LANSCOPE
Professional Service

DARKTRACE

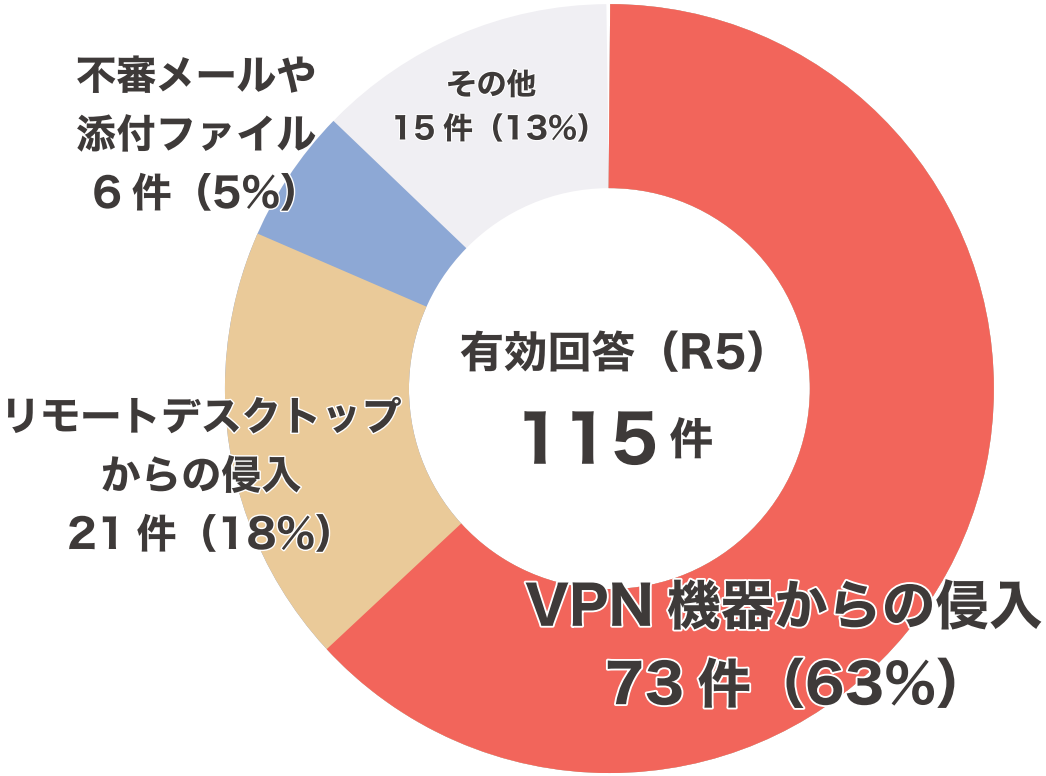
VPNのセキュリティリスクとは？
対策や被害事例を解説

１．情報セキュリティの現状と対策

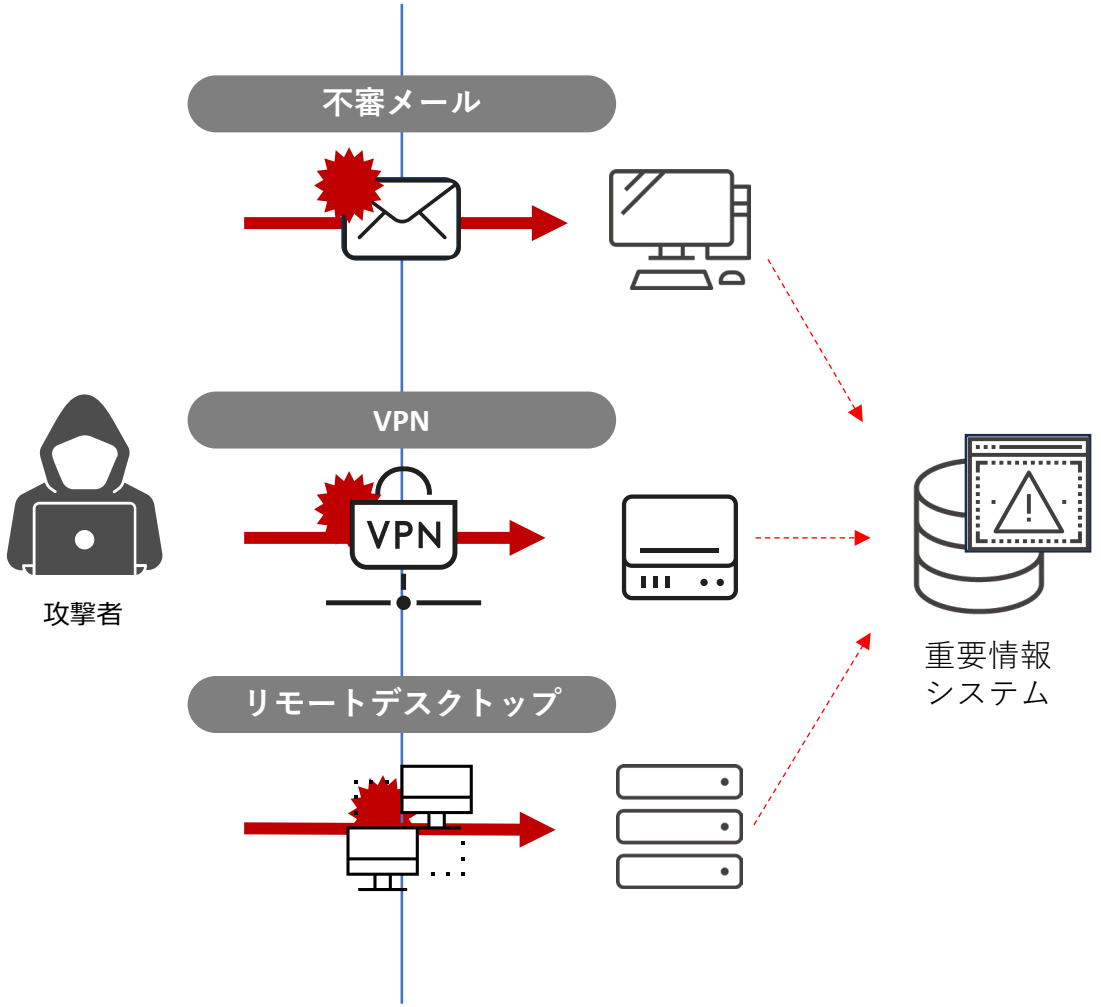
「情報セキュリティ10大脅威」の上位に「内部ネットワークへ侵入する脅威」が常にランクイン

