Endpoint Manager Cloud

CylancePROTECT

情報漏洩対策も、ウイルス対策も！

月額1,000円！クラウドで実現する PC セキュリティ！

脆弱性を狙った攻撃が新たに登場！ 2022年はサイバー攻撃などの外部脅威が占める結果に

2021年に登場したテレワーク等のニューノーマルな働き方を狙った攻撃も継続でランクイン

	順位	組織	昨年順位
外部	1位	ランサムウェアによる被害	1位
外部	2位	標的型攻撃による機密情報の窃取	2位
外部	3位	サプライチェーンの弱点を悪用した攻撃	4位 ↑
外部	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位 ↓
内部	5位	内部不正による情報漏えい	6位 ↑
外部	6位	脆弱性対策情報の公開に伴う悪用増加	10位 ↑
外部	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
外部	8位	ビジネスメール詐欺による金銭被害	5位 ↓
	9位	予期せぬIT基盤の障害に伴う業務停止	7位 ↓
内部	10位	不注意による情報漏えい等の被害	9位 ↓

※引用：IPA「情報セキュリティ10大脅威2022」 https://www.ipa.go.jp/security/vuln/10threats2022.html

今期のポイント

脅威は、**外部からの攻撃**と**内部からの情報漏えい**の２パターンで**外部からの脅威が半分以上を占める**

注目は、新たに登場した「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」で、**脆弱性対策が施される前**に攻撃を受ける脅威が急増

多彩な働き方が拡がる中、**社外におけるセキュリティ対策が**間に合わず狙われる傾向にある

内部不正による情報漏えいがランクアップ！退職者などの情報持ち出し事件が多発している

© MOTEX Inc.

ここ数年はマルウェア・ランサムウェア攻撃が増加中！凶悪化することで被害も拡大中です

食品加工業

ランサムウェア攻撃を受け**一部工場の操業を停止**せざるを得なくなった。大半のシステムは復旧していたが、**さらなる攻撃で顧客や従業員のデータが危険にさらされるリスク**を考慮して社内のIT専門家および第三者のサイバーセキュリティ専門家と協議の上、身代金を支払った

身代金支払額
約12億円

インフラ業

システムにマルウェアが侵入して短時間で **100GB 以上のデータが搾取**。**その一部をインターネットに公開すると脅迫**があり身代金要求を受けていた。同時に第三者がパイプラインへの攻撃を可能とする情報を入手したため、**燃料パイプラインの操業を停止。一部地域で燃料が不足**して住民はパニックに陥った。

身代金支払額
約4億8000万円

医療機関

電子カルテがランサムウェアに感染。**バックアップデータも暗号化**されたため復旧に時間を要した。
結果、過去処方した薬剤や診療履歴が分からず、**一時診療が出来なくなった**。約2ヶ月診療人数を制限しつつ対応。身代金要求を受けていたが応じなかった。

身代金支払額
0円（支払いに応じず）

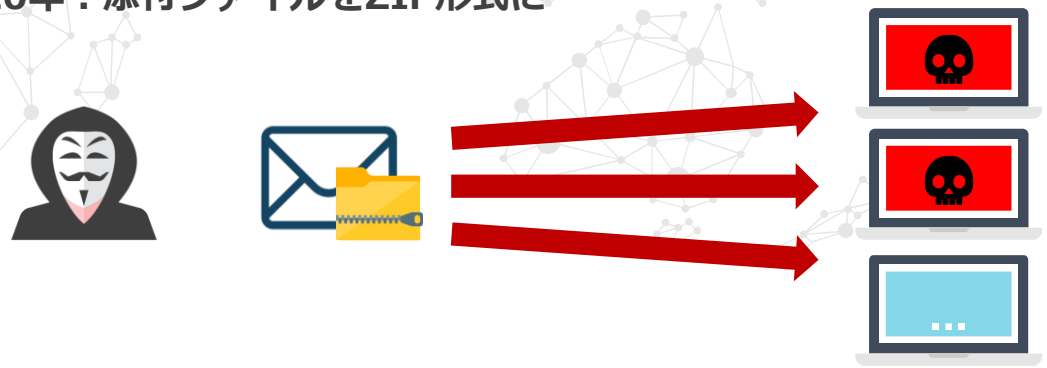
© MOTEX Inc.

Emotetによる被害が再燃！対策するも攻撃手法を進化させ凶悪化し続けています

Emotetの攻撃手法

2019年：Wordの添付ファイル

2020年：添付ファイルをZIP形式に



© MOTEX Inc.

価値がある情報が故に社内や関係者からの悪意のある情報漏えいが急増しています

外部指摘で初めて発覚するケースも・・・自社のみならず委託先やグループ内など範囲が広いケースが増加

退職者による情報漏えい

転職先である競合企業へ、**顧客情報や技術情報などの秘密情報を持ち出す**などで損害を受けたと、損害賠償請求に発展

情報収集の悪用

証券会社の委託先SEが、顧客のIDとパスワードを盗み、**顧客に成りすまして資産売却・現金化**、損害額は2億円に上る

個人情報の入った機器を転売

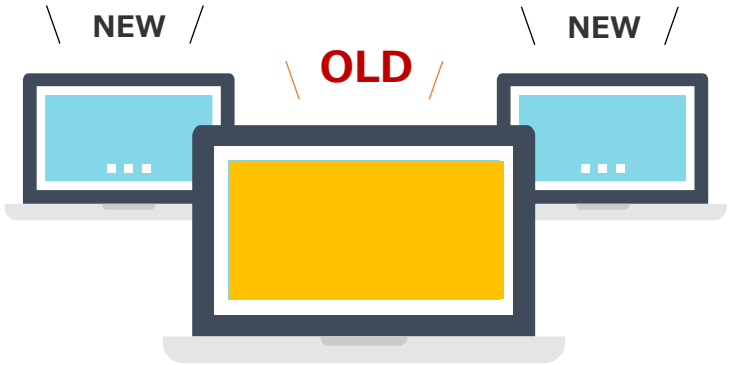
業務用のノートPCを無許可で持ち出し業務を行ったのち、約14万件の個人情報が保存されたノートPCを**オークションにて転売し収入**を得ていた

© MOTEX Inc.

