

いつもご愛読ありがとうございます

ご回答いただいた方の中から抽選で計20名様にステキなプレゼント!

## LANSCOPE NEWS 102号 読者アンケート

対象期間：2023年8月1日(火)～9月30日(土)まで

いつも『LANSCOPE NEWS』をお読みいただき、誠にありがとうございます。今後も皆様により良い情報をお届けできるよう、ぜひご意見・ご感想をお聞かせください。対象期間中、本アンケートにご協力いただいた方の中から、抽選で計20名様に心ばかりの品をお贈りいたします。ぜひご応募ください!

**応募方法** 専用フォームからアンケートにご回答ください。

LANSCOPE NEWS アンケート 検索



※当選者の発表は賞品の発送をもって代えさせていただきます。  
※下記の賞品説明の画像はイメージです。  
※賞品は2023年10月より順次発送を予定しております。

1

### お取り寄せグルメ

お取り寄せグルメ(5,000円相当)をプレゼント!  
有名レストランや老舗料亭のお料理、人気スイーツなどをお楽しみください!



2  
名様

2

### MOTEXゴルフボール

MOTEXオリジナルのゴルフボールです。  
「TITLEIST AVX」を1スリーブ(3球)プレゼント!



2  
名様

3

### バンニャバッグ

MOTEXの大人気マスコットキャラクター「バンニャ」のぬいぐるみマグネットが、「みっちり」詰まった特製「バンニャバッグ」をプレゼント!



8  
名様

4

### 3in1充電ケーブル

ご好評いただいているノベルティグッズをプレゼント!



Lightning / Micro-USB / USB Type-Cの3種類の端子を備えた便利なUSBケーブルです

8  
名様

## 『LANSCOPE NEWS』購読お申し込み(無料)・お届け先情報変更・送付停止について

組織変更やご異動・ご転職、オフィス移転などに伴い、『LANSCOPE NEWS』送付先情報のご変更を希望される場合は、下記Webサイトの各フォームよりお手続きください。

LANSCOPE エンドポイントマネージャー オンプレミス版 プロダクトサイト  
「各種お問い合わせ」ページ



STEP1: 「LANSCOPE エンドポイントマネージャー オンプレミス版」で検索

STEP2: Web サイト上部メニューバーの「お問い合わせ」→「LANSCOPE NEWS」とお進みください。

STEP3: 「購読お申し込み」「お届け先情報変更」「送付停止」の各フォームにてお手続きをお願いします。

# LANSCOPE

## NEWS

2023 SUMMER  
Presented by MOTEX Inc.

Vol.102

MOTEXの旬な情報をお届けする広報誌





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。

働き方を、平和に変える。

**MOTEX**

# LANSCOPE NEWS

2023 SUMMER  
Presented by MOTEX Inc.

Vol.102



### 03 TOP MESSAGE

“総合セキュリティカンパニー”として  
サイバーセキュリティの幅広い課題を解決する 新しいプロダクト・サービスをご提供

### 05 PRODUCTS : エンドポイントマネージャー

PC・スマホの一元管理ニーズとその実態とは？  
“エンドポイントマネージャー クラウド版”の利用傾向と最新ロードマップ

### 07 SERVICE : サイバープロテクション

AIアンチウイルス“サイバープロテクション”「Cylance」&「Deep Instinct」最新情報

### 09 PRODUCTS : セキュリティオーディター

Microsoft 365 の監査ログを可読化し、25ヵ月分のログ保管・一括出力が可能に  
“セキュリティオーディター”最新バージョンアップ情報

### 11 SERVICE : プロフェッショナルサービス

新たに MOTEX の LANSCOPE ブランドに加わった“プロフェッショナルサービス”  
なぜ今、セキュリティ診断が必要なのか？ MOTEX の脆弱性診断&クラウドセキュリティ診断をご紹介

### 14 INTEGRATED PRODUCTS : Darktrace

Darktrace 新情報/オプション製品のご紹介  
“自己防御する受信箱”がメールの真偽を自動識別する「Darktrace/Email」

### 16 CASE STUDY

・フリー株式会社様：Darktrace 導入事例  
・SCSK サービスウェア株式会社様：エンドポイントマネージャー オンプレミス版・クラウド版 導入事例  
・株式会社ユーグレナ様：エンドポイントマネージャー クラウド版 導入事例

### 19 PRACTICE : 活用レポート

PC 導入の季節を乗り切る！  
“エンドポイントマネージャー オンプレミス版”を活用した効率的なPCのキitting・メンテナンス方法

### 21 REPORT : 前101号 読者アンケート結果レポート

### 23 CONTENTS

デジタル注意報 / MOTEX TOPICS / note はじめました / SNS 公式アカウントご紹介  
編集部メッセージ / ご協力企業様・ライター紹介 / 読者アンケート

# TOP MESSAGE

新しいプロダクト・サービスを  
幅広い課題を解決する  
サイバーセキュリティの  
総合セキュリティカンパニー”として



代表取締役社長  
宮崎 吉朗

## ご挨拶

日頃よりエムオーテックス(MOTEX)のプロダクト・サービスをご愛顧いただき、誠にありがとうございます。MOTEXとLANSCOPEブランドのプロダクト・サービスの旬な情報をお届けする広報誌『LANSCOPE NEWS』、本102号は2023年度最初の号となります。大変遅ればせながら、今年度もどうぞよろしくお願いいたします。

## MOTEXは、サイバーセキュリティに関する幅広い課題解決をご支援する“総合セキュリティカンパニー”へ

さて、本年2月にお届けした前101号でもお伝えしましたが、昨年度はMOTEXが大きく変化した年となりました。2022年4月に親会社である京セラコミュニケーションシステム(KCCS)のセキュリティ事業部と事業統合したことにより、従来“LanScope Cat / An(現LANSCOPEエンドポイントマネージャー オンプレミス版/クラウド版)”やAIアンチウイルス“LANSCOPEサイバープロテクション(旧CPMS)”といった

エンドポイント対策のプロダクト・サービスに加え、Webアプリケーション・ネットワーク・クラウドサービスの脆弱性診断(セキュリティ診断)サービスや、ネットワークセキュリティ領域において、NDR「Darktrace(ダークトレース)」といった新しいソリューションがラインナップに加わりました。

これにより、MOTEXはサイバーセキュリティの領域において皆様の課題解決をご支援できる幅が大きく拡がり、より多くの

価値を皆様にお届けできるようになりました。また、これらのプロダクト・サービスをお客様に分かりやすくお示しできる『LANSCOPE』ブランドに統一しております。創業以来、多くのお客様にご愛顧いただいている“LanScope Cat / An”ゆかりの『LANSCOPE』ブランドのもと、既存、そして新たなプロダクト・サービス、私共がご支援できる領域をご認知いただけますと幸いです。

## MOTEXが提供するプロダクト・サービス

NISTセキュリティフレームワーク



自動化・効率化・モバイル管理・IT資産管理・操作ログ管理・情報漏洩対策・外部脅威対策  
**プロダクト事業**  
 セキュリティ診断  
 セキュリティソリューション  
**セキュリティサービス事業**

# MOTEX NEWS 2023

- 2月 Feb.** - IT資産管理・MDM “LANSCOPE エンドポイントマネージャー クラウド版”、管理コンソールのセキュリティ機能を強化した最新バージョンをリリース
- 3月 Mar.** - “LANSCOPE エンドポイントマネージャー クラウド版”、市場シェア 25% でトップシェア獲得!  
※ 株式会社テクノ・システム・リサーチが2023年3月に発表した「2023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 2022年 ブランド別市場シェア」分野
- 4月 Apr.** - 「第32回 Japan IT Week 春/第20回 情報セキュリティ EXPO【春】」に出展  

4年ぶりに出展!  
MOTEXブース@東京ビッグサイト
- 6月 Jun.**
  - セキュリティ診断・ソリューション “LANSCOPE プロフェッショナルサービス”、診断項目を厳選し、Webアプリケーション・ネットワーク・Microsoft 365 の「ここだけは押さえておくべき」脆弱性を低コスト・短期で診断する『セキュリティ健康診断パッケージ』を提供開始  
→13 ページで詳しくご紹介
  - 増大するサプライチェーン攻撃への対策として、サプライヤーのセキュリティ対策状況を可視化・一元管理するサプライチェーンリスク評価サービス「Panorays」を提供開始
  - 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(オンプレミス版/クラウド版)”、ChatGPTへの書き込みログ取得機能を実装した最新バージョンをリリース  
→6 ページで詳しくご紹介

## 直近と今後のセキュリティトレンドと私たちMOTEXからのご提案

さて、今年度も変わらず、サイバーセキュリティのインシデントはさらに増えております。お客様にとっては、セキュリティ対策が必要なのは分かっているがどこから手を付けたらいいのか、あるいは、こうした対応には専門性が必要となるなか、十分なセキュリティ人材やリソース、専門ツール導入予算の確保ができるのかなど、さまざまな課題をお持ちかと思っております。

私たちMOTEXとしては、まずは主力プロダクトである“LANSCOPE エンドポイントマネージャー”でお客様のエンドポイントの状況・課題を見る化し、適切な対策をご検討いただくことをご提案し続けております。従来の“オンプレミス版”も引き続き多くのお客様にご活用いただいておりますし、最近では、テレワークや業務システムのクラウド化に伴い“クラウド版”に多くのお引き合いをいただいている状況です。「セキュリティ対策の一丁目一番地」である「エンドポイント管理」にお困りのお客様がいらっしゃいましたら、ぜひお声がけいただければと思います。

また、Emotetに代表されるマルウェアの被害も拡大しております。こちらに対しては、未知のマルウェアに有効な、次世代型AIアンチウイルスをご提供するマネージドサービス“LANSCOPE サイバープロテクション(旧CPMS)”を多くのお客様にご採用いただいております。今年度は、EPP(事前防御)・EDR(事後対応)・MDR(導入/運用支援)・SOC(専門家による24時間365日監視)が一つにまとまったフルマネージドサービス

「CylanceGUARD」を、本年秋より提供予定です。今回、本誌7ページにて先行してサービス内容をご紹介させていただきますが、サイバーセキュリティ対策のすべてをお任せいただけるサービスになっておりますのでご期待いただければと思います。

社会的に問題となっているサイバー攻撃の多くは、私たちが業務上使用するさまざまなシステムの脆弱性を突いたものになります。事業統合によって新たに提供を開始した“LANSCOPE プロフェッショナルサービス(旧 SecureOWL)”には、情報処理安全確保支援士などの難関国家資格を有するエンジニアやコンサルタントが在籍しており、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(脆弱性診断)」をご提供しております。2004年のサービス開始(当時KCCS)以来、官公庁(自治体)をはじめとする幅広い企業・組織のシステムを診断してきた実績があり、豊富なノウハウを持つセキュリティエンジニアによる手作業での丁寧な診断と、具体的な対策を反映した分かりやすいレポートのご提供は、多くのお客様にご満足いただき、リピートいただいております。

Webアプリケーション、ネットワーク、クラウドサービスのセキュリティ対策も、エンドポイントと同じく、まずは自社の課題を見る化し、適切な対策をご検討いただくことが対策の「第一歩」と考えております。MOTEXでは、一般的に高価格で、利用されるお客様にとっても診断を受けるまで、そして受けてからも負担がかかるセキュリティ診断を、もっとお手軽にお試しいただけるよう、手続きが容易かつ明瞭な価格提示が可能な「セキュリティ

健康診断パッケージ」をご用意しました。(6月末より提供開始/本誌13ページにてご紹介)特に昨今は、クラウドシフトが進む中で、クラウドサービスの設定不備による情報漏洩事件が頻発しております。クラウドサービス事業者が提供する基盤なので安心安全だというわけでは決してなく、私たち利用者側が適切に各種機能の設定を行いながら活用していくことが前提です。ご利用中のクラウドサービスに不安がある場合は、ぜひ私たちがまでご相談いただければと思います。

さらに、昨今はターゲットとする企業に直接サイバー攻撃を仕掛けるのではなく、関連企業や取引先・委託先企業の脆弱性を狙って攻撃し、その企業を踏み台として最終的にターゲット企業に不正侵入を行うサプライチェーン攻撃が増大しています。そのような中、MOTEXでは6月末にサプライチェーンリスク評価サービス「Panorays(パノレイズ)」の提供を開始しました。海外を含めた関連会社のセキュリティ対策が可能となるソリューションですので、ご興味ございましたらぜひ担当までお声がけください。

## プロダクトの機能改善・新機能、そして新サービスに乞うご期待!

このように、事業統合によりパワーアップしたMOTEXは、今年度も積極的にプロダクトの機能改善・新機能リリース、および新サービスの提供開始を予定しております。「総合セキュリティカンパニー」として、お客様のサイバーセキュリティ全般の課題解決にお役立ただけの企業を目指してまいりますので、今後とも何卒よろしくお願いいたします。

## PC・スマホの一元管理ニーズとその実態とは？

# “LANSCOPE エンドポイントマネージャー クラウド版”の利用傾向と最新ロードマップのご紹介

“LANSCOPE 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する統合エンドポイント管理です。発売当初からご提供している“オンプレミス版（旧 LanScope Cat）”に加え、スマホ管理が可能な“クラウド版（旧 LanScope An）”も提供しており、国内2万社を超えるお客様にご利用いただいています。

