DARKTRACE

Darktrace ご提案資料
AIを活用したNDR（ネットワーク検知・対応）

株式会社 アイ・アイ・エム

2023年12月

目次

１．情報セキュリティの現状と対策

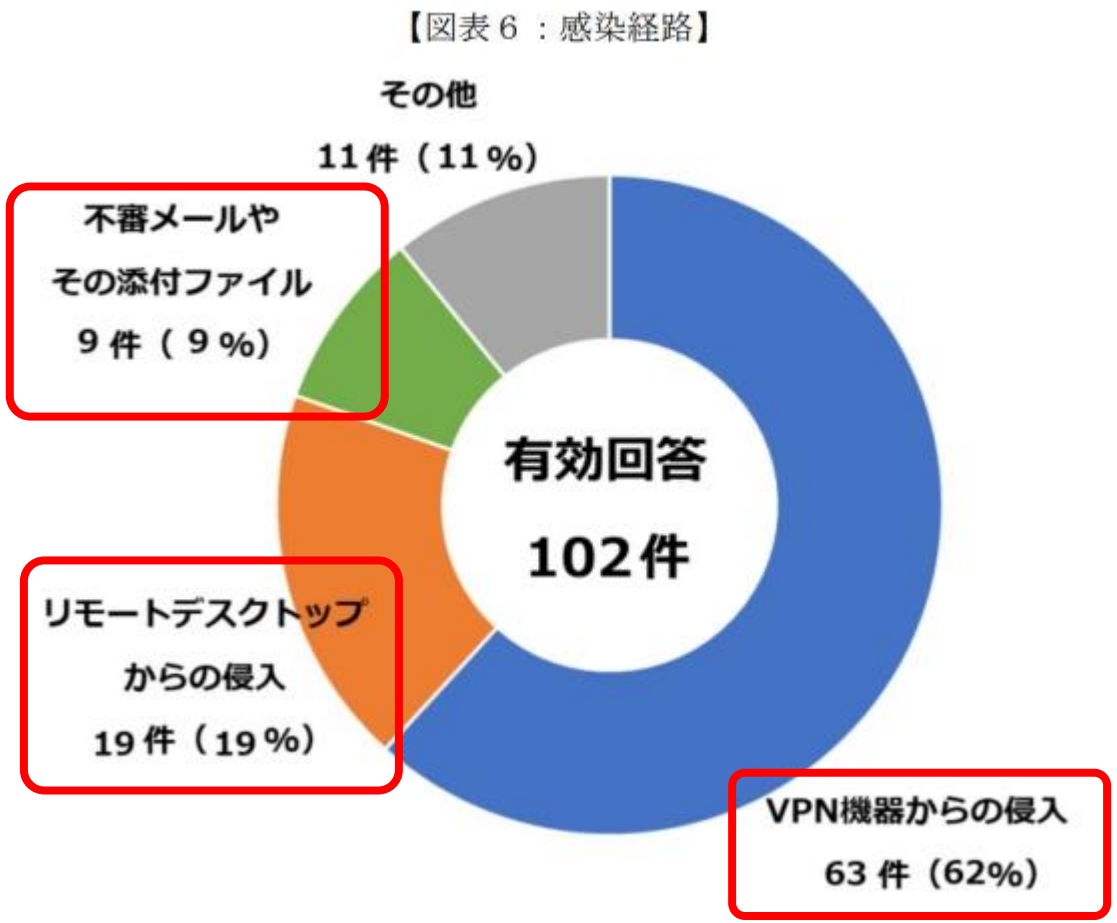
「情報セキュリティ10大脅威」の上位に**「内部ネットワークへ侵入する脅威」**が常にランクイン

