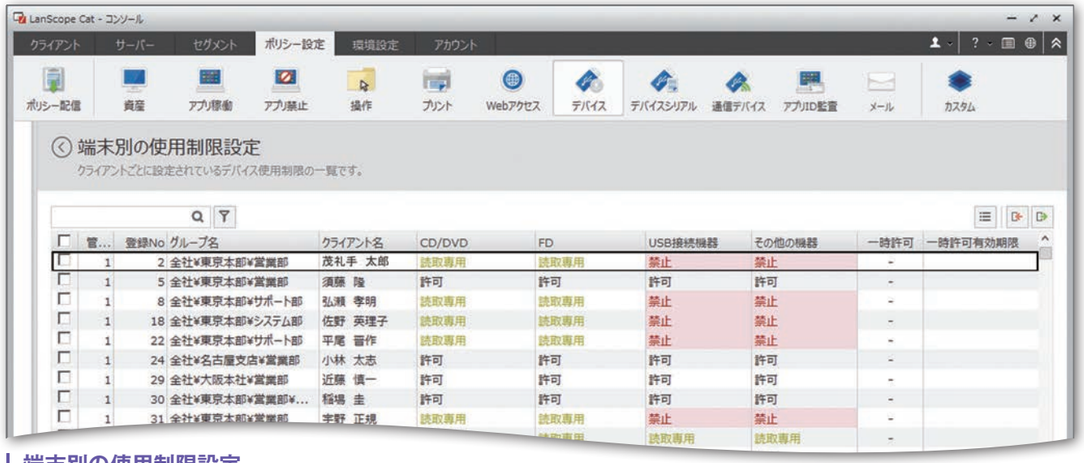
Step2 ホワイトリスト

特定のUSBメモリのみ利用可能

Step3 分散運用



部署内でデバイスの運用



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。

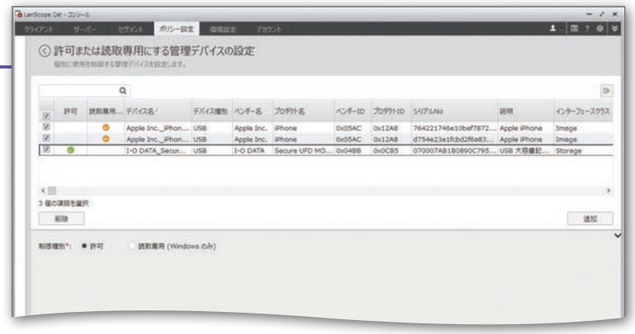
暗号化USBメモリなど、特定のデバイスだけを利用許可できます。

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にでき、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

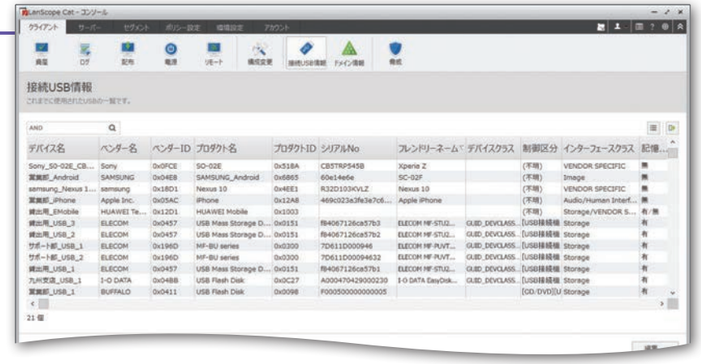
SD カードなど個体を識別する番号のないデバイスに対しても個別に許可／読み取り専用／一時許可／一時読み取り専用の設定が可能です。



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

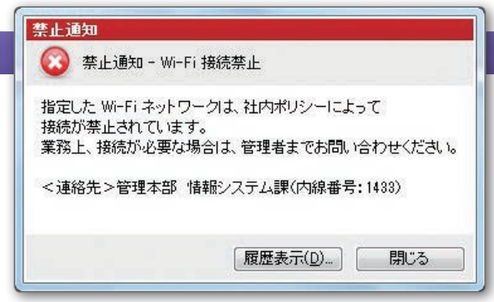
デバイス責任者設定

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 アドレスごとでの 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

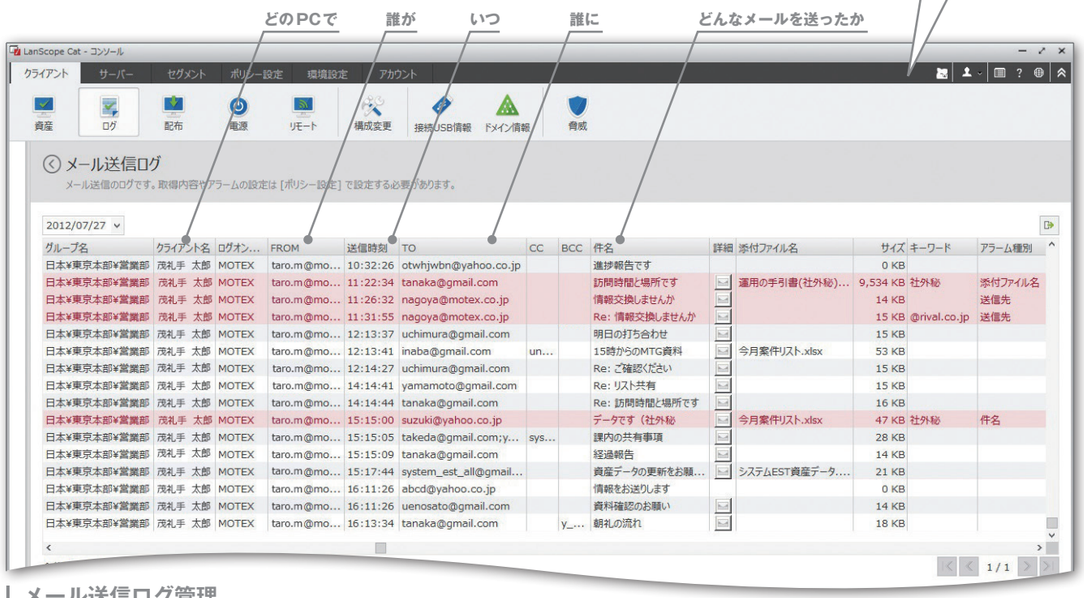
紛失／盗難は一つもありません！私物 USB メモリの利用も完全シャットアウト。

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、Cat 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。

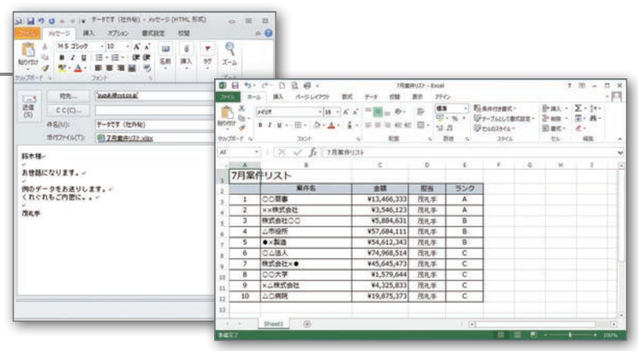


メール送信ログ管理

「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

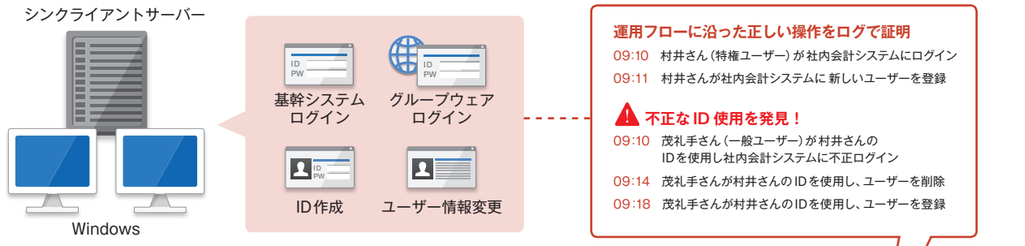
メールファイルをログからワンクリックで呼び出し、メールの本文や添付ファイルの確認ができます。