攻撃を受けない環境づくり、攻撃を受けた際の防御・再発防止策を打てる体制づくりをしましょう

リスクは多岐に渡るため、まずは基本の設定をしっかり行うことがセキュリティリスクを減らす事に繋がります

脆弱性対策



最新の脆弱性情報をキャッチアップし、OSやアプリを**常に最新の状態**にすることで脆弱性対策しましょう

内部情報漏えい対策

操作履歴を取得し、**リスクにつながる操作を制御**すると共に社員に対し**セキュリティ啓蒙**を行いましょう

サイバー攻撃対策

攻撃を検知・隔離をすることで感染させない対策・体制を整えましょう

© MOTEX Inc.

エンドポイントマネージャー クラウド版 × CylancePROTECT のマルウェア対策

© MOTEX Inc.

PC・スマホ・タブレットの一元管理をクラウドで実現
「使いやすい」管理コンソールで、充実の「IT 資産管理機能」と「MDM 機能」を実装

IT review 顧客評価No.1
使いやすい管理コンソール

充実の PC 管理
操作ログ・セキュリティ
PC 管理に必要な機能を網羅

Apple・Google の認定プログラム対応
充実の「モバイル管理」

© MOTEX Inc.

エンドポイントマネージャー クラウド版 × CylancePROTECT で、事前・事故対策が可能です。

事前対策

セキュリティの基本となる OS のアップデート管理や業務と関係の無いサイトへの利用制御が必要です。

マルウェア対策

次世代型 AI アンチウイルスである CylancePROTECT と連携が可能でモジュール配布が可能です。

事後対策

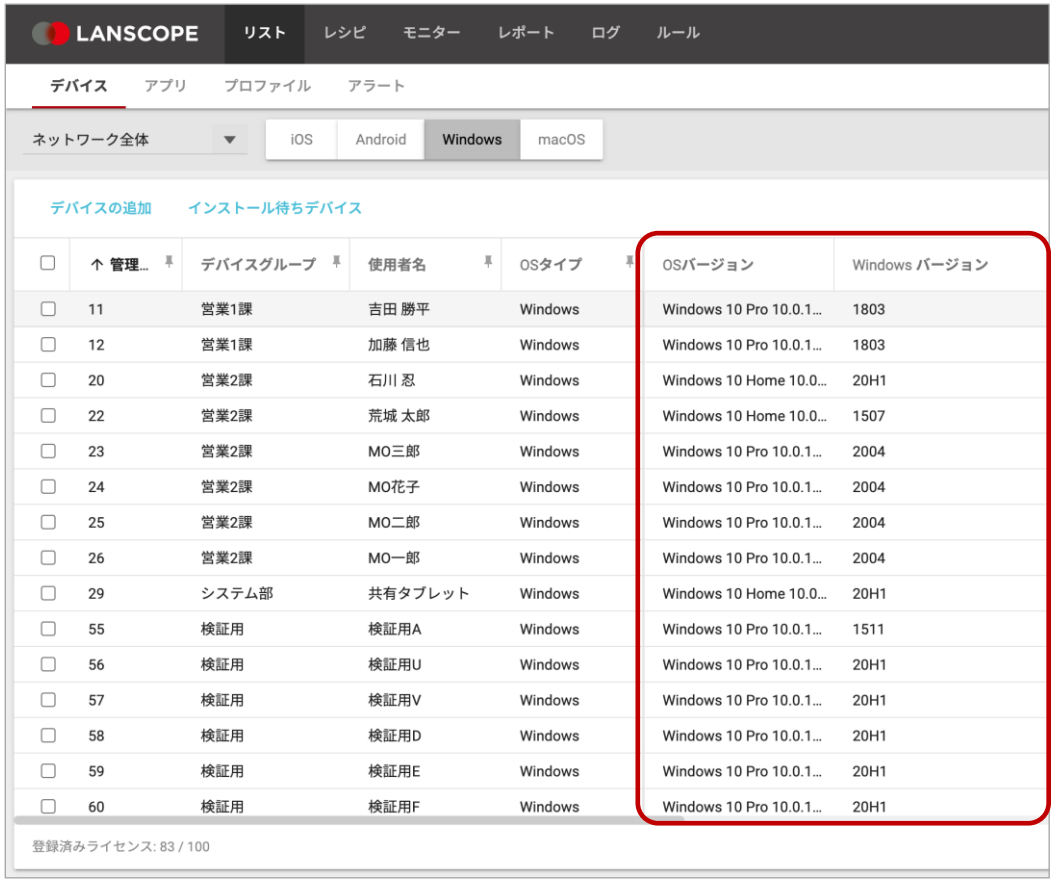
有事の際は、どの操作が原因なのかを確認し、再発防止に役立てます。

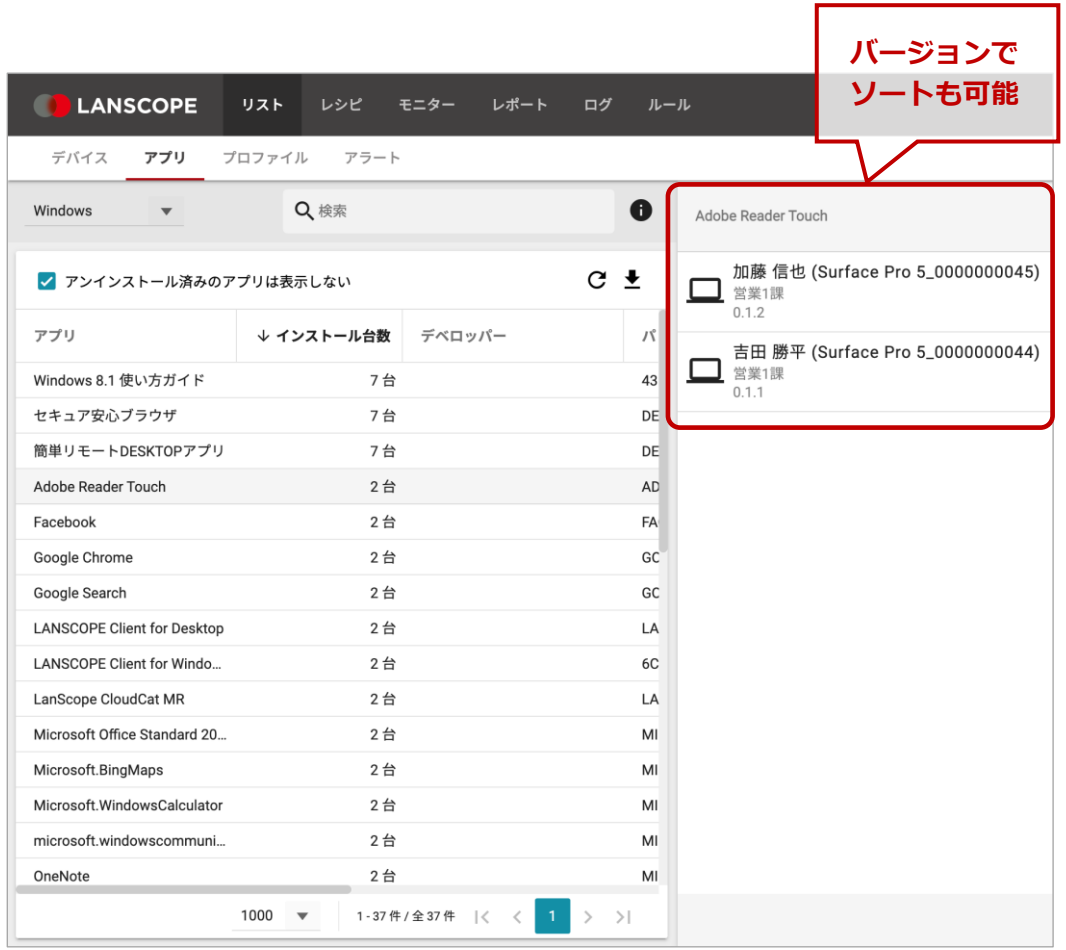
© MOTEX Inc.

事前対策（エンドポイントマネージャー クラウド版）

© MOTEX Inc.