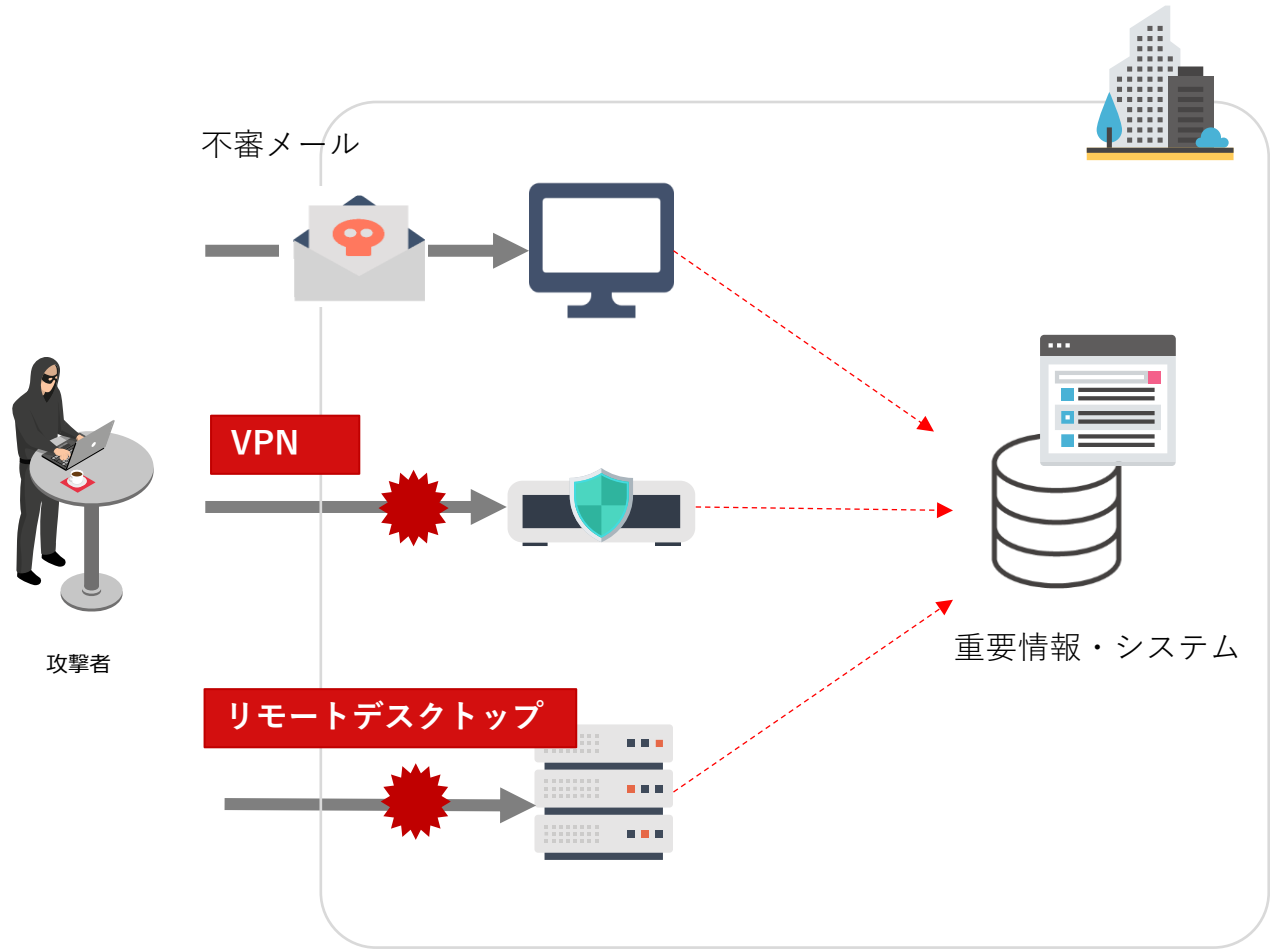
順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドビジネス）	NEW

※引用：IPA「情報セキュリティ10大脅威2023」

- 標的型攻撃メールなどを起点に、内部へ侵入され、重要情報がランサムウェアで暗号化される。
- サプライチェーンであるグループ企業、取引先企業、または海外関連会社など、セキュリティ対策の弱い組織から自社へ侵入される。
- テレワークに伴い急遽導入したソフトウェアや VPN 等の脆弱性を悪用し侵入される。