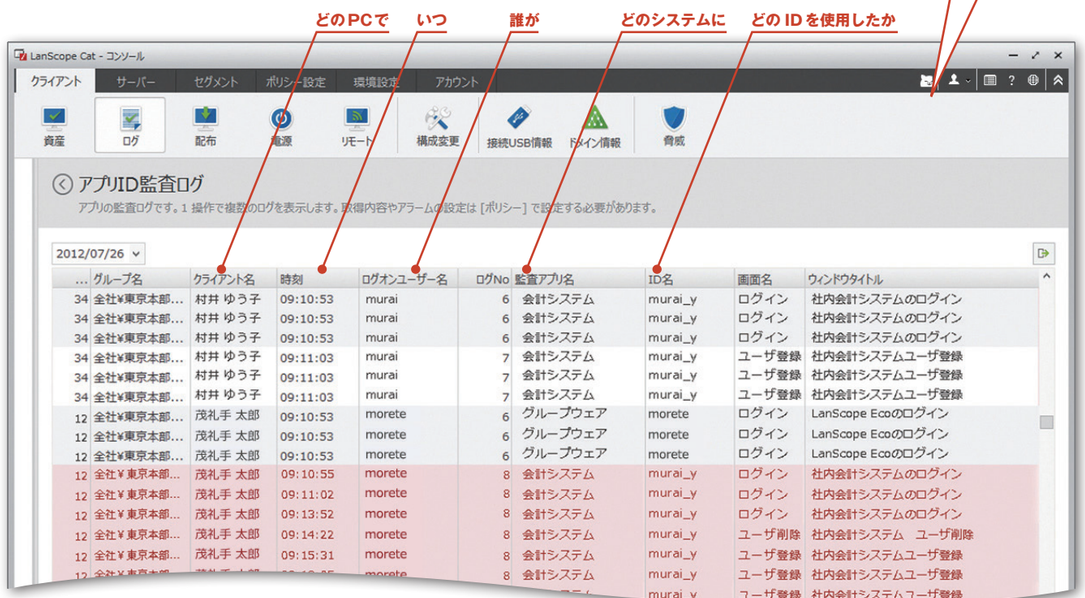


アプリID監査 V バーチャルキャット対応 ※専用ライセンスの購入が必要です。

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。

User's Voice

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。

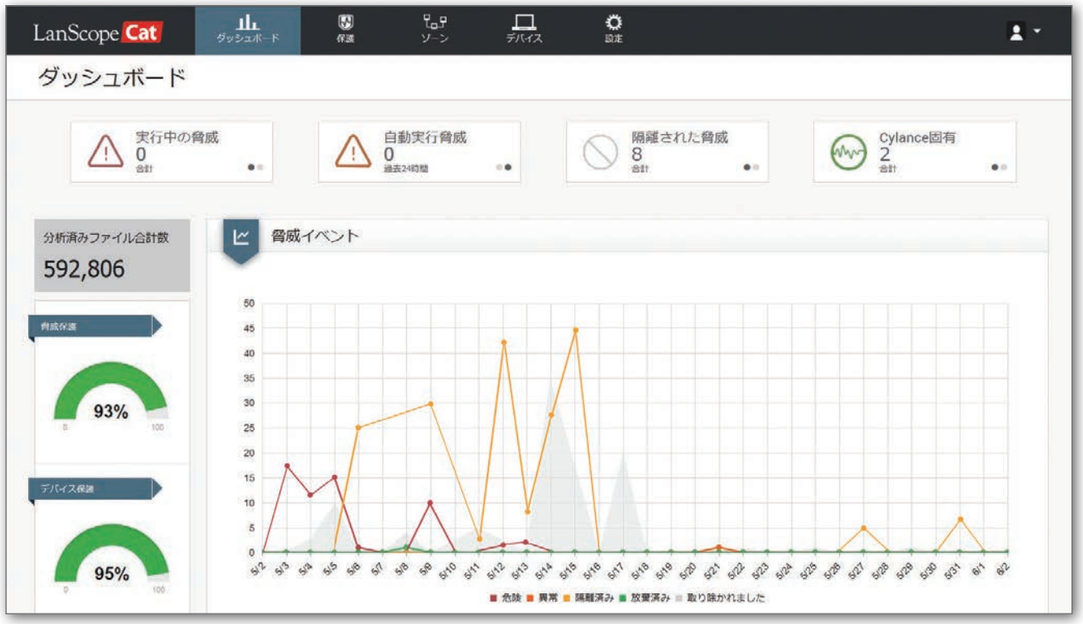
グループウェアや CRM、業務システムなどの各システムに対し「どの PC で」「いつ」「誰が」「どの ID でログインしたか」を収集し、不正なログインがないかを監視しています。人や日時などの条件でログ検索し、複数システムにまたがった利用状況確認ができるようになったのは大きな成果です。

マルウェア対策 New

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

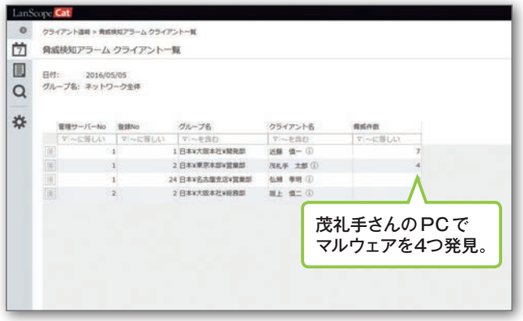
実行／自動実行されている脅威の数、隔離した脅威の数、Cylance社のみが発見した脅威数の合計値と24時間以内の件数が確認できます。検知したマルウェアを、危険／異常／隔離済みに分類しレポートします。管理者はマルウェアの詳細内容を確認した上で、許可するか、隔離するかを選択できます。また、マルウェア検知状況を脅威／ゾーン（任意で設定した端末のグループ）／端末に分けて確認し、どこにセキュリティリスクがあるかを把握できます。

マルウェア／エクスプロイト対策機能

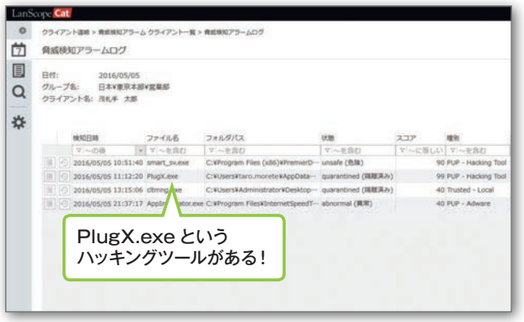
ファイルアクション	危険なファイル、異常なファイルを AI が検知し自動隔離することでマルウェアの実行を防ぎます。 また、検出したファイルをクラウドにアップロードし、詳細な分析を行い、危険性を判定するための情報をフィードバックします。
メモリアクション	OS のメモリ上で稼動中のプロセスを監視し、脆弱性の悪用やメモリ上で動作するほかのプロセスを利用した攻撃／権限昇格を検知し、攻撃が成功する前にブロックします。
スクリプト制御	Office 製品のマクロ実行や PowerShell や VBScript、JScript などのスクリプト実行の検知やブロックを行います。

Step1 カレンダーで脅威の有無を確認。

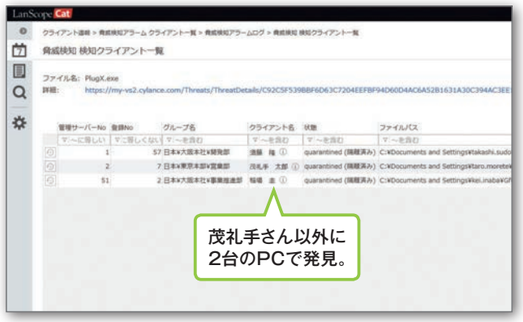
Step2 どのPCで何件の脅威があったかを確認。



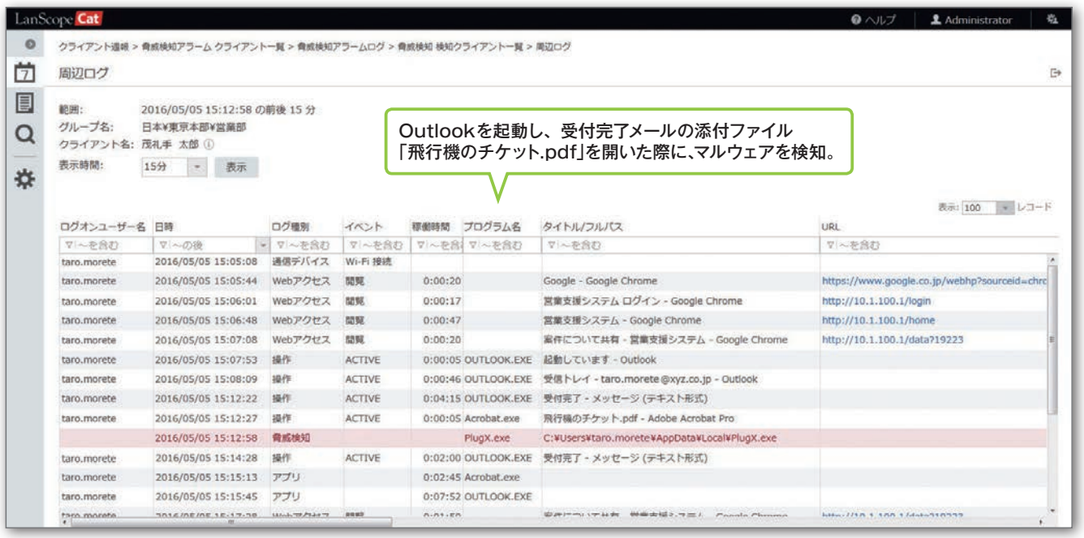
Step3 どんなマルウェアを検知したかを確認。



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。

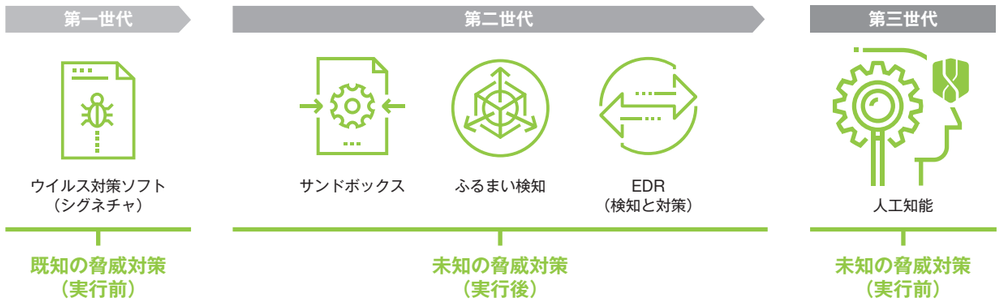
User's Voice 事後対策の限界により事前対策へ方針転換！未知のマルウェアも感染前に隔離。

