MOTEX

民間企業に学ぶ!!
校務DX実現にLNSCOPEでできること

2023年10月

エムオーテックス株式会社

会社概要

会社名	エムオーテックス株式会社
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 （2012年から資本参加）
事業内容	自社製品の開発・販売、サイバーセキュリティのコンサルティング・ソリューション導入・運用監視サービス

拠点

本社	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	名古屋市中区錦1-11-11 名古屋インターシティ 3F
九州営業所	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3F

校務DXの推進に水を差すセキュリティの課題

ICT利活用の推進に水を差されないよう
セキュリティ対策に「いい製品」をご提案ください

システムの**設定ミス**で進路アンケート結果が生徒に漏えい

学内関係者のユーザー名やメアドが**外部サイトで流通**

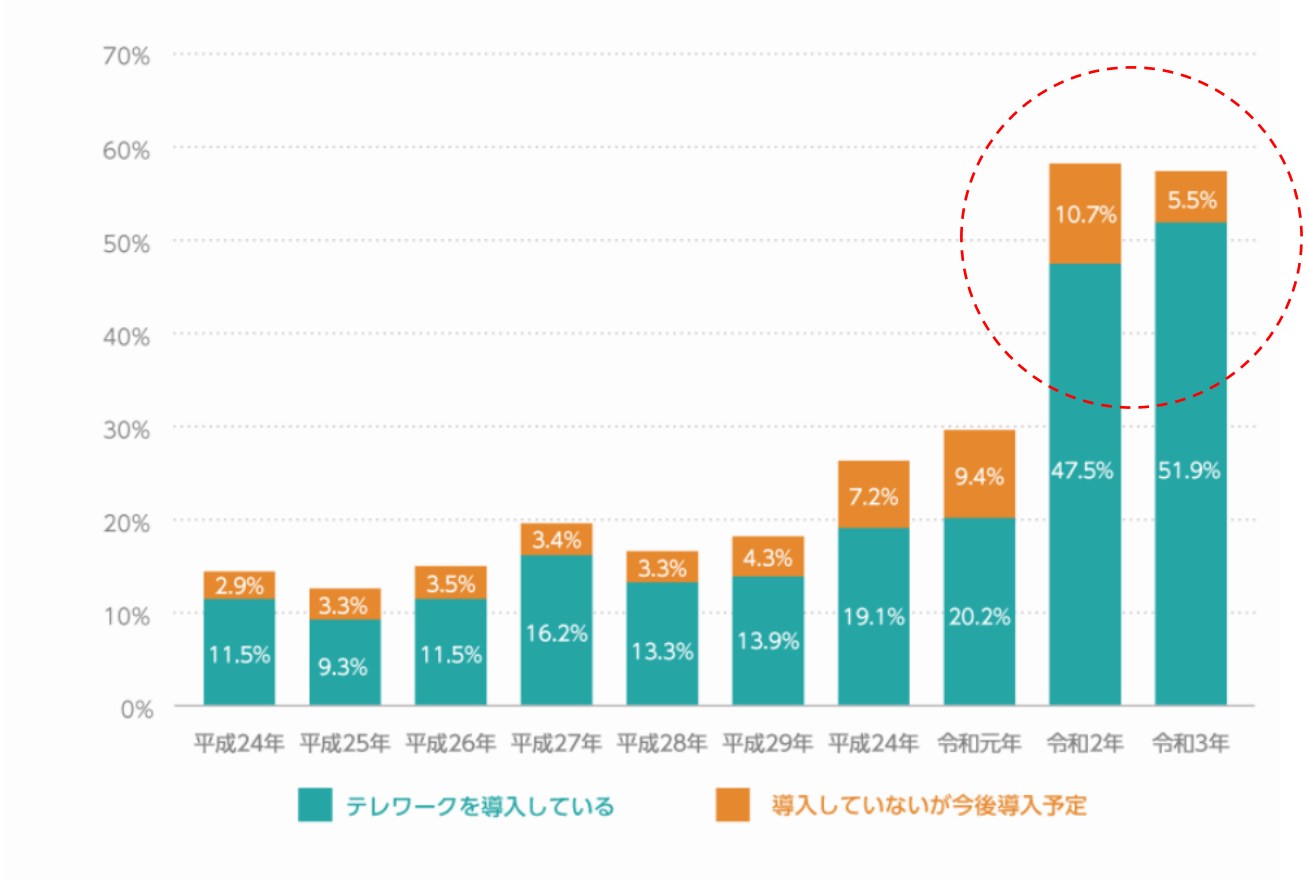
学校見学会中止の通知**メールを誤送信**

生徒の個人情報含む**USBメモリを紛失**

情報漏えいが**いじめ**につながったと認定

セキュリティ対策は民間に学ぶべし！

例えばテレワークは3年前から半数以上の企業が実施
今でも民間企業で選ばれている製品が「いい製品」



出典：テレワーク総合ポータルサイト - 厚生労働省「企業におけるテレワーク導入状況の推移」
https://telework.mhlw.go.jp/telework/trs/