その中で、昨今は“LANSCOPE エンドポイントマネージャー クラウド版（以下エンドポイントマネージャークラウド版）”を、従来のMDM（Mobile Device Management）ツールとして導入するケースだけでなく、IT資産管理ツールとしても導入するケースが増えています。“エンドポイントマネージャー クラウド版”には、MOTEXが“オンプレミス版”で培ってきたPC向けの各種機能も充実させており、2020年に“エンドポイントマネージャー クラウド版”にWindowsの操作ログ管理機能を実装して以降、直近はWindows・macOS向けの機能（=IT資産管理ツールの役割）を大幅に強化してまいりました。それを受けて、特に最近ではPC・スマホの両方を“エンドポイントマネージャー クラウド版”の管理下に置くという傾向が強まっており、この点は注目に値します。

本記事では、PC・スマホの一元管理ニーズとその実態に触れつつ、“エンドポイントマネージャー クラウド版”の最新トピックスやロードマップについてご紹介します。

## PC・スマホの一元管理 ～ニーズとその実態～

従来は、PCはオンプレミス型のIT資産管理ツール、スマホ・タブレットはクラウド型のMDMツールで管理することが「当たり前」でした。しかし、昨今は業務システムや社内サーバーのクラウドシフトや、テレワークやハイブリッドワークなどの新しい働き方の導入による所在（社内/社外）を問わないデバイス管理へのニーズが増加し、IT資産管理ツールもクラウドシフトが進んでいます。

そして、IT資産管理ツールのクラウドシフトとともに多くのお客様において検討が進んでいるのが、PC・スマホの一元管理です。MOTEXが実施したアンケート結果では、“エンドポイントマネージャー クラウド版”で導入を検討しているお客様の半数がPC・スマホの一元管理を希望されていました。しかし、実際にPC・スマホの両方を“エンドポイントマネージャー クラウド版”で一元管理できているお客様は約20%に留まっている（2023年5月末時点）という実態もあります。このようにニーズと実態に乖離が生まれている要因としては、多くのお客様が“エンドポイントマネージャー クラウド版”でまずはPC管理から実施し、その後スマホの管理もまとめていく（その逆もまた然りです）といった流れを取られていることにあります。その証拠に、ユーザー様の2023年5月時点でのPC・スマホの一元管理率は約20%で、約2年前と比較して6%上昇しています。

この利用実態のデータやお客様から実際に伺うお話から、今後も一元管理を行うユーザー様は増えていくと考えています。“エンドポイントマネージャー クラウド版”の強み、そして多くのお客様に選ばれている理由は、充実のIT資産管理機能とMDM機能を持ち合わせ、組織のPC・スマホを一元管理できる点にあります。MOTEXでは、これからも「PC・スマホをクラウドで一元管理できる」というコンセプトのもと、プロダクトの新機能実装・機能改善に取り組んでまいりますので、今後のロードマップにもぜひご期待ください。右記では、予定を含む新機能をトピックスとしてご紹介します。

### PC・スマホ一元管理のニーズと実態

#### ニーズ

PC・スマホを一元管理していきたいと回答したユーザー様



※弊社アンケート結果より（2023年4月）

#### 実態

PC・スマホを一元管理しているユーザー様



約2年



※弊社調べ

## TOPIC 1 「ChatGPT」の書き込みログ取得に対応

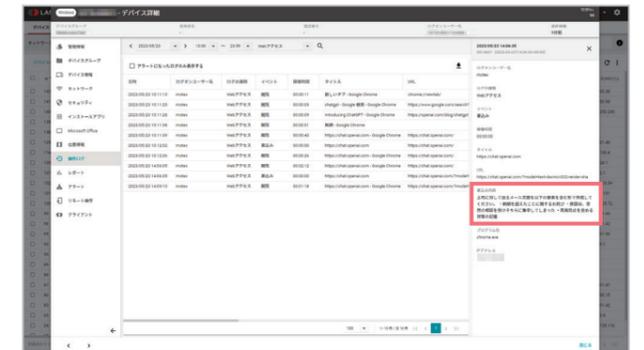
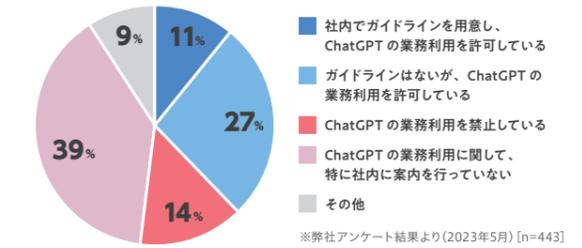
昨今、OpenAI社が開発した自動応答チャット・生成AI「ChatGPT」が非常に大きな話題となっています。さまざまな業務の効率化や生産性向上につながると期待される一方で、機密情報の入力による情報漏洩や、ChatGPTの回答に誤った情報が含まれており、それをそのまま業務に利用してしまうなどのリスクが考えられます。MOTEXが行ったアンケートでは、「社内でガイドラインを用意し、ChatGPTの業務利用を許可している」と回答された組織はまだ全体の11%に留まりましたが、今後はChatGPTの業務利用に関してガイドラインを進められる組織も増えてくると考えられます。

そのような中で、ガイドライン策定後に課題となるのが、ガイドラインを守った利用ができていないかを確認する方法です。MOTEXでは、このようなニーズにお応えするため、OpenAI社のChatGPT (<https://chat.openai.com/>) に書き込んだ内容を「Web書き込み」ログとして取得できるよう“エンドポイントマネージャー”オンプレミス版・クラウド版の機能を改良しました。（2023年6月）ChatGPTに問い合わせた内容をWeb書き込みログから把握できるため、社内ルール・ガイドラインを遵守した利用ができていないか、利用実態の把握にご活用いただけます。

※ オンプレミス版においてChatGPTの書き込みログを取得するためには、Webアクセス管理機能が必要です。

ChatGPTへの書き込みログの確認（エンドポイントマネージャー クラウド版 管理コンソール）▶

### ChatGPTの業務利用およびガイドライン化の実態



## TOPIC 2 ログアラートレポート機能を実装

前述のアンケート結果の通り、組織によってはChatGPTの利用を禁止している場合もありましたが、“エンドポイントマネージャー クラウド版”では、業務上行ってほしくない操作をアラートに設定することも可能です。最新バージョンでは、操作ログのアラートをレポート形式で確認できる機能を新たに実装しました。グループ単位で日付ごとにアラートの発生数を表示するため、「アラート発生数が極端に多い日」を視覚的に把握できます。

ログアラートレポート機能 ▶



## TOPIC 3 オンラインストレージを介したファイル・アプリ配信機能

今後、Windowsにおけるファイル配信機能の改良を予定しています。現仕様では、デバイスに配信したいファイルやアプリを、ファイルサーバーなどのネットワーク上の共有フォルダに配置する必要があります。そのため、配信時にはデバイスが社内ネットワークに接続している必要があり、テレワーク利用のデバイスなどが社内ネットワークに接続していない場合は配信できないという課題がありました。

この課題に対し、今回の機能改良では、配信したいファイルやアプリをオンラインストレージ（Amazon Simple Storage Service [Amazon S3] など）に配置し、配信できるようになります。これにより、デバイスがインターネットに接続されていれば、対象の配布物を配信できるようになります。“エンドポイントマネージャー クラウド版”のメリットである「デバイスの所在（社内/社外）を問わない管理」の機能を強化してまいります。

# Cyber Protection

## AIアンチウイルス「LANSCOPE サイバープロテクション」 「Cylance」&「Deep Instinct」の最新情報をご紹介します！

「LANSCOPE サイバープロテクション(旧 CPMS)」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ており、この2種類のアンチウイルスは、お客様の環境や用途に応じて選択いただけます。今回は「Cylance」および「Deep Instinct」、それぞれの最新情報をご紹介します。

**多くの導入実績とEDR(有償オプション)が利用可能**

CylancePROTECT CylanceOPTICS

- ・国内の導入実績を重視されるお客様
- ・インターネット非接続環境での運用をお考えのお客様
- ・EDR要件への対応をお求めのお客様

**幅広いOSやファイルタイプに対応**

deep instinct

- ・コストを重視されるお客様
- ・PCとスマホにウイルス対策ソフトを導入したいお客様
- ・EXEファイルだけでなくWordやExcelなど多くのファイルタイプへの対応をご要望のお客様

### TOPIC 1 : Cylance 最新情報

専門家による 24 時間・365 日の監視・分析を行う新サービスを提供開始予定！

#### EDRが求められる背景

MOTEXは、2016年にEPP(Endpoint Protection Platform)の「CylancePROTECT」、2018年にEDR(Endpoint Detection and Response)の「CylanceOPTICS」の提供を開始しました。おかげさまで、「CylancePROTECT」の導入社数は1,700社を突破し、多くのお客様にご利用いただいています。

MOTEXは以前から、標的型攻撃やランサムウェアへの感染対策として、事前防御の必要性を訴求してきました。しかし、近年ではテレワークやDXなどに伴う環境の変化、高度なサイバー攻撃の増加により、

事前防御だけではなく、万が一の場合に備えた事後対策をあわせてご検討される企業・組織が増えています。背景には、マルウェア感染によって多くの被害が発生しているという報道が後を絶たないためだと考えられます。また、マルウェアに感染した企業の対策においては、事前防御だけではなく、万が一感染してしまったり、社内環境への侵入があった場合でも早期に異変に気づき、しかるべき対策を行ったという報道も多いことから、事後対策であるEDRをご検討されるお客様が増えています。

#### EDR導入で求められること

EDRはマルウェア感染の予防を目的としたEPPとは異なり、マルウェア感染後の対応支援や怪しい挙動の監視を目的とする製品となります。そのため、導入をご検討される場合は以下の要素がポイントになります。

- ・調査機能や封じ込め機能が十分に備わっていること
- ・自社でリアルタイムに監視と分析が行える体制が整っていること
- ・自社での運用が困難な場合は、MDR(Managed Detection and Response)サービスを提供している企業が存在すること
- ・前提として、検知力の高いEPP製品(事前防御の役割)を導入していること

#### 高性能なEPP・EDRとMDRによって徹底的に運用負荷を低減した「CylanceGUARD」

MOTEXでは、2023年の初秋に24時間・365日対応のMDR(Managed Detection and Response)サービスを搭載した「CylanceGUARD」を提供開始する予定です。「CylanceGUARD」は、高性能なEPP「CylancePROTECT」およびEDR「CylanceOPTICS」を、BlackBerry社のサイバーセキュリティの専門家によって監視するサービスになります。「CylanceGUARD」を導入することで、以下をご提供することが可能です。

- ・サイバーセキュリティの博士号を持ち、SOC(Security Operation Center)コンテスト優勝経験のあるBlackBerry社の専門家による24時間365日の監視
- ・AIとエンジニアによる解析により、アラート通知によるお客様の負荷を大幅に軽減
- ・平均応答時間(MTTR)わずか9分という迅速なレスポンス(BlackBerry社調べ/2022年時点)
- ・月次および四半期ごとのレポートにより、お客様のセキュリティ状況を可視化

EDR導入における課題として、検知するたびに通知が届き、お客様ご自身で対応するには工数がかかること、詳細な情報が得られないこと、レスポンスが遅いことが挙げられます。しかしながら、「CylanceGUARD」ではこれらの課題を解決することが可能です。ぜひご検討いただけますと幸いです。

CylanceGUARD EPP・EDR・導入/運用支援・SOCが1つにまとまっている！

<b>CylancePROTECT</b> 高性能AIにより99%マルウェアを防御	<b>CylanceOPTICS</b> マルウェアの侵入経路を特定再発防止策の検討に	<b>Threat Zero</b> PROTECT・OPTICSの設定をチューニング	<b>SOC</b> セキュリティアナリストが24時間365日フルサポート
--	--	--	--

### TOPIC 2 : Deep Instinct 最新情報

中堅・中小企業向けに、「Deep Instinct」とサイバー保険を組み合わせ、インシデント発生時の対応を支援する新しいパッケージ『Deep Instinct SOMPO安心サポートパック』を提供開始！

#### 新サービスリリースの背景

MOTEXのパートナーであるSOMPOリスクマネジメント株式会社様より、「Deep Instinct SOMPO安心サポートパック」の提供が開始されました。昨今、サイバーセキュリティの脅威はますます高度化していますが、特に中堅・中小企業様におかれては、限られたリソースの中、専門的な知識を要するサイバー攻撃対策を実施することへのハードルが非常に高くなっています。この問題に対処するため、今回新たに中堅・中小企業様向けに包括的なサイバーセキュリティソリューションを提供してまいります。

「Deep Instinct」は、ディープラーニングを活用してマルウェア攻撃を検出・防止する高性能な次世代型AIアンチウイルスで、既知および未知の脅威に対して高い効果を発揮します。しかしながら、どのサイバーセキュリティソリューションも100%の安全を提供することはできず、「Deep Instinct」も例外ではありません。インシデントが発生した場合、企業・組織は対応を迫られ、さらには経済的な損失を被る可能性があります。そこで、この「Deep Instinct SOMPO安心サポートパック」によって、このギャップを埋めることが可能です。

