LANSCOPE

サイバーセキュリティは、経営課題。

●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　〒108-0073 東京都港区三田 3-5-19 住友不動産東京三田ガーデンタワー 22F　TEL：03-3455-1811
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
長崎 Innovation Lab　〒850-0862 長崎県長崎市出島町 1-41 クレインハーバー長崎ビル 3F

TEL：0120-968-995　受付時間 平日 9:30-12:00, 13:00-17:30（祝祭日除く）
E-mail: sales@motex.co.jp
URL: www.motex.co.jp

●お問い合わせは当社へ

●記載の会社名およびプロダクト名・サービス名は、各社の商標または登録商標です。
●プロダクトの仕様・サービスの内容は予告なく変更させていただく場合があります。
●MOTEX はエムオーテックス株式会社の略称です。

2023. 6発行

© MOTEX Inc.

Secure Productivity

安全と生産性の両立

安全だけを追い求めても、

働く人を縛るシステムなら意味がない。

生産性だけを追い求めても、

高リスクなシステムなら意味がない。

必要なのは、安全と生産性の両立。

矛盾するように見えるこの2つの要素を

独自の技術・発想で成立させる、

それが、私たちMOTEXの使命です。

MOTEX

令和を、
平和に働く。

プロダクト・サービス

MOTEXはセキュリティ戦略立案の支援から、プロダクト・サービスの提案・導入・運用、インシデント対応、さらに教育まで、総合的かつ網羅的にカバーするサイバーセキュリティのトップブランドとして、お客様の「安全と生産性の両立」を支援してまいります。

LANSCOPE

MOTEX が提供するサイバーセキュリティブランド

統合エンドポイント管理

Endpoint Manager　エンドポイントマネージャー

エンドポイントマネージャーは組織の IT 資産管理・内部不正対策・ウイルス対策をオールインワンでカバーします。1996 年にリリースした「オンプレミス版」に加え、スマホ管理も可能な「クラウド版」も提供しており、国内 20,000 社※を超える導入実績があります。※ 弊社調べ

AI アンチウイルス

Cyber Protection　サイバープロテクション

サイバープロテクションは、AI を活用したアンチウイルスで、既知のマルウェアはもちろん、未知・亜種のマルウェアからもデバイスを防御します。高性能な AI アンチウイルス「CylancePROTECT」や「Deep Instinct」を MOTEX のマネージドサービスとして提供します。

クラウドセキュリティ監査

Security Auditor　セキュリティオーディター

セキュリティオーディターは、Microsoft 365 の監査ログを収集し、利用状況の見える化や情報漏洩などのインシデントにつながる操作の把握が可能です。ルール違反の操作や不正な操作があった場合、連携したビジネスチャットから管理者と利用者本人に自動通知も可能です。

セキュリティ診断・ソリューション

Professional Service　プロフェッショナルサービス

サイバーセキュリティのさまざまな領域に対し、セキュリティプロフェッショナルの知見を活かした「セキュリティ診断」と「セキュリティ製品・ソリューション」で、巧妙化するサイバー攻撃などのリスクから組織を守ります。

ー セキュリティ診断（脆弱性診断）

セキュリティ診断とは、システムやネットワークなどを調査し、システム上の脆弱性や政治目的によるハッキング攻撃、個人情報を狙った内部犯行などのさまざまなセキュリティリスクを洗い出すサービスです。セキュリティの専門家が、攻撃手法の研究結果や、実際の運用経験のフィードバックを基に、攻撃者の視点でさまざまな擬似攻撃を行い、脆弱性や耐性を診断します。

ー Darktrace（NDRソリューション）

Darktrace（ダークトレース）は、ネットワークやクラウドなどの異常通信・行動をリアルタイムに自動検知・可視化する NDR ソリューションです。AI による機械学習と数学理論を用いた通信分析で自己学習し、通常とは異なる通信パターンを検知することで未知の脅威に対応することができます。

データプラットフォーム

データアナライザー powered by MUCV (Splunk Cloud)