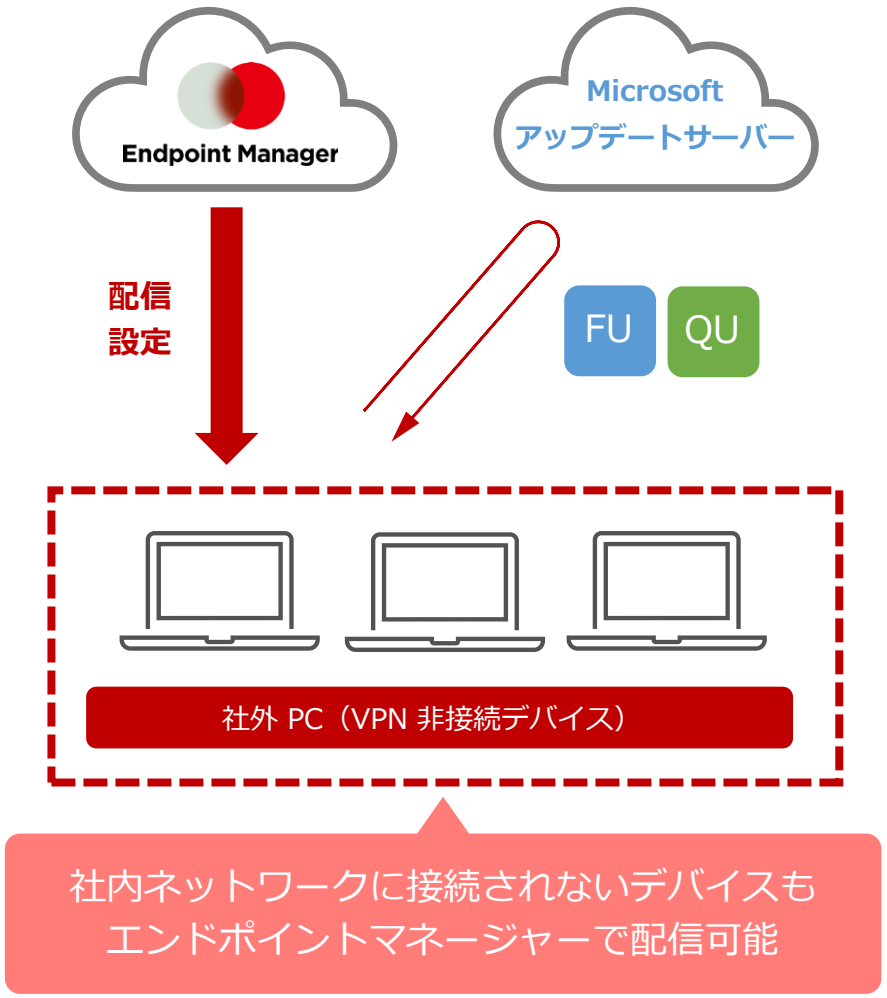
重要なのは「最新の状態を保つこと」！ OS・アプリのバージョンを把握できます

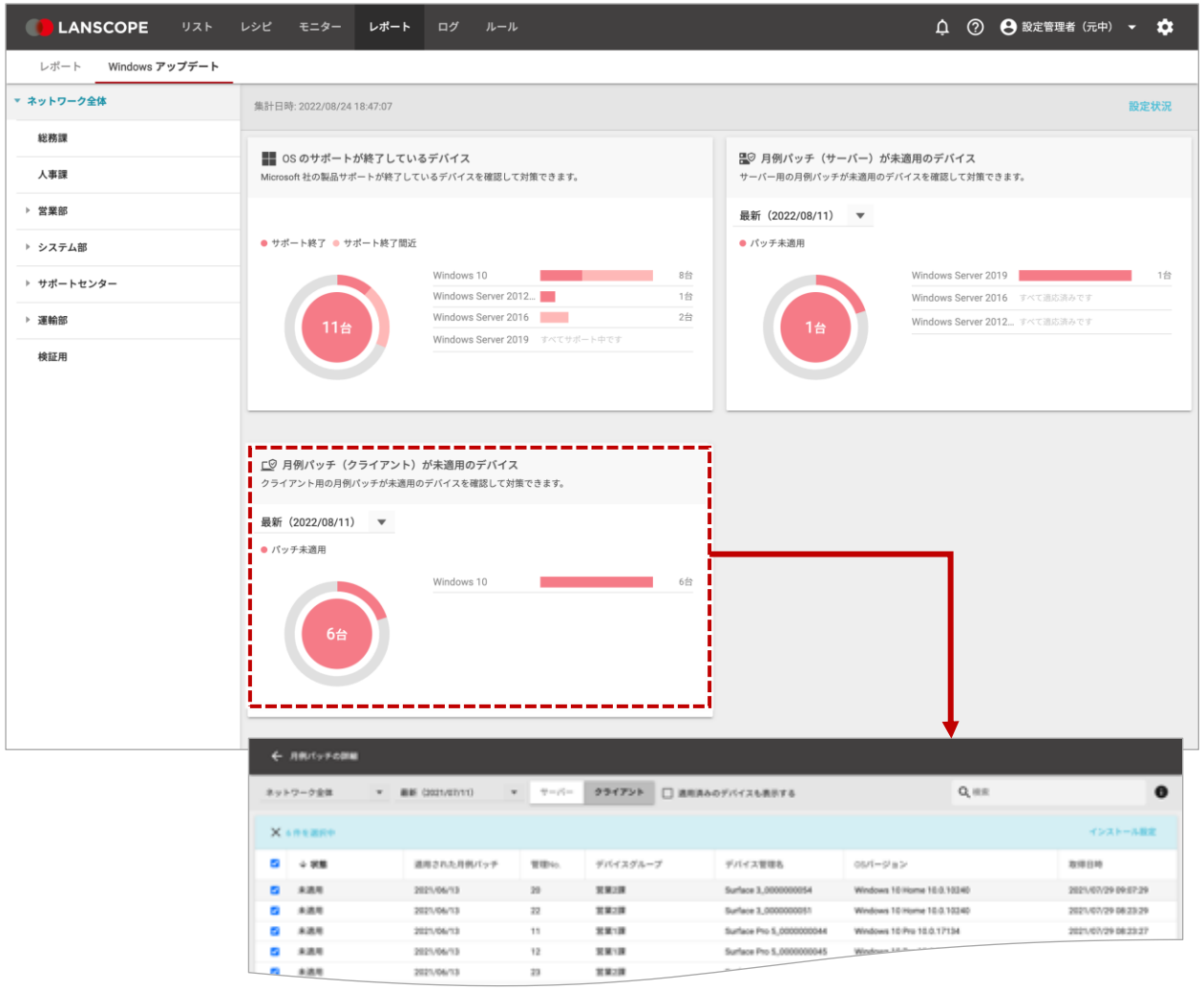




© MOTEX Inc.

機能更新・品質更新プログラムの適用状況を、“視認性の良い” レポート形式で把握
1Click で未適用デバイスを確認し、最新のプログラムを適用





© MOTEX Inc.

マルウェア対策：CylancePROTECT

© MOTEX Inc.