#### サービスの詳細

「Deep Instinct SOMPO安心サポートパック」は、「Deep Instinct」と、インシデント発生時の企業の対応を支援する専用サポートデスクの提供、および、これらのサービスに損害保険ジャパン株式会社(損保ジャパン)のサイバー保険が自動付帯されるパッケージとなっております。まさに平時と有事の両方をカバーする包括的なサイバーセキュリティソリューションをご提供します。

**メリット**

- ・「Deep Instinct」による高精度な保護機能により、お客様に安心感をご提供
- ・インシデント発生時の企業の対応を専用サポートデスクが包括的に支援
- ・インシデントによる損失を、自動付帯されるサイバー保険が一定額まで補償することで、財務的なリスクを軽減
- ・中堅・中小企業様向けの、導入と運用が容易なソリューション

価格は1台あたり年間4,800円(税抜)となります。なお、保険金の支払い対象となるインシデントは、「Deep Instinct」をインストールした端末に起因したインシデントに限定されないため、導入展開が完了していない状況で万が一情報漏洩が発生しても対応できる可能性もあります。ぜひ一度ご検討ください。

万が一のサイバー攻撃やセキュリティインシデントに迅速かつ効果的に対応するために、以下のサービスが自動付帯されています

<b>被害を最小限</b>	<b>インシデント発生時のサポート支援</b>
<b>deep instinct</b> 次世代型AIアンチウイルス Deep Instinct ディープラーニングを採用 未知の脅威や標的型攻撃を事前に検知・防御	<b>SOMPO</b> サイバー保険 損害保険ジャパン インシデント対応支援サービス セキュリティインシデント発生時にサポート(情報漏洩/情報漏洩のおそれ) 情報漏洩またはそのおそれ発生した場合 最大400万円の補償

お問い合わせ先 ▶ SOMPOリスクマネジメント株式会社 プロダクト推進部  
✉ 10\_di-sales@sompo-rc.co.jp

詳細はこちら ▶ 

# Security Auditor

## Microsoft 365 の監査ログを可読化し、25ヵ月分のログ保管・一括出力が可能に “LANSCOPE セキュリティオーディター” 最新バージョンアップ情報をご紹介します！

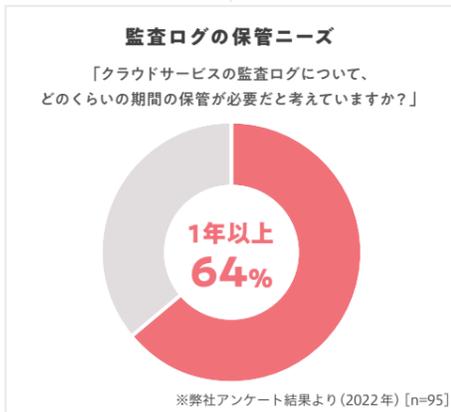
“LANSCOPE セキュリティオーディター (旧 SYNCBIT / 以下セキュリティオーディター)” は、Microsoft 365 の監査ログを収集し、利用状況の見える化や、情報漏洩などのインシデントにつながる操作の把握を可能とします。今回は、監査ログの保管に関する考え方や課題とともに、セキュリティオーディターのログ保管・一括出力機能と  
いった最新アップデート情報をご紹介します。

### 監査ログは1年以上保管するのが望ましい

そもそも「監査ログ」とは、システムやアプリケーションの利用履歴・操作ログなど、情報システムの利用状況を記録するログのことを指します。監査ログは、不正アクセスや情報漏洩などのセキュリティインシデントが発生した場合に、原因の調査・特定や再発防止の検討に役立ちます。そのため、一般的に監査ログは1年以上保管することが望ましいとされています。

MOTEXが実施したクラウドサービスの監査ログの取り扱いに関するアンケート結果では、64%の企業・組織が1年以上のログ保管が必要だと回答しており、日本セキュリティ監査協会や内閣サイバーセキュリティセンター(NISC)も1年以上のログ保管が望ましいと提言しています。

全体の6割以上が、監査ログを「1年以上保管したい」と回答  
法令・ガイドラインなどでも、1年以上の保管が推奨されています。



インシデントの内容の全体像を正しく分析するためにログは長期間保存しておく。  
保存期間は1年以上とすることが望ましい。

出典：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」

1年間のイベントを保持することができれば、  
概ねコンプライアンス規制に適合する。

出典：SANS Institute 「Successful SIEM and Log Management Strategies for Audit and Compliance」

### しかし! Microsoft 365 監査ログの保管日数は基本90日間・・・

Microsoft 365 を利用している企業・組織にとって、監査ログの保管日数は重要な課題となり得ます。というのも、Microsoft 365 では、プランごとにログの保存日数が異なりますが、Microsoft 365 E5 および Office 365 E5 以外のプランでは、基本的に90日間が標準となってしまうからです。1ユーザーあたり月額750円でログ保存期間を1年間に延長することができますが、Microsoft 365 E3 あるいは Office 365 E3 以上のプランで契約していることが前提となっています。

実際に各社の利用プランの状況を見ると、ほとんどの企業・組織においてログ保存日数が90日間の状況です。しかし、監査ログは1年以上保管することが望ましいとされているため、Microsoft 365 を利用する企業にとっては、ログ保存期間の延長が必要となってきます。

**Microsoft 365 におけるログ保存期間の比較** ※ 2023年6月時点の Microsoft 公式サイト掲載情報です。

	Microsoft 365 Business			Microsoft			Office		
	Basic	Standard	Premium	E3	E5	F3	E1	E3	E5
ログ保存期間	90日	90日	90日	90日	1年	90日	90日	90日	1年
1ユーザーあたりの月額	750円	1,560円	2,750円	4,500円	7,130円	1,000円	1,250円	2,880円	4,750円
ユーザー数の上限	300	300	300	無制限	無制限	無制限	無制限	無制限	無制限
ログ保存オプション	×	×	×	+月額750円で1年間保存可能	+月額250円で10年間保存可能	×	×	+月額750円で1年間保存可能	+月額250円で10年間保存可能

**Microsoft 365 のプランの内、1年以上ログ保存が可能な Microsoft 365 E5 / Office 365 E5 を利用している企業は4% 監査ログ保存日数90日のプラン利用が大多数**

**現在お使いの Microsoft 365 / Office 365 のプランを選択してください**

Microsoft 365 Business Basic	7%
Microsoft 365 Business Standard	27%
Microsoft 365 Business Premium	6%
Microsoft 365 E3	24%
Microsoft 365 E5	4%
Microsoft 365 F3	0%
Office 365 E1	8%
Office 365 E3	2%
Office 365 E5	0%
利用していない・分からない	17%
その他	5%

※利用プランについての弊社アンケート結果(2022年) [n=83/複数回答可]

### Microsoft 365 監査ログにおける課題

Microsoft 365 の監査ログには、ログの保存期間以外にも課題があります。

#### ●バックアップを取る際のログ出力件数

1つ目は、ログのバックアップを取る際の制約です。90日間以上ログを保管するためには、Microsoft 365 で提供されている監査ログの出力機能を利用する必要がありますが、この出力機能は1回のログ出力数の上限が5万件までとなっています。多くの企業・組織において保管が必要なログをバックアップするには、対象のユーザーやログ種別などを絞り込まないと出力できず、現実的には日々の運用が難しいという問題があります。

#### ●ログの可読性

2つ目は、Microsoft 365 で確認できる監査ログは、例えば「ユーザー種別」という項目の値が「4」などと表示されており、この「4」が何を意味するものなのか、Microsoft の公開情報を確認して照合する必要があります。このように、ログはあってもログそのものだけでは、ログの意味が読み解けないのも大きな運用上の課題になってきます。

### “セキュリティオーディター”は、可読化した25ヵ月分のログ保存と一括出力が可能に

MOTEXの“セキュリティオーディター”では、Microsoft 365 監査ログの生ログ(ログそのもの)と共に、Microsoft 公開情報などのログを読み解くのに必要な情報と突合して可読化したログを保管できます。さらに、直近3ヵ月間のログには、レポート機能やアラート機能があり、GUI(グラフィカルユーザーインターフェース)で柔軟な検索が可能です。

2023年6月のバージョンアップでは、ベーシックプラン1ユーザーあたり月額300円のまま、25ヵ月分の長期ログ保管機能を実装しました。長期保管用ログでは、レポートや検索はできませんが、25ヵ月間の過去ログを一括出力することが可能です。インシデント発生時の網羅的な調査や定期的なバックアップにご活用いただける機能を低コストでご提供します。Microsoft 365 のプランであれば、1年間のログ保存には、E3 以上のプランで1ユーザーあたり月額750円のオプションが必要ですが、“セキュリティオーディター”であれば、その半額以下の月額300円で、それより長い約2年間のログ保存が可能です。

“LANSCOPE セキュリティオーディター”最新バージョン  
ベーシックプラン(月額300円)におけるログ保存日数を約2年間に延長

90日 (約3ヵ月) → 約2年 (25ヵ月)

月額750円 (1年間保存) Microsoft 365 E3 以上のオプション

月額300円 (約2年間保存) LANSCOPE セキュリティオーディター

Microsoft 365 オプションの半額以下で約2倍の期間のログ保存が可能!

### 管理者側の設定ですぐに始められる無料体験版

“セキュリティオーディター”の無料体験版は、フル機能を50ユーザーまで60日間提供しています。クラウドサービスのため、インターネット環境さえあれば管理者側の設定のみで、従業員の方が業務利用している端末などに影響を与えずに、Microsoft 365 監査ログの解析が可能です。

体験版ご利用時にご不明点などがあっても、導入後と同じサポートメンバーが電話・メールでお客様の運用をサポートします。導入後の運用で重要なサポート対応について、事前にご確認いただいたうえで導入検討をしていただけます。

実際、お客様からは体験版利用開始後すぐに、「ゲストユーザー招待を禁止しているはずなのに、招待している人がいた」「ファイルの社外共有を禁止しているつもりだったのに、共有できてしまっていた」などといったお声を頂戴しています。お客様の Microsoft 365 のセキュリティにおいて、想定している状況と現在の実態に乖離がないかご確認いただけますので、ぜひ一度無料体験版をお試しください。

“LANSCOPE セキュリティオーディター”  
60日間無料体験版お申し込みはこちら

※記載の価格はすべて税抜価格です。

## 新たにMOTEXのLANSCOPEブランドに加わった“LANSCOPE プロフェッショナルサービス” なぜ今、セキュリティ診断が必要なのか？ MOTEXの脆弱性診断&クラウドセキュリティ診断をご紹介します！

2022年4月の京セラコミュニケーションシステム (KCCS) セキュリティ事業部との事業統合により、MOTEXのLANSCOPEブランドには、新たに“LANSCOPE プロフェッショナルサービス (旧 SecureOWL / 以下プロフェッショナルサービス)”が加わりました。“プロフェッショナルサービス”では、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 (専門家) の知見を活かした「セキュリティ診断サービス」と「セキュリティ製品・ソリューション」をご提供しており、巧妙化するサイバー攻撃などのリスクから企業・組織を守ります。

本記事では、“プロフェッショナルサービス”が提供するさまざまなサービスやソリューションのうち、脆弱性やクラウドサービスの設定を診断する「セキュリティ診断サービス」に焦点を当ててご紹介します。

### “プロフェッショナルサービス”の「セキュリティ診断サービス」の特長

“プロフェッショナルサービス”の「セキュリティ診断サービス」は、2004年(当時KCCS)から提供を開始し、サイバーセキュリティ業界の中でも古くからサービスを提供している老舗です。現在まで、官公庁(自治体)をはじめとする幅広い企業・組織の12,000以上のサイト・システムの診断実績があり、豊富なノウハウと多数の難関国家資格保有者(情報処理安全確保支援士)によるサービスで、脆弱性対策やクラウドサービスの設定にお困りのお客様にご愛顧いただいております。

今回は、「そもそもなぜ診断が必要なのか?」「なぜMOTEXの“プロフェッショナルサービス”が選ばれるのか?」を、「脆弱性」および「クラウドサービスの設定」、それぞれの切り口で解説していきます。



### 減らない不正アクセス被害、ガイドラインや政府の規制も強化

まずは、「脆弱性」についてです。脆弱性とは、攻撃者が狙う弱点であり、一般的にプログラムの不具合や設計ミスが原因となります。また、プログラムだけではなく、システムを利用する「ヒト」も弱点となることが多く、標的型攻撃における関係者を装った不正メールは、まさに人の脆弱性を攻撃の起点としています。

昨今盛んに報じられている通り、不正アクセスはますます増加しています。標的型攻撃によるランサムウェアの被害で業務が停止する。取引先などのサプライチェーンが狙われて機密情報が漏洩する。新規のWebサービス公開後に脆弱性を突かれて個人情報が漏洩する。このようなニュースが珍しいものではなくなりました。さらに、攻撃者はサイバーセキュリティ対策が遅れている企業を狙う傾向にあり、警視庁の調査でも、ランサムウェア被害の半数以上は中小企業であることが明らかになっています。