エンドポイントマネージャーで取得した資産情報や操作ログを Splunk Cloud に転送し、働き方やセキュリティリスクの可視化を支援します。また、エンドポイントマネージャーで取得したログを効率的にレポート化できる「LANSCOPE App for Splunk」も用意。レポートフォーマットを作成することなく、連携後すぐにエンドポイントマネージャーで取得した情報を可視化できます。

リモートサポート ヘルプデスク

Remote Desktop　リモートデスクトップ powered by ISL Online

遠隔地にあるサーバーや PC・スマホへの「リモート操作」「画面共有」を実現する組織向けのリモートコントロールツールです。トラブル時のヘルプデスク対応、テレワークの従業員からの問い合わせ対応など、現地に直接行くことができないシーンにおいても対応を効率化できます。

サポートサービス

MOTEXではプロダクト・サービスが持つ機能・サービスを最大限にご活用いただきたいと考えています。ご用意しているさまざまなサポートサービス※で、プロダクト・サービスをご導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。

※ プロダクト・サービスによってサポートサービスの内容は異なります。詳細はお問い合わせください。

ヘルプデスクサービス

プロダクト・サービス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、チャットによるサポート対応を行っています。サポートセンターを開設して 15 年以上、お客様のサポートをしていく中で蓄積されたノウハウで、運用を支援します。

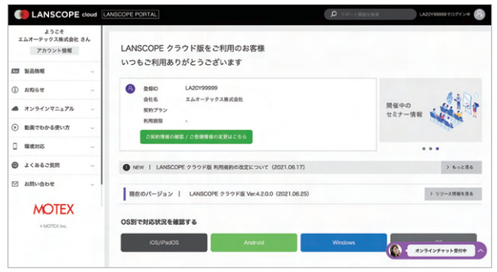
お客様向けサポートサイト

プロダクトの最新情報、マニュアルや FAQ、契約情報の確認など、ご利用中のお客様向けのコンテンツをご用意している専用サイトです※。

※ 掲載コンテンツはプロダクト・サービスによって異なります。

主な掲載内容

- My LANSCOPE（契約情報 / 保有ライセンス情報）
- プロダクトのリリース / 障害情報
- マニュアル
- 動画で分かる使い方
- よくあるご質問 / 各種申請フォーム



LANSCOPE NEWS（定期刊行誌）

MOTEXの旬な情報をお届けする広報誌「LANSCOPE NEWS」では、市場動向やプロダクト・サービスの最新情報を発信。年に3回、ユーザー様・パートナー様に郵送しています。