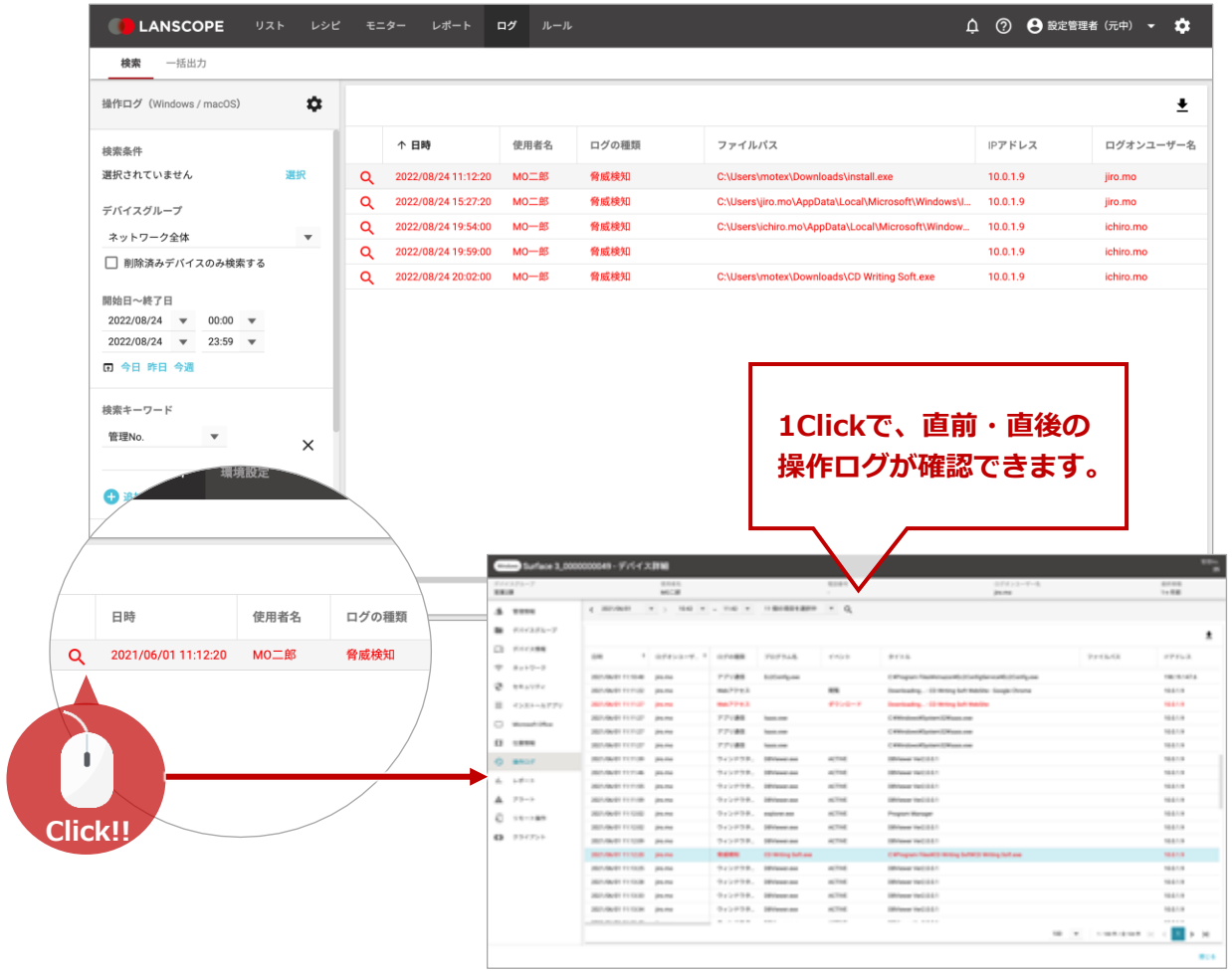
AI を活用した次世代型アンチウイルス製品と連携し、操作ログから、未知・亜種のマルウェア感染原因を特定

CylancePROTECT × Cloud LANSCOPE Endpoint Manager

マシーンラーニングの特許技術を活用した「予測脅威防御」で、マルウェアの特徴点を見つけて実行前に検知・隔離します。エンドポイントマネージャー クラウド版と連携することで、マルウェアに感染してしまった直前の操作を特定。原因の追求や再発防止に活用できます。

- 検知率は99% *
未知のマルウェアも
検知・隔離
- PC への負荷が小さく
快適なパフォーマンス
を発揮
- 月額450円/台から！
ニーズに合わせて
必要なプランを選択

https://www.lanscope.jp/cpms/



* 2018 NSS Labs Advanced Endpoint Protection Test 結果より

© MOTEX Inc.