侵入経路は「メール」から「VPN機器・リモートデスクトップ」へ変化

企業・団体等における感染経路



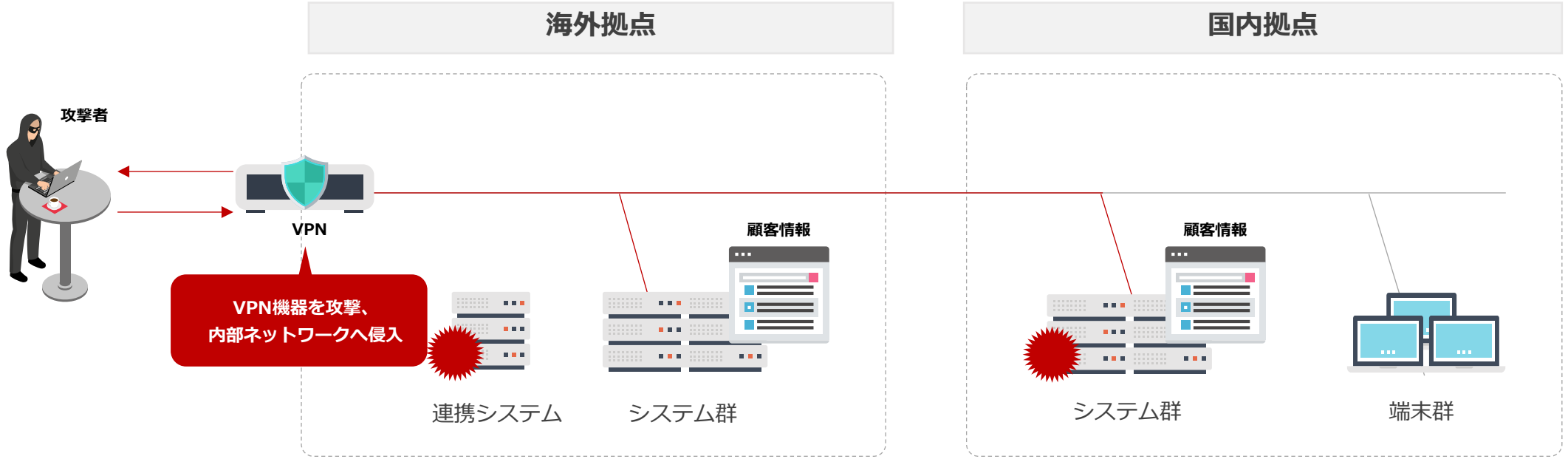
参照：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf



海外法人のVPN機器への攻撃をきっかけに内部ネットワークへ不正侵入・個人情報約1.6万件が流出

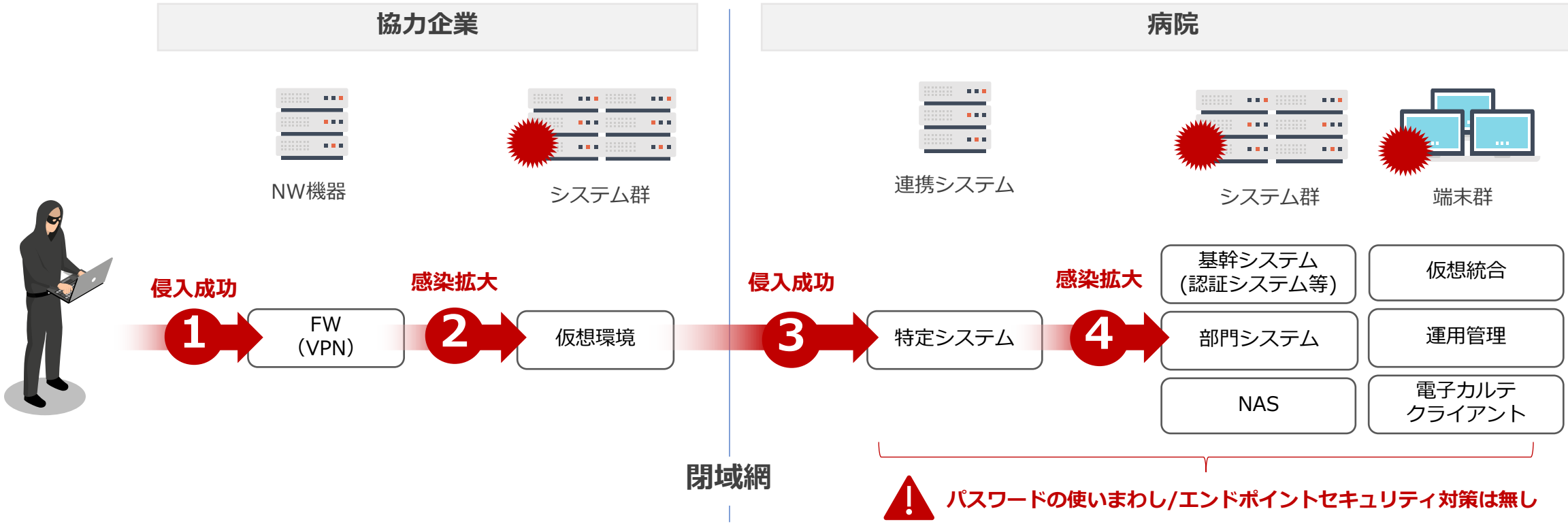
2020年11月、某ゲーム会社のデータが暗号化され、メールやファイルサーバーが使えなくなり一時業務停止に追い込まれた。さらに攻撃者は盗んだ情報をネット上に暴露すると脅し身代金を要求。漏洩した可能性のある個人情報は顧客や株主情報など約1.6万件と言われている

＜課題＞・新型コロナウィルス感染に起因するリモートアクセス増大への備えとして、旧型のVPV機器を残していた。
・VPN機器の脆弱性/設定不備の把握と管理



取引先企業のVPN機器が攻撃され、病院のシステムに侵入拡大、病院の機能が停止

2022年10月、大阪の某医療機関がランサムウェア攻撃を受け、電子カルテシステム等が暗号化された。侵入口は給食委託事業のVPN装置、パスワードの辞書攻撃などを用いて侵入。システム復旧は2ヶ月を要し、完全に診療を再開できたのは約2ヶ月後の2023年1月11日



VPN機器で有効な3つの対策を紹介します

セキュリティ対策	概要
常にアップデートや最新のパッチ適用を行う	VPNのアップデートや最新のパッチ適用を、定期的に行うことが挙げられます。 パッチ適用やアップデートを行うことで、VPNに存在するセキュリティ上の脆弱性を修正し、VPNの通信が傍受される・不正アクセスを招くといった、攻撃のリスクを低減することが可能だからです。 VPNの開発元が提供する情報を基に、VPNは常に最新の状態を保つことを心がけましょう。
VPN機器の認証・パスワードを強化する	VPNサーバーへの接続時に必要な、認証とパスワードの強化を行うことです。認証やパスワードを強化することで、不正アクセスや情報漏洩などのセキュリティリスクを低減できるためです。 例えば、VPN接続を行う際に必要な「VPNサーバーへの認証」手続きは、IDやパスワードだけでなく、電子証明書やワンタイムパスワードなどの「多要素認証」を導入することで、セキュリティを強化できます。 またパスワードの強化を図るためには「パスワードを長くする」「英字や数字・記号を織り交ぜ、複雑にする」「定期的にパスワードを変更する」といった方法が効果的です。
定期的に脆弱性診断を実施する	VPN機器の脆弱性や設定不備をチェックすることを目的に、定期的に脆弱性診断を行い、リスクを把握しましょう。