MOTEXでは上記の他にも、プロダクト・サービス特有のサポートメニュー（無償/有償）をご用意しています。

Endpoint Manager

LANSCOPE エンドポイントマネージャー
クラウド版 / オンプレミス版

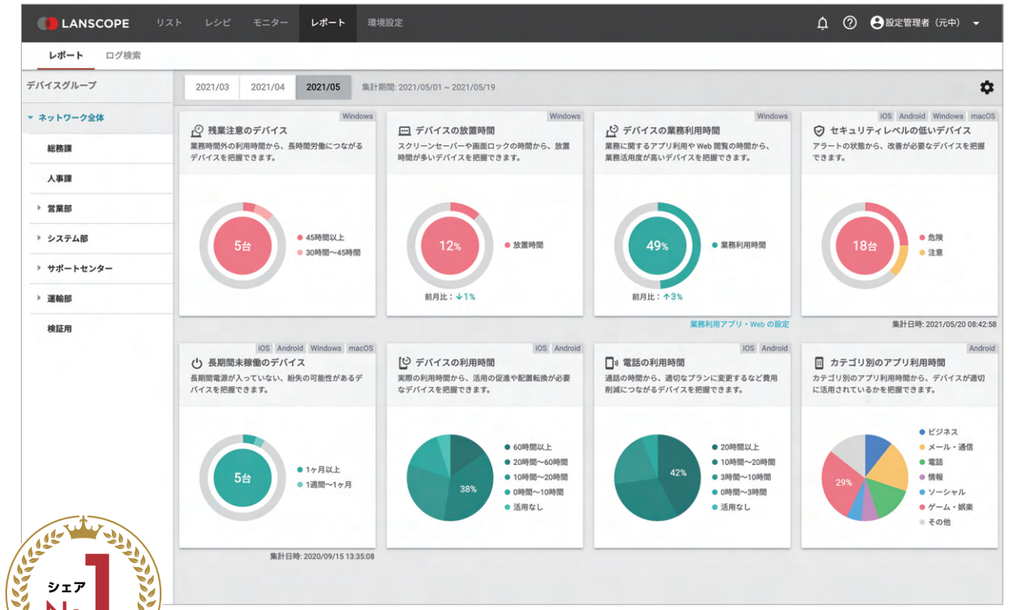
統合エンドポイント管理で PC・スマホの情報漏洩対策を支援

エンドポイントマネージャーは組織の IT 資産管理・内部不正対策・ウイルス対策をオールインワンでカバーします。1996年にリリースした「オンプレミス版」に加え、スマホ管理も可能な「クラウド版」も提供しており、国内 20,000※1 社を超える導入実績があります。

ニーズに合わせて導入できるクラウド版・オンプレミス版をご用意

クラウド版	オンプレミス版
PC だけでなく、スマホ・タブレットもまとめて管理したい	インターネットに接続されないデバイスもまとめて管理したい
社内 LAN に接続されないテレワークデバイスもリアルタイムに管理したい	Microsoft Azure や AWS などの保有している IaaS 基盤で利用したい
サーバーの管理やバージョンアップに運用コストをかけたくない	サーバーの管理は自社で行いたい

組織内で利用されているデバイスの資産情報の自動収集や PC 設定の遠隔制御、操作ログの取得やセキュリティ対策、業界最高峰の AI アンチウイルスとの連携など、エンドポイント管理に必要な機能を搭載しています。



シェア No.1※2
PC資産・PCセキュリティ SaaS市場 メーカーシェア

Cloud LANSCOPE Endpoint Manager

使いやすい管理コンソール

IT 資産管理・情報漏洩対策を支援する豊富な機能を搭載しても、エンドポイントマネージャーならではの「使いやすさ」を追求。シンプルに構成されたメニューで、取得した情報を分かりやすいレポートで表示します。

マルチ OS・グローバル対応

Windows・macOS を一元管理。国内だけでなく海外拠点のデバイスも管理できます※3。また、クラウド版は Windows・macOS だけでなく、iOS・Android のスマホ・タブレットも一元管理できます。

業界最高峰のAIアンチウイルスと連携

AI（人工知能）を活用したアンチウイルス「LANSCOPE サイバープロテクション」と連携。未知の脅威でも実行前に検知・隔離します。エンドポイントマネージャーの操作ログからマルウェアの侵入原因を簡単に調査することが可能です。

豊富なシステム連携

SIEM、勤怠管理、ソフトウェア資産管理ソリューションなど、組織で利用されるさまざまな製品と連携。また、クラウド版は API を公開しているため、社内で利用している自社開発のシステムと連携するなど、業務の効率化を促進します。

※1 弊社調べ
※2 株式会社テクノ・システム・リサーチが 2022 年 3 月に発表した「2021-2022 年版 エンドポイント管理市場のマーケティング分析」の「PC 資産・PC セキュリティ SaaS 市場 メーカーシェア 2021年 ブランド別市場シェア」分野
※3 海外拠点のデバイス管理は利用条件があります。

Cyber Protection

LANSCOPE サイバープロテクション
powered by CylancePROTECT / Deep Instinct

業界最高峰の AI アンチウイルス

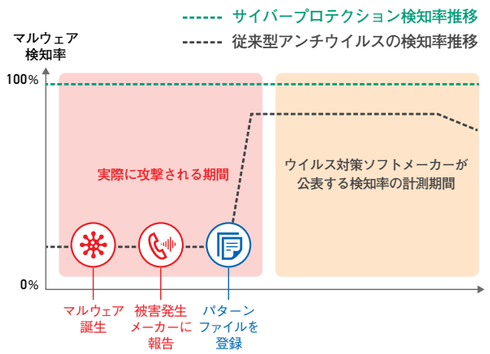
サイバープロテクションは、AI を活用したアンチウイルスで、既知のマルウェアはもちろん、未知・亜種のマルウェアからもデバイスを防御します。高性能な AI アンチウイルス「CylancePROTECT」や「Deep Instinct」を MOTEX のマネージドサービスとして提供します。