このような背景から、2023年3月に情報処理推進機構(IPA)から「ECサイト構築・運用セキュリティガイドライン」が公開されました。本ガイドラインには、ECサイト構築時の要件として「ECサイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する」、運用時の要件として「ECサイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する」という記載があり、いずれも「必須要件」となっています。

また、政府も規制を強化しており、経済産業省では、2024年3月末までにすべてのECサイトにおいて脆弱性対策と本人認証を導入することを事業者が義務付ける方針を固めています。今や脆弱性診断は、「できればやったほうがよいもの」から「必ず実施しなければならないもの」になっているのです。

### 診断を受けることに対する担当者の負担・・・そこで! MOTEXの「脆弱性診断サービス」

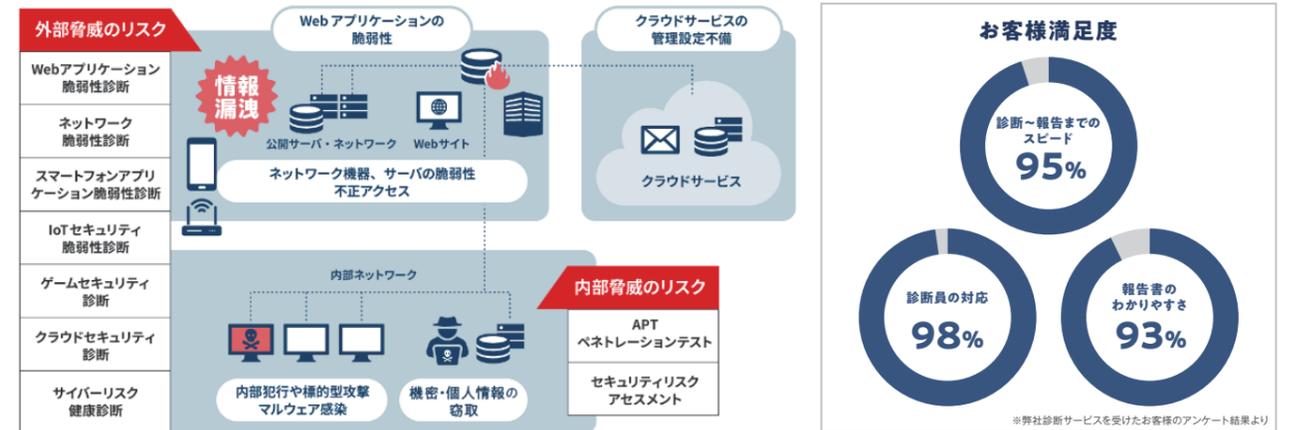
ECサイト事業者も、それ以外の事業を生業とする企業も、近年はDX化の流れもあり、ビジネス拡大のためにWebサービスという手段を用いることが多くなっています。事業の企画から開発、運用やサポートまでさまざまな業務があり、対応できる人員にも限りがある中で、さらに脆弱性診断をマストで実施しなければならないことはかなりの負担となります。診断自体は外注となりますが、実は、診断を受ける前の見積りや、診断環境の準備、診断中の問い合わせ対応、脆弱性が見つかった際の対策などが本業の傍らで発生するため、診断を受ける

側にも非常に多くの工数がかかるのです。

さらに昨今は、クラウド化や認証方式の多様化、リッチなプロトコルの使用、複雑なアプリケーションの仕様なども相まって、課題が多様化しています。画一的で標準化された脆弱性診断サービスでは十分な診断ができない、診断対象のシステムに合った対策が示せないといったことが想定され、一般的に安価な脆弱性診断を提供するベンダーのサービスや、最近の潮流であるクラウド(SaaS)型診断ツールの利用にはこのような傾向があるため、業者選定される際には注意が必要です。

MOTEXの“プロフェッショナルサービス”では「セキュリティ診断サービス」の提供を開始した当初から、さまざまなお客様の課題に向き合い、柔軟に対応してまいりました。「お客様の負担を少しでも減らしたうえで、課題を解決し、ビジネスの目標達成を支援できる」、そのようなサービスを目指しています。豊富な実績により培ってきたノウハウ

をシステム化し、セキュリティエンジニアのチーム力によってさまざまな診断サービスをリーズナブルな価格でご提供しており、「最適で柔軟なサービス提供」「スピーディーな診断」「対話重視のサポート」という点で高い満足度を頂いております。脆弱性診断でお困りの場合は、ぜひMOTEXにお声がけください。



### クラウドサービスの設定不備によるセキュリティ事故が頻発

次に、「クラウドサービスの設定」についてです。

2020年から2021年にかけて、大手であるSalesforceの設定不備が起因となった情報漏洩事故が立て続けに発生し大きな問題となりました。Salesforceのユーザーは金融業や情報通信業、地方公共団体など多岐にわたっており、当時は金融庁や内閣サイバーセキュリティセンター(NISC)からも注意喚起がなされる事態となりました。

2022年には、申込フォームやアンケートフォームの設定ミスにより数十から数百の個人情報が漏洩する事故が多発しました。

また、大手旅行会社において、クラウドのアクセス権限の誤設定により1万人超の個人情報が漏洩するという大きなセキュリティ事故も発生しました。

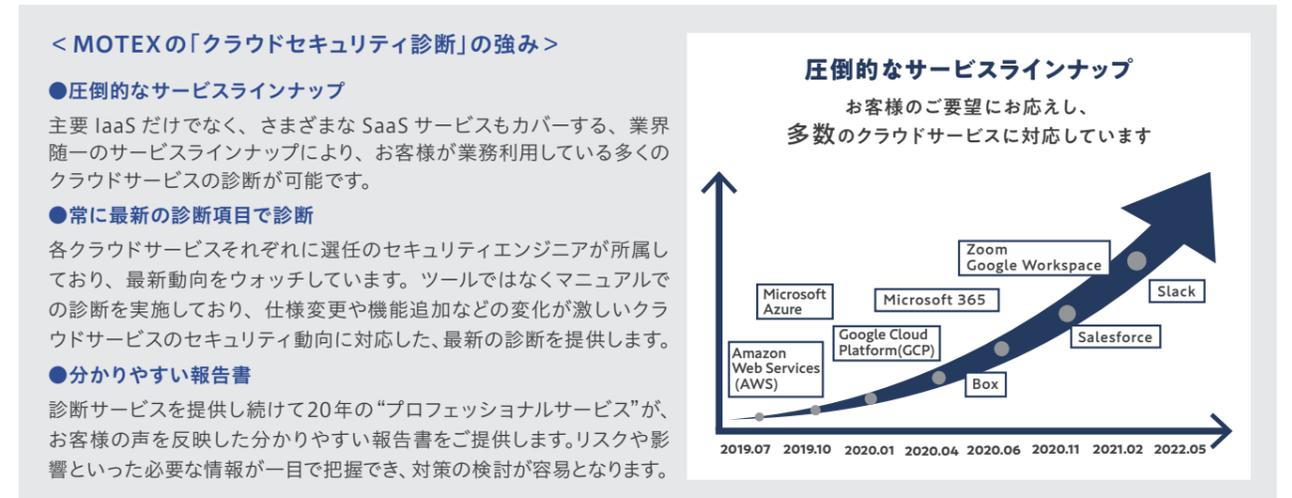
そして2023年。まだ年の半ばですが、自動車メーカーで215万人の個人情報が流出する事故や、医薬品メーカーで取引先情報約11,000件が漏洩した事故が報じられています。どちらも詳細は発表されていませんが、クラウドサービスの設定不備が原因と言われています。

### クラウドの設定ミスはユーザーの責任!? そこで! MOTEXの「クラウドセキュリティ診断サービス」

クラウドサービス提供事業者とユーザーの責任分担を定義したクラウド責任共有モデル上、クラウドサービスにセキュリティ機能を備えた設定を準備するのは事業者側の責任範囲となりますが、その機能を正しく使用して設定をするのはユーザー側の責任となるため、これらのセキュリティ事故も一概に事業者側の責任とはなりません。クラウドサービスによっては非常に難解で複雑な設定項目も、正しく設定する責任はユーザー側にあります。よって、「よく分からないからデフォルト値のままにしよう」とか「使いやすさからどこからでもア

クセスできるようにしよう」などといった安易な設定方法は非常に危険です。

こうした背景もあり、クラウドサービスの管理設定にセキュリティ上の問題が無いか確認する、“プロフェッショナルサービス”の「クラウドセキュリティ診断」の需要も年々増加しています。MOTEXは脆弱性診断の老舗ベンダーとして、業界に先駆け2019年からクラウドセキュリティ診断を提供しており、以来、診断対象のクラウドサービスを拡充してまいりました。



## 「クラウドセキュリティ診断」のサービス内容・診断イメージ

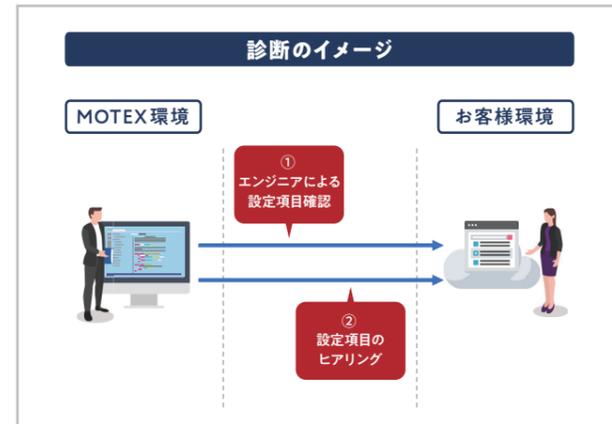
「クラウドセキュリティ診断」では、クラウドサービスの管理設定に対して、主にCISベンチマーク(※)を参考としたMOTEX独自項目によるセキュリティアセスメントを実施します。

※ CIS ベンチマーク：CIS はセキュリティの促進を目的とした米国の非営利団体で、本団体により精査されたソフトウェアやクラウドサービスに対するセキュリティ基準がベンチマークとして公開されています。

まず、お客様側でご対応が必要となるのは以下の2点です。

- (1) 設定手順をもとにクラウドサービスの診断用アカウントを作成する
- (2) 診断用の問診票に必要情報を記入する

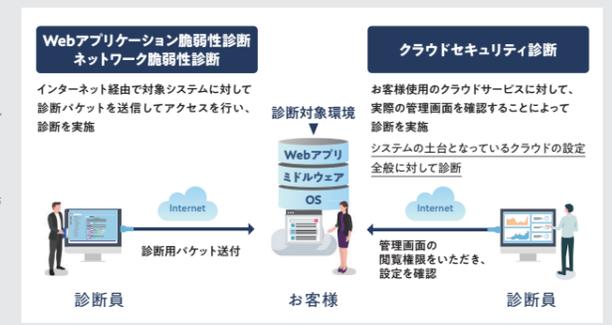
その後、①MOTEXのエンジニアがお客様の環境にアクセスし、実際の管理設定を確認します。また、並行して②お客様の運用状況を中心にヒアリングも行い、さまざまな観点でクラウドサービス利用にセキュリティ上の問題が無いかチェックします。診断に費やす期間は約1ヵ月で、診断後は診断結果をまとめた報告書をご納品します。報告書の提出から3ヵ月間は、診断内容などについてお問い合わせが可能です。「利用中のクラウドサービスの設定に不安がある」「第三者のチェックを受けたことがない」というお客様がいらっしゃいましたら、ぜひMOTEXにご相談ください。



### <「脆弱性診断」と「クラウドセキュリティ診断」の違い>

「脆弱性診断」では、アプリケーションやミドルウェアの脆弱性を、診断用パケットを送信するといった検査手法で診断します。SQLインジェクションやクロスサイトスクリプティング(XSS)といったWebアプリケーションの開発ミスや、ミドルウェア・OSのバージョンアップ不備による脆弱性、不要なポートの設置といったサーバーの設定不備などを見つけることができます。

「クラウドセキュリティ診断」では、お客様がご利用中のクラウドサービスの管理設定を、実際の画面を確認することによって診断します。(クラウドセキュリティ診断では診断用パケットを送信するといった検査手法は用いないため、お客様のクラウド環境に対して負荷や設定変更といった影響は与えません)管理者の認証や、アクセス管理、ログ管理などの設定ミスを見つけることができます。



## ポイントを押さえた、リーズナブルでスピーディーな診断を！「セキュリティ健康診断」シリーズのご紹介

さて、今回は以下の内容をお伝えしてきました。

- ・脆弱性診断は「必ず実施しなければならないもの」に変化
- ・MOTEXの柔軟な脆弱性診断サービス
- ・クラウドサービスの管理設定も診断が必要

万が一セキュリティ事故が発生してしまった場合、単純に事業の損失や賠償が発生するだけではなく、多くの報道から自社ブランドイメージを著しく損なうことになります。そのため、診断を実施せず、セキュリティリスクを残したままビジネスを進めることはお勧めできません。

しかし、それは今後より一層のセキュリティ投資が必要になるということでもあります。診断サービスはプロフェッショナル(専門家)によるサービスである以上、費用は決して安くはありません。また、定期的に診断を実施する場合、毎回フルスペックの診断を受けていたら事業の採算が取れなくなってしまうということも考えられます。