しかしながら、課題があり対策が困難なことも…

アップーデート対応が困難、攻撃されても気づけないなど課題がある。

アップデートが多い

VPN機器の脆弱性に対するアップデート回数が多く、年に何度も発生するため、都度対応するのが大変

リードタイムが無防備に

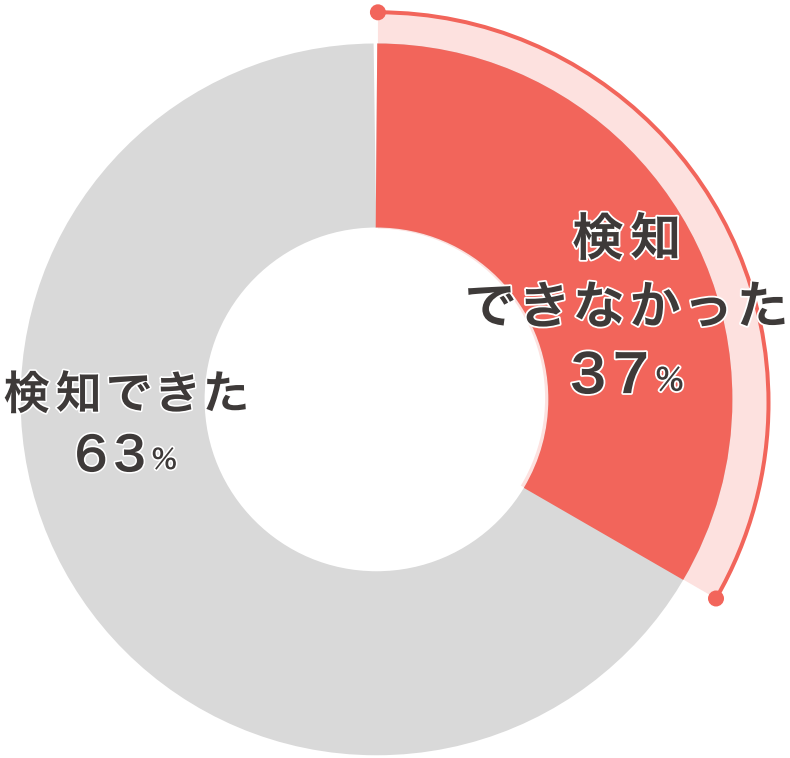
人手不足や工数の問題で、VPNの脆弱性対策リードタイムが発生。その間、無防備になってしまう

攻撃に気付けない

ネットワーク機器に対する攻撃なので、エンドポイントのアンチウイルスでは気付きづらい・気づいたときには遅い

侵入された企業のうち約4割が脅威を検知できなかったという実態も･･･

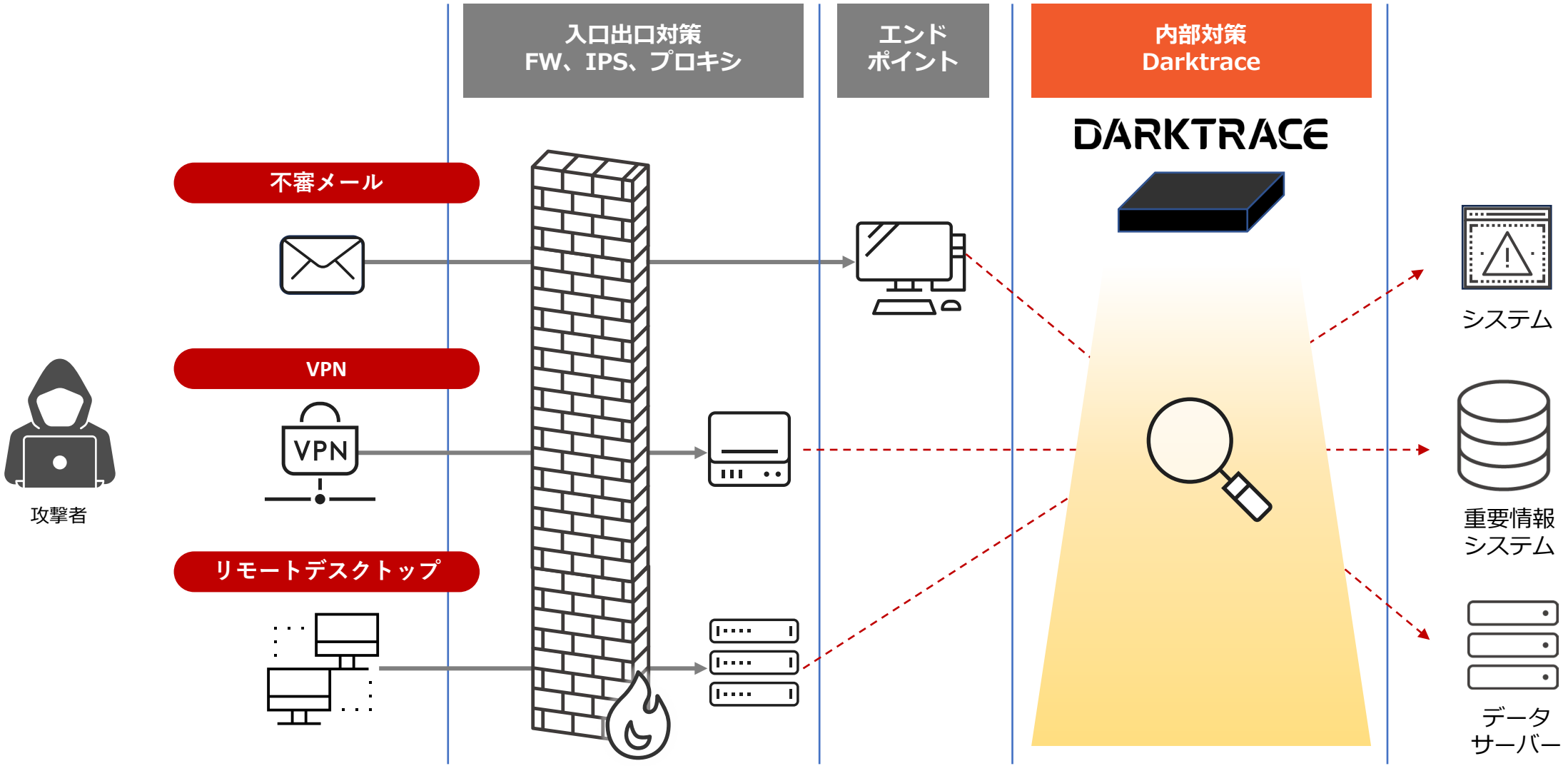
Q.社内ネットワークへの
侵入に気づいたきっかけは何ですか？



・ネットワーク機器
・サーバーシステム
・メールシステム
・エンドポイント管理

※2023年MOTEXセミナーアンケートより（N=119）

全ての経路の通り道である「ネットワーク」における異常の察知が効果を発揮します！



2. AIを活用したNDR製品 「Darktrace」 のご紹介

入口出口対策をすり抜け内部へ侵入してくる脅威をネットワークで網羅的にモニタリング（検知・対処）

DARKTRACE

NDR
国内市場シェア
No.1※

Darktraceはネットワーク機器に流れるトラフィックを基に、AI（機械学習）を活用して、ネットワークに接続した様々なデバイスやユーザーの行動パターンを学習・分析することで、未知のサイバー攻撃や内部不正の兆候を検知します。