3年前
コロナ禍で8割以上の民間企業がテレワークを実施

付け焼刃だったテレワークが制度として定着

現在
セキュリティ対策についても検討・改善が行われている

校務DXでの提案にイチ押し

コロナ禍のテレワーク需要で導入企業が急増！
市場シェアNo.1を獲得したクラウドIT資産管理ツール

Cloud
LANSCOPE
Endpoint Manager

PC資産・PCセキュリティSaaS市場
メーカーシェアNo.1を獲得

シェア No.1※

※株式会社テクノ・システム・リサーチ「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

選ばれて30年。ぜひセキュリティ対策にLANSCOPEをご提案ください

LANSCOPE Endpoint Manager Cloud

LANSCOPE Endpoint Manager On-premises

LANSCOPE Endpoint Manager for IaaS

LANSCOPE Endpoint Manager × Splunk

LANSCOPE データアナライザー powered by MUCV

LANSCOPE Cyber Protection powered by CylancePROTECT

LANSCOPE Cyber Protection powered by CylanceOPTICS

LANSCOPE Cyber Protection powered by Deep Instinct

LANSCOPE Remote Desktop

LANSCOPE Security Auditor

LANSCOPE Professional Service

- Webアプリケーション脆弱性診断パッケージ
- ネットワーク脆弱性診断パッケージ
- クラウドセキュリティ診断パッケージ
- サイバーリスク健康診断パッケージ
- グループセキュリティレポーティングパッケージ
- Webアプリケーション健康診断パッケージ
- ネットワーク健康診断パッケージ
- Microsoft 365健康診断パッケージ
- サプライチェーンリスク評価パッケージ powered by Panorays
- ネットワーク脅威検知パッケージ powered by Darktrace

本日お伝えしたいこと

1 ゼロトラストに必要な機能の半分がそろう！
LANSCOPEの幅広いラインナップ

2 LANSCOPE エンドポイントマネージャークラウド版が
多くの民間企業で選ばれている理由

3 EDRとEPPどちらがより重要？
“本当に守れる”外部脅威対策とは

本日お伝えしたいこと

1 ゼロトラストに必要な機能の半分がそろう！
LANSCOPEの幅広いラインナップ

2 LANSCOPE エンドポイントマネージャークラウド版が
多くの民間企業で選ばれている理由

3 EDRとEPPどちらがより重要？
“本当に守れる”外部脅威対策とは

ゼロトラストに必要な機能の半分がそろう！LANSCOPEの幅広いラインナップ

ゼロトラストで必要とされる11の技術要素のうち5つをカバー
中でも「MDM」「アンチウイルス」がおすすめです

図２ いわゆるゼロトラストセキュリティに関する要素技術

		①アクセスの真正性に関する要素技術	
	①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
	①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
	①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
		②通信の安全性に関する要素技術	
	②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
①	②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
		③端末・サーバの安全性に関する要素技術	
②	③-1	モバイル端末管理（MDM）(Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③	③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
	③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
④	③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
⑤	③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
	③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

※これらは、「教育情報セキュリティポリシーに関するガイドライン」（令和4年3月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