CylancePROTECT がマルウェア対策におすすめな理由

マルウェア検知率99%以上！

最新鋭の AI 技術を活用した次世代型のアンチウイルス

クラウド型のサービスのため

社内ネットワークへの接続不要・インターネットで管理可能

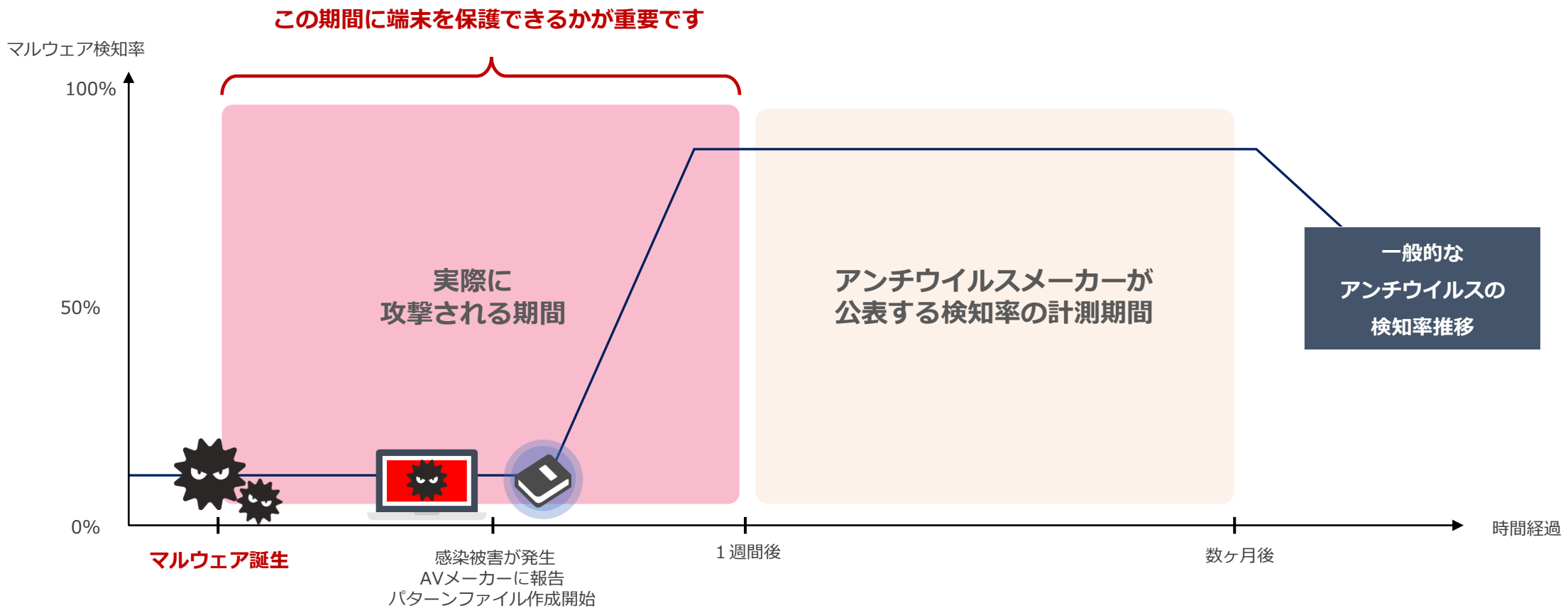
AI 技術を活用したシグニチャレスの独自のマルウェア検知手法のため、

頻繁な更新は不要。更新は半年に1度でOK

© MOTEX Inc.

従来型アンチウイルスではゼロディ（＝未知のマルウェア）を止めることが難しい

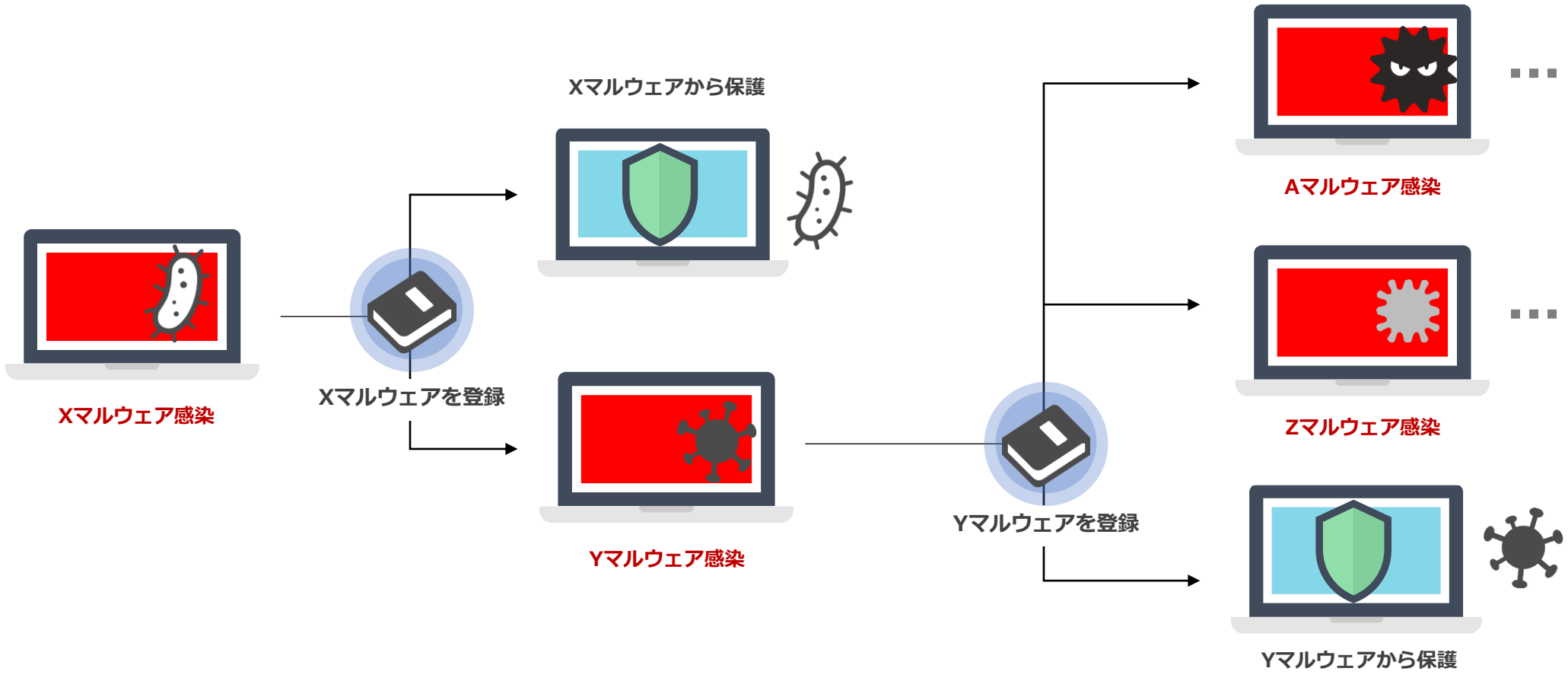
シグネチャ型は被害が発生してからパターンファイルを作成するため、その間に感染してしまう危険性があります



© MOTEX Inc.