- AIアナリスト
- 未知の攻撃検知
- 内部不正検知
- エージェントレス
- ネットワーク可視化
- 不正通信の自動遮断

https://www.lanscope.jp/professional-service/service/product/darktrace/

生物の免疫(immune)が、外的や環境変化に対抗するような仕組みをITセキュリティシステムに適用

AIネットワーク脅威検知

DARKTRACE

ケンブリッジ大学の数学者と、英国の国家サイバーセキュリティに携わったメンバーで2013年に設立

英国ニュース紙「TIME」において、世界で最も影響力のある100社に選ばれる

英国政府主催「AI安全サミット」にサイバーセキュリティ専業企業として唯一招待（2023年）

https://darktrace.com/ja

内部ネットワークに接続している機器を全て監視！検知力と運用工数が大幅削減されます

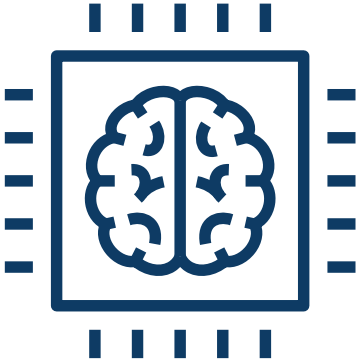
監視領域の広さ

- **ネットワークのトラフィックを監視**するため網羅的な監視が可能。
- 社内ネットワークに留まらず**個人端末・クラウドサービスにも対応**

EDRが非対応機器も対策

- エージェントレス
- EPPやEDRなどのエンドポイント対策が**非対応なレガシーOSや専用機器なども脅威検知が可能**

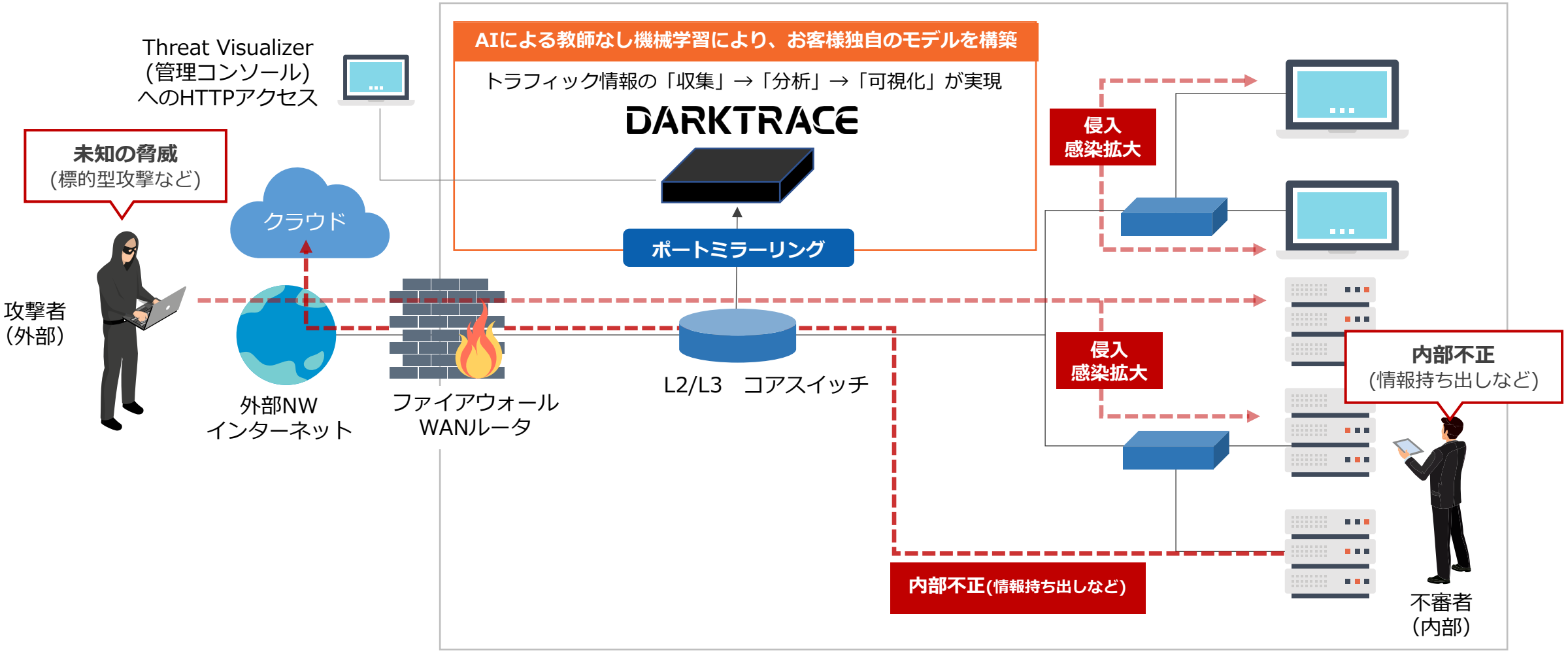
管理工数が少ない



- AIが**24時間365日監視・対応**
- AIの自律的学習により**ルールの定義やチューニングの手間がかからない**
- アップデートは**年1回程度**

トラフィックをポートミラーリングで流すだけ！ルール定義・詳細設定不要で他システムへの影響はなし

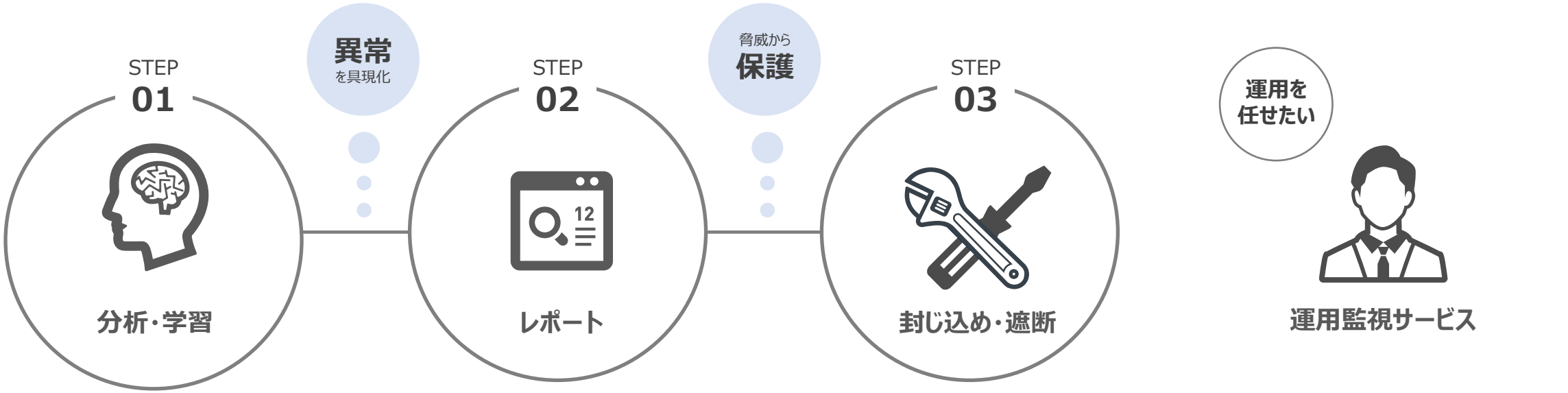
AIがネットワーク機器に流れるトラフィックを基に、ネットワークに接続した様々なデバイスやユーザーの行動パターンを学習・分析・遮断します