CylancePROTECT

deep instinct™

高性能の AI を活用して マルウェアの検知率は 99% 以上※

一般的なアンチウイルスソフトでは、パターンファイル登録後に検知が可能となる一方、サイバープロテクションは、パターンファイルを使わない AI による「予測防御」を採用することで、マルウェアの種類・時期に関係なく安定した検知率を保持しています。



※ CylancePROTECT：2018 NSS Labs Advanced Endpoint Protection Test 結果より / Deep Instinct：Unit221B 社調べ

世界中で導入されている AI を活用した高性能なアンチウイルスを、MOTEX が提供するサポートと共に導入できます。統合エンドポイント管理「LANSCOPE エンドポイントマネージャー」を提供してきた実績、企業のセキュリティ対策に関して得られた知見をもとに、安心してご利用いただけるようサポートします。

point 1　未知のマルウェアを防御

AI を活用した予測検知が可能で、未知・亜種のマルウェアも 99% の検知を実現します。また、エージェントの更新頻度が少なく通常運用時の CPU 負荷が小さいため、PC 利用の快適なパフォーマンスを維持できます。

point 2　安心の国内導入実績

MOTEX ではサイバープロテクションを、これまで国内のお客様 2,000 社以上に導入した実績があります。初期運用のサポートから導入後の製品保守サービスまで専任スタッフが提供するため、安心してご導入いただけます。

point 3　万が一の時も頼れるサービス

未知のマルウェアを“100%”防御することは残念ながらできません。しかし、MOTEX では万が一マルウェアに感染してしまった場合でも、セキュリティインシデントに対する原因の特定と封じ込め、影響範囲の調査を行い、被害を最小限に抑え、いち早い復旧を支援するサービスを提供しています。

万が一のインシデント発生時は MOTEX の「インシデント対応サービス」

インシデント対応サービスは、デバイスのマルウェア感染を発端としたセキュリティインシデントに対する原因の特定と封じ込め、影響範囲の調査を行い、インシデントによる被害を最小限に抑え、いち早い復旧を支援するサービスです。マルウェア解析のスペシャリストが、感染状況の調査から影響範囲を特定。封じ込めをはじめとした復旧支援と、今後どのように対策すべきかといったコンサルティングを行います。

調査～報告は 1 ヶ月で対応
速報は日々提供

幅広い OS を調査
Windows・macOS・Linux 対応

海外拠点のデバイス
にも対応

Security Auditor

LANSCOPE セキュリティオーディター

> Microsoft 365の監査ログを自動収集し、利用状況を見える化

セキュリティオーディターは、Microsoft 365 の監査ログを収集し、利用状況の見える化や情報漏洩などのインシデントにつながる操作の把握が可能です。ルール違反の操作や不正な操作があった場合、連携したビジネスチャットから管理者と利用者本人に自動通知も可能です。

> 1ユーザー月額300円のコストパフォーマンス

クラウドサービスの監査ログについて、6割以上の管理者が「1年以上は保存したい」と回答※1。また、ガイドライン※2 でもログは1年以上保管することが望ましいと定義されており、長期保存が推奨されています。

Microsoft 365では契約ライセンスによって、保存期間が異なり、長期保存を行いたい場合は追加コストが必要な場合があります。セキュリティオーディターは月額300円で過去2年分※4 のログを管理コンソールから把握できるため、コストメリットが大きいプロダクトです。

Microsoft 製品とセキュリティオーディターの比較※3

	Microsoft 365 E3	Microsoft 365 E5	Security Auditor
保存期間	90日	1年	2年※4
月額費用	3,910円 /ユーザー	6,200円 /ユーザー	300円 /ユーザー

※1 弊社セミナー参加者様のアンケート結果より
※2 特定非営利活動法人 日本セキュリティ監査協会「サイバーセキュリティ対策マネジメントガイドライン Ver2.0」、内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン」など。
※3 価格は全て税抜きです。
※4 現在のログ保存期間は 90 日間です。次期バージョンで実装予定です。