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。

LanScope Cat は、CylancePROTECT® をOEM搭載　「プロテクトキャット Powered by Cylance」

特長 ① AIエンジンを活用したAIアンチウイルス

プロテクトキャットは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。

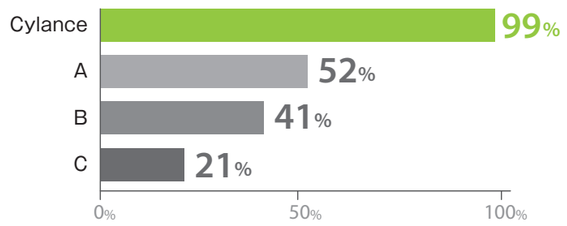


特長 ② マルウェア検知率99%以上※を実証

※2018 NSS Labs Advanced Endpoint Protection Test 結果より

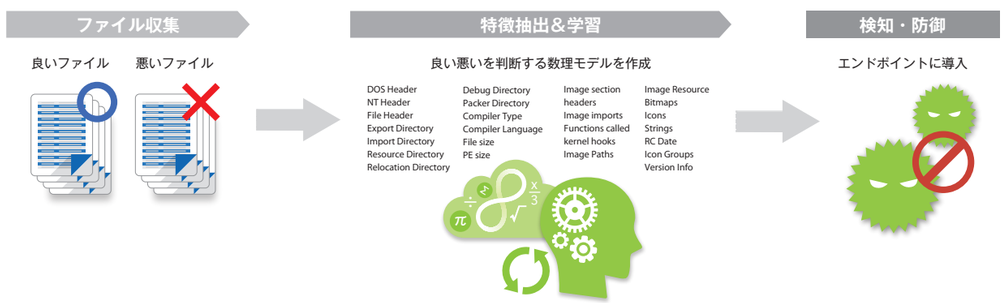
全米75都市でアンビリーバブルツアー開催。

- 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
- Cylance 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（2016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。マルウェアか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。

マルウェア実行制御

- AI（人工知能）で脅威を予測
- マルウェアの実行を阻止
- シグネチャ不要
- 毎日のスキャンが不要
- ファイルシステム変更時にスキャン
- 潜在的に望ましくないプログラムが環境に侵入するのを拒否

メモリ保護

- メモリの悪用防御
- 脆弱性攻撃の防御
- プロセスインジェクション防御
- 特権昇格の防御
- シェルコード／ペイロード攻撃の防御

スクリプト制御

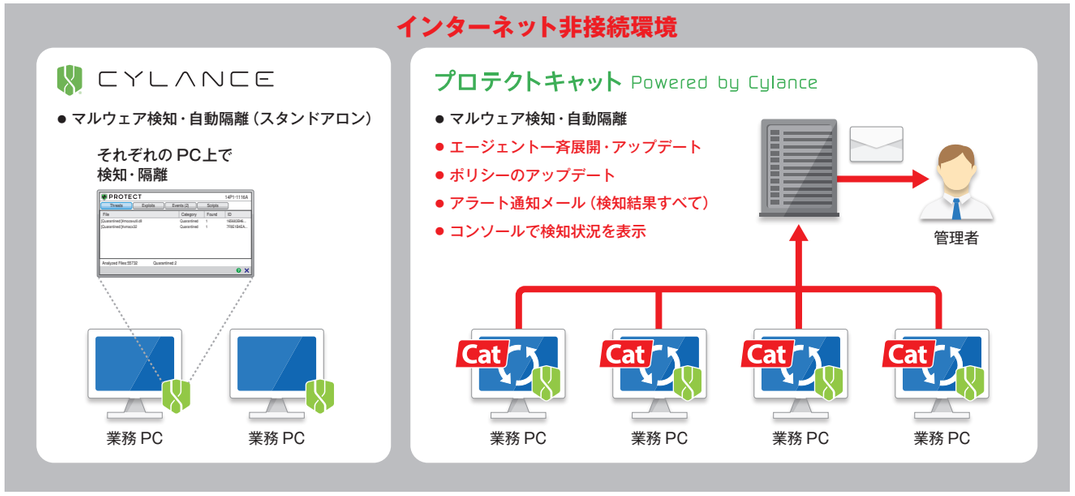
- 不正なパワーシェルとアクティブスクリプトの制御
- 危険なVBA／マクロを制御
- ファイルを残さない攻撃の阻止
- 危険なドキュメントファイルの制御

アプリケーション制御

- 機器で利用する機能を限定して利用バイナリを制御
- 不正なバイナリの実行を阻止
- 任意のバイナリの変更を防止
- Windows の変更は許可

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 Cat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

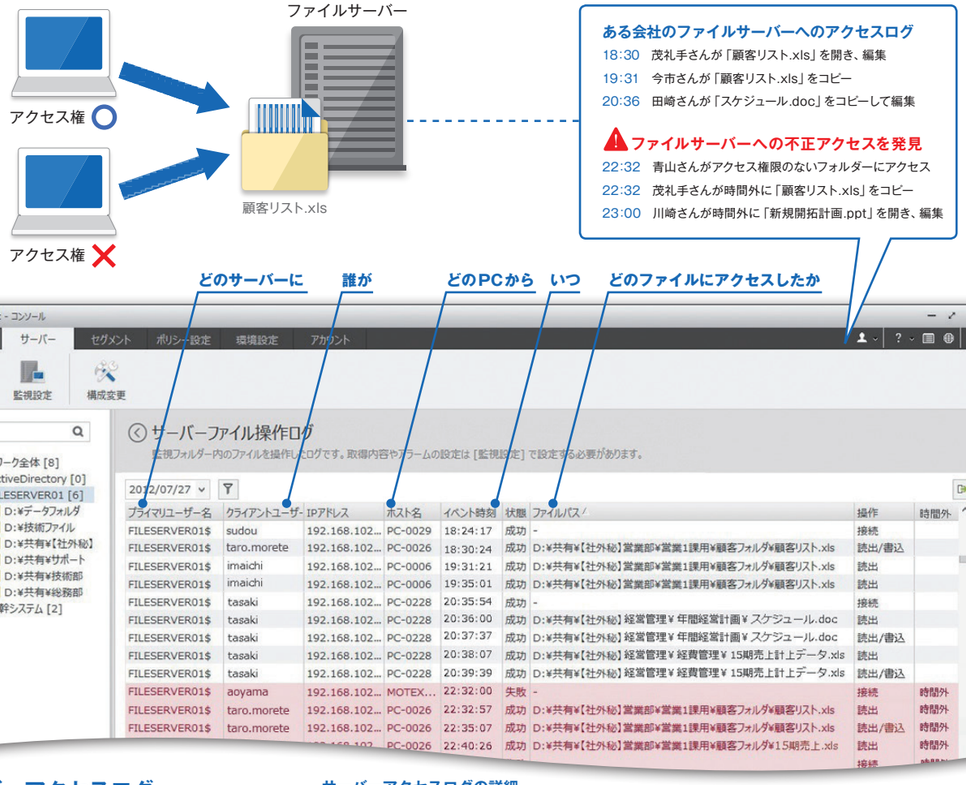
「Cylance Japan Partner of the Year」を２年連続受賞

エムオーテックスは、Cylance Japanの「2017 Japan Partner of the Year」を受賞しました。
これにより、MOTEX は国内販売実績２年連続の No.1 獲得となります。MOTEX は今後もサイランス ジャパンとのパートナーシップを深め、より付加価値の高い製品・サービスの提供を通じて、お客様のセキュリティ課題解決に貢献してまいります。

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跡として活用できます。

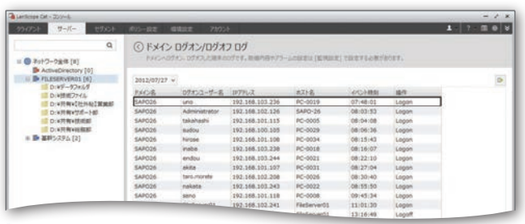


サーバーアクセスログ

「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、コンピューター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。

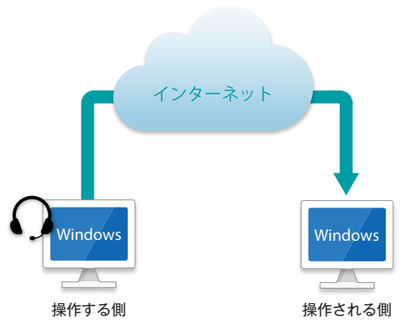
リモートコントロール ISL Online

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。

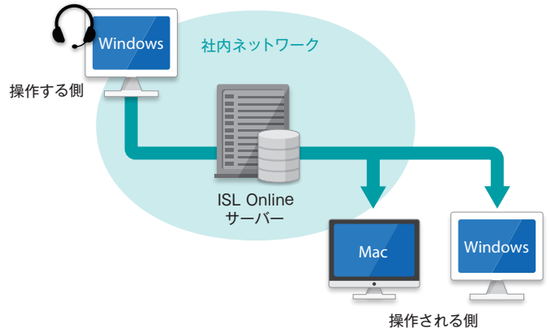
リモート操作やWeb会議により、業務の効率化を実現します。

リモート操作で、ヘルプデスク業務やメンテナンス作業を効率化し、解決率と満足度を向上させます。また、遠隔地のメンバーとのWeb会議で、コミュニケーションの活性化を図ることができます。システム構成は、クラウド版かオンプレミス版かを選択できます。

クラウド　サーバーを設置／構築する必要がなく、インターネット経由で低コストかつ簡単に利用できます。



オンプレミス　専用線／ VPN などで接続されたLAN 内に限定した接続が可能です。



ヘルプデスク（ワンタイム型）

遠隔サポートが必要な人にワンタイムパスワードを入力させるだけで、すぐにリモート操作が開始できます。インストールすることなく、簡単にヘルプデスク業務に活用できます。