17

LANSCOPE エンドポイントマネージャー

クライアント型のWebフィルタリングで、
場所を選ばず同じ条件でWeb利用を制御。

LANSCOPE サイバープロテクション

AIアンチウイルスに統合された、
防御にフォーカスした負荷の少ないEDR。

L2Blocker

ネットワーク内のARPパケットを読み取り、
不正端末のアクセスを検知、遮断。
（LANSCOPE エンドポイントマネージャーとの連携製品です）

出典：「GIGAスクール構想の下での校務DXについて」
令和５年３月８日　GIGAスクール構想の下での校務の情報化に関する専門家会議

ゼロトラストに必要な機能の半分がそろう！LANSCOPEの幅広いラインナップ

MDMとしての機能を十分の備えながら
PCのIT資産管理が充実しているのはLANSCOPEだけ

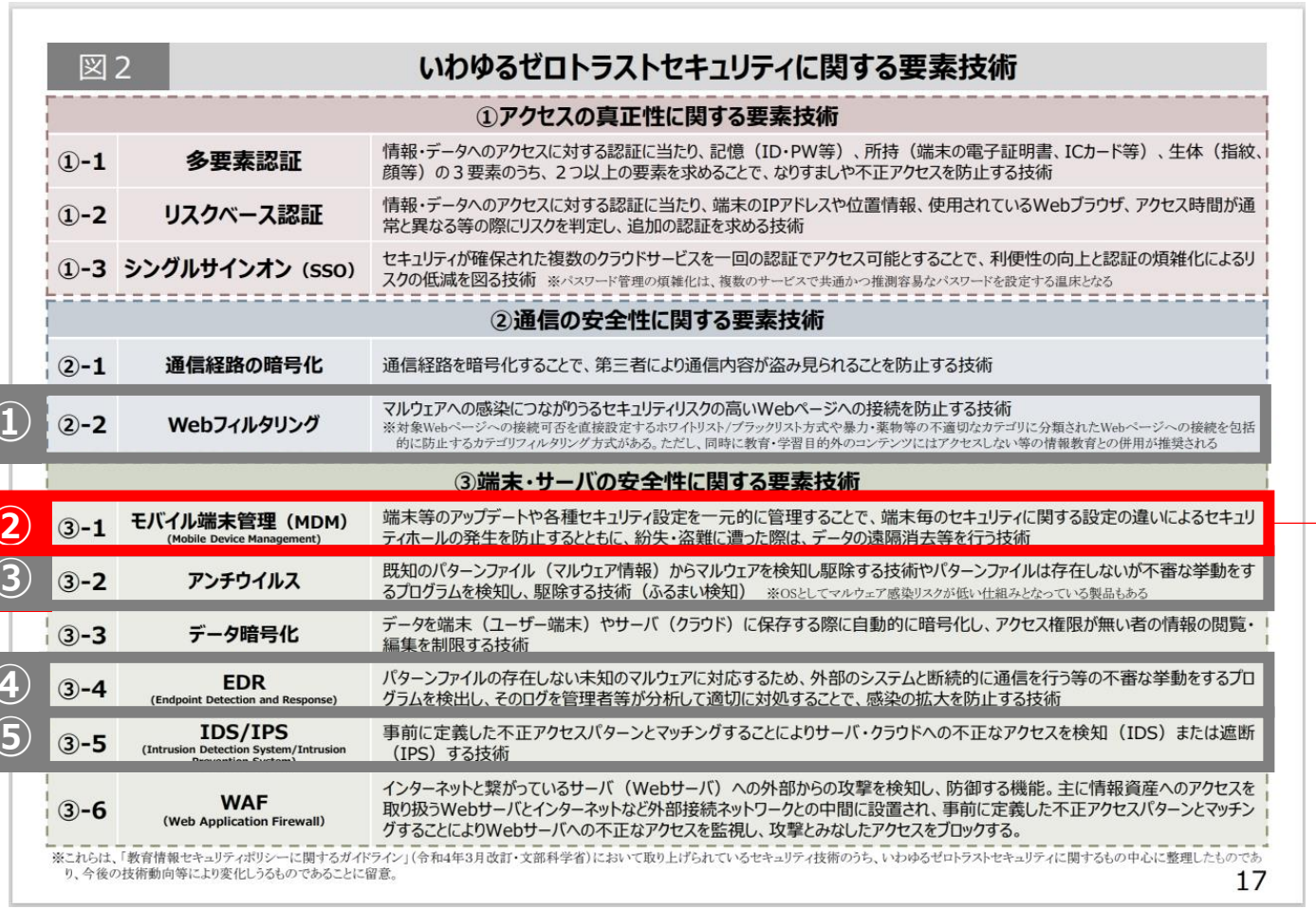


図2 いわゆるゼロトラストセキュリティに関する要素技術

		①アクセスの真正性に関する要素技術	
	①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
	①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
	①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
		②通信の安全性に関する要素技術	
	②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
①	②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
		③端末・サーバの安全性に関する要素技術	
②	③-1	モバイル端末管理（MDM）(Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③	③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
	③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
④	③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
⑤	③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
	③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

※これらは、「教育情報セキュリティポリシーに関するガイドライン」（令和4年3月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