Microsoft 365 の OneDrive や SharePoint 上に、個人情報や社外秘情報を保存するシーンが増えています。重要な情報が従業員によって持ち出されていないか、不正なアクセスによる情報漏洩のリスクは無いか、Microsoft 365 の利用状況を把握することが大切です。

セキュリティリスクの可視化

Microsoft 365 製品（OneDrive / SharePoint / Microsoft Teams / Azure Active Directory）の監査ログを閲覧しやすいよう整形し、管理コンソールでレポーティングします。セキュリティインシデントにつながる、ファイルの共有、ゲストユーザーの招待などの操作を把握できます。

ルール違反時の自動通知

Microsoft Teams などのビジネスチャットと連携することで、Microsoft 365のセキュリティルール違反を管理者と利用者本人に通知。従業員へのセキュリティルールの浸透を支援します。

問い合わせ対応時間の削減

バックオフィスに集中する問い合わせ対応をチャットボット機能で自動応答します。「PC故障時の対応」など、よくある問い合わせはプリセットされているため、簡単に利用を開始できます。

Professional Service

LANSCOPE プロフェッショナルサービス
セキュリティ診断（脆弱性診断）

セキュリティリスクを見逃さない、プロフェッショナルサービス

プロフェッショナルサービスは、サイバーセキュリティのさまざまな領域に対し、セキュリティプロフェッショナルの知見を活かした「セキュリティ診断」と「セキュリティ製品・ソリューション」で、巧妙化するサイバー攻撃などのリスクから組織を守ります。

情報システム全体のリスクチェックを支援するセキュリティ診断（脆弱性診断）

- Web アプリケーション脆弱性診断
- ネットワーク診断
- クラウドセキュリティ診断
- サイバーリスク健康診断

MOTEX では上記の他にも、脅威から組織を守るさまざまな診断サービスをご用意しています。
詳細はお問い合わせください。

2004年にサービスを提供開始して以来、さまざまな業界に対してセキュリティ診断を実施しています。外部脅威に対する診断だけでなく、セキュリティコンサルティングサービスで培ってきたノウハウを基にした内部脅威診断など、お客様のさまざまなニーズに合わせたサービスを提供しています。

point 1　10,000件以上の実績、豊富な診断ノウハウ

サービス開始から約 20 年間、官公庁から民間企業まで幅広い業種のお客様に対して、さまざまなセキュリティ対策を支援。なかでもWebアプリケーション脆弱性診断は10,000システム以上の診断実績があります。

point 2　難関国家資格取得者による診断

合格率 15% ～ 20%、サイバーセキュリティの難関国家資格「情報処理安全確保支援士」が 40 名以上在籍。スキル・経験が豊富な診断員を中心に、責任を持って、お客様へのサービス提供を行います。

point 3　90%以上の高いリピート率

診断の丁寧さや提示する報告書の分かりやすさにご満足いただき、毎年多くのお客様からリピート診断のご相談があります。「報告までのスピード」「診断員の対応」「報告書の分かりやすさ」の各項目で満足度は 90%※を超えています。

クラウドサービスの普及でニーズが高まるクラウドセキュリティ診断

クラウドセキュリティ診断は、クラウドサービスの管理設定上の不備に対して、外部からの攻撃や内部情報漏洩のリスクが存在しないか、確認する診断サービスです。
契約しているクラウドサービスの設定不備を発見し、会社全体のポリシーを基準に是正を進めるための現状把握に最適なサービスです。
国内の多くの組織で利用されている主要なクラウドサービスに対応しています。

クラウドセキュリティ診断 対応クラウドサービス

- **SaaS セキュリティ診断**
  - Microsoft 365
  - Google Workspace
  - Zoom
  - Box
  - Salesforce
  - Slack
- **IaaS セキュリティ診断**
  - Amazon Web Services
  - Microsoft Azure
  - Google Cloud Platform
  - ニフクラ

クラウドサービス利用のリスク

新機能リリースによるリスク
クラウドサービスは、ユーザーの知らない間に続々と新機能が追加・変更され、利用者側が気づかぬうちに、セキュリティ上のリスクを抱えてしまう可能性があります。