リモート操作画面

ライセンスは同時に接続する分だけ

購入が必要なライセンスは、管理者の数や管理端末数ではなく同時接続数となります。例えば、管理者が5人で管理端末が100台あっても、同時接続数が1であれば、1ライセンスの購入となります。

リモートアクセス（常駐型）

常駐モジュールをインストールした PC やサーバーに対し、管理者がパスワードを入力するだけで、リモート操作が開始できます。夜間や休日などのメンテナンス作業に活用できます。

Web会議 ※Mac 端末管理非対応

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。離れた拠点や出張先からも会議に参加できるので、交通費の削減やコミュニケーションの活性化に役立ちます（同時 1 接続につき PC10 台まで参加できます）。

リモートコントロール管理一覧

デスクトップ共有	デスクトップ画面を共有したり、見せたりすることができます。
アプリケーション共有	選択したアプリケーションだけを相手と共有することができます。
キーボード&マウス操作	キーボードとマウスの操作を相手に委ねることができます。
ファイル転送	ISL インターフェースにドラッグするだけで、ファイルやフォルダーを転送できます。
ホワイトボード（書き込みツール）	相手の画面にペンツール等で書き込み（マーキング）することができます。
チャット（テキスト・音声／ビデオ）	テキストチャットで会話することができます。ウェブカメラとヘッドセットを使用したビデオ通信が可能です。
画面拡大・縮小・カラー数変更	PC 環境に合わせて画面の拡大／縮小ができます。高画質画面から低速接続用の 8 色設定まで画面カラー数を変更できます。
セッション再接続	同じセッションを維持したまま再起動の実行が可能です。
レコーディング	セッション内容を記録した動画データを、オペレーターまたはクライアント PC 上に保存することができます。
ブラックスクリーンモード	オペレーターの操作内容を一時的にクライアントから見えないようにすることができます。
遠隔プリント	クライアント PC 上のファイルをオペレーターの PC に接続されているプリンターから印刷することができます。

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

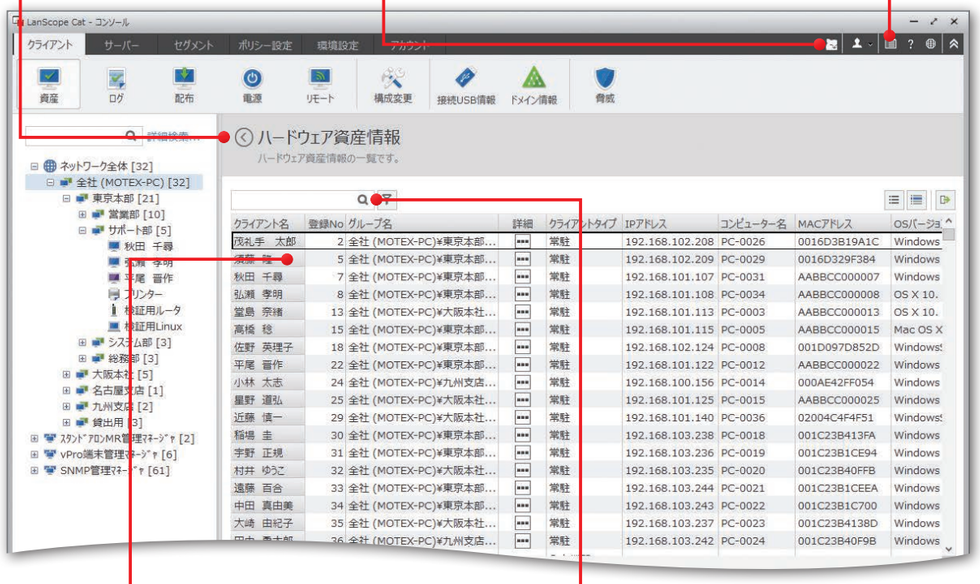
システム管理者の効率を重視した設定用のコンソール

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 この画面で何をするのか、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。

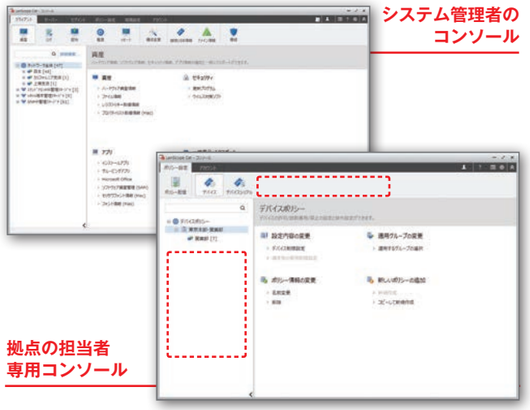


列の固定 列を固定し、Excel ライクに閲覧できます。

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ので、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オン・ログオフや閲覧内容、設定内容の履歴を保存できます。