17

出典：「GIGAスクール構想の下での校務DXについて」
令和５年３月８日　GIGAスクール構想の下での校務の情報化に関する専門家会議

LANSCOPE エンドポイントマネージャー

- PC・スマホ・タブレットの一元管理をクラウドで実現。
- 充実の「IT資産管理機能」と「MDM機能」を搭載。
- 使いやすい管理コンソールが評価されて、IT review 顧客評価No.1※を獲得

※ MDM・EMM部門 IT資産管理部門・ログ管理部門 統合運用管理部門の4部門でLeader獲得

ゼロトラストに必要な機能の半分がそろう！LANSCOPEの幅広いラインナップ

「マルウェア感染を未然に防ぐ」を実現
どこよりもお手軽でカンタンなAIアンチウイルス

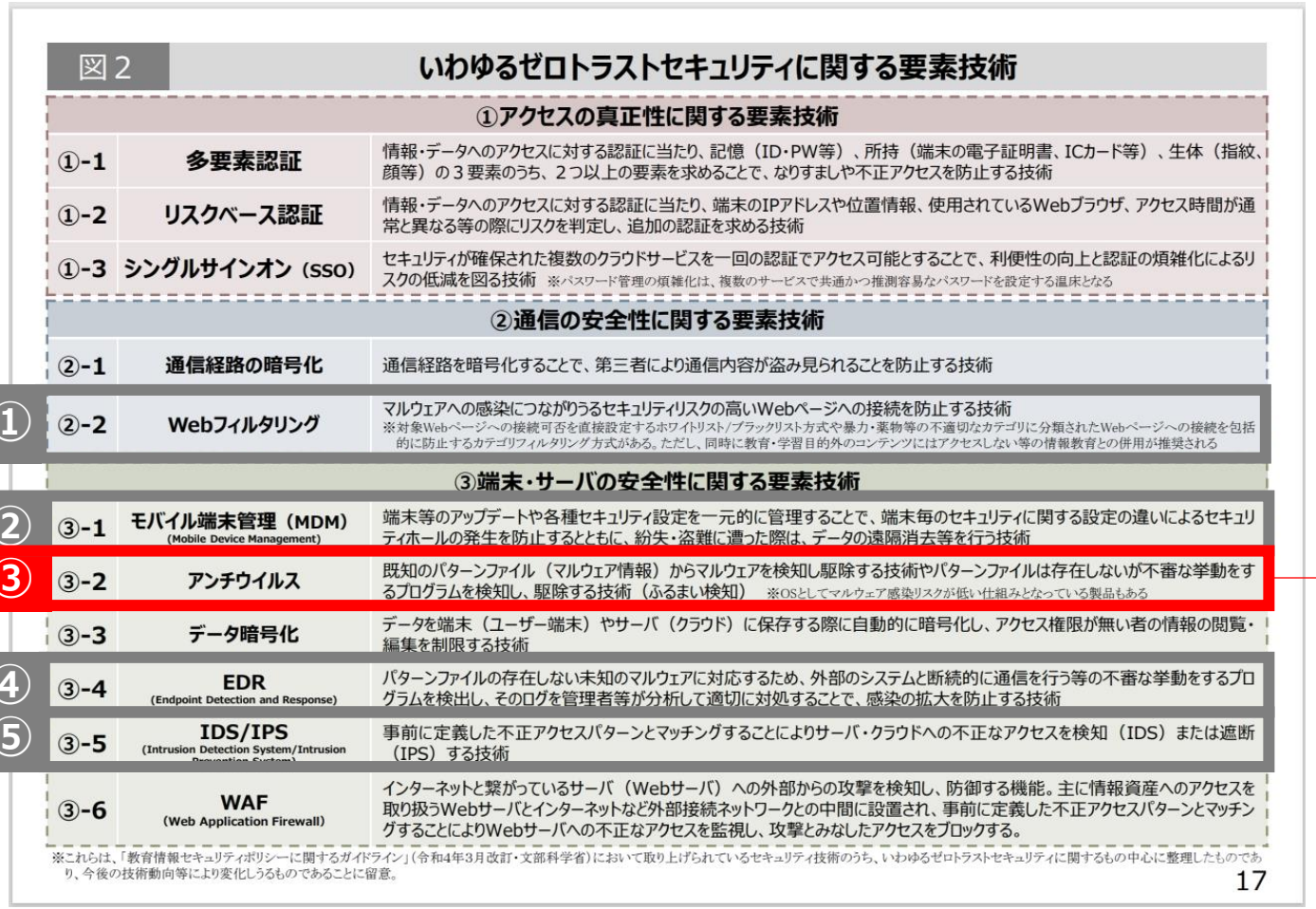


図2 いわゆるゼロトラストセキュリティに関する要素技術

	①アクセスの真正性に関する要素技術		
	①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
	①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
	①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
	②通信の安全性に関する要素技術		
	②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
①	②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
	③端末・サーバの安全性に関する要素技術		
②	③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③	③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
	③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
④	③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
⑤	③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
	③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