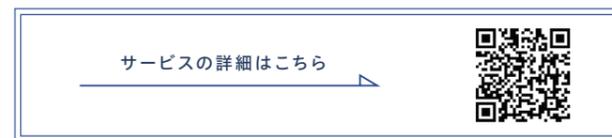
このような背景もあり、MOTEXでは多くのお客様からのご要望を受け、定期的に無理なく高品質な診断をお受けいただけるプランをご用意しました。2023年6月より、「Webアプリケーション健康診断」「ネットワーク健康診断」「Microsoft 365健康診断」という3種類の

Webアプリケーション健康診断	ネットワーク健康診断	Microsoft 365健康診断
¥300,000	¥200,000	¥360,000
MOTEX選定重要画面5画面まで 1年間の問い合わせサポート付き	お客様ご指定の1IPまで 1年間の問い合わせサポート付き	Microsoft 365 1テナントまで 3ヵ月間の問い合わせサポート付き

※記載の価格はすべて税抜価格です。

「セキュリティ健康診断」をご提供しております。

「ポイントを押さえた診断項目」を「リーズナブルな価格」と「スピーディーな対応」で診断するサービスとなっておりますので、「予算が取れないので、リーズナブルに脆弱性診断を依頼したい」「初めての脆弱性診断で、どこに相談したらいいのかわからない」といったお悩みがございましたら、ぜひMOTEXまでお問い合わせください。



### <「健康診断」というサービス名の由来>

Webアプリケーションにおいては、IPAが公開している「ウェブ健康診断」という簡易的な脆弱性診断仕様があります。これは、2009年に全国の地方自治体のWebサイトを診断する際に作成した診断仕様がはじまりで、当時の仕様検討や診断作業にもMOTEXのメンバーが関わっていました。今回のサービス提供開始にあたり、単に安価なだけでなく、しっかりと裏打ちのある内容の診断であることを皆様にお伝えたく、「健康診断」というサービス名となりました。



※IPAサイト掲載

## 連携製品

# DARKTRACE

## Darktrace 新情報/オプション製品のご紹介

### “自己防御する受信箱”が メールの真偽を自動識別する 「Darktrace/Email」

提供：Darktrace

MOTEXは2022年10月、英国のDarktrace社と代理店契約を締結し、同社のAIセキュリティソリューションの提供を開始しました。「Darktrace(ダークトレース)」は、企業・組織のネットワークの packets を収集し、ネットワーク全体の通信状況の可視化を図るとともに異常な挙動を検知するNDR(Network Detection and Response)製品です。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します。今回は、新情報として「Darktrace」のオプションのEメールセキュリティ製品をご紹介します。

製品の詳細はこちら



### 事前定義やブラックリストに依存せず、 メール送受信の「癖」を機械学習する次世代の AIメールセキュリティ

Darktrace社のEメールセキュリティ製品である「Darktrace/Email」は、各組織固有の普段の通信パターンを独自開発のAIが常に学習し、そこから逸脱する通信異常をリアルタイムに自律検知するという、ネットワークセキュリティにおける「自己学習型」AIアプローチ(本誌前号101号でご紹介)を応用した、アプライアンスの導入が不要なオプション製品です。

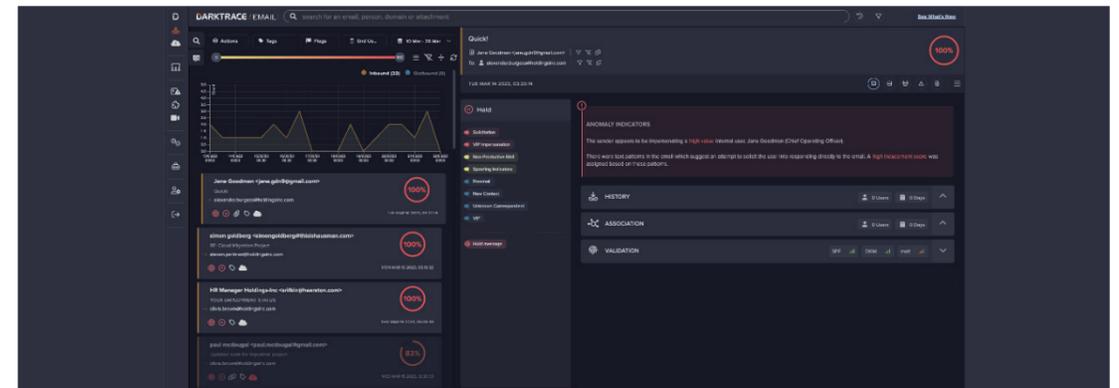
「Darktrace/Email」は、個々のユーザーが送受信するEメール本文や件名における普段の文体やスタイル、Eメール上の人間のコミュニケーションの癖や習慣、定常パターンを機械学習しながら、Eメールの送受信トラフィックを双方完全に可視化します。通常やりとりする相手は誰かなどの外部連絡先との関係性、Eメールの未読・既読、どのリンクをクリックしたかなどの閲覧行動、特定のEメールを他に受け取ったのは誰かなどの文脈など、AIが組織固有のEメールの使い方を常時理解し続けます。ルールベースのEメールゲートウェイをすり抜ける、定常に見せかけた巧妙な標的型メール攻撃などを、

通常業務に影響なくリアルタイムかつ自律的に検知・無害化する世界初の製品で、2019年の発売以来、現在世界で3,000社以上の組織で利用されている、これまでにないアプローチのEメールセキュリティ製品です。

セキュリティ対策の最後の砦はEメールを受信して開封する人間です。従業員に対して怪しいメールや添付ファイルの開封をしないように警告を繰り返しても、性善説に基づく注意喚起にはどうしても限界があります。一般論として、組織は職場におけるコラボレーションツールとしてEメールに依存し続けています。サイバー脅威の94%が依然としてEメールを発端していると言われる中、標的型攻撃のパターンや脅威インテリジェンスを学習するのではなく、むしろユーザーの挙動や習慣、Eメール通信自体を学習することが最良の対策ではないかという思いから「Darktrace/Email」は開発されました。

### ジャーナリング設定、API連携のみの容易な導入

Darktrace社のクラウドサーバー上で稼働する「Darktrace/Email」は、Microsoft 365、Google Workspaceなどの主要なグループウェアにおいて、ジャーナリング設定およびAPI連携のみで容易に導入でき、MXレコード(Mail Exchangerレコード)の変更も不要です。



## エンジニアの意欲向上につながる、安全と生産性を両立した自由度が高いITインフラの整備に「Darktrace」が貢献

ブラックリストや事前定義に依存することなく、常時機械学習を続ける定常状態からの逸脱度に応じて、「Eメールを受信者へ受信させない (Hold Message)」「Eメールを受信トレイからジャンクフォルダに移す (Move To Junk)」「リンクをクリックするための確認工程を挟ませる (Lock Link)」「リンクをクリックさせない (Double Lock Link)」「リンクを削除する (Delete Link)」「添付ファイルを変換して無害化 (Convert Attachment)」「添付ファイルを取り除く (Strip Attachment)」「なりすましのユーザー名を削除してヘッダーアドレスを表示 (Unspoof)」などの種々のアクションを自律的に発動することで、ソーシャルエンジニアリング、スパイフィッシング、アカウントの乗っ取りなど、Eメールを取り巻くあらゆるサイバー脅威を早期に自律検知します。

### 「Darktrace/Email」事例紹介

信頼できる取引先や同僚の書き方のスタイルを巧みに模倣する「なりすまし攻撃」はますます増加し、昨今ではChatGPTのような生成型AIの急速な普及により、なりすましメールがこれまで以上に大量生産される「新型ソーシャルエンジニアリング攻撃」が流行の兆しを見せています。偽メールが大量に自動生成されることでメール本文の長さや量が増大する一方、悪意あるリンクや添付ファイルを含むなりすましEメールは減少傾向にあると言われています。

右記では、このような中、人間が自分自身でEメールの真偽を識別することはもはや不可能であると悟り、Darktrace社のAIを駆使して、よりシステムティックかつ自律的な対策でEメールセキュリティを強化したいと考えた、さいたま市に本社を置く電気機器製造企業A社の事例をご紹介します。

### 国内導入事例

#### ゲートウェイ製品をすり抜けたEmotetを真っ先に自律検知

A社では、サイバー攻撃への対応力を身につける啓発教育の一環として、数年前から従業員に対して標的型攻撃を模した訓練メールを送信するペネトレーションテストを定期的に行っていました。なかなか開封率が下がらないという状況が続いていました。同社では、世の中で巧妙ななりすまし攻撃や未知のサイバー脅威が増加する中、AIでこのような「人の脆弱性」をなくしたいと考え、「Darktrace/Email」の無償評価プログラムを開始。すると、即座にGoogle Workspaceのネイティブセキュリティコントロールをすり抜けたEmotetが検知されました。管理画面で確認できた検知内容には、あるユーザーに宛てられた当該Eメールに含まれる怪しいWebサイトのURLや、そのEメールの異常度がパーセンテージで示されており、Eメール自体は迷惑メールフォルダに自動的に振り分けられました。Googleが検知したのは、約1週間後に同じ攻撃を受けてからでしたが、「Darktrace/Email」では未知のマルウェアであってもリアルタイムに検知し、早期に適切なアクションを取れたことで、その真価を見出すことができました。

A社では、全従業員と子会社の一部社員を含む約960のGoogle Workspaceユーザーアカウントを対象に運用を行っており、担当者2名体制で、2日に1回、15分ほどかけて「Darktrace/Email」の管理コンソールを確認しています。実運用開始後は、幸いにもEmotetのような高異常度のEメールは受信しておらず、ユーザーからも必要なEメールが届かない、必要な添付ファイルが削除されているなどの過検知の報告もありません。AIがそのユーザーにとって異常だと自律判断したメールのみが迷惑メールフォルダに振り分けられており、従来は不可避だった識別漏れをAIが自律的にカバーするという次世代のEメールセキュリティ体制を実現しました。

2007年に設立され、プリントシール機の開発・製造・販売をはじめとする「ガールズトレンドビジネス」などを手がけるフリー株式会社。同社は、ユーザーの会員情報や画像情報などの個人情報や画像情報を安全に管理するため、業務におけるルールを厳格化し、セキュリティを強化してきた。しかし、クラウドサービスの利用や、若手を中心としたITエンジニアからのスキルアップのための積極的な社外交流を希望する声もあり、「安全と生産性を両立したセキュリティ対策」の重要性が高まってきた。そこで、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、AIを活用したNDRソリューション「Darktrace」を導入。導入の経緯や効果などについて、フリー株式会社 ガールズ総合研究所 所長 三輪 哲也 氏と、同研究所 戦略プラットフォーム部 フリーネットサービス担当 加藤 真一 氏に話を聞いた。

### フリー株式会社 様

設立：2007年(平成19年)4月  
業種：ゲーム・アミューズメント機器



#### 導入の経緯

#### プリントシール利用者の個人情報保護と、従業員の生産性向上が課題

同社の主力ビジネスであるプリントシール機は、年間のべ1億人(同社調べ)に利用されている。また、同社のプリ画(プリントシール機で作成した写真シールの画像)取得・閲覧サービスのユーザーも2,200万人ともなり、蓄積された画像や会員情報といった重要情報の保護は、事業存続に関わる大きなテーマである。また、サービスサイト運営に関わるITエンジニアは業務上こうした重要情報に触れるため、会社として従業員を守るためにも、インシデント発生時にしっかりと原因を調査・分析できる仕組みづくりが必要であった。

同社では従来、外部接続に対してファイアウォールやプロキシサーバーなどで入口を固める対策を行っており、外部アクセスが必要となるクラウドサービスなどは原則使用禁止としていた。リスクと生産性を天秤にかけた結果、業務プロセスが閉鎖的になっており、ITエンジニアからはクラウドサービスなどを利用し、社外との積極的な交流を求める声も多く上がっていた。

そこで、会社の上場や、テレワーク環境への対応などもある中、安全を担保しつつ事業の中心であるITエンジニアの意欲も向上できるよう、セキュリティ対策の方針を「禁止からモニタリングへ」移行し、より自由度の高いセキュリティ基盤を整備していくこととなった。

#### 選定のポイント

#### 侵入経路特定にはカバー範囲が広いNDRが適していた

同社が「Darktrace」を選定したポイントは次の通りだ。

##### ●経路と原因の追跡

昨今、ランサムウェアや標的型攻撃といった内部ネットワークに侵入する脅威が多発している。ある程度の侵入を前提とした対策

として、「いつ、どの経路で入ってきて、何をしたか」をモニタリングし、侵入された後に早期発見、早期対応できる仕組みであった。

##### ●ネットワーク型の製品

エージェントインストールが不要なネットワーク型のソリューションであり、端末への負荷が少なく、ネットワークにつながっているPC以外のIT機器もカバー可能であった。

##### ●IT部門の運用負荷軽減

AIを活用してネットワークに接続したさまざまなデバイスやユーザーの行動パターンを学習・分析し、未知のサイバー攻撃や内部不正の兆候を検知するため、管理者が細かくツールを設定する必要がない。また、日々の運用面においても、脅威レベルでアラートが厳選された分かりやすいレポート・解説が示されるため、インシデント発生時の対応や判断に時間を要さず、管理者の運用負荷軽減につながった。

#### 導入の効果・今後の展望

#### 従業員が安心してITを利用し、サービスを生み出せる環境が整った 今後はさらなる安定稼働を目指す

「Darktrace」の導入により全ての通信を把握されたことで、有事の際に早期検知・対応できる体制を構築できているという安心感が生まれた。事業において重要情報を取り扱う中でも、仕組みでセキュリティを担保し、従業員の心理的な安全性を確保。自由度が高いITインフラによって、従業員は自社や他社のさまざまなサービスが使えるようになり、総合エンターテインメント企業として各自が自らの意思でさまざまなことを試せる風土が醸成された。

今後の会社を取り巻く環境によっては、週次・月次レポートや運用のマネージドサービスを検討していくなど、引き続きMOTEXのサポートを得て、安定稼働を実現していきたいとのことだ。

※ MOTEX からご提供するDarktrace製品のラインナップは予定の内容です。変更が生じる場合がございますのであらかじめご了承ください。

※本記事は、2022年12月取材当時の内容です。



2023年9月末まで  
キャンペーン中!