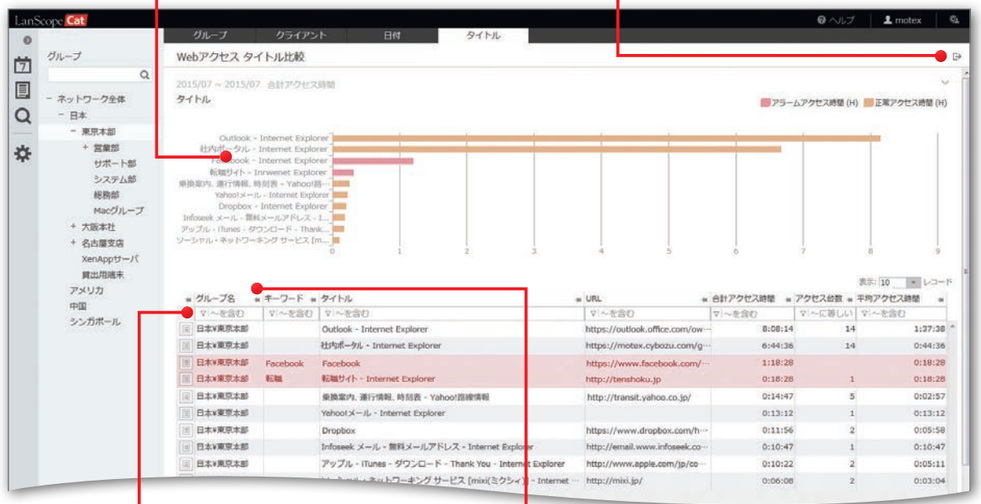


組織全体での運用を実現するWebコンソール

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。

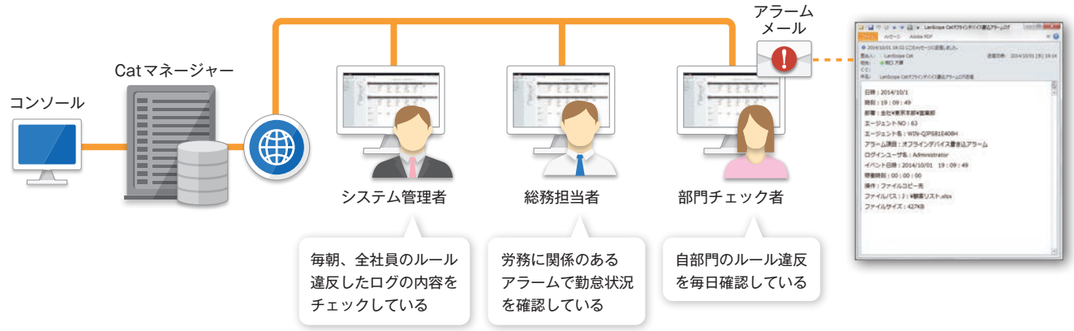


検索／フィルター すべての項目で、フィルターや検索ができます。

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。



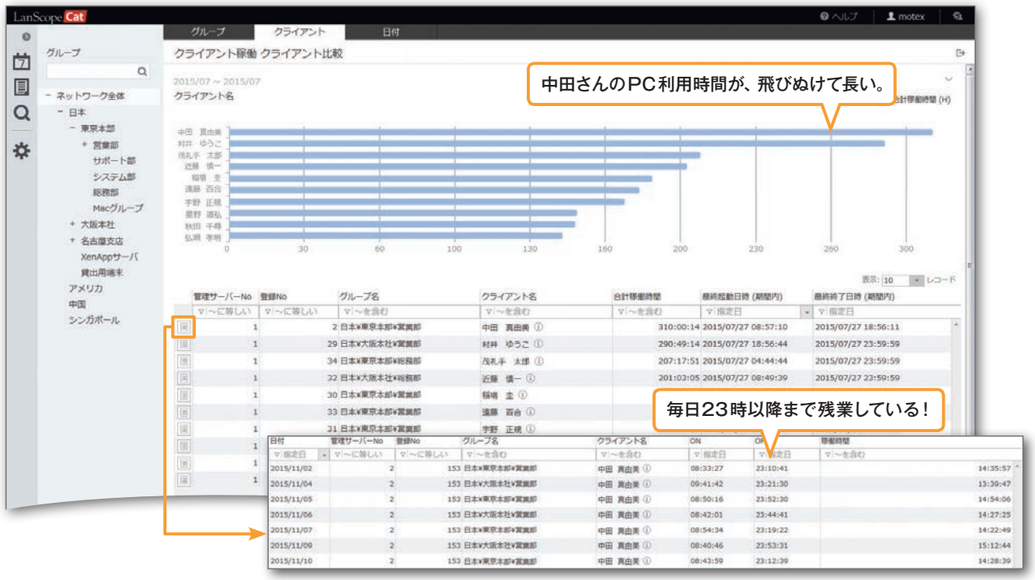
レポート －Webコンソール－

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。

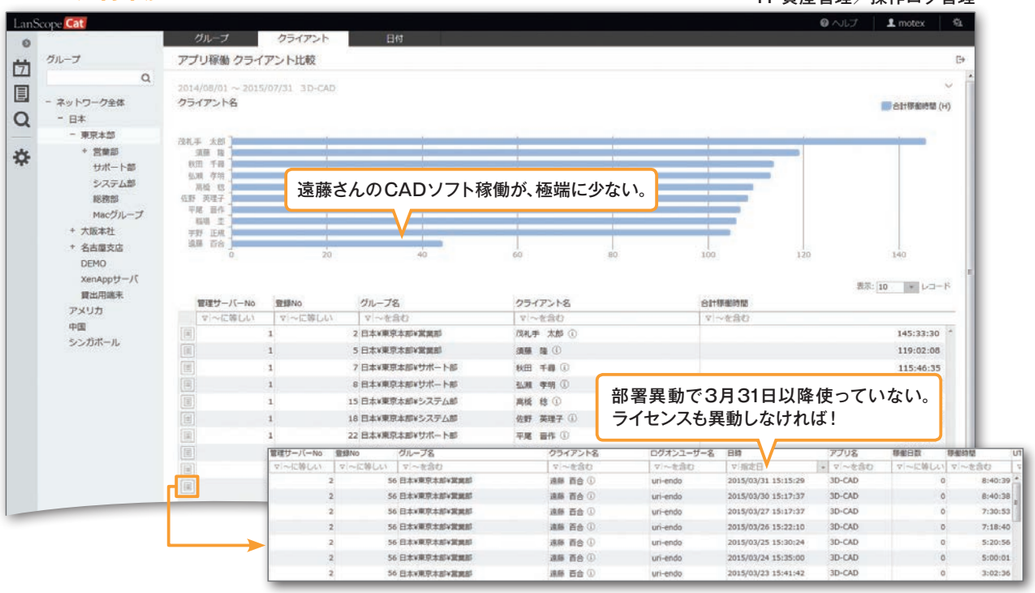
クライアント稼働 クライアント比較

IT 資産管理／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

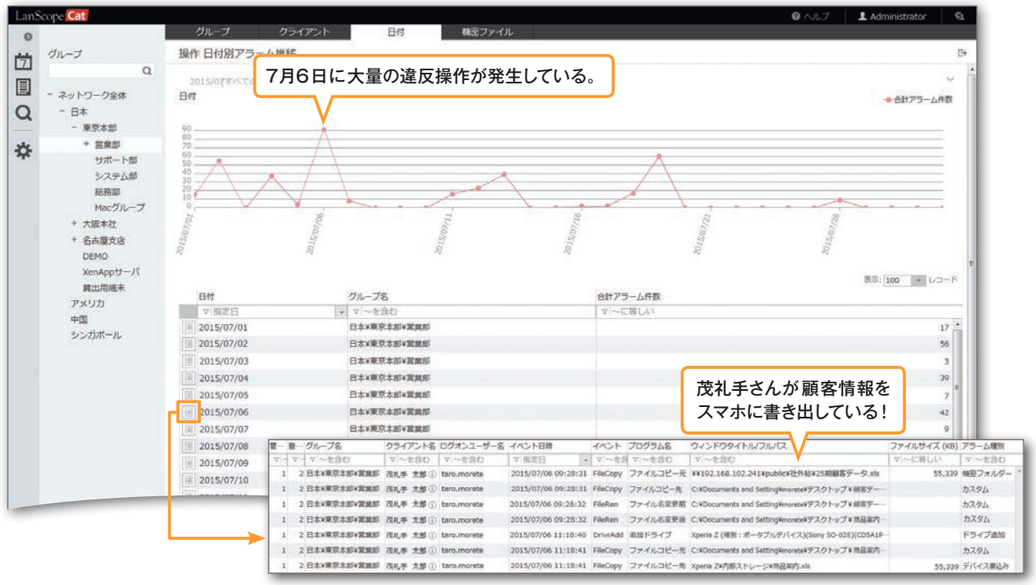


USB書き出しや印刷による情報漏えいリスクを把握できます。

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。

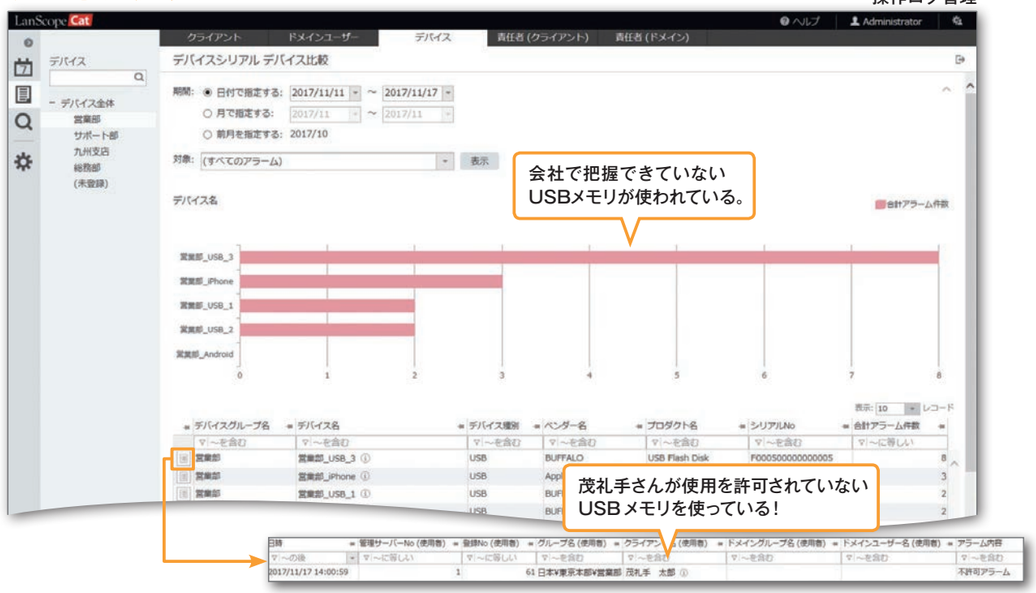
操作 日付別アラーム推移

操作ログ管理



デバイスシリアル デバイス比較

操作ログ管理

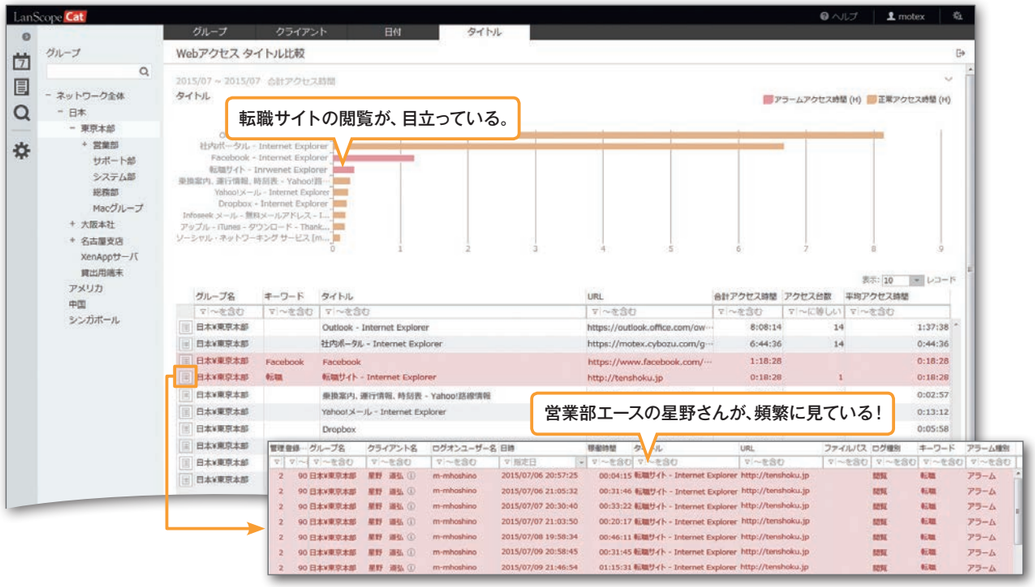


Webやメールが適切に活用されているか、分析できます。

社内ポータルの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。

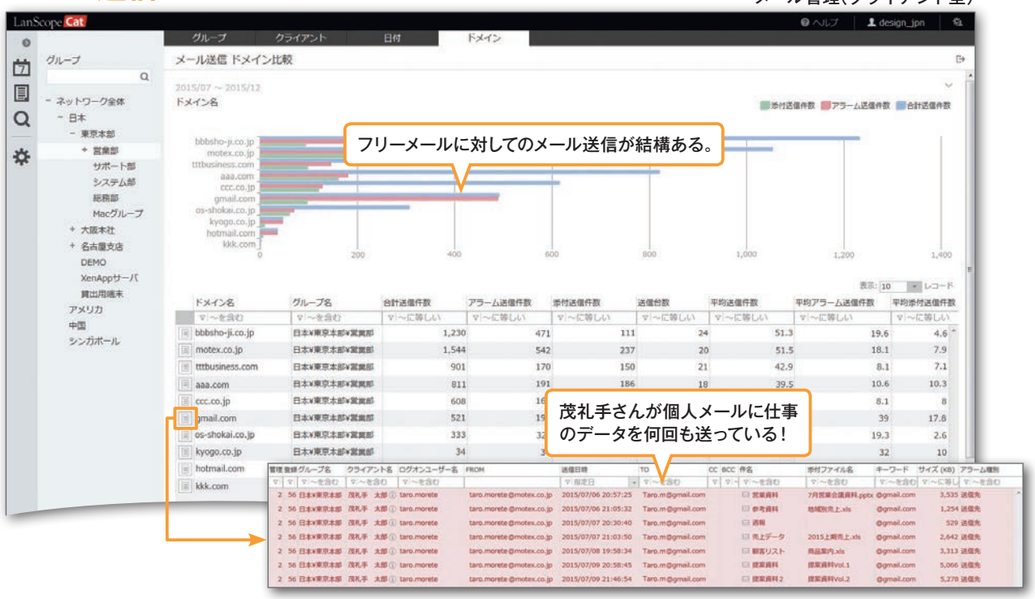
Webアクセス タイトル比較

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)