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

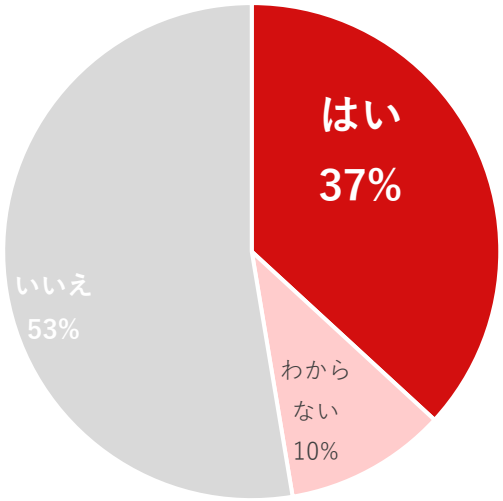




出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

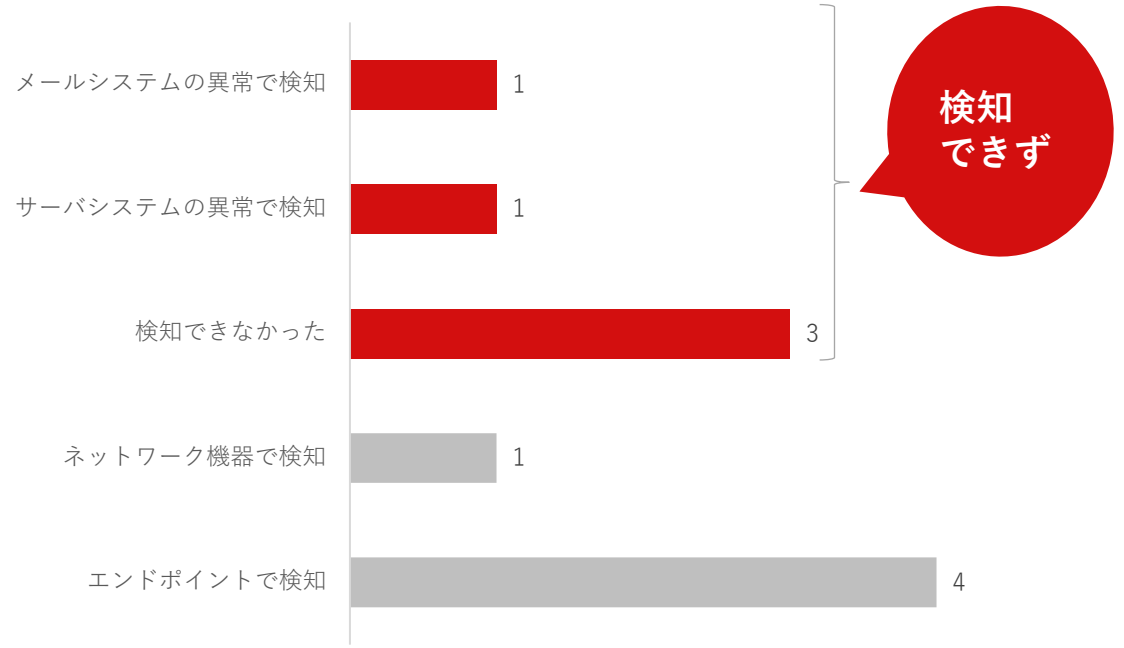
約4割のお客様にて**「内部ネットワークへの侵入を経験」**
しかし、**エンドポイントなどで脅威を検知できていない**

Q.マルウェアに感染し、内部ネットワークへ侵入されたことはありますか？



どうやって気づきましたか？

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？



MOTEXアンケートより
N=19

「ポリシー設計・適用の難しさ」や「攻撃者よる検知回避手法の確立」により

“エンドポイント対策頼み” にはできない

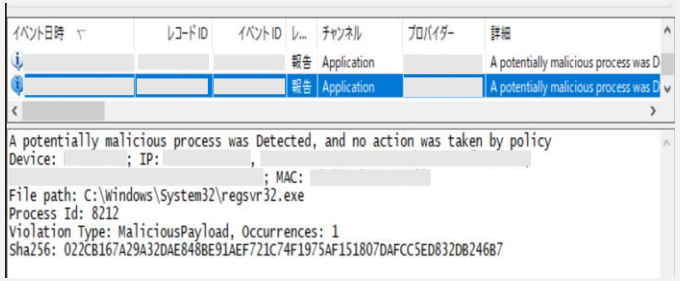
① 検知ポリシーの課題

□ ポリシー設計無しでの運用

EPP/EDRを導入しているにも関わらず、検知アラートが生成されない場合がある。
製品理解やセキュリティスキル等がなく、最適なポリシー設計ができておらず、本来の攻撃をすり抜けてしまうことがある。

□ 業務優先のポリシー設計

EPP/EDRを導入しているにも関わらず、検知アラートが生成されない場合がある。
過検知が続くことから、業務影響を鑑み、検知しないように設定変更することで、本来の攻撃をすり抜けてしまうことがある。



② 攻撃者による検知回避

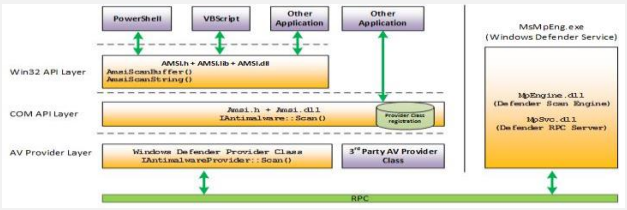
□ Living Off The Land

クラッキングツールを追加で送り込むことなく、侵害したシステム内にビルドインされているツールやバイナリを活用して攻撃を行うことで、通常の挙動として検知を回避する手法が確認されている。