攻撃に使われるのは使い捨ての未知のマルウェアばかり…すり抜けが増えてしまう

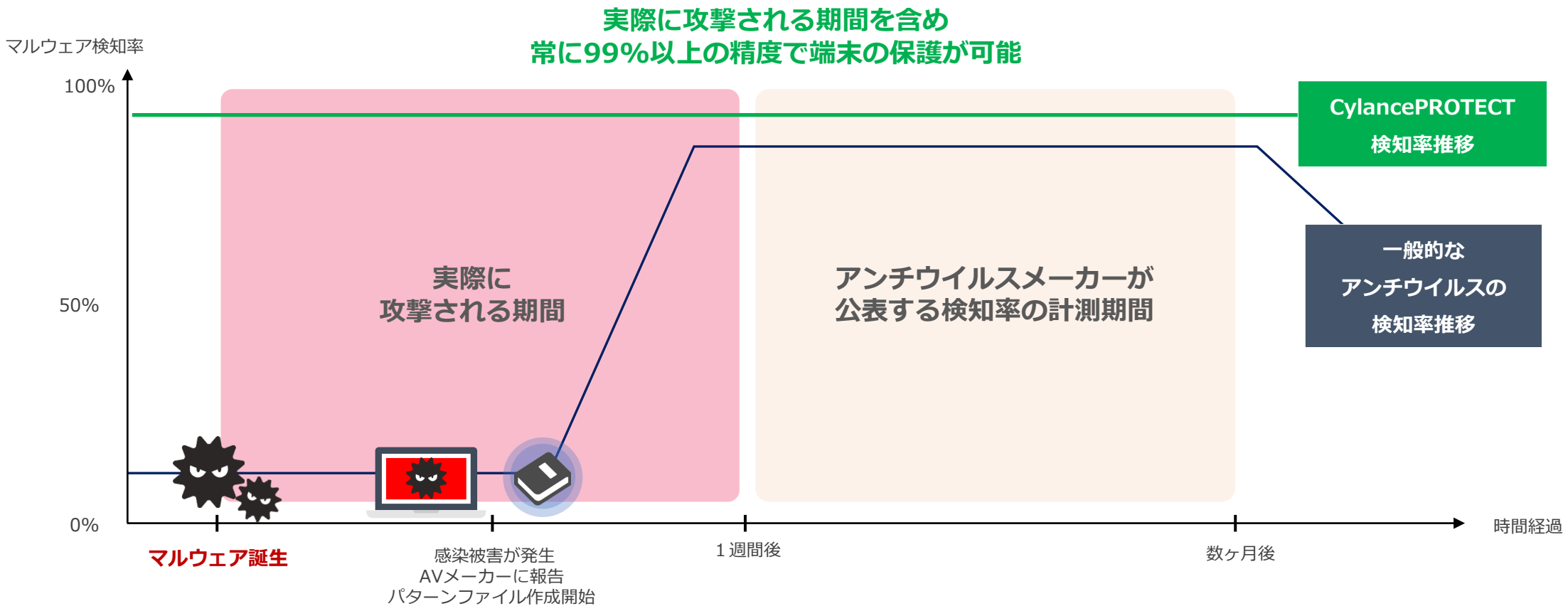
進化により新しいマルウェアが次々と出現するため、シグネチャによる検知には限界が生じます



© MOTEX Inc.

AI を活用した「予測脅威防御」で未知マルウェアも 99%以上の高精度で防御

AI 技術を活用したシグニチャレスの独自のマルウェア検知手法のため、パターンファイルの有無に左右されない検知精度

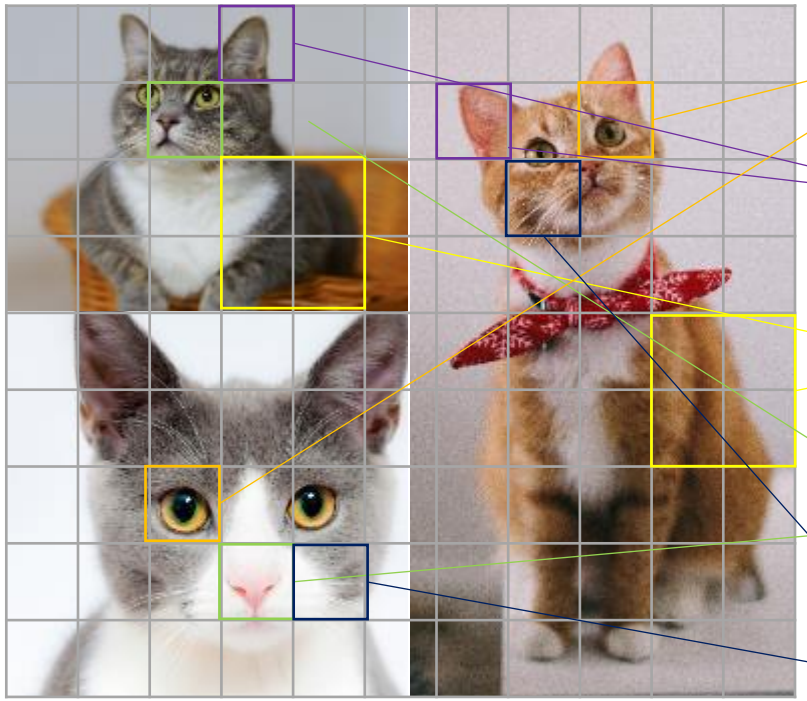


© MOTEX Inc.

AI が画像を詳細に分析し特長を機械学習！一致要素をDNAレベルで総合的に判断

AI によるマシンラーニングによる高精度な分析が、高精度なマルウェア検知が実現します

10億以上のファイル



大きな目が2つ

三角の耳

ふわふわの体毛

ピンク色の鼻

長いひげ

700万の特徴点

猫の可能性 99%

猫のサンプル写真を細かに分析し

猫の特長を学習

対象の写真を細かに分析し

猫の特長と一致するかで猫かどうかを判定

© MOTEX Inc.