AI（機械学習）によりゼロデイ攻撃や内部不正など未知の脅威を検知

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、内部脅威(不正)にも幅広く手を打つことが可能

モニタリングとインシデント対応の強力サポートに加え、人による運用監視サービスをご用意



AIによる分析・検出

ルールや事前設計に依存せず、
移動分析・学習を自立して継続。
通常の挙動を学習し、
通常と異なる挙動を検出

インシデントレポート

不審な挙動・攻撃の時系列を
トラッキングし
関連する挙動を自動で紐づけ
対応策を提案

リアルタイムに対処

数秒以内に攻撃を封じ込め
リアルタイムに遮断
スマホで再接続指示が可能

常時監視・調査・対応支援

現場経験が豊富な専任アナリストが
常時監視・調査・対応支援
アナリストによる詳細レポートや
LANSCOPEを活用した調査も可能

検知 ← → 自動対処 ← → 運用監視

※オプションです

ネットワークに接続するだけで簡単に導入可能、AIがネットワーク全体を可視化し未知の脅威を検知

すぐに使い始められる

アプライアンス型で
最短1時間程度で簡単に導入可能

【特徴】

①事前の設計やルール定義、詳細設定が不要

②他システムに影響なし

※ お客様のNW環境によって、
アプライアンスの設置場所のご相談が必要です。

分かりやすい画面構成

3Dグラフィックによる
ネットワーク可視化で分析効率化

対象ネットワーク全体のパケットを取得し、
リアルタイムで通信を可視化。

日本語化されたGUI

オフィス/テレワーク、クラウド、メール環境
制御系ネットワークなど業務環境をビジュアル化。

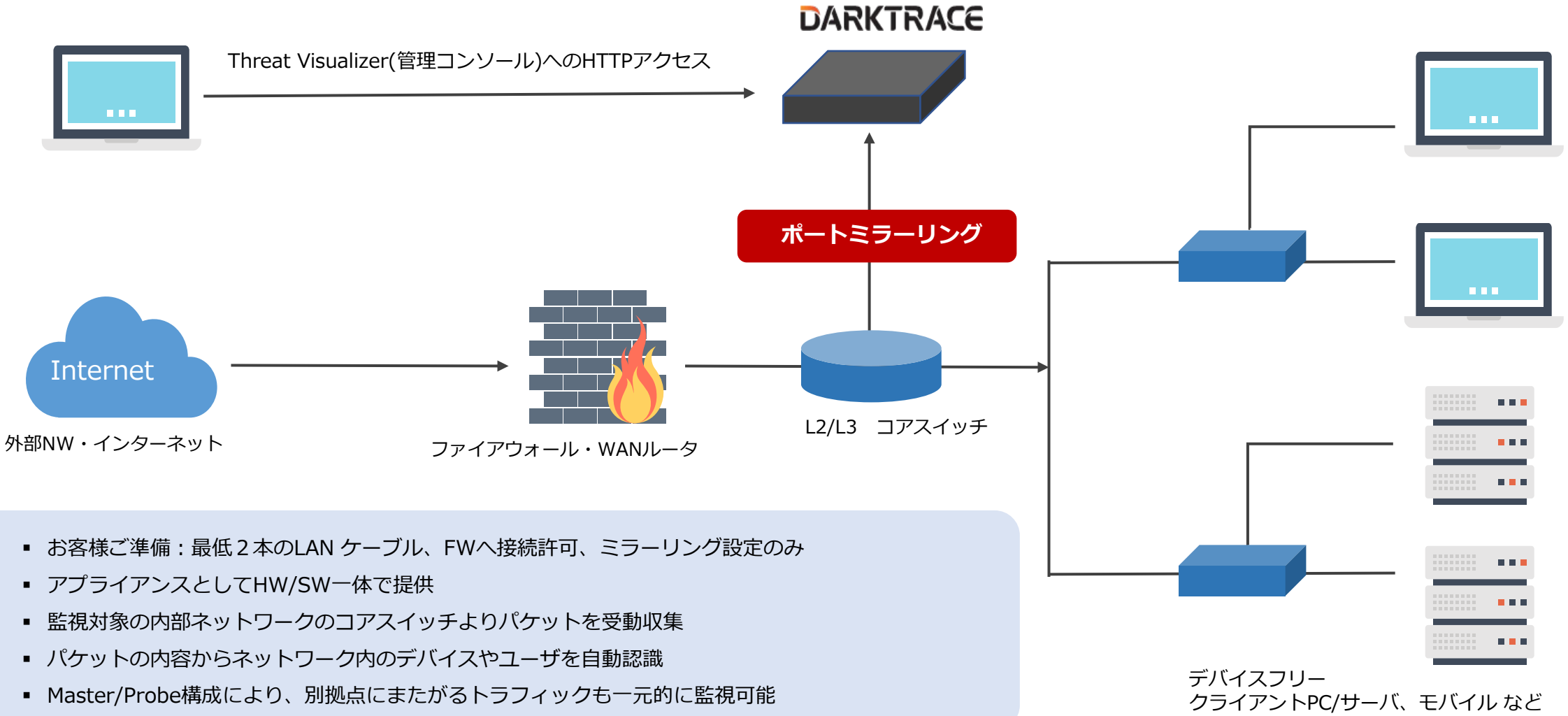
AIによる脅威検知

AI（機械学習）によりゼロデイ攻撃や
内部不正など未知の脅威を検知

「教師なし機械学習」

により自社環境固有のユーザやデバイスの
生活パターンを常に分析

トラフィックをポートミラーリングで流すだけ、
ルール定義、詳細設定不要で他システムへの影響もございません。

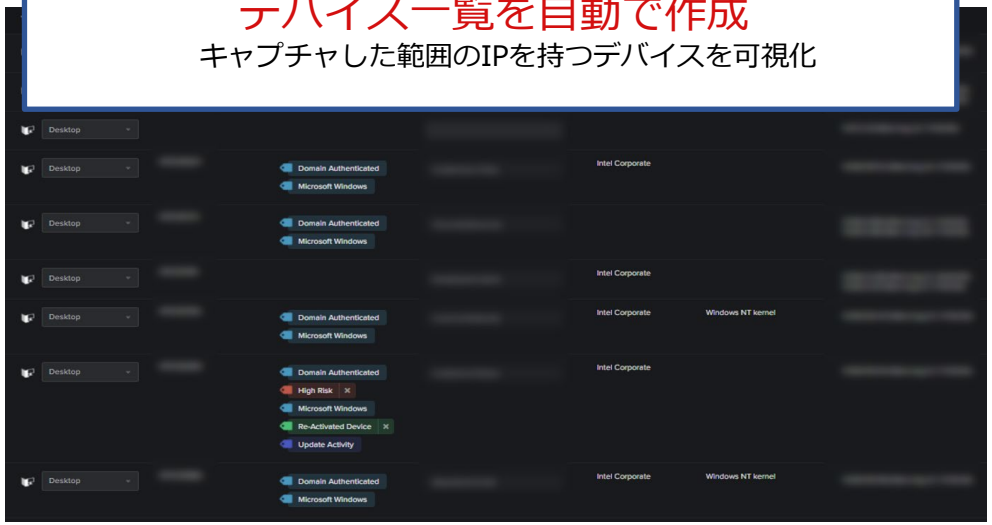


- お客様ご準備：最低２本のLAN ケーブル、FWへ接続許可、ミラーリング設定のみ
- アプライアンスとしてHW/SW一体で提供
- 監視対象の内部ネットワークのコアスイッチよりパケットを受動収集
- パケットの内容からネットワーク内のデバイスやユーザを自動認識
- Master/Probe構成により、別拠点にまたがるトラフィックも一元的に監視可能