出展： https://lolbas-project.github.io/

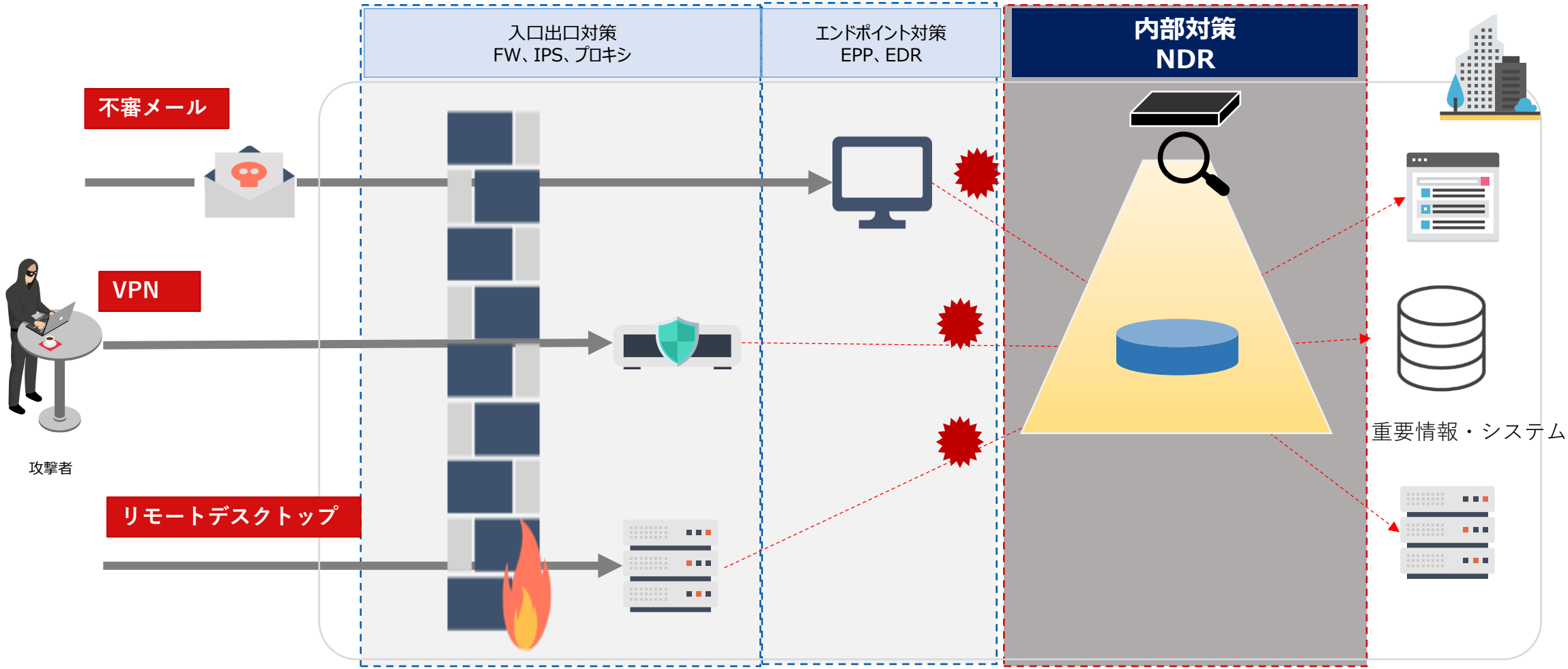
□ AMSI バイパス

AMSIはWindows10に実装されている統合インターフェイス。スクリプトの処理内容などをEPP/EDRに送ってスキャンできるが、そのスキャンを回避する手法が確認されている。



出展： https://learn.microsoft.com/en-us/windows/win32/amsi/how-amsi-helps

NDR（Network Detection and Response）とは、ネットワーク機器に流れるトラフィックを分析し、外部からの攻撃や内部不正などの兆候を可視化・検知するセキュリティ手法を指します。