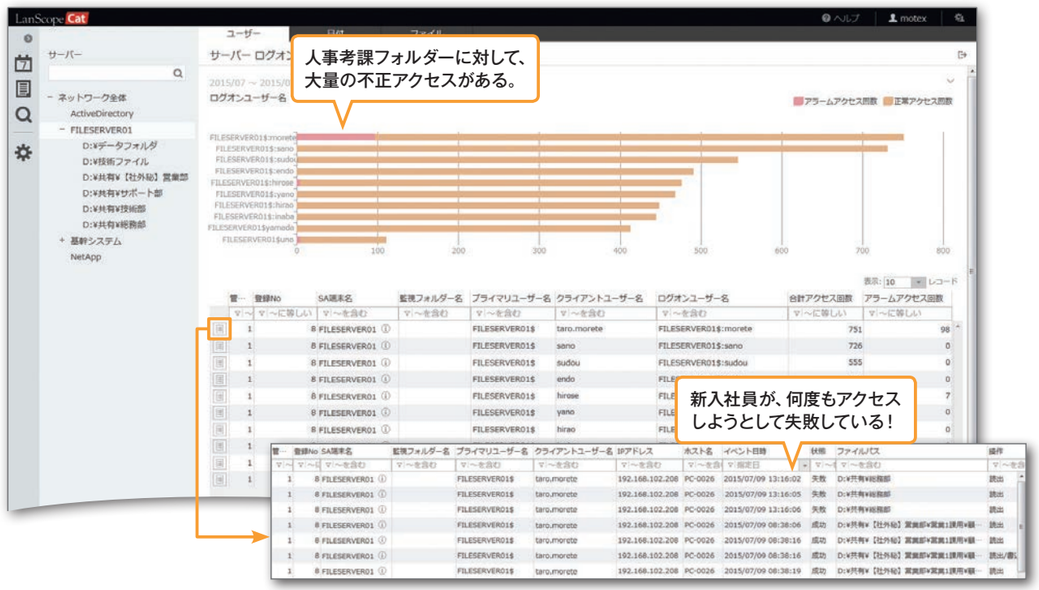


サーバーやネットワークへの不正なアクセスを発見できます。

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。

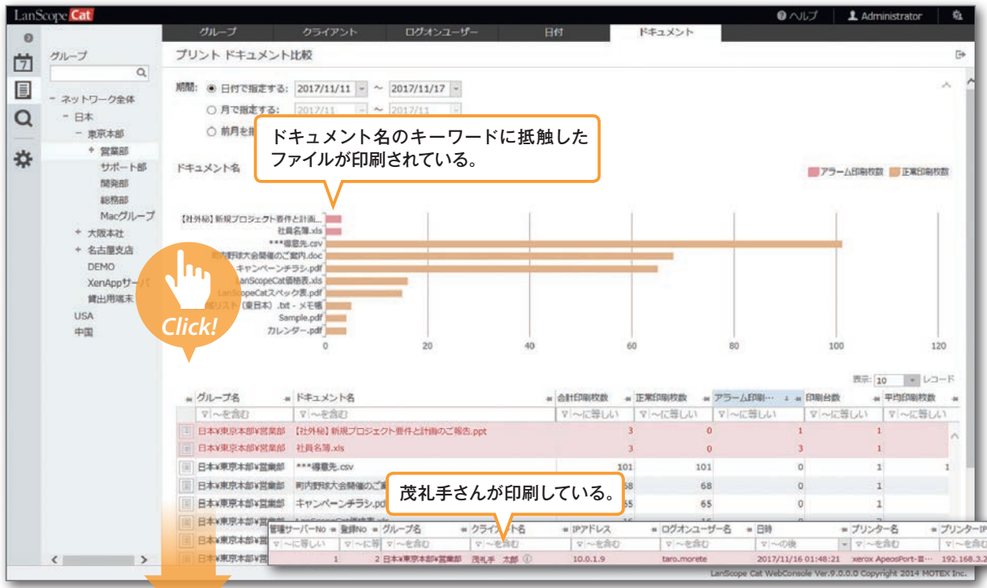
Excel データ出力

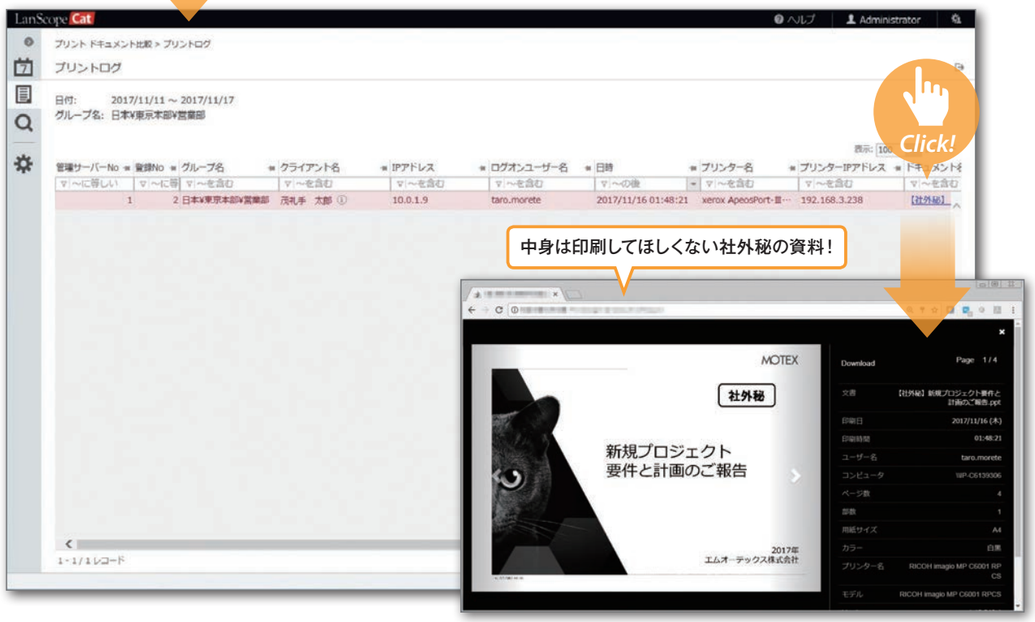
ワンクリックで、グラフと表数値のデータを連動させた形で Excel 出力できます。出力した Excel データを自由に加工して、高度なデータ検索／抽出ができます。

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



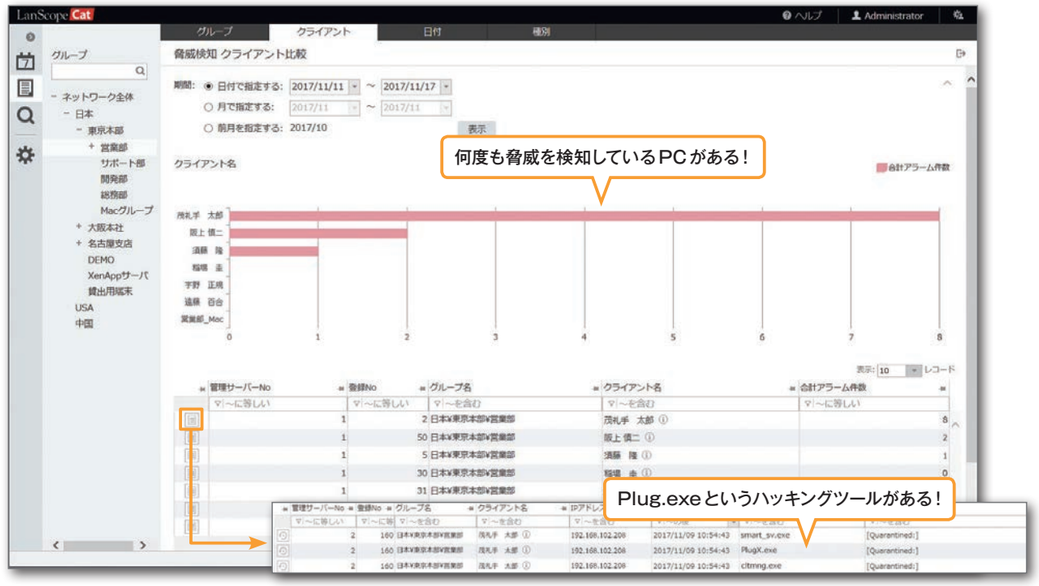


•プリントイメージは専用ライセンスの購入が必要です。

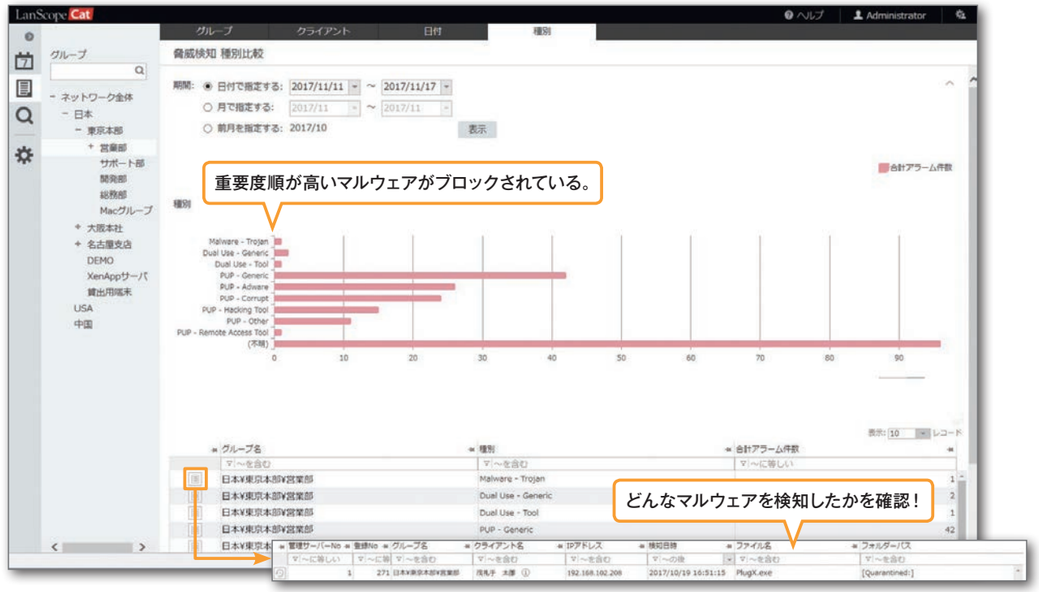
脅威検知

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、脅威の重要度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