ネットワーク全体の通信を可視化することで、**セキュリティ分析作業が効率化します。**

デバイス一覧を自動で作成

キャプチャした範囲のIPを持つデバイスを可視化

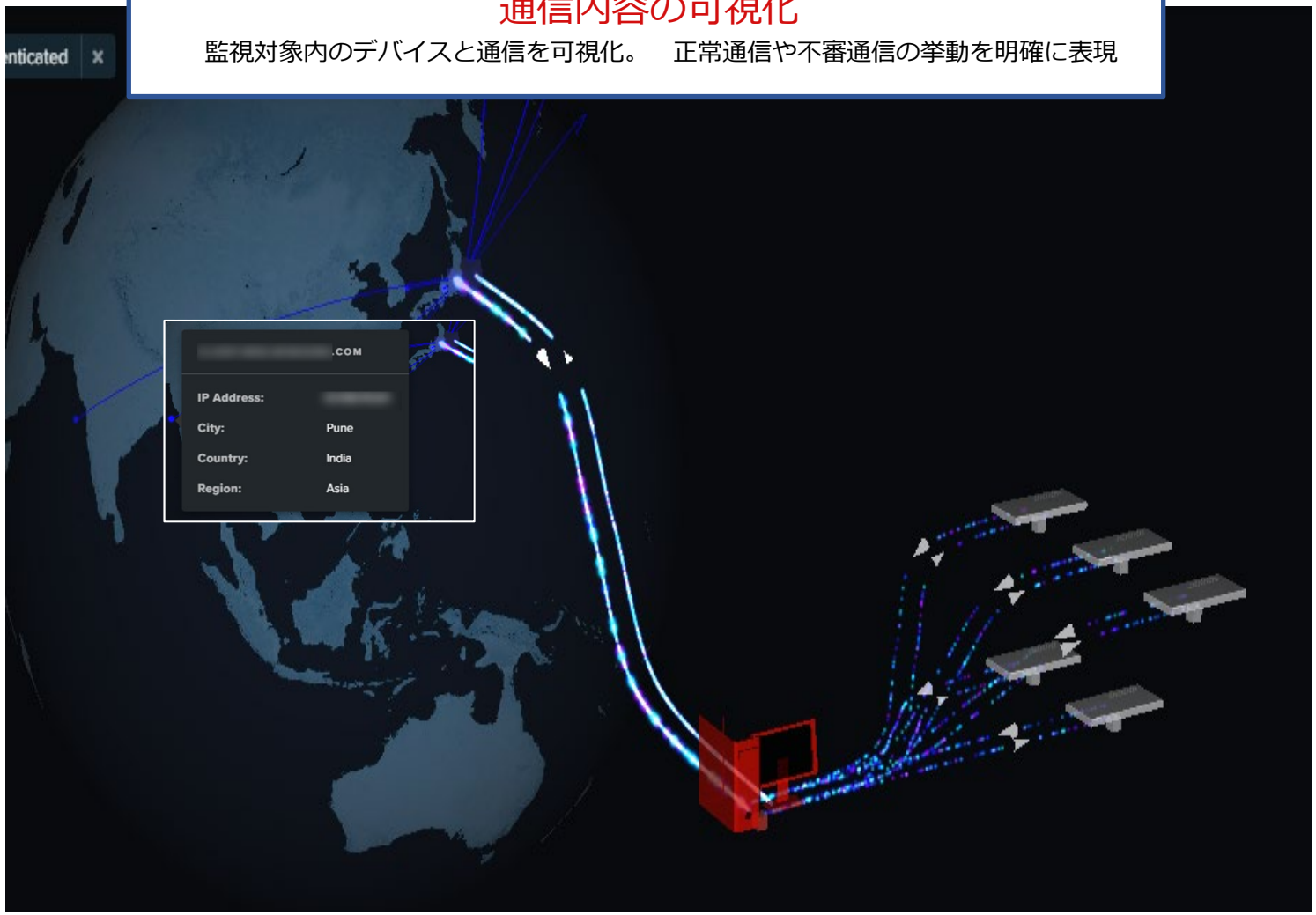


時系列で通信内容を収集

検知したイベント情報を確認し、検知時の関連情報を把握・調査可能

通信内容の可視化

監視対象内のデバイスと通信を可視化。　正常通信や不審通信の挙動を明確に表現



大変なアラートの脅威判定や影響調査をAIが脅威レベルを自動で判別・自動的に詳細レポートを生成します

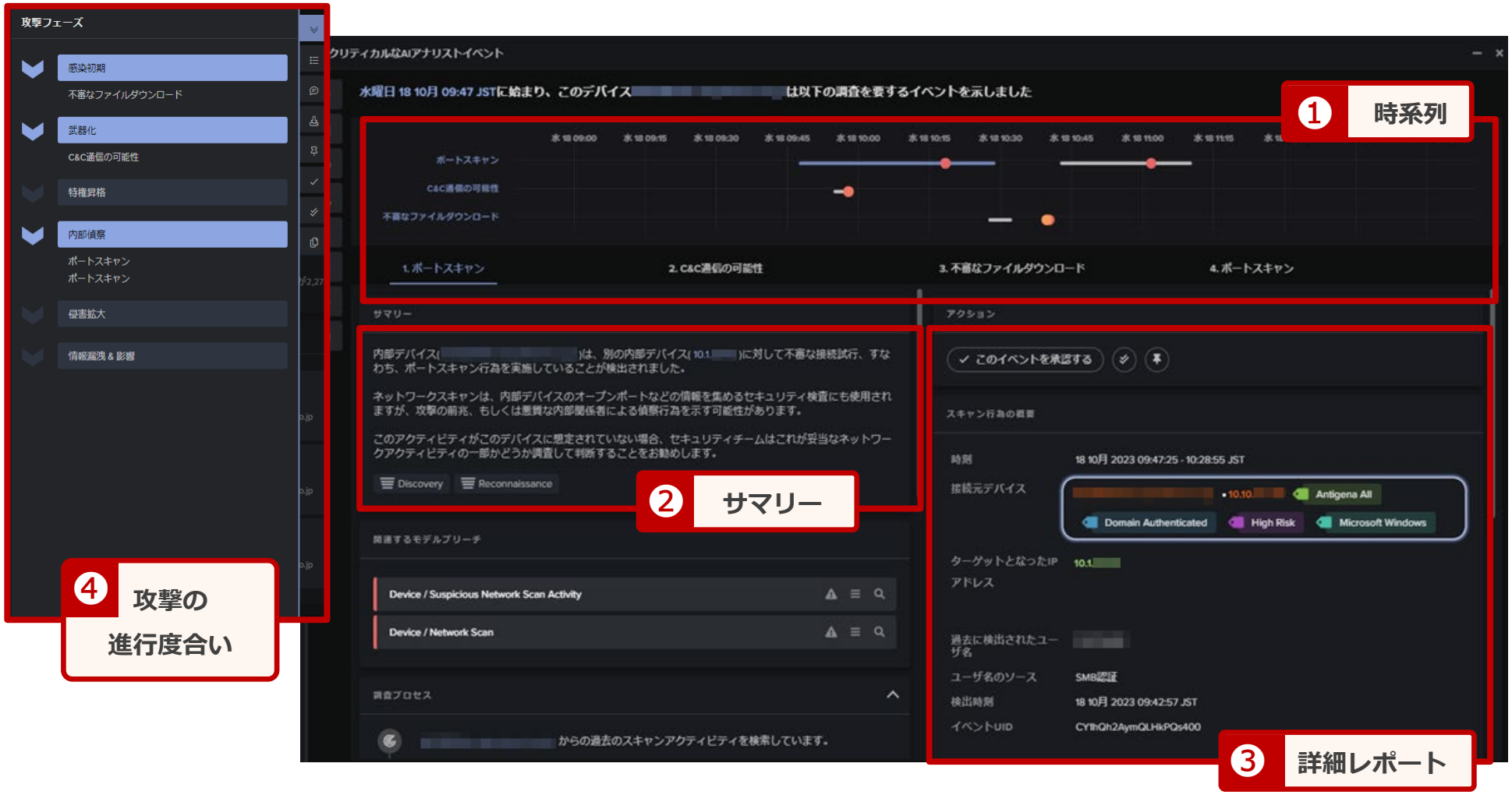
内部ネットワーク内で過去に発生していない珍しい通信として検知、このような未知の通信も、Darktraceは予兆レベルで検知可能