２． AIを活用したNDR製品 「Darktrace」 のご紹介

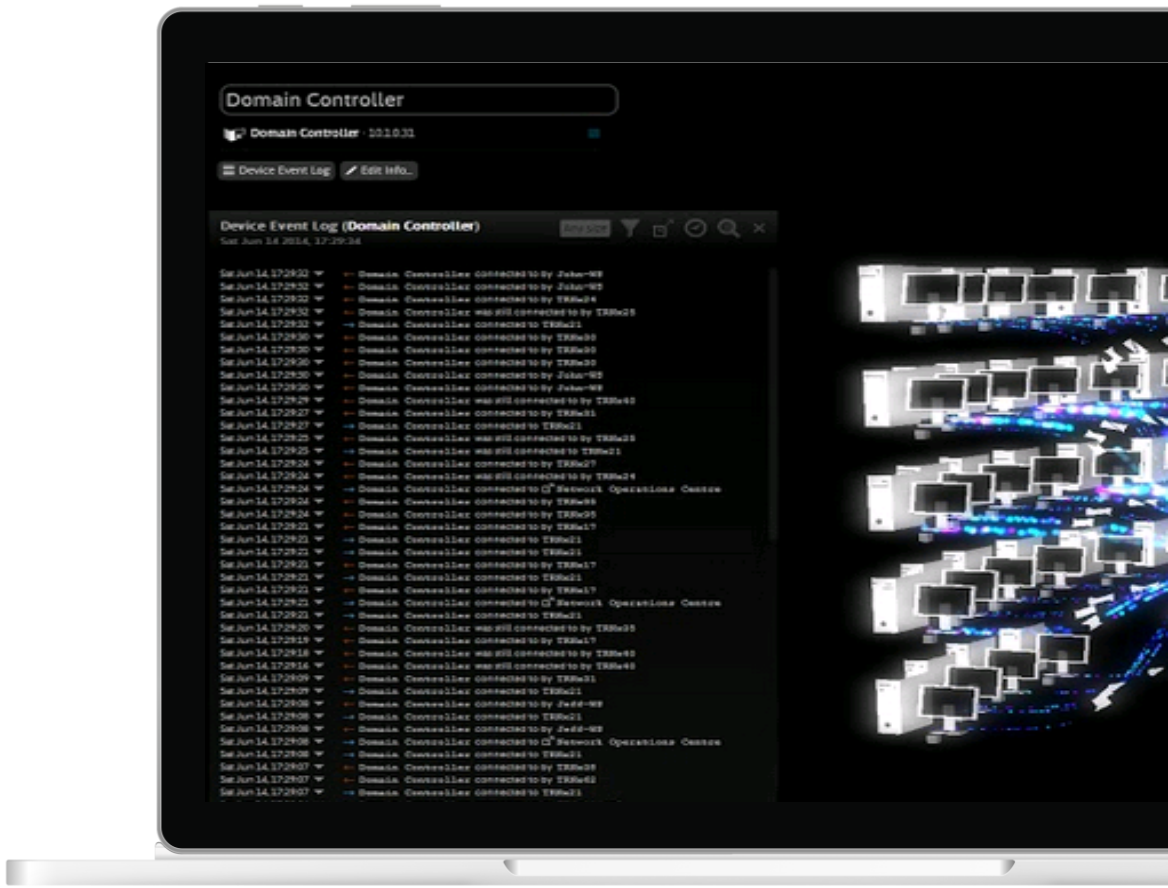
入口出口対策をすり抜け、内部へ侵入してくる脅威をネットワークで網羅的に検知・対処

DARKTRACE

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/



[DTL1]

全世界で 8,800社※ 以上が導入、日本国内でも様々な業種で利用されています。

日本国内の導入実績

DARKTRACE

2016年の日本進出から現在までに182社以上の導入実績

[DTL1]