利用者側の責任にも…
クラウド事業者と利用者の責任範囲の分界点上、クラウドサービスの管理設定不備によりセキュリティインシデントが起きた場合、利用者側の責任となりかねません。

※ 弊社調べ

DARKTRACE

LANSCOPE プロフェッショナルサービス

Darktrace（NDRソリューション）

ネットワークの脅威を検知・可視化するNDRソリューション

Darktrace（ダークトレース）は、企業・組織のネットワークのパケットを収集し、ネットワーク全体の通信状況の可視化と異常な挙動を検知するNDRソリューション※です。AIによる機械学習と数学理論を用いた通信分析で自己学習し、通常とは異なる通信パターンを検知することで未知の脅威に対応可能。LANSCOPE プロフェッショナルサービスの主力ソリューションの一つとして、MOTEXが提供するサポートと共に導入できます。

Darktrace のコンセプト（脅威に対するアプローチ）

人類の免疫システムに着想を得たDarktraceの自己学習型AIは、企業・組織のネットワークの定常状態を学習し、定常状態から外れた異常な挙動を検知します。従来の手法では発見できなかった微細な異常を捉えることで巧妙化するサイバー攻撃や内部不正を検知することが可能となります。

※ Network Detection and Response の略。社内のネットワークトラフィックを監視、ネットワーク全体を可視化し、既知、未知の脅威に対応する製品です。

Darktraceは、従来のネットワークのセキュリティ監視のみにとどまらず、エンドポイントやクラウド環境までセキュリティ監視の対象とできます。また、AIによる自動分析や検知・自動遮断といった機能で、サイバー攻撃による被害を最小限に抑制し、システム管理者の運用負荷を軽減します。

point 1　AI を活用し、未知の脅威を検知

「教師なし機械学習」により、企業・組織の環境固有のユーザーやデバイスの利用パターンを分析。対応が難しいゼロデイ・標的型攻撃などの外部脅威に加え、内部不正にも幅広く対策することが可能です。

point 2　ビジュアライズされたネットワーク可視化で調査時間を短縮

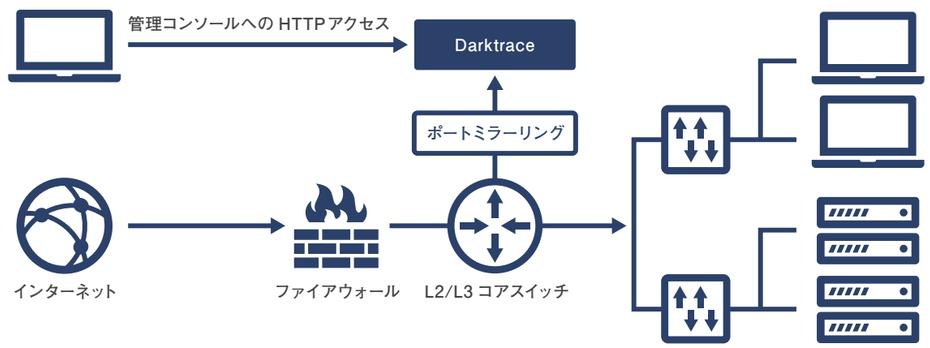
Darktraceで検知したイベントが発生しているデバイス単体の詳細情報から、接続先ネットワークの情報まで時系列でさかのぼり、一連のイベントの発生状況を画面上で再現します。また、通信パケットの情報をエクスポートすることも可能であり、フォレンジック分析による詳細調査も可能です。

point 3　ユーザーやシステムへの影響が少ないモニタリング型の構成

Darktraceは監視対象ネットワークのコアスイッチからポートミラーリングでパケットを収集して動作します。このため、ユーザーやシステムへの影響は最小限となります。

短期間で簡単に導入可能な構成イメージ

アプライアンス型で導入が簡単です。トラフィックをポートミラーリングで流すだけで、ルール定義や詳細設定が不要なため、他システムへの影響が少ない構成です。



- お客様でのご準備：LANケーブル、ファイアウォールへの接続許可、ミラーリング設定
- アプライアンスとしてハードウェア / ソフトウェアー体で提供
- 監視対象の内部ネットワークのコアスイッチよりパケットを収集
- Master/Probe 構成により、複数拠点の監視が可能