①イベントフローの可視化
関連性の高いイベントを
攻撃フェーズ毎に自動的に
関連付け

②自動的にレポートが生成
生成されたレポートを元に
関連部門と容易に連携可能
日本語対応済

③対応時間の削減
複数アラートを
1つのレポートで対応

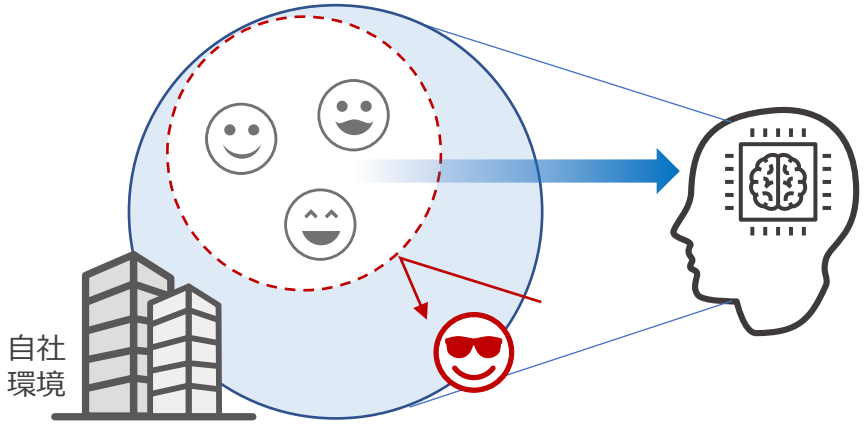
④攻撃度侵攻度を可視化
Cyber Kill Chain FWに沿っ
てわかりやすく表示