※ Darktrace社資料から抜粋　2023年12月時点

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

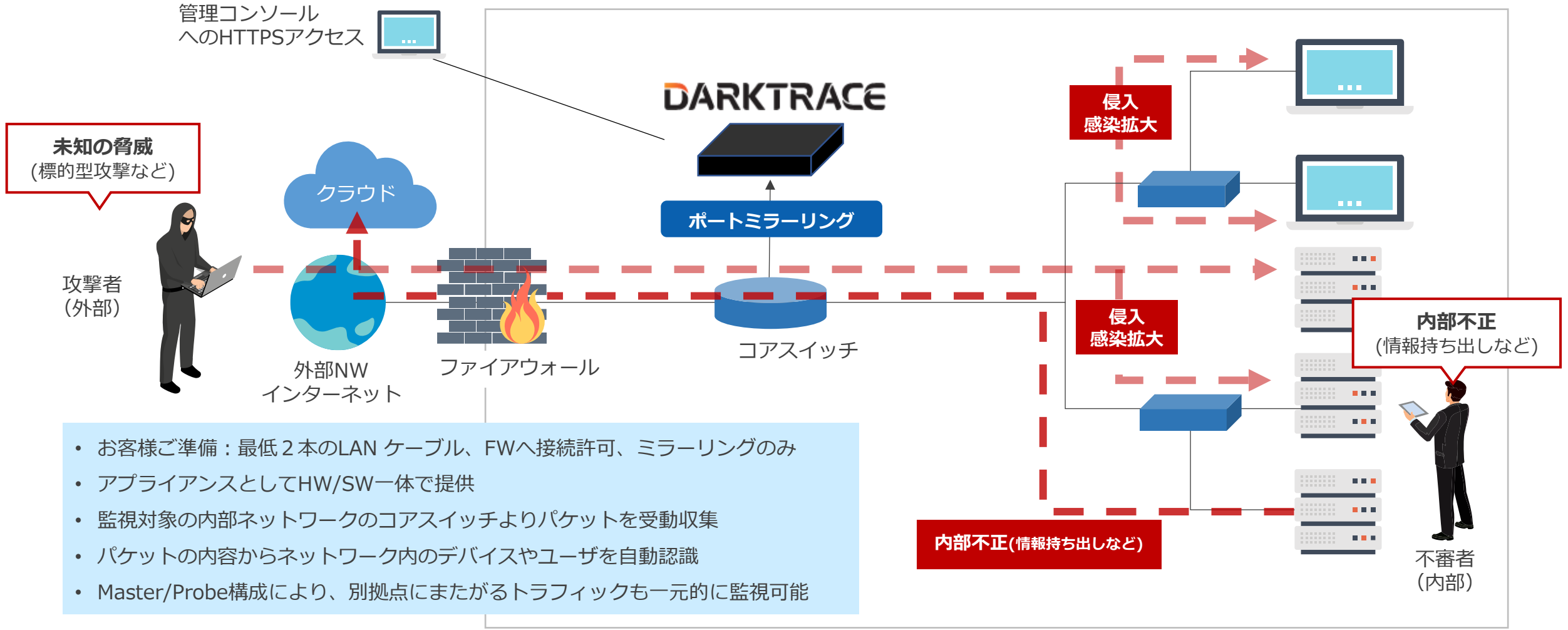
「教師なし機械学習」

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

特徴① ： アプライアンス型で最短1時間程度で簡単に導入可能

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**

ネットワーク機器に流れるトラフィックを基にAIを活用しサイバー攻撃や内部不正の兆候を検知



- 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

特徴② ： 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

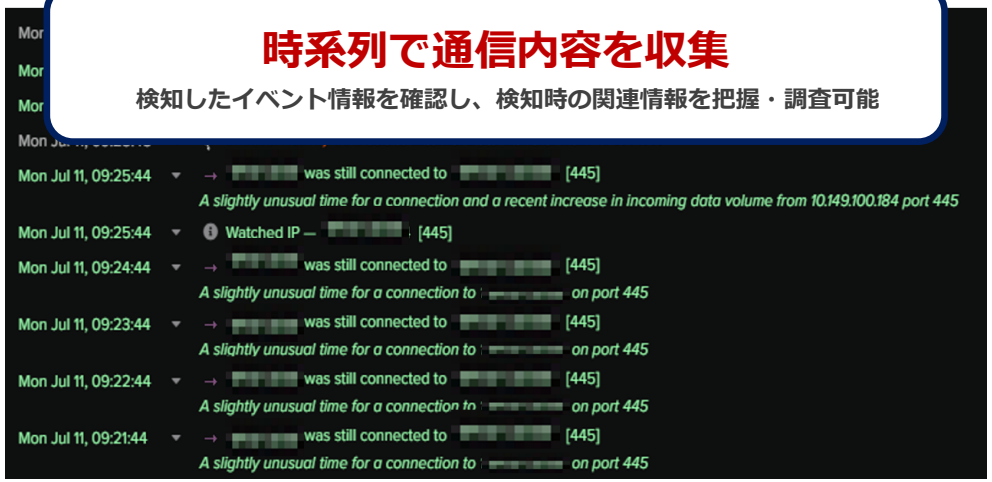
ネットワーク全体の通信を可視化することで、セキュリティ分析作業が効率化します。

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



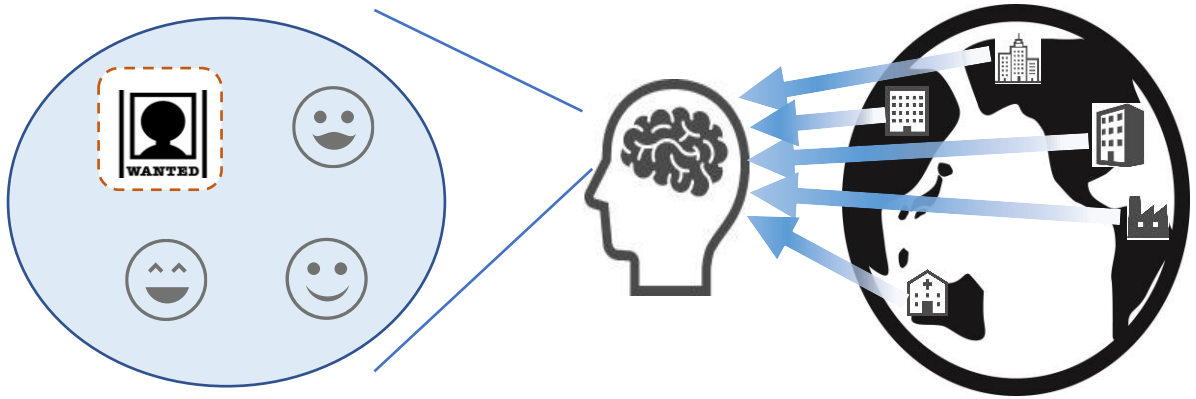
通信内容の可視化

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