LANSCOPE データアナライザー

powered by MUCV (Splunk Cloud)

データプラットフォーム「Splunk Cloud」を活用し、働き方の見える化や情報漏洩対策を支援

エンドポイントマネージャーで取得した資産情報や操作ログを Splunk Cloud に転送し、働き方やセキュリティリスクの可視化を支援します。また、エンドポイントマネージャーで取得したログを効率的にレポート化できる「LANSCOPE App for Splunk」をご用意。レポートフォーマットを作成することなく、連携後すぐにエンドポイントマネージャーで取得した情報を可視化できます。

LANSCOPE データアナライザーの特長

データ分析基盤としてMUCV※1を採用

SIEM 市場のリーダー製品「Splunk Cloud」を利用したデータ分析プラットフォーム MUCV を採用。大量のデータの取り込み・分析が可能な高性能データ分析基盤と、エンドポイントマネージャーの収集データを活かしたレポートテンプレートをご提供します。

SaaS基盤のデータ分析プラットフォーム

SaaS 基盤のデータ分析プラットフォームなので、お客様側での分析基盤やストレージの準備、バージョンアップが不要です。ご契約後、データ連携の設定のみで利用可能で、メンテナンスの工数もかかりません。

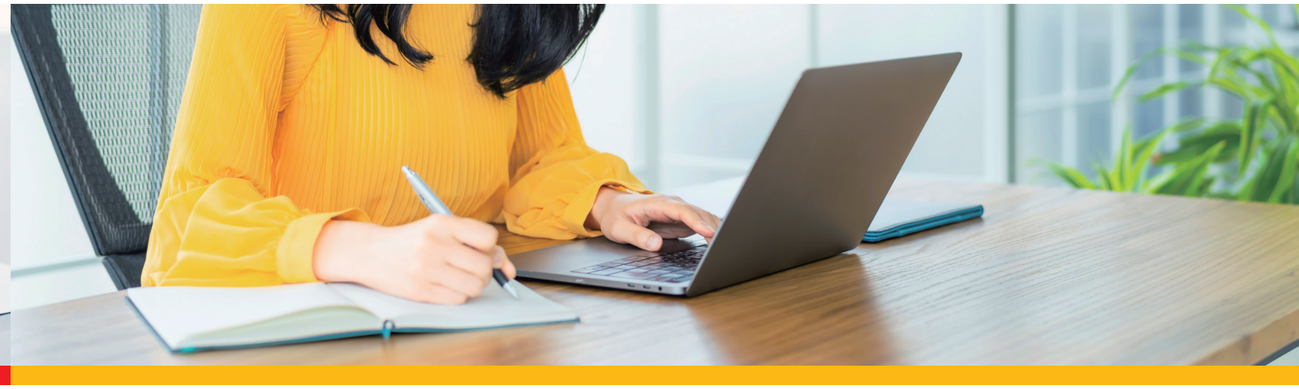
要件に応じたレポートテンプレートを用意

エンドポイントマネージャーの収集データから、「労務可視化」「インシデント対応」「内部不正モニタリング」「ソフトウェア脆弱性管理」といったさまざまなユースケースに対応したレポートを、データ連携後すぐに活用できます。

さらなる拡張性

データアナライザーはエンドポイントマネージャー以外のシステムから生成されるログも収集・分析が可能。Splunkbase に公開されている 2,000 種類を超えるレポートテンプレートを活用し、データ分析の拡張性が高まります※2。

※1 Macnica U ’s Case Visualizer の略
※2 エンドポイントマネージャー以外のデータ解析はマクニカ社によるサポートとなります。



Remote Desktop

LANSCOPE リモートデスクトップ

powered by ISL Online

リモート操作により、ヘルプデスクやメンテナンス業務を効率化

リモートデスクトップ powered by ISL Online は、遠隔地にあるサーバーや PC・スマホへの「リモート操作」「画面共有」を実現する組織向けのリモートコントロールツールです。トラブル時のヘルプデスク対応、テレワークの従業員からの問い合わせ対応など、現地に直接行くことができないシーンにおいても対応を効率化できます。また、お客様の環境に合わせて、オンプレミス版・クラウド版を選択いただけます。