※これらは、「教育情報セキュリティポリシーに関するガイドライン」（令和4年3月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

17

LANSCOPE サイバープロテクション

- AIを使った次世代型アンチウイルス
- 99%の高い検知率※で企業をセキュリティリスクから守る
- 高性能のAIアンチウイルスと安心のサポート体制を、低価格でご提供

※ 2018 NSS Labs Advanced Endpoint Protection Test結果より

出典：「GIGAスクール構想の下での校務DXについて」
令和５年３月８日　GIGAスクール構想の下での校務の情報化に関する専門家会議

本日お伝えしたいこと

1 ゼロトラストに必要な機能の半分がそろう！
LANSCOPEの幅広いラインナップ

MDMの提案におすすめ

2 LANSCOPE エンドポイントマネージャークラウド版が
多くの民間企業で選ばれている理由

3 EDRとEPPどちらがより重要？
“本当に守れる”外部脅威対策とは

エンドポイントマネージャーとは

全国9,000社以上のお客様にご導入
MDMとPCのIT資産管理をクラウドでご提供

LANSCOPE
Endpoint Manager

日経コンピュータ 2023年8月31日号
顧客満足度調査 2023-2024運用管理・仮想化ソフト／サービス
（クライアント） 部門 1位

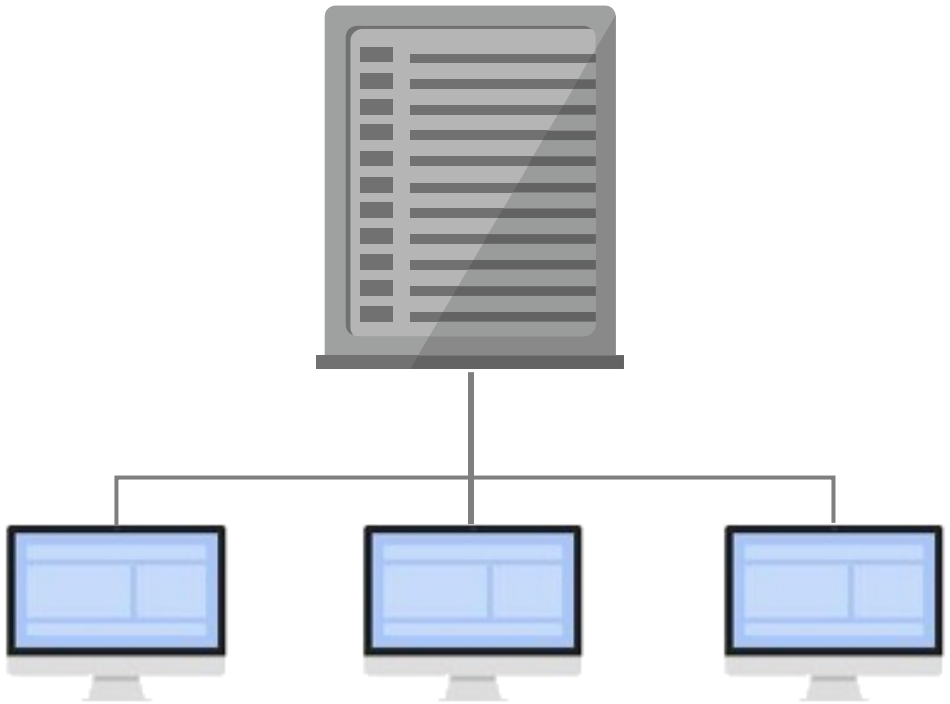
株式会社テクノ・システム・リサーチ
「PC資産・PCセキュリティSaaS市場 メーカーシェア
2022年 ブランド別市場シェア」分野