Darktraceは「通常業務＝正解」としてAIが常に自律的に学習しています

Darktraceのアプローチ（ホワイトリスト型検知手法）

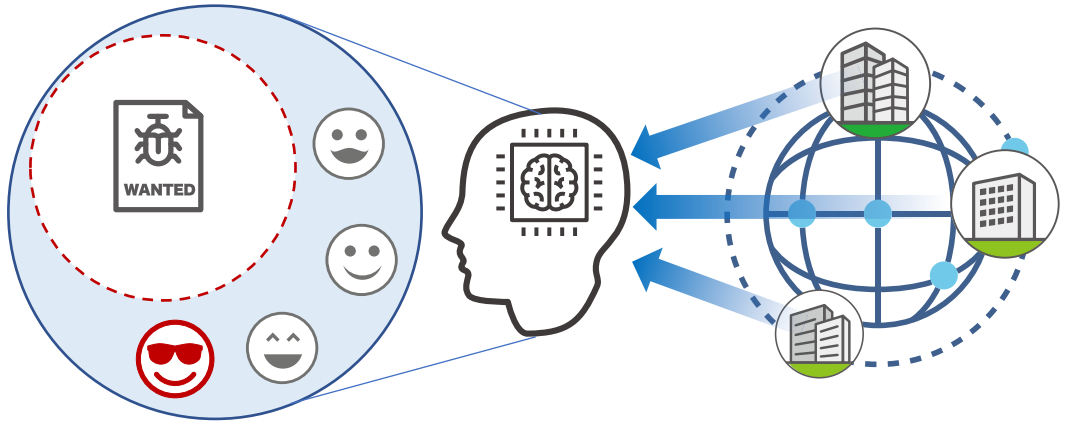
内部の情報を学習、**通常と外れた挙動**が異常



- お客様自身の通常業務＝正解 とするアプローチ
- ユーザー一人一人の行動を学習
- よって過検知・誤検知が極めて少ない
- 定期的なアップデートも不要

他社のアプローチ（ブラックリスト型検知手法）

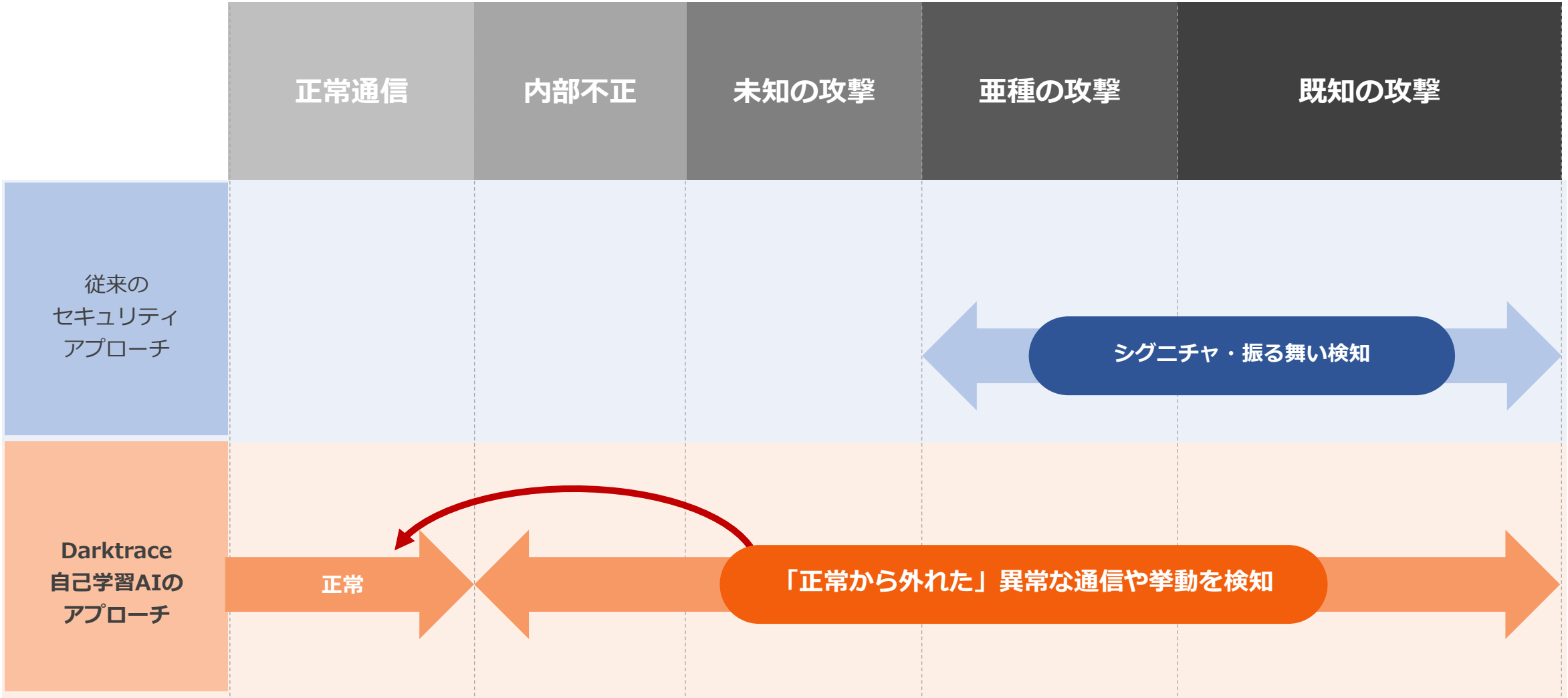
外部の情報を学習、**不正な値と一致した挙動**が異常



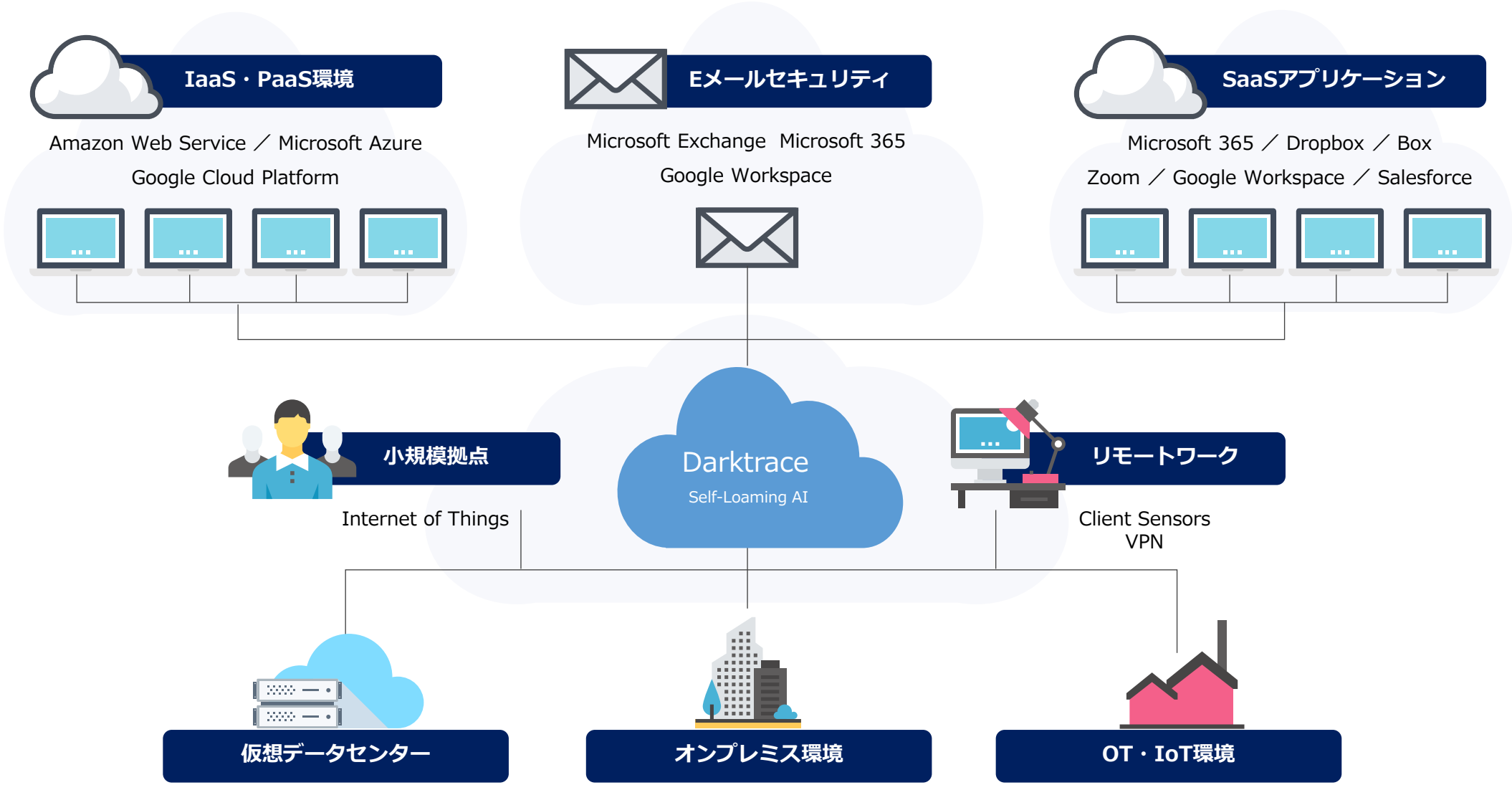
- グローバルから脅威情報 = 正解とするアプローチ
- ベストプラクティスを作り個社に適用
- 国の文化、組織文化に合わない点も生じる
- 情報が陳腐化するため、適宜アップデートが必要

Darktraceはシグニチャではなく普段を正常として脅威検知を行うため、未知やゼロデイ攻撃にも有効です

●脅威種別に対対するアプローチMAP



オフィスなどの内部ネットワークに加えテレワークやクラウドも含めた包括的なセキュリティ対策へ拡張可能



※本調査は、NDR製品である「Darktrace」の評価プログラムを利用して提供いたします。
※AI学習上の特性により、**従業員数250名以上の企業様が対象**となります。

社内ネットワークに潜むリスクを無料調査します

1. PCへの**インストール不要！**ネットワークに接続するだけで導入完了！
2. 自社のセキュリティの現状と課題点を可視化した**レポート＆解説付!**
3. セキュリティ専門家が結果を**わかりやすく解説・報告会**を開催！

セキュリティは**経営課題**です
経営層の皆様もぜひ**報告会**にご参加ください！

リスク評価を申し込む

https://www.lanscope.jp/professional-service/form-contact/darktrace-report/

構成等ヒアリング&打合せ
弊社　お客様

機器設定/出荷
弊社　お客様

機器現地設置
お客様

評価期間（1か月）
学習期間 → レポート①報告会 → レポート②報告会 → レポート③報告会

LANSCOPE
Professional Service

ペネトレーションテスト

侵入時の影響把握とリスクの可視化　|　導入済のソリューションの有効性チェック

12,000件以上のお客様を診断してきた経験豊富なセキュリティのプロフェッショナルが疑似的なサイバー攻撃を行い、御社の攻撃耐性を調査！セキュリティ強度を把握しリスクを可視化・対策できます。また新たなセキュリティ投資時の稼働チェックにも最適です。

こんな課題をお持ちの方におすすめです

十分対策しているけど本当にこれで大丈夫なのか

セキュリティ強化はどこが最優先なのか

新しく環境構築したがセキュリティに問題がないか

https://www.lanscope.jp/professional-service/service/assess_consulting/malware_assess/

担当営業にお問い合わせください

お問い合わせ

■ プロフェッショナルサービス営業部

大阪本社　06-6308-8980

東京本部　03-3455-1811

E-mail　security-sales@motex.co.jp