社内ネットワークに潜む  
外部脅威・内部不正などのリスクを無料調査中!  
評価プログラムのお申し込みはこちらから!



## Endpoint Manager On-premises & Cloud 導入事例

### “LANSCOPE エンドポイントマネージャー オンプレミス版”と “クラウド版”をハイブリッド運用し、在宅勤務の情報漏洩対策に活用

SCSKグループのなかでコンタクトセンターやバックオフィス業務を中心に、ITを活用したBPO(ビジネス・プロセス・アウトソーシング)事業を手がけるSCSKサービスウェア株式会社。同社では、業務利用のスマホ端末やテレワーク利用のPC端末を含めたIT資産管理とセキュリティ強化のために、“LANSCOPE エンドポイントマネージャー オンプレミス版”および“クラウド版”(以下エンドポイントマネージャー オンプレミス版/クラウド版)を順次導入してきた。導入の経緯や効果などについて、同社 システム統括部 副部長の柴田 裕之 氏と同部 第二運用課の森 達昭 氏に話を聞いた。

#### SCSK サービスウェア株式会社 様

設立：1983年(昭和58年)3月  
業種：情報通信業  
デバイス数：オンプレミス版 4,200台/クラウド版 1,100台

##### 導入の経緯

#### 法令対応やスマホの普及を背景に セキュリティ対策を強化

2005年の個人情報保護法施行以降、同社でもセキュリティへの意識・対策の重要性が高まった。当時の対策はファイアウォールやアンチウィルスソフト導入が中心であったが、インシデントによる情報漏洩への対策や内部不正抑止を目的としたPC操作ログの取得のため、2008年に“エンドポイントマネージャー オンプレミス版”を導入した。その後、スマホの業務利用が増えたことで、2013年に“クラウド版”も導入。PCと同等の機能を持つスマホを適切に管理するため、端末管理や制御の仕組みなどの運用面も整備した。

##### 選定のポイント

#### 管理コンソールの使い勝手の良さ、 機能面の優位性が決め手に

“エンドポイントマネージャー オンプレミス版”の選定ポイントとして、柴田氏は、直感的に操作ができるWebコンソール画面で、取得したい情報が一覧化されたり、レポート生成されたりすることや、他製品との比較における機能面の優位性を挙げた。“クラウド版”については、先行して導入した“オンプレミス版”との連携や、スマホとPCを一元管理できる点が選定の決め手となった。

##### 導入の効果

#### 在宅勤務への移行・拡大に伴い、 社内のセキュリティ環境を社外でも維持

同社では「間接部門のスタッフが基幹系システムなどを扱う社内ネットワーク」と「BPO事業で利用する外部の環境」という2つの



環境で“エンドポイントマネージャー オンプレミス版”を利用している。特にBPOサービスでは、コールセンターの対応履歴といった重要な情報を顧客企業の環境で保管するケースがあるため、より厳密なポリシーでの端末管理が求められる。情報漏洩対策として、私物のUSBメモリーやスマホの接続を防ぐため、デバイス制御機能などを活用しているとのことだ。

また、“クラウド版”については、導入当初は業務用スマホを管理するMDMとして利用していたが、在宅勤務が普及したことで、社内ネットワーク外で利用する持ち出しPCの管理にも活用することになった。端末紛失時の対応フローとして位置情報確認や、業務に不要なアプリのインストールや起動を防ぐソフトウェア・アプリケーション管理の機能を活用しているという。

##### 今後の展望

#### 自社活用で得られたノウハウや知見を、 顧客企業に対しても展開

同社では、従業員の自席PC側には“エンドポイントマネージャー オンプレミス版”の、自席PCの仮想デスクトップ(画面転送)になっていてデータを保持しないようにしている持ち出しPC側には“クラウド版”のエージェントをインストールしており、「ハイブリッド運用」を行っている。さらにその後、“オンプレミス版”の管理サーバーを仮想化(IaaS上に移行)するなど、ビジネスニーズに応じて利用形態を変化させている。

今後は、この自社運用で蓄積したノウハウを、同社がBPOサービスを提供する顧客企業に対しても展開していく。

※本記事は、2022年11月取材当時の内容です。

MOTEXのIT情報サイト「wiz LANSCOPE」では、同社が手がける“エンドポイントマネージャー”運用サポートサービスやその事例についてもご紹介しています。

IT運用サポートサービス  
「PrimeDesk®」とは?



電気通信事業者への  
運用サポート事例



IT製品の検証等を手がける  
企業への運用サポート事例



## Endpoint Manager Cloud 導入事例

### オンプレミス型のIT資産管理ツールから クラウド型の“LANSCOPE エンドポイントマネージャー クラウド版”に移行 テレワークなど多様化する働き方に合わせたデバイス管理とサーバーの運用負荷を削減

2005年に設立された株式会社ユーグレナ。微細藻類ユーグレナ(和名:ミドリムシ)、クロレラなどを活用した食品、化粧品等の開発・販売やバイオ燃料などの製造開発を手がける同社は、テレワーク制度の導入といった社員の働き方の多様化を受け、PC・モバイル端末の一元管理や操作ログの管理に課題を抱えていた。そこで、それまで利用していたオンプレミス型のIT資産管理ツールから“LANSCOPE エンドポイントマネージャー クラウド版(以下エンドポイントマネージャー)”へ移行した。導入の経緯や導入後の効果などについて、株式会社ユーグレナの菌田 玲子氏(ユーグリーサクセス課 課長)に話を聞いた。

#### 株式会社ユーグレナ 様

設立：2005年(平成17年)8月  
事業内容：  
1. ユーグレナ等の微細藻類等の研究開発、生産  
2. ユーグレナ等の微細藻類等の食品、化粧品の製造、販売  
3. ユーグレナ等の微細藻類等のバイオ燃料技術開発、環境関連技術開発  
4. バイオテクノロジー関連ビジネスの事業開発、投資等  
デバイス数：690台



##### 導入の経緯

#### オンプレミス型のIT資産管理ツールの 運用で顕在化した課題

同社では、従来はオンプレミス型のIT資産管理ツールを導入していた。しかし、コロナ禍やテレワーク制度の導入により、自宅などの社外で働く社員が増えるなど、業務環境が変化。社内ネットワークへの常時接続が前提の仕組みとしていたPC操作ログ等の取得がリアルタイムに実施できなくなるという課題を抱えていた。また、会社の成長に伴い従業員が増え、管理する業務端末も増えたことで、ログを保存するサーバーの容量が逼迫。ログの保存期間が短くなったり、サーバーメンテナンスに時間を要するといった課題も顕在化した。

そのため、情報セキュリティ対策の一環であるログ取得や、今後のサーバーのメンテナンスにかかる担当者の負荷軽減を考慮し、クラウド型のIT資産管理ツールへの移行を検討した。

##### 選定のポイント

#### 60日間無料体験版で使いやすさを実感 決め手はPC・スマホの一元管理

エンドポイントマネージャーは、取得した操作ログを標準で2年間保存可能で、クラウド型製品のため、サーバーの運用・メンテナンスも不要。長期的・安定的にログが保存できる点が導入の決め手となった。

加えて、菌田氏は「PC・スマホの一元管理が可能」と「使いやすさ」も挙げた。エンドポイントマネージャーは、USBメモリーの利用制御機能などを搭載するなど、PC管理に必要な各種機能が充実しているうえに、MDMとしてスマホも管理可能だ。さらに、日々利用する管理ツールは「使いやすさ」が重要であるが、管理コンソールを直感的に操作することができたという。

##### 導入の効果

#### IT資産の状況が可視化できたことで、 よりきめ細かな対応が可能になった

従来は、IT資産管理の点でもリアルタイムな状況把握が難しく、Excelの資産台帳で運用していた。しかし、エンドポイントマネージャーはインターネット接続されている端末の情報を自動取得するため、リアルタイムかつ正確に資産状況が把握できるようになり、手運用を完全に廃止。関連会社の端末も含めて統合管理し、全端末の棚卸を短期間かつ精度高く実施できるようになったという。

また、エンドポイントマネージャー上に管理を一本化したことで、端末の在庫管理や修理対応などを外部委託している業者との連携が効率化されたり、Windowsアップデートの適用状況を把握できるようになったことで、未適用の端末を利用してはいる社員に適切なフォローができるようになった。

##### 今後の展望

#### スマホ管理を エンドポイントマネージャーに統合 クラウドの強みを活かし、 セキュリティ体制の再構築へ

菌田氏によると、今回の導入が、テレワーク時代に合ったクラウドベースのネットワーク環境にシフトする第一歩となり、「リモートワークに最適な環境・体制を構築するベース」になったという。今後も、会社の成長・働き方の多様化により管理端末が増えていくなかで、スマホ管理など、エンドポイントマネージャーのまだ使い切れていない他の機能も利用して、より効率的かつ効果的なIT資産管理体制を構築していきたいという。

※本記事は、2022年11月取材当時の内容です。

# Endpoint Manager On-premises

## PC 導入の季節を乗り切る！

# “LANSCOPE エンドポイントマネージャー オンプレミス版”を活用した効率的な PC のキitting・メンテナンス方法

**CHECK !**  
PC導入時に知っておきたい“LANSCOPE エンドポイントマネージャー オンプレミス版”活用方法

3月～4月は組織変更や人事異動、新入社員の入社などが重なり、企業・組織のIT資産管理担当者様にとっては、大量の新しいPCの手配やキitting作業に追われる季節です。また、それらの対応に加えて、引き続き正しく資産管理を行っていくためにも、会社・組織の新しい情報に合わせて“LANSCOPE エンドポイントマネージャー オンプレミス版（以下エンドポイントマネージャー）”のグループ情報や資産情報のメンテナンスも実施する必要があります。今回は新しくPCを導入した際に役立つ、“エンドポイントマネージャー”を活用した効率的なキitting方法とメンテナンス情報をお伝えします。

### POINT 1 「配布機能」を活用した業務アプリの自動インストール

“エンドポイントマネージャー”の「配布機能」では、ファイルやアプリケーションを指定したタイミングで配布・実行することができます。さらに、「新規クライアントへの配布設定」という機能もあり、事前にOSのバージョンやインストールアプリの条件を設定しておくことで、クライアント(MR)インストール時に条件に一致すると自動で事前設定した配布物を配布・実行することができ、新しいPCに対するキitting作業の工数削減にご活用いただけます。以下に、この新規クライアントへの配布設定手順をご紹介します。

#### STEP 1 自動インストールするアプリケーションの設定

PCのキitting時に自動インストールしたいアプリケーションを「配布物の作成」から設定します。この時、配布・実行のスケジュールを設定する項目がありますが、クライアント(MR)インストール時にインストールさせたい場合には「すぐに配布する」「すぐに実行する」を選択します。

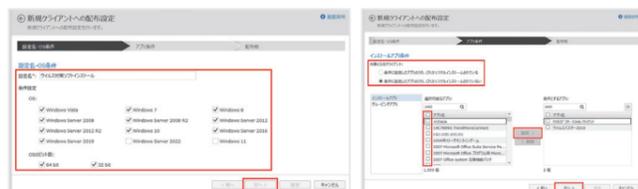


#### STEP 2 アプリケーションを自動インストールする条件の設定

次に、自動インストールする条件を「新規クライアントへの配布設定」から設定します。

条件は、OSとインストールされているアプリケーションから設定できます。例えば、PCのキitting時にウイルス対策ソフトをインストールしたい場合には、ここで「OSがWindows 11」、かつ、「指定したウイルス対策ソフトがインストールされていない」という条件を設定すると、指定したウイルス対策ソフトをインストールさせることができます。

なお、この配布設定は、OSの種類で条件を設定できるため、サーバーOSにはアプリケーションをインストールさせたくないといったシーンにもご活用いただけます。



**MEMO**  
配布物の作成時にアプリケーションに設定されているパラメーターを付与することで自動インストールが可能です。  
※アプリケーションにより動作は異なります

#### STEP 3 クライアント (MR) をインストールする

新しくクライアント(MR)をインストールした際、STEP 2で指定した条件に基づいて自動的に配布・実行が行われます。配布結果は「クライアントへの配布一覧」でご確認いただくことができます。