MDM・EMM部門
IT資産管理部門・ログ管理部門
統合運用管理部門の4部門でLeader獲得

従来の考え方

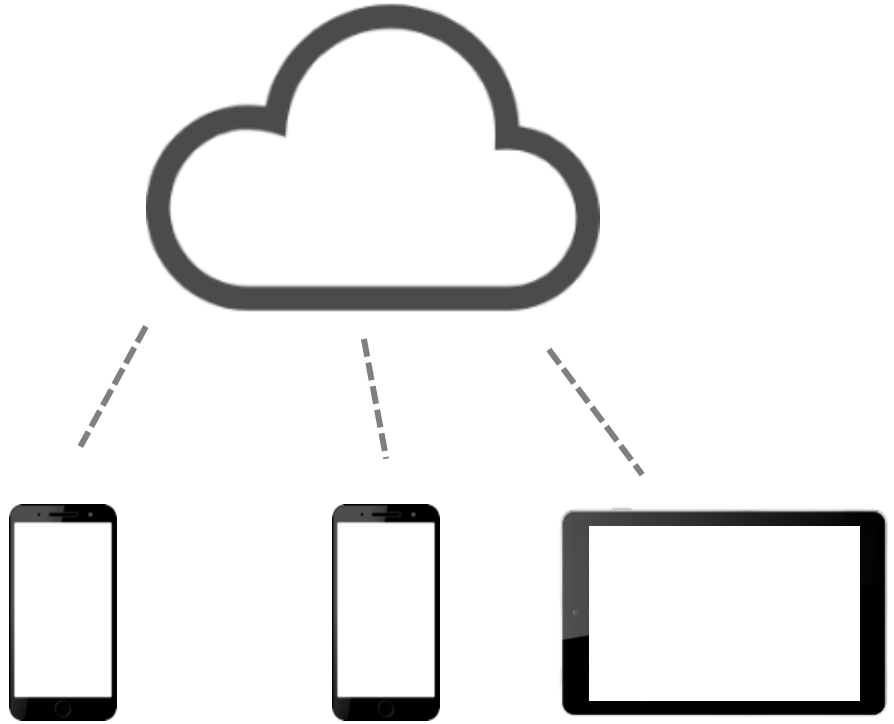
IT資産管理＝オンプレ

1つの建物の中で使うIT資産を管理



MDM＝クラウド

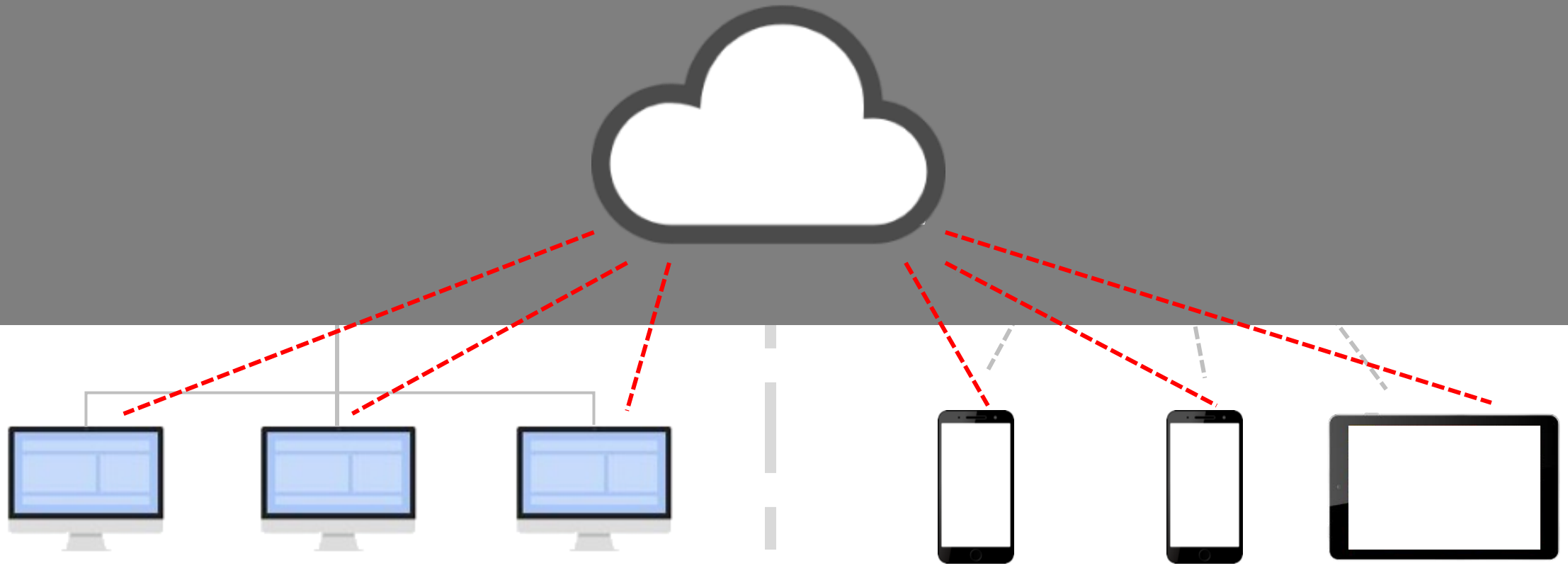
外に持ち出す特殊なデバイスを管理



DX・テレワークが始まると・・・

IT資産管理＋MDM

PC・スマホ・タブレットをまとめてクラウドで管理



クラウドですべて管理できるようにすればDX・テレワークのニーズにマッチする！

エンドポイントマネージャーのコンセプト

MDM機能を備えながら、PCのIT資産管理・セキュリティ対策が充実した特徴的なクラウド型製品へ

1990年～

30年にわたるPCのIT資産管理製品の提供、ノウハウの蓄積

2013年～

MDMリリース

2017年～

PC管理機能を追加しリニューアル

Cloud LANSCOPE Endpoint Manager

エンドポイントマネージャーが選ばれている理由

なぜ選ばれているの？

MDM機能を備えながら、PCのIT資産管理・セキュリティ対策が充実したクラウド型製品は他にありません。

なぜPC管理が強いの？

MOTEXはもともとPCのIT資産管理・セキュリティ対策で30年以上の実績！ノウハウを現在進行形で投入しています。