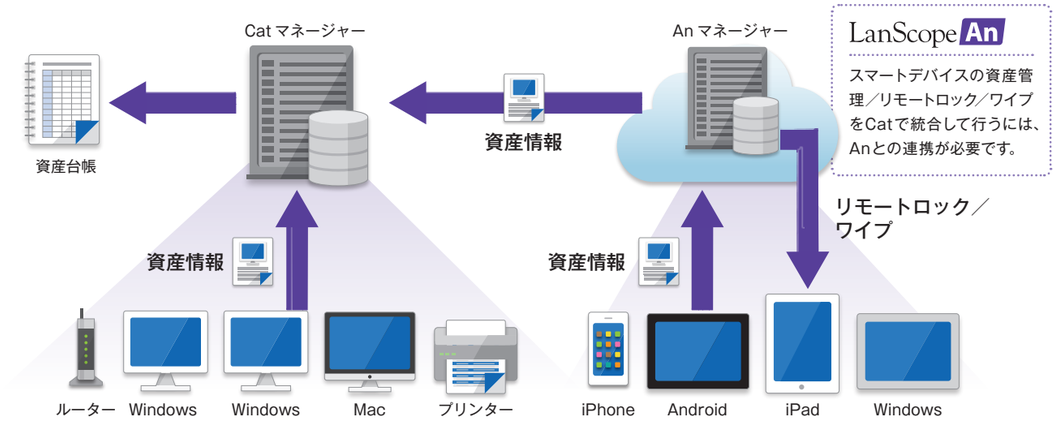
脅威検知 種別比較



スマートデバイス管理

スマートデバイスを、安全に業務活用できる環境をつくります。

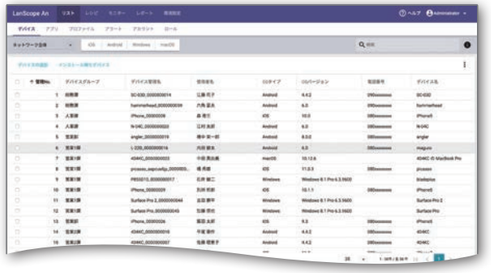
クラウドで、iOS／Android／Windows／macOS を一元管理できます。デバイス情報やアプリ情報の自動取得や盗難・紛失時にはリモートロック／ワイプができます。また定期的に位置情報を取得、デバイスの活用状況を見える化できます。



LanScope An
スマートデバイスの資産管理／リモートロック／ワイプをCatで統合して行うには、Anとの連携が必要です。

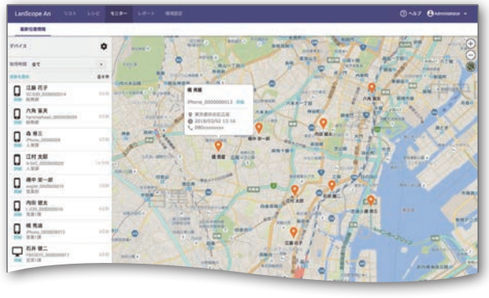
資産管理

デバイスの資産情報を自動で収集し、iOS／Android／Windows／macOSの混在環境や、複雑なOSバージョン管理の手間を削減できます。



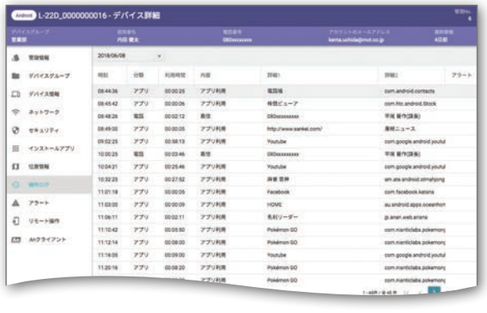
位置情報管理

最新の位置情報を地図上に表示し、複数デバイスの所在を一目で把握できます。また移動履歴を記録し、行動管理や紛失／盗難時のデバイスの発見に役立ちます。



操作ログ管理

スマホ／タブレットが利用されているか、操作ログを取得し、費用対効果を見える化できます。またAndroidであれば、アプリ毎の利用回数／時間も取得できます。



レポート

取得した操作ログや資産情報のデータからレポートを自動作成し、デバイスが本来の目的に沿って活用できているか見える化します。

User's Voice

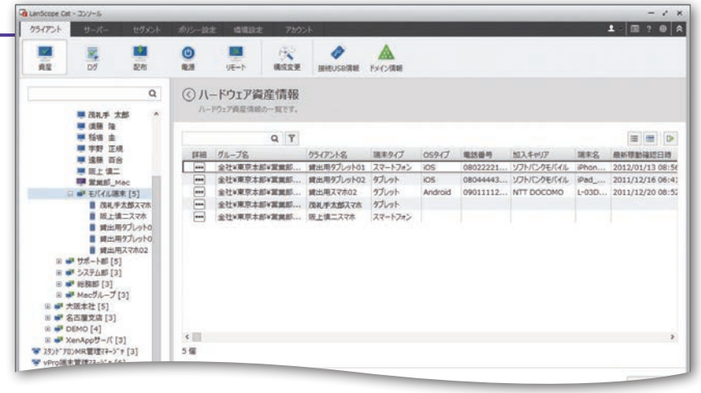
万が一の紛失、電源が OFF になっていると対策が打てない！でも、LanScope An なら…

営業担当者から紛失の連絡があり、探そうとキャリアに連絡しても既に電源が OFF に…An の導入後は電源 OFF になる前の位置情報を把握でき、付近の交番に届けられている端末を無事に発見。これまでに 2 台の紛失デバイスの発見につながっています。

PCとスマートデバイスの資産情報を、1つの画面でまとめて管理できます。

LanScope Cat 連携

An で収集した OS タイプ、OS バージョン、加入キャリア、Wi-Fi、MAC アドレスなど、スマートデバイスの資産情報を、Cat に自動取り込みができます。また、Catの画面で選択したスマートデバイスに対して、ワンクリックで An のリモートロック／ワイプ実行画面を呼び出せます。



24時間365日対応の紛失サポート窓口を利用できます。

24/365 紛失サポート（オプション）

紛失に気づいたのが深夜の場合など、会社と連絡が取れず対応が遅れると、情報漏えいのリスクが高まります。本サービスでは、24 時間 365 日利用できるお客様窓口の専門スタッフが代行してリモートロック／ワイプを実行します。休日や深夜の対応ができずにお困りの管理者様におすすめです。