### POINT 2 “エンドポイントマネージャー”のグループメンテナンス

“エンドポイントマネージャー”ではクライアント(MR)を部署ごとや拠点ごとにグループ分けして管理しますが、組織変更・人事異動や新しいPCの導入がある際、この「グループ」のメンテナンスが実施できていないと、意図した資産管理ができない可能性があります。グループのメンテナンス方法はいくつかありますが、今回は複数の端末情報をまとめてメンテナンスする際に便利な方法を3つご紹介いたします。

#### CASE 1 ハードウェア資産情報をエクスポートし、編集してインポートする

ハードウェア資産情報をCSVファイルとしてエクスポートし、Excelなどで各グループ(グループ1～5)を新しい情報に編集します。その後は「一括インポート」から編集したCSVファイルを取り込むことで、新しい情報を反映させることができます。



**MEMO**  
グループ名の先頭に「01」「02」などの数字を記入することで、管理コンソールにおいてグループツリーを意図した順番に並べることができます。

#### CASE 2 「メッセージ・アンケート機能」で端末の利用者自身から情報を収集する

「メッセージ・アンケート機能」を利用してPCの利用者に自身が所属するグループを回答してもらい、その情報を基にグループ構成を変更できます。「メッセージ・アンケート配布」よりアンケートを作成します。質問項目によって各グループ(グループ1～5)を設定することでグループメンテナンスを実施できます。



**MEMO**  
アンケート作成時に「グループ情報のファイルを使用する」という設定を利用すると、アンケートの質問に対して、現在のグループ情報を選択式で回答させることができます。

#### CASE 3 Active Directory の OU 情報と連携する

WindowsのActive DirectoryにおけるOU(組織単位)の構成情報をグループ構成としてインポートできます。

Active Directoryからログオンユーザー名とOU情報をCSVファイルとしてエクスポートします。このCSVを「一括インポート」から“エンドポイントマネージャー”にインポートすると、Active DirectoryのOU情報に基づいてグループが作成され、OUに所属するPC端末を一括で対象グループに移動することができます。

No.	ログオンユーザー名	OU01	OU02	OU03	OU04
1	taru.motere	会社	東京本部	営業部	営業1課
2	kunihito.hida	会社	東京本部	営業部	営業2課
3	hirohide.negami	会社	東京本部	CS部	サポート1課
4	masanori.morimitsu	会社	東京本部	CS部	サポート2課
5	toru.katogi	会社	大阪本社	営業部	営業3課
6	kazumi.maeshiro	会社	大阪本社	営業部	営業4課
7	bundo.kumita	会社	大阪本社	CS部	サポート3課

**MEMO**  
インポート時に、キー項目は「ログオンユーザー名」とし、インポート項目は「OU1」を「グループ1」といった形でグループ情報と紐づけます。

**お役立ち情報!**

グループメンテナンス方法は、LANSCOPE POTALに掲載の「グループ構成を最新の状態にする」の資料もご覧ください。

<https://tryweb2.motex.co.jp/users/jp/onlinehelp/inflection/#C9-442>  
※ログインにはID/PWが必要です

# LANSCOPE NEWS 101号 読者アンケート結果レポート

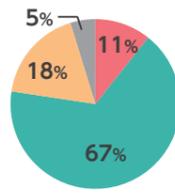
調査期間：2023年2月1日～3月31日 | 回答方法：Web | 有効回答数：168

前号（2023年2月）において、LANSCOPE ユーザー様をはじめとする購読者の皆様にお伺いした、お勤め先のセキュリティ対策に関するアンケートの結果をご報告します。



## Q1 情報セキュリティ対策の状況を教えてください。十分実施できていると思いますか？

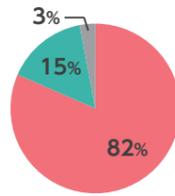
それぞれの企業が属する業界で示されているガイドラインに沿ってセキュリティ対策を実施されていることが多いようです。しかし、約2割の企業においては、ガイドラインを把握していなかったり、ガイドラインを把握していても業界水準以下の対策状況であると感じておられることが分かりました。企業・組織におけるセキュリティ対策は、第一歩として専門機関や業界団体が推奨するガイドラインを確認することが大切です。



- 1 業界における情報セキュリティガイドラインを把握しており、水準以上の対策状況だと思う
- 2 業界における情報セキュリティガイドラインを把握しており、水準並みの対策状況だと思う
- 3 業界における情報セキュリティガイドラインを把握しているが、水準以下の対策状況だと思う
- 4 分からない

## Q2 自社の情報セキュリティ上の課題について把握できていますか？

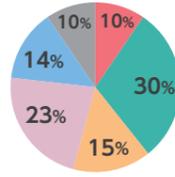
8割以上の企業が、自社の課題を把握できていると回答されました。しかし、約2割の企業においては、課題を把握できていなかったり、外部からの指摘によって課題に気付かれることがあるようです。中には、「第三者に確認してもらったことがないため、自社内で課題を十分把握できているのか、妥当性が分からない」といったご意見もありました。必要なセキュリティ対策を検討するには、まずは自社の課題を把握することが重要です。



- 1 自社で把握できている
- 2 取引先など他社からの指摘によって把握している
- 3 把握できていない

## Q3 新たな情報セキュリティ対策を行う場合、どのようなタイミングで実施しますか？一番近いものをお選びください。

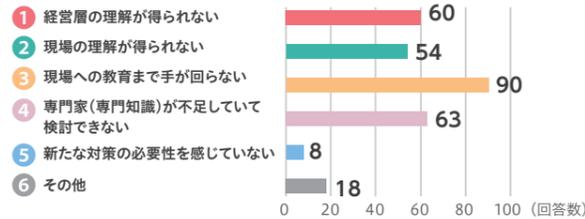
昨今、度々重大なセキュリティインシデントの報道がありますが、こうした時事ニュースをきっかけに、自社の対策を見直す企業や、専門機関からのガイドライン発表を受けて新しいセキュリティ対策に取り組まれる企業が多いようです。「その他」には、IT機器の入れ替え時や、ISMSなどの監査、親会社や取引先といった関係先の方針変更といったきっかけがありました。



- 1 自社での事件・事故などをきっかけに、経営層から指示があったとき
- 2 他社での事件・事故の報道などをきっかけに、経営層から指示があったとき
- 3 法令などが公布されたとき
- 4 情報セキュリティ専門機関(IPAなど)からガイドラインが発行されたとき
- 5 所属業界の情報セキュリティガイドラインが発行されたとき
- 6 その他

## Q4 新たな情報セキュリティ対策を実施するうえで、どのような課題がありますか？（複数選択可）

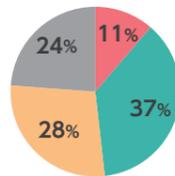
「現場への教育まで手が回らない」という回答が最も多く、情報システム担当者や関係者のセキュリティリテラシーが高くても、なかなか現場の一般社員までセキュリティ教育が行き届かないという実情が見えてきます。「その他」には、必要な予算が割けないといった費用面での課題が多く挙げられました。



- 1 経営層の理解が得られない
- 2 現場の理解が得られない
- 3 現場への教育まで手が回らない
- 4 専門家(専門知識)が不足していて検討できない
- 5 新たな対策の必要性を感じていない
- 6 その他

## Q5 パートナー企業や業務委託先企業の情報セキュリティ対策状況を把握していますか？

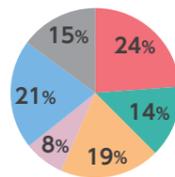
昨今はターゲットとする企業に直接サイバー攻撃を仕掛けるのではなく、関連会社や取引先・委託先企業の脆弱性を狙って攻撃し、その企業を踏み台として最終的にターゲット企業に不正侵入を行う「サプライチェーン攻撃」が増加しています。パートナー企業や委託先企業の対策状況を把握しているかという質問に対しては、約半数の企業が定期的な確認をしていると回答されました。しかし、半数の企業では、取引開始時のみ単発で確認をしていたり、特に確認はしておらず対策状況を把握できていないことが分かりました。



- 1 対策状況は把握しており、定期的な状況が改善されていることを確認している
- 2 対策状況を把握しており、定期的な状況の確認をしている
- 3 取引開始時に対策状況を確認し、それ以降は把握していない
- 4 把握していない

## Q6 業務利用しているモバイル端末のウイルス対策について、ご利用のOSと対策状況を教えてください。

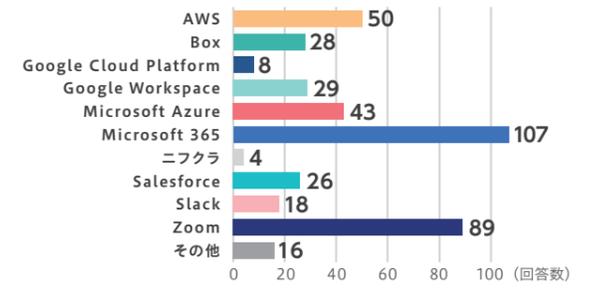
テレワークの普及によって、従業員に業務端末としてスマホやタブレットを配布する企業も増えています。こうした端末は従来の携帯電話とは異なり、PCと同等の機能を備えているため、適切な管理とセキュリティ対策が必要です。モバイル端末へのセキュリティ対策について伺ったところ、半数以上の企業においてウイルス対策を実施されていることが分かりました。



- 1 すでに対策している(iOS)
- 2 すでに対策している(Android)
- 3 すでに対策している(iOS/Android両方)
- 4 対策はしていないが、不安はない
- 5 対策をしていないため、不安がある
- 6 モバイル端末を利用していない

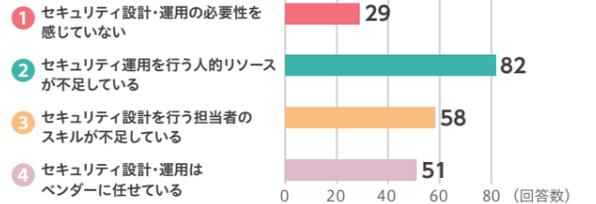
## Q7 業務利用しているクラウドサービスを教えてください。(複数選択可)

昨今、多くの企業においてDX推進やテレワークの普及が進み、業務システムのクラウド化が著しくなっています。業務利用しているクラウドサービスについてお伺いしたところ、Office製品をサブスクリプションで利用できる「Microsoft 365」が最も多く、その他にもWeb会議システムの「Zoom」や、さまざまなシステムの基盤となっている「AWS」が多く挙げられました。また、「その他」の中には、セキュリティ上の課題から「基本的にクラウドサービスは利用しない」と回答された企業も見受けられました。



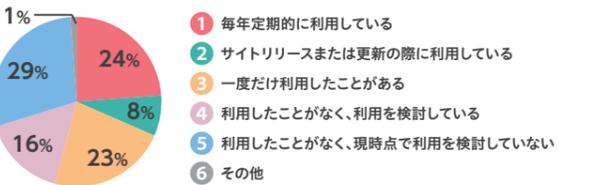
## Q8 業務利用しているクラウドサービスのセキュリティ設計・運用状況について教えてください。(複数選択可)

Q7に関連して、クラウドサービスのセキュリティ対策の運用についてお伺いしたところ、「セキュリティ運用を行う人的リソースが不足している」という回答が最も多い結果となりました。各種クラウドサービスのセキュリティ設定や監査ログの管理といった日々の運用には専門知識が必要なことから、多くの企業において、セキュリティ人材の確保や管理担当者様の負荷増大に悩まれていることがうかがえます。

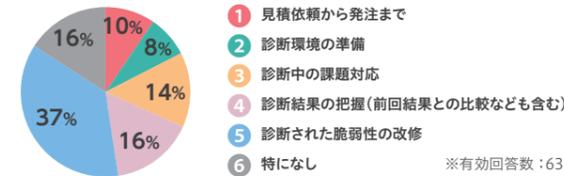


## Q9-1 セキュリティ診断サービスの利用状況について教えてください。

セキュリティ診断(脆弱性診断)サービス(他社サービスを含む)の利用状況についてお伺いしたところ、半数以上の企業において、1回以上は利用されたことがあるという結果になりました。しかし、約3割の企業では、今までに利用したことがなく、特に利用の検討もされていないという状況が分かりました。



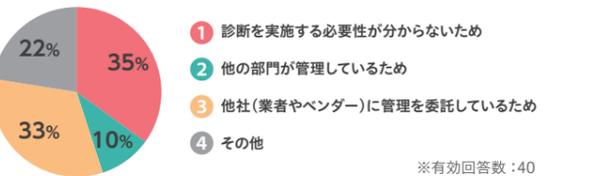
## Q9-2 Q9-1で「①毎年定期的に利用している」または「②サイトリリースまたは更新の際に利用している」を選択された場合、セキュリティ診断サービスを利用する際、負担に感じる工程を教えてください。(複数選択可)



- 1 見積依頼から発注まで
- 2 診断環境の準備
- 3 診断中の課題対応
- 4 診断結果の把握(前回結果との比較なども含む)
- 5 診断された脆弱性の改修
- 6 特になし