なぜMDMにPC管理？

ずばり運用負担の軽さ！PC・スマホ・タブレットを利用場所を問わず1画面で管理できるストレスのなさがメリットです。

エンドポイントマネージャーの機能ラインナップと価格

充実のMDM・PC管理機能
これだけの機能がついて月額500円/1台※

資産管理	**操作ログ管理**	**記録メディア制御**
紛失対策	**ファイル配布**	**通信機器制御**
レポート	**位置情報管理**	

※価格は税別です。ベーシックライセンスの場合。別途登録料が必要です。

【導入事例】校務端末管理としてエンドポイントマネージャーを採用

某市役所 教育委員会様

ライセンス構成：ベーシックライセンス600L

販売金額：3,600,000円（税別）

- 教育委員会の校務系端末更改の入札案件。
- 当初はオンプレ製品での導入を検討していたが、ゼロトラスト推進のためにクラウド製品でご提案したところ、ご評価いただき、応札。
- PCのIT資産管理だけでなく、PC操作ログ・外部メディア制御機能によるセキュリティ対策にもご期待いただいている。

本日お伝えしたいこと

1 ゼロトラストに必要な機能の半分がそろう！
LANSCOPEの幅広いラインナップ

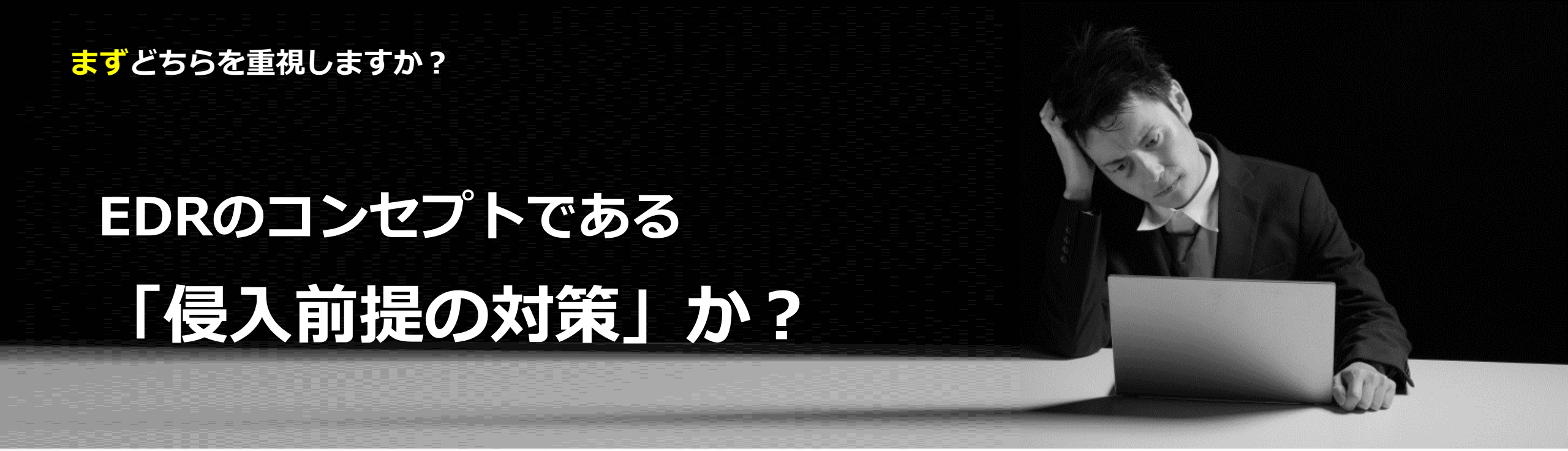
2 LANSCOPE エンドポイントマネージャークラウド版が
多くの民間企業で選ばれている理由