Pick Up

LanScope An Free

紛失／盗難対策機能のみを無料でご利用できます。

パスワードポリシー

パスワードの桁数や、英字、数字、複合文字使用など、会社共通のパスワードポリシーをデバイスに一括で適用できます。（iOS、Android のみ対応）

リモートロック／ワイプ

万が一の際に、遠隔操作でデバイスの画面ロック、ワイプを実行できます。

拾った人の 96%がデータにアクセスしています。

User's Voice

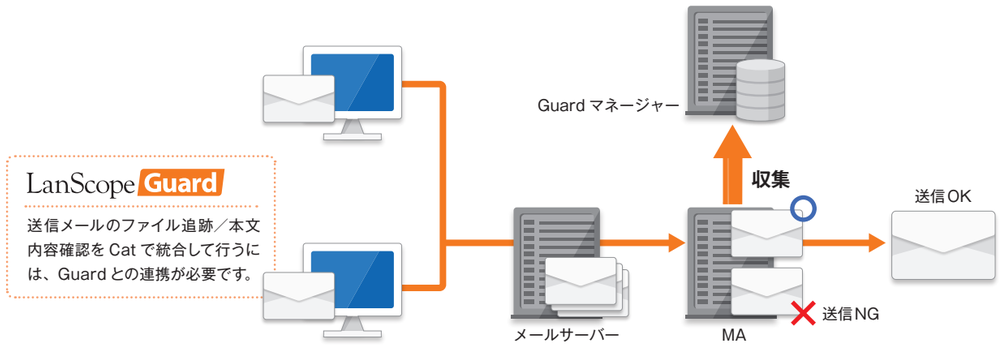
まずは最低限の対策！スマホのテスト導入時に紛失／盗難対策がしっかりできました。

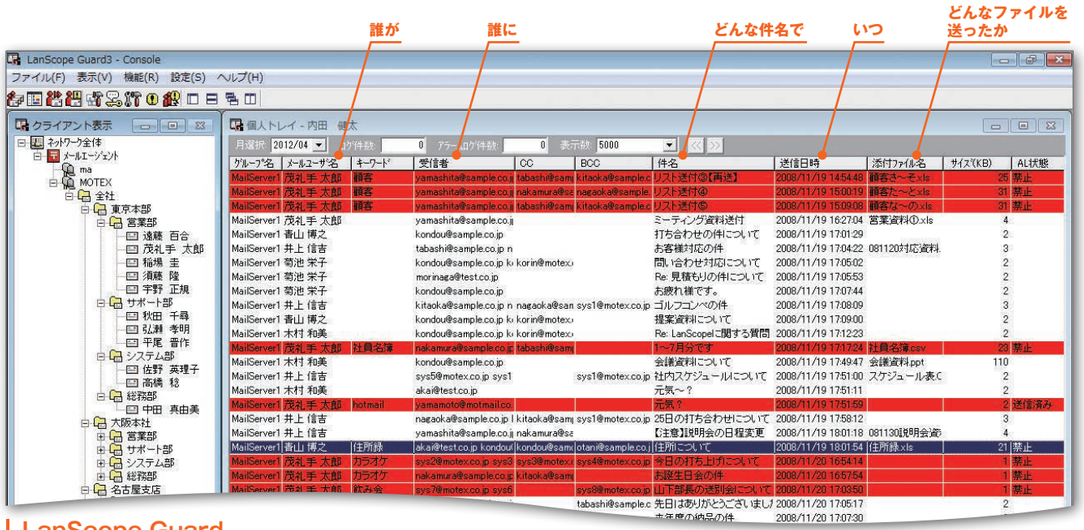
テスト導入なので管理ルールもなく、どこまで管理すべきかわからないため、MDM のツール選定に困っていました。An Free は、まず無料で最低限の紛失対策ができ、有償版へ移行すれば、今後検討していた資産管理やアプリ管理がそのままの環境で利用できるので安心して導入できました。

メール管理 ゲートウェイ型

送信メールを適切に管理し、機密情報の漏えいを防ぎます。

メールゲートウェイサーバーで送信メールの内容を記録します。機密ファイルの添付など違反メールは送信を禁止し、送信者と管理者にメールで通知できます。不正なメールの送信を抑止し、ユーザーのセキュリティモラルを向上させます。





LanScope Guard

「誰が」「いつ」「誰に」「どんな件名で」「どんなメールを送ったか」を記録できます。メーラーに依存せず、差出人／宛先（TO/CC/BCC）／本文／添付ファイルが把握できます。また、宛先や件名／メール本文が「顧客情報」などのキーワードに抵触したメールに対して違反通知をしたり、送信禁止にできます。

Pick Up

送信状況と状態を把握

ワイヤードリストは、社内から社内外へ送信の傾向を色別で表示します。社内の特定の人物が社内外へ送信するメールの実態を「赤」「青」「黄色」「白」で詳細に表示します。

▯ メールの送信がない ▮ 1通以上メールを送っている
▮ 定数以上メールを送っている※ ▮ 禁止（アラーム）メールを送っている

※値は任意設定が可能

ワイヤードリスト画面

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 Cat 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 Cat 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 Cat 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斉受信すると、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 Cat 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。
	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が条件です。
ハードウェア資産管理	古い端末など DMI に準拠しない機種ではマシンシリアル、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。
	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。
アプリ管理・ソフトウェア資産管理	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。
	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。

2018年6月6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。

制限事項／注意事項

IT 資産管理

更新プログラム管理	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
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 Cat 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。
	モダン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。

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。
	デバイス書き込みアラームはリムーバブルディスクとポータブルデバイスに対する書き込み操作が対象です。外付け HDD に対する書き込み操作はアラームとなりません。
	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。
	ファイル閲覧ログは、OS の「最近使った項目」の情報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。
プリントログ	Windows8、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。
	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。
ログオン・ログオフログ	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 ／ Opera ／ Netscape ／ Sleipnir ／ Lunascape ／ Donut Q ／ Donut RAPT ／ unDonut+mod ／ 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。 タイトル : 対応ブラウザすべて URL : Internet Explorer ／ Google Chrome ／ Mozilla Firefox アップロード、ダウンロード、Web 書き込み : Internet Explorer ・アップロード、ダウンロードの禁止は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。
	Office365、G Suite、Dropbox ではログの取得はできますが、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 Web App、Gmail の送信メールで、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、Windows 8 モードで起動した場合は、ログ取得対象外です。 ・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
	Office365 の Outlook Web App 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。
	Windows 10 の Internet Explorer を利用した場合や、Internet Explorer を管理者権限で実行した場合、クラウドストレージへのアップロード、Web 書き込みログが取得できません。
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。

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 ・モジュールベイの 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。
	UASP 機器と認識されるデバイスは、禁止設定をしても禁止されません。 読み取り専用にすることは可能ですが、VID ／ PID ／シリアル No. で個別許可することはできません。
	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。
デバイスシリアル管理	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。
通信デバイス制御	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、パ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。

2018年6月6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。

制限事項／注意事項

メール管理

メール送信ログ管理	メール送信ログは Outlook 2007／2010／2013／2016 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。

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（CylancePROTECT 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（CylancePROTECT 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（CylancePROTECT 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 環境下に導入する場合、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。
vPro リモコン	vPro テクノロジーで接続する場合の条件は以下のとおりです。 ・インテル ® vPro™ テクノロジーに対応し、デュアルコアのインテル ® Core™ i5 vPro™ プロセッサーおよびインテル R Core™ i7 vPro™ プロセッサーを搭載している ・グラフィックコントローラがプロセッサーに内蔵されたシステムである ※上記システムであってもグラフィックカードを追加した場合は利用できません。また、無線 LAN 経由での接続は行えません。

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、許可設定をしてい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 ～ 8.3 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。
	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	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。

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 ～ 7.6、NEC：VirtualPCCenter4.1、Amazon： Amazon WorkSpaces 【SBC 方式】　VMware：Horizon6.2 ／ 7 RDSH、Citrix：XenApp5.0 ～ 7.6、 Microsoft：Remote Desktop Service（Windows Server 2008 R2 ／ 2012）
	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）。
	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。
アプリ制御	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。
Webフィルタリング	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。
デバイス制御	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。

2018年6月6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。

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 Cat 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 Cat 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 Cat 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 Cat 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 Cat 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\inetsrv\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】 回避方法はありません。

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 Cat 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 Cat 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 Cat 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 Cat 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 Cat 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 Cat 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。

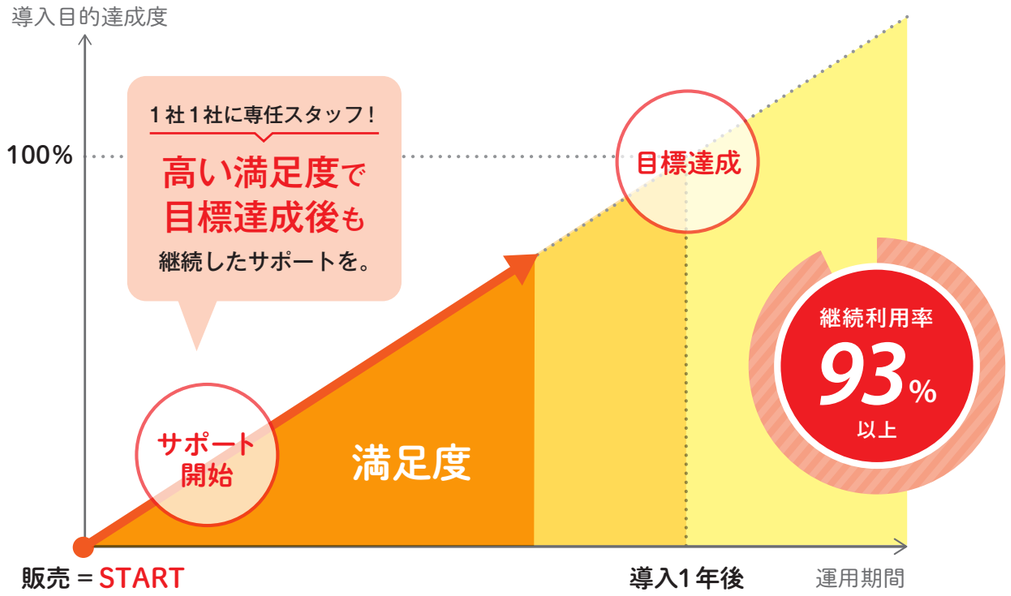
富士通株式会社 「Interstage Charset Manager」

操作ログ	【現象】 LanScope Cat 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。

2018年6月6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 シリーズ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 シリーズ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 Cat 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

プロテクトキャットで検知したインシデントを、「LanScope Cat」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

Cat Portalを通じて最新の情報をお届けします。

Cat Portal 保守契約ユーザー様専用サイト

Cat 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。LanScope Cat の最新プログラムや運用のための各種資料、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 Cat 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。

猫ナビ LanScope 運用ナビゲーション

よくあるご質問

LanScope Cat 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。

LanScope Cat

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。

MyLanScope

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。

MY LanScope

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

ご導入後、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に、専用のWebナビゲーションコンテンツを使いながらサポートいたします。

引き継ぎフォローサービス

LanScopeのご担当者が変更／追加された場合、オリジナルキットを用い、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シリーズ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。

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シリーズの最新情報、MOTEXの今をご紹介します。

トレーニングセミナー ※一部有償

LanScope シリーズの導入から運用までのカリキュラムを、ハンズオン（実機操作）形式で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