セキュリティ診断サービスの利用にあたっては、診断結果の把握や診断された脆弱性の改修など、診断後の対応に苦慮されている実情がうかがえます。

## Q9-3 Q9-1で「⑥利用したことがなく、現時点で利用を検討していない」を選択された場合、その理由は何ですか？一番近いものをお選びください。



- 1 診断を実施する必要性が分からないため
- 2 他の部門が管理しているため
- 3 他社(業者やベンダー)に管理を委託しているため
- 4 その他

「診断の必要性が分からない」「ベンダーに任せている」といった回答が多く、また「その他」には「予算がない」といった回答もありました。

## Q10-1 NDR製品の導入状況について教えてください。

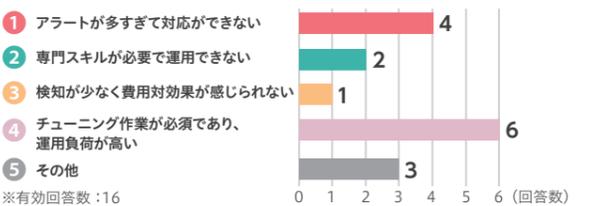
最後にNDR製品の導入状況についてお伺いしました。NDR製品を実際に導入して利用している企業は約1割にとどまっているものの、導入を検討されている企業は約3割いらっしゃいました。エンドポイントだけでなく、ネットワーク全体のセキュリティレベルを上げるソリューションの検討が進んでいるようです。



- 1 利用している
- 2 検討している
- 3 利用の予定はない
- 4 利用をやめた

## Q10-2 Q10-1で「①利用している」または「④利用をやめた」を選択された場合、NDR製品導入時の課題について教えてください。

一方で、実際にNDR製品を利用されたことがある企業においては、アラートへの対応や、チューニング作業といった管理担当者様の運用負荷が課題となっていることがうかがえます。



- 1 アラートが多すぎて対応ができない
- 2 専門スキルが必要で運用できない
- 3 検知が少なく費用対効果が感じられない
- 4 チューニング作業が必須であり、運用負荷が高い
- 5 その他

多くのご回答をいただき、誠にありがとうございました。皆さまがより良いセキュリティ体制を構築できるよう、本調査結果がお役に立てば幸いです。また、本調査にありましたウイルス対策、Microsoft 365をはじめとしたクラウドサービスのセキュリティ対策、セキュリティ診断サービス、NDR製品については、今号の製品・サービス情報にて、MOTEXが提供する各種プロダクト・サービスを幅広くご紹介しております。ぜひ、貴社のセキュリティ対策にお役立ていただけるものがないかご覧いただき、ご検討いただけますと幸いです。

# デジタル注意報



茂礼手 太郎  
茂礼手課長と呼ばれている。  
何かとやらかしては、  
布施木君に注意される

前号からご紹介している、茂礼手課長と布施木さんのデジタル注意報。  
前回は「セキュリティ 7つの習慣」について、  
チェック形式でご紹介しましたが、皆さんはいくつ当てはまりましたか？  
えっ、1～9個の「雨」でしたって!? それはいけませんねえ。  
では、今号から数回にわたり紹介する「セキュリティ 20の事例」を読んで、  
セキュリティリテラシーを上げていきましょう。



布施木 ます子  
布施木君と呼ばれている。  
なんだかんだと  
茂礼手課長をサポート

## 理解を深める20の事例とQ&A

～ 陥りがちな落とし穴「オフィス編」～

その対応、合っていますか？ 正しい選択肢を選びましょう！

### Q1 面倒だからと、パスワードの文字列を単純なものに設定した

情報システム部門から「社内システムのパスワードを初期値から変更するように」という通達を受け取り、「飼っているペットの名前(英小文字)」「自分の誕生日」を組み合わせた文字列でパスワードを設定した。

- ① 英数字を組み合わせているのでOK
- ② ペットの名前は推測できないのでOK
- ③ 英字(大文字・小文字)や数字、記号を混ぜた方がよい



### Q2 業務の利便性が落ちるからと、管理者権限のIDとパスワードを部署内で共有した

部署の業務システムは、担当者ごとに情報へのアクセス権限が細かく設定されているが、担当者の不在時に業務の利便性が落ちるので、全ての情報へアクセスできる管理者権限のIDとパスワードを共有する運用が続いている。

- ① 共有しても問題ない
- ② 共有するのは問題がある



## A1 ③ 英字(大文字・小文字)や数字、記号を混ぜた方がよい



**解説** パスワードは他人から推測されやすい文字列に設定すると、簡単に推測される可能性があります。社内システムなどの認証用IDとパスワードが他人に知られると、情報漏洩事故につながります。

### パスワードが盗まれるとどうなる被害に遭う？

IDとパスワードは、ITシステムやサービス等を利用するユーザーが本人であることを証明するための大切な情報です。企業システムの管理者情報が漏れれば社内ネットワークに不正に侵入され、重要情報が外部に盗み出されてしまう可能性があります。

こうした被害に遭わないためには、パスワードを推測されにくい、強いパスワードに設定する対策と、パスワードを盗まれないように適切に管理する対策が欠かせません。

- Point 1** 社員番号や生年月日、名前、ペットの名前など、他人から推測されやすい情報は使わない
- Point 2** 英字(大文字・小文字)や数字、記号を混ぜ、8文字以上のできるだけ長い文字列に設定する
- Point 3** パスワードを書いたメモなどを、目の付くところに貼らない



### MEMO パスワード作成時のルール例

利用するWEBサイトごとに、長く、複雑な文字列で作ったパスワードを設定し、記憶するのは困難です。一例として、オリジナルの文章をもとに、長く、推測されにくく、使い回すことのないパスワードを作る方法をご紹介します！

実際に「123456」「password」「abc123」などの単純な文字列がよく使われています。また、「1qaz」は一見意味のない文字列に見えますが、キーボードの一番左の縦配列です。

もし、手帳などの紙に書いて保管する必要がある場合は、他の文字やダミーパスワードを追加するなどして、わかりにくくする工夫が必要です。

- Step 1** まず適当なフレーズを一つ決める  
「3時のおやつは、カステラが一番」
- Step 2** ローマ字化する(数字と句読点は残す)  
「3ji no oyatsu wa, kasutera ga 1ban」
- Step 3** 単語の頭文字だけを拾っていく  
「3jnow,kg1b」
- Step 4** 大文字・小文字を変更したり、記号を変更または追加したりする  
「3Jnow,#Kg1b」
- Step 5** パスワードの先頭と末尾に配置する文字をあらかじめ決めておく(サイト名が「simple」であれば、先頭は「s」、末尾は「e」)  
「s3Jnow,#Kg1be」-完成!

## A2 ② 共有するのは問題がある



**解説** パスワードは誰かと共有したり、使い回したりすることのないようにしましょう。社内システムなどにアクセスするためのIDやパスワードは、他人に知られないようにする必要があります。

- Point 1** 特に管理者アカウントは、システムを利用する全てのユーザーに影響を与えてしまいます。第三者に知られると、システムを乗っ取られ、情報が外部に盗み出される可能性もあります。
- Point 2** 退職者がパスワードを知ったままになってしまうと、不正が行われた場合に犯人の追跡が難しくなります。IDやパスワードは共有しないことが大事です。
- Point 3** 同じパスワードを設定するなどの「使い回し」も、どれか一つのパスワードが漏れてしまったら、あらゆるシステムやサービスにログインが可能になってしまうため、やめましょう。



# MOTEX TOPICS

2023 Winter / Spring

最近、MOTEXであった  
さまざまな出来事をご紹介します！

bannya\_motex



20230101

MOTEXのマスコットキャラクター・組織を守る番猫「バンニャ」。好評につき、今年も毎月旬な装いに变身して、公式SNSとオフィスに出発しています！

#季節のバンニャ #SNS発信中

bannya\_motex



20230221

デジタルトラストをテーマとしたオンラインイベント「MOTEX DAYS.2023-WINTER-」を開催！次回はAIをテーマとしたSUMMER(8月末予定)を開催準備中です。乞うご期待！

#MOTEX DAYS #オンラインイベント

bannya\_motex



20230318

2月1日から3月18日(サイバーの日)は「サイバーセキュリティ月間」でした。MOTEXでは、プロダクトマネージャーやセキュリティアナリストが「サイバーセキュリティの重要性」を啓蒙したり、セキュリティ人材の裾野を広げる活動を行っています。

#エバンジェリスト #講演 #執筆

bannya\_motex



20230403

MOTEXでは「熱量と想像力で挑戦し、変化を楽しむプロであれ」という価値観「MOTEX VALUE」を大切にしています。熱量(Passion) 想像力(Imagine) 挑戦(Try)の頭文字から取った「PIT(核)」がメンバーの合言葉です！

#MOTEX VALUE #合言葉はPIT

bannya\_motex



20230405

春の展示会シーズンは「情報セキュリティEXPO」や「日経クロステックNEXT」などの展示会に多数出展しました。今後も、オフラインイベントでLANSCOPEブランドの製品・サービスの最新情報をお届けしてまいります！

#オフラインイベント #展示会

bannya\_motex



20230412

Deep Instinct社より「PARTNER OF THE YEAR AWARD 2023」をいただきました。MOTEXは今後も同社と連携し、高性能なAIアンチウイルスをより手軽に導入・運用いただけるよう、サービス・販売を強化してまいります。

#Deep Instinct #パートナー

bannya\_motex



20230416

ラグビーチーム・リコーブラックラムズ東京のリーグ最終節の試合に冠協賛し、「LANSCOPE MATCH DAY」を開催。バンニャも秩父宮ラグビー場に参戦！チームのマスコットキャラクターのラムまる君と一緒に応援しました♪

#ラグビー応援 #ブラックラムズ東京

bannya\_motex

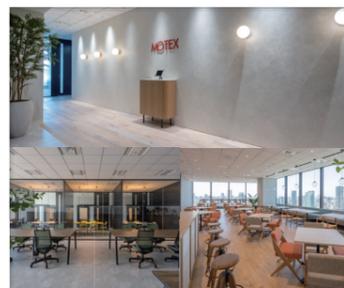


20230425

MOTEXのインサイドセールス部門が、スマートキャンプ社主催のアワードで優秀賞を受賞しました。今後も、お客様にLANSCOPEブランドの製品・サービスの有益な情報をお届けしてまいります。

#インサイドセールス

bannya\_motex



20230508

MOTEX東京本部は5月より住友不動産東京三田ガーデンタワー(最寄り:三田駅・田町駅)に移転しました。お近くにお越しの際はぜひお立ち寄りください。

#オフィス移転 #MOTEX東京本部

エバンジェリスト達が

note

はじめました

ぜひご覧ください！



総合セキュリティカンパニーとして、

「より多くの皆さまに“サイバーセキュリティの重要性”やトレンド、お役立ち情報をお伝えしていきたい」

「MOTEXの取り組みを知ってもらいたい」という想いから、

この度noteの企業公式アカウント(ブログ)を立ち上げました。

プロダクトマネージャーやセキュリティアナリスト、情報システム担当者をはじめとしたMOTEXのメンバーが、企業の経営層からビジネスパーソン、セキュリティに興味・関心がある一般の方までお読みいただける有用なコンテンツを発信してまいります！ぜひご覧ください。

FOLLOW US!

旬な情報をお届け! / MOTEX公式SNSアカウント

NEW



Facebook  
エムオーテックス株式会社  
@motex.jp



Twitter  
MOTEX\_LANSCOPE  
@MOTEXPR



YouTube  
MOTEX公式\_LANSCOPE  
@LanScopePR



note

note  
エムオーテックス  
(MOTEX) 公式



編集部メッセージ

今年度初めての『LANSCOPE NEWS』102号のお届けとなります。いよいよ暑さが厳しくなってまいりましたが、皆様いかがお過ごしでしょうか。

MOTEXは昨年度、サイバーセキュリティに関する幅広い課題解決をご支援する「総合セキュリティカンパニー」を目指し、4月に京セラコミュニケーションシステム(KCCS)のセキュリティ事業部(旧SecureOWL)と事業統合し、10月にはすべての製品・サービスをLANSCOPEブランドに統一するなど、大きく変化しました。また世の中では、生成AI「ChatGPT」が登場。セキュリティの領域では、ますます進化するAIにどのように対処するか、あるいはAIをどのように活用していくかに注目が集まっています。誌面でもAI関連の情報を多く掲載しておりますので、ぜひご覧ください。

NEWS編集部では、これからも、サイバーセキュリティやMOTEX・LANSCOPEの旬な情報を皆様にお届けしてまいります。今後ともご愛読の程よろしくお願ひ申し上げます。

[企画・編集]

MOTEX ブランドコミュニケーション部 (NEWS編集部)  
坂本 琴音・湯口 真輝・大場 美鈴

Special Thanks!! / ご協力企業様

- P 8 : SOMPORリスクマネジメント株式会社 様
- P14 : ダークトレース・ジャパン株式会社 根本 祥平 様
- P16 : フリュー株式会社 様
- P17 : SCSKサービスウェア株式会社 様
- P18 : 株式会社ユーグレナ 様

MOTEXライター

- P 3 : 宮崎 吉朗
- P 5 : 武藤 諒
- P 7 : 西村 忍・疋田 一平
- P 9 : 池田 淳
- P11 : 熊坂 渉・金原 将人
- P19 : 笹山 真実子