正解となるモデルを「外部」と「内部」のどちらに求めるか？の違い

他社のアプローチ

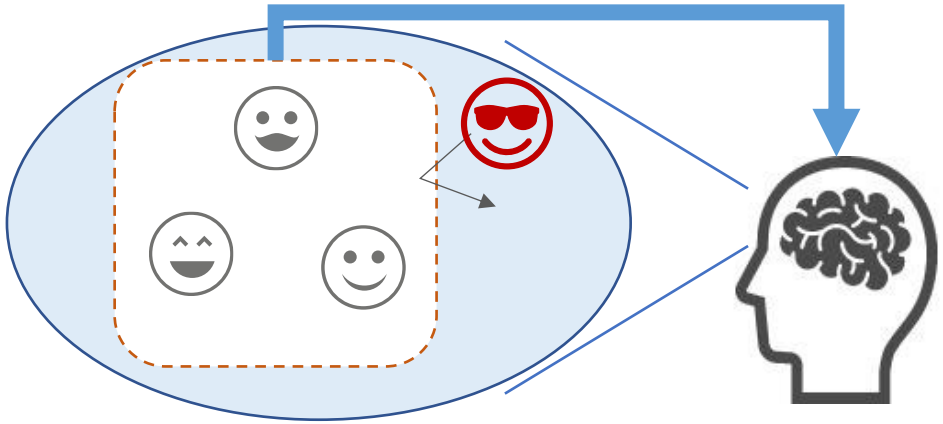
外部の情報を学習、**不正な値と一致した挙動**が異常



- ✓ **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のアプローチ

内部の情報を学習、**通常と外れた挙動**が異常

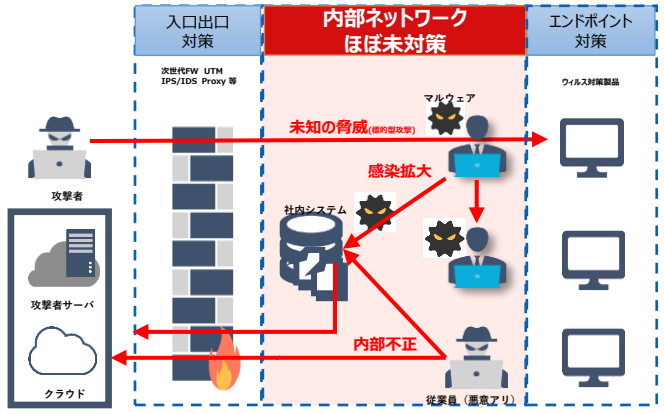


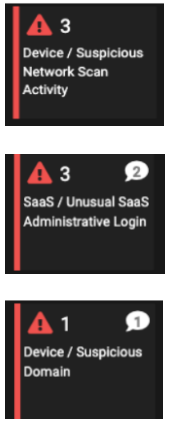
- ✓ **お客様自身の通常業務**＝正解 とするアプローチ
- ✓ ユーザー一人一人の行動を学習
- ✓ よって過検知・誤検知が極めて少ない（ユーザー様談）
- ✓ 定期的なアップデートも不要

2種類のAIにより「多種多様な脅威の検知」と「運用の省力化」を実現

①教師なし機械学習で異常を検知

- 異常 ＝「いつもと異なる」「周りと異なる」挙動を検知
- ハッカーが攻撃をすれば、**必ずいつもと違う挙動が発生する**。





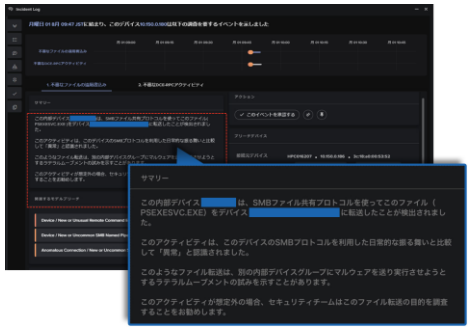
✓ アラート

外部や内部からの脅威を見逃さない
“多種多様な脅威の検知”が可能な**検知アプローチ**

②サイバーAIアナリストが検知した異常を分析

- アナリストの分析手法を学んだAIが、検知した異常を **自律的にトリアージ**
- AIが作成するレポートをもとに**素早く**判断でき、脅威に対し効率的に対処可能