3 EDRとEPPどちらがより重要？
“本当に守れる”外部脅威対策とは

アンチウイルスの提案におすすめ

まずどちらを重視しますか？

EDRのコンセプトである
「侵入前提の対策」か？



EPPのコンセプト
「予防ファースト」か？

EPP・EDR の役割の違い：インフルエンザへの対応

予防 | **感染** | **調査・治療**

ワクチン接種

インフルエンザ発症

体温を計測

医者の診療（調査）

処方箋等で治療

EPP・EDR を当てはめる

EPP で予防 | **感染** | **EDR で調査・復旧**

ファイル防御 → 振る舞い防御

EPP をすり抜けてマルウェア感染 → 異常検知 → 封じ込め → 調査 → 復旧

EPP・EDR の役割の違い：インフルエンザ予防

予防

感染

調査・治療

ワクチン接種

インフルエンザ発症

体温を計測

医者の診療（調査）

処方箋等で治療

EPP・EDR を当てはめる

EDRの運用は大変!!

感染ご対応の運用コストが大きく

導入したが使いきれないという声も…

EPP で予防

感染

EDR で調査・復旧

ファイル防御

振る舞い防御

EPP をすり抜けてマルウェア感染

異常検知

封じ込め

調査

復旧

まず重視すべきはEPP！
「予防ファースト」のサイバープロテクションなら99%の脅威を防御

●NIST サイバーセキュリティフレームワーク コア：５つの機能

LANSCOPE Cyber Protection

AI技術を活用した画期的な手法で
超高精度のマルウェア検知

必要に応じて
EDR を導入

対応リソース
（誤検知への対応）

ほぼ無し

EDR機能もサイバープロテクションでご提供可能

サイバープロテクションの特徴

99%※の脅威を防御し、手軽にセキュリティレベルを向上
画期的検知手法のAIアンチウイルス

マルウェア検知率99%※

AIで作成された数理モデルが、
マルウェアをリアルタイムに検知。

快適なパフォーマンス

パターンファイルの更新不要。
最小限の負荷で稼働します。

導入も管理もカンタン

クラウド型なので、面倒なサーバ構築や
メンテナンスも不要です。

※2018 NSS Labs Advanced Endpoint Protection Test結果より

AIアンチウイルスと従来型アンチウイルスの違い

AIの活用により、攻撃者が作成したばかりの
まだ使われていないマルウェアであっても検知を実現

	LANSCOPE サイバープロテクション	従来型アンチウイルス
既知のマルウェア防御	○	○
未知のマルウェア防御	○	×
ファイルレスマルウェア防御	○	×
エクスプロイト攻撃防御	○	×
誤検知	ほとんど0	なし（パターンマッチングのため）
感染検知	○	×
感染調査	○	×
復旧対応	○	×

マルウェア検知エンジンは
2つのAIアンチウイルスからニーズに応じて選択できます

多くの導入実績とエンドポイントマネージャー との連携

CylancePROTECT

- 多数の国内の導入実績
- LANSCOPE エンドポイントマネージャー との連携が可能
- インターネット非接続環境で運用可能
- **EDR オプションあり**

幅広いOSやファイルタイプに対応

deep instinct

- EXE ファイルだけでなくWordやExcel など多くの ファイルタイプに対応
- スマートフォン対応
- 複数エンジンでの防御、**端末隔離機能を標準搭載**

製品に関するお問い合わせ

■ 営業本部

大阪本社	06-6308-8980
東京本部	03-3455-1811
名古屋支店	052-253-7346
九州営業所	092-419-2390
E-mail	sales@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター	0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間	9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ	support@motex.co.jp