LANSCOPE リモートデスクトップの特長

画面共有・ファイル転送もできる双方向操作型

画面乗っ取り型だけでなく、「画面共有」で双方が操作できる双方向操作型。ファイル転送もその場でサクサク快適に実行できます。

接続先にプログラムのインストールが不要

接続先のデバイスにはプログラムのインストール不要で接続可能。デバイスの環境を意識せずに作業ができます。

シンプルなUIでマニュアル配布や研修が不要

初めて使う方でも簡単に使い始めることができるユーザーインターフェースが特長です。システム部門だけでなく総務やカスタマーサポート担当など、さまざまな方にお使いいただけます。

低コストで導入できるライセンス体系

ライセンス購入は同時接続数分のみ。管理デバイスが100台でも、同時接続数が1であれば1ライセンスのみで導入可能です。

ご検討中のお客様向けコンテンツ

MOTEXのプロダクト・サービスをご検討いただくための、さまざまなコンテンツをご用意しています。

オンライン相談サービス

自席で管理画面や提案資料をご覧いただきながら、専任スタッフがプロダクトをご紹介します。プロダクトのご紹介はもちろん、どのように管理・運用して会社・組織の課題を解決できるのか、ご理解いただけます。「画面を共有して管理画面を操作しながら説明してもらえるので、分かりやすい」とご好評いただいているサービスです。

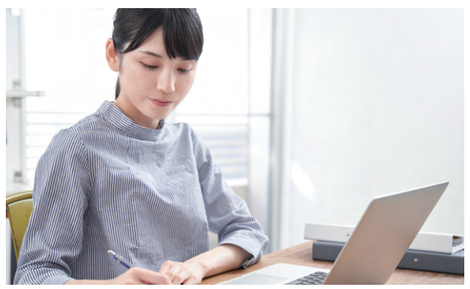
無料体験版

各プロダクトでは無料でお試しいただける体験版をご用意しています※。実際にご利用いただき、自社の要件にマッチするか、課題解決ができるかなどの運用イメージを持っていただいたうえで、ご導入いただけます。

※ プロダクトによって体験版の利用条件は異なります。

定期セミナー

プロダクト・サービスをご紹介するセミナーをオンライン形式（LIVE配信）で定期的に行っています。プロダクト・サービスの概要からお客様に選ばれるポイントまでをご紹介。また、セミナー内でご参加者様からの QA にもお答えします。



資料ダウンロード

「3分でわかる」プロダクト・サービスのご紹介資料やユーザー様の導入事例集、また、導入前に検討・確認しておきたいお役立ち資料も多数ご用意しています。

お見積り

お客様の要件をお聞きし、最適なプランをご提案します。また、プロダクト・サービスによってはWebサイトからのお申し込み後、すぐに概算見積をご案内する「簡単お見積り」もご用意しています。

会社名	エムオーテックス株式会社（MOTEX Inc.）
代表取締役社長	宮崎 吉朗
設立	1990年7月
従業員数	413名（2022年4月現在）
株主	京セラコミュニケーションシステム株式会社
所在地	■ 大阪本社 大阪府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 ■ 東京本部 東京都港区三田 3-5-19 住友不動産東京三田ガーデンタワー 22 階 ■ 名古屋支店 愛知県名古屋市中区錦 1-11-11 名古屋インターシティ 3階 ■ 九州営業所 福岡県福岡市博多区博多駅前 1-15-20 NMF 博多駅前ビル 2階 ■ 長崎 Innovation Lab 長崎県長崎市出島町 1-41 クレインハーバー長崎ビル 3階
事業内容	サイバーセキュリティに関するプロダクト開発・サービス事業
ISMS 認証	認証基準：ISO/IEC 27001:2013 / JIS Q 27001:2014 認証登録番号：IS 656320
参加団体・協会	社団法人 日本コンピュータシステム販売店協会（JCSSA） 一般社団法人 IT 資産管理評価認定協会（SAMAC）