未来に発生するマルウェアを予測して検知！あらゆる未知・亜種のマルウェアから保護

CylancePROTECT の検知方式は、2年以上前の過去の検知エンジンでも、未知のマルウェアを予測検知しています

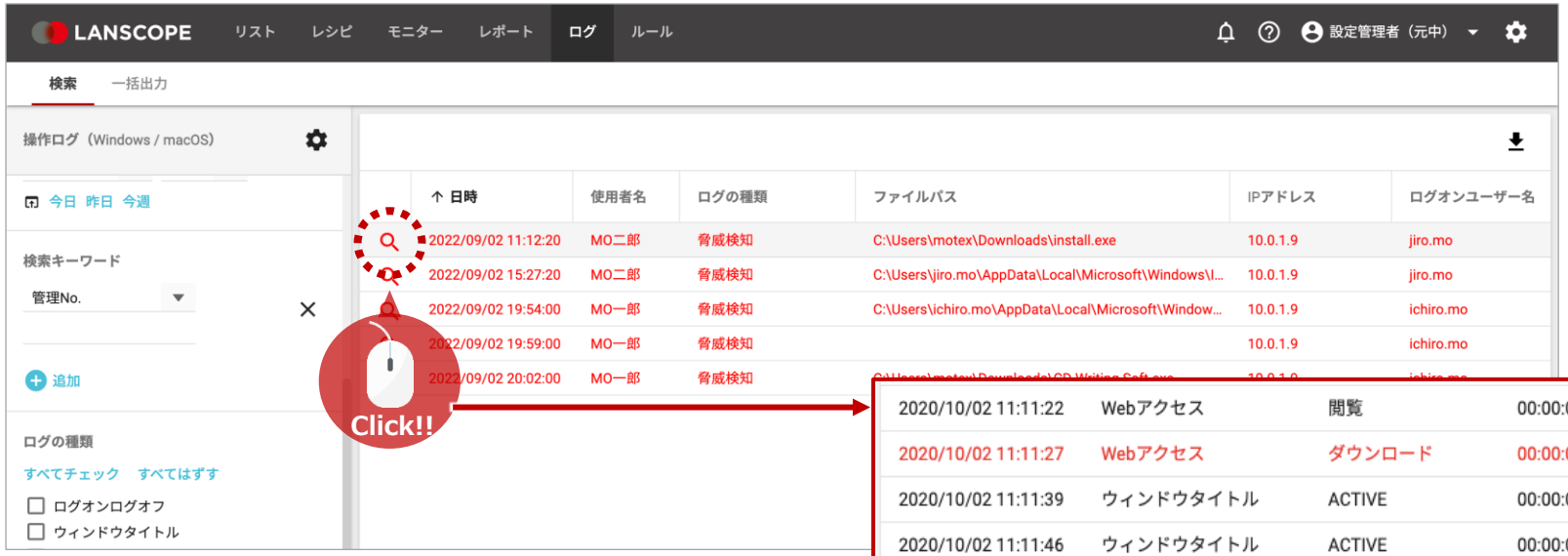
© MOTEX Inc.

事後対策

© MOTEX Inc.

感染した原因（人の操作）を追跡！原因が分かれば再発防止策がとれます

CylancePROTECT で検知した情報を操作ログから検索し、1Click で原因を特定できます



11時11分に、ある Web サイトにアクセスして、そこから CD 書込みソフトのインストーラーをダウンロードしている！

2020/10/02 11:11:22	Webアクセス	閲覧	00:00:03	Downloading... - CD Writing Soft WebSite - Google Chrome
2020/10/02 11:11:27	Webアクセス	ダウンロード	00:00:03	Downloading... - CD Writing Soft WebSite
2020/10/02 11:11:39	ウィンドウタイトル	ACTIVE	00:00:07	DBViewer Ver2.0.0.1
2020/10/02 11:11:46	ウィンドウタイトル	ACTIVE	00:00:08	DBViewer Ver2.0.0.1
2020/10/02 11:11:55	ウィンドウタイトル	ACTIVE	00:00:04	DBViewer Ver2.0.0.1
2020/10/02 11:11:59	ウィンドウタイトル	ACTIVE	00:00:02	DBViewer Ver2.0.0.1
2020/10/02 11:12:02	ウィンドウタイトル	ACTIVE	00:00:08	Program Manager
2020/10/02 11:12:02	ウィンドウタイトル	ACTIVE	00:00:06	DBViewer Ver2.0.0.1
2020/10/02 11:12:09	ウィンドウタイトル	ACTIVE	00:01:15	DBViewer Ver2.0.0.1
2020/10/02 11:12:20	脅威検知		00:00:00	C:¥Program Files¥CD Writing Soft¥CD Writing Soft.exe

© MOTEX Inc.

検知したマルウェア以外の「端末に潜む脅威」を発見、攻撃の流れを操作を紐づけて可視化

CylancePROTECT の検知力に加え、調査・封じ込め・復旧まで一連の対応が可能で、負荷の少ない EDR 機能です

攻撃防御 → **継続監視** → **自動対処** → **脅威ハンティング（ InstaQuery ）** → **関連情報の入手（FocusData）**

CylancePROTECT

CylanceOPTICS®

マルウェア以外の「危険なプロセス」や「コマンドの実行」も検知・隔離可能

© MOTEX Inc.

Endpoint Manager Cloud × CylancePROTECT

急増・凶悪化する外部脅威にクラウド製品で対抗

AI を活用した次世代型アンチウイルスで対策できます。

攻撃されない体制構築のための「事前対策」、
感染させない「マルウェア対策」、原因を特定する「事後対策」の実現を支援します

© MOTEX Inc.

製品版へのデータ引き継ぎが可能です！

エンドポイントマネージャー クラウド版の体験版は 60日間たっぷり利用できます。十分に機能を検証していただき、ご検討ください。

設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。

また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。マニュアルやオンラインで学べるトレーニング動画も公開しています。

© MOTEX Inc.

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

・記載の会社名および製品名・サービス名は、各社の商標または登録商標です。

・MOTEX はエムオーテックス株式会社の略称です。

© MOTEX Inc.