✓ インシデント化



✓ レポート化

重要なインシデント対応に**専念できる**
“運用の省力化”が可能

特徴③　AIによる脅威検知： AIが自動で脅威を分析、トリアージ「 サイバーAIアナリスト」

＜Emotet感染の検知事例＞

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し詳細な自動的にレポートを**日本語**で生成します！

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

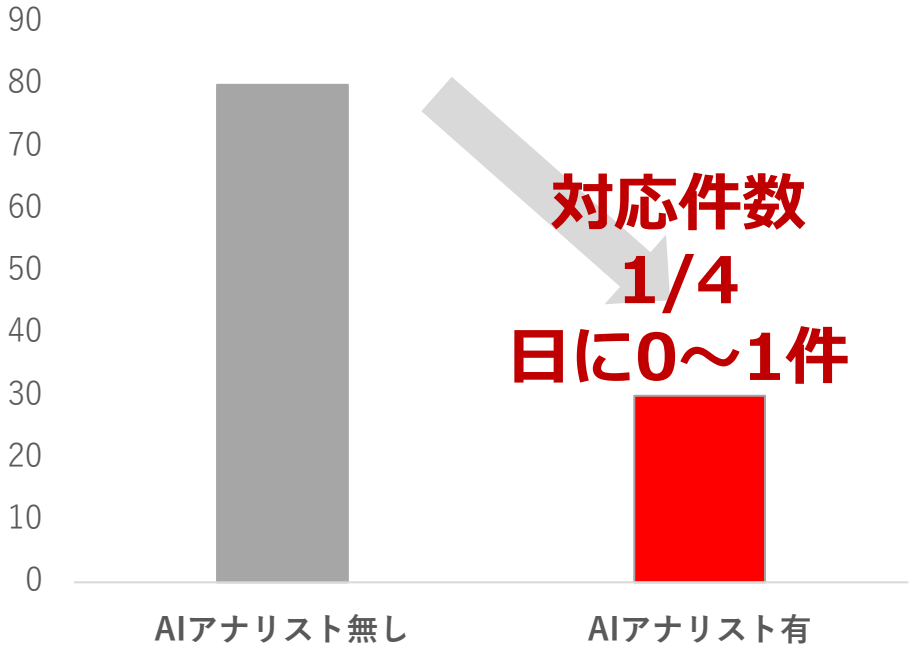
生成されたレポートを元に
関連部門と容易に連携可能
日本語対応済

③対応時間の削減

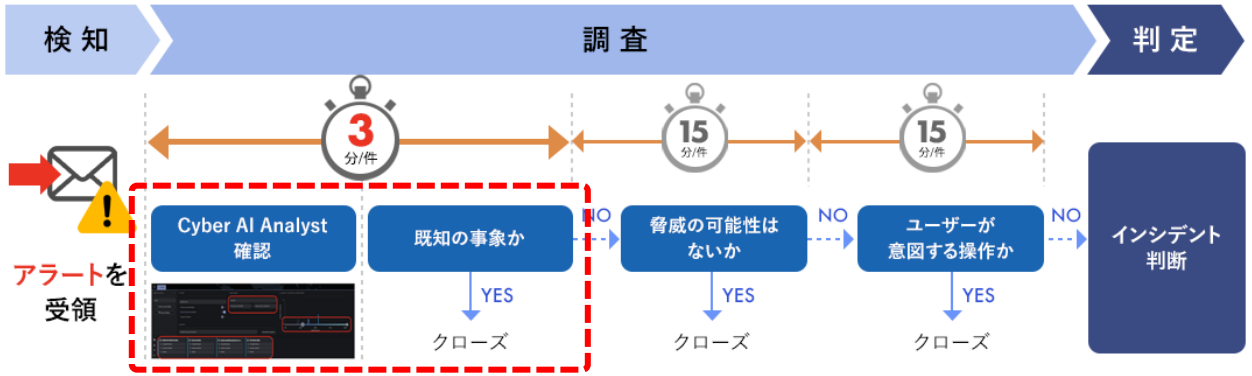
複数アラートを
1つのレポートで対応

サイバーAIアナリストはセキュリティ運用の工数を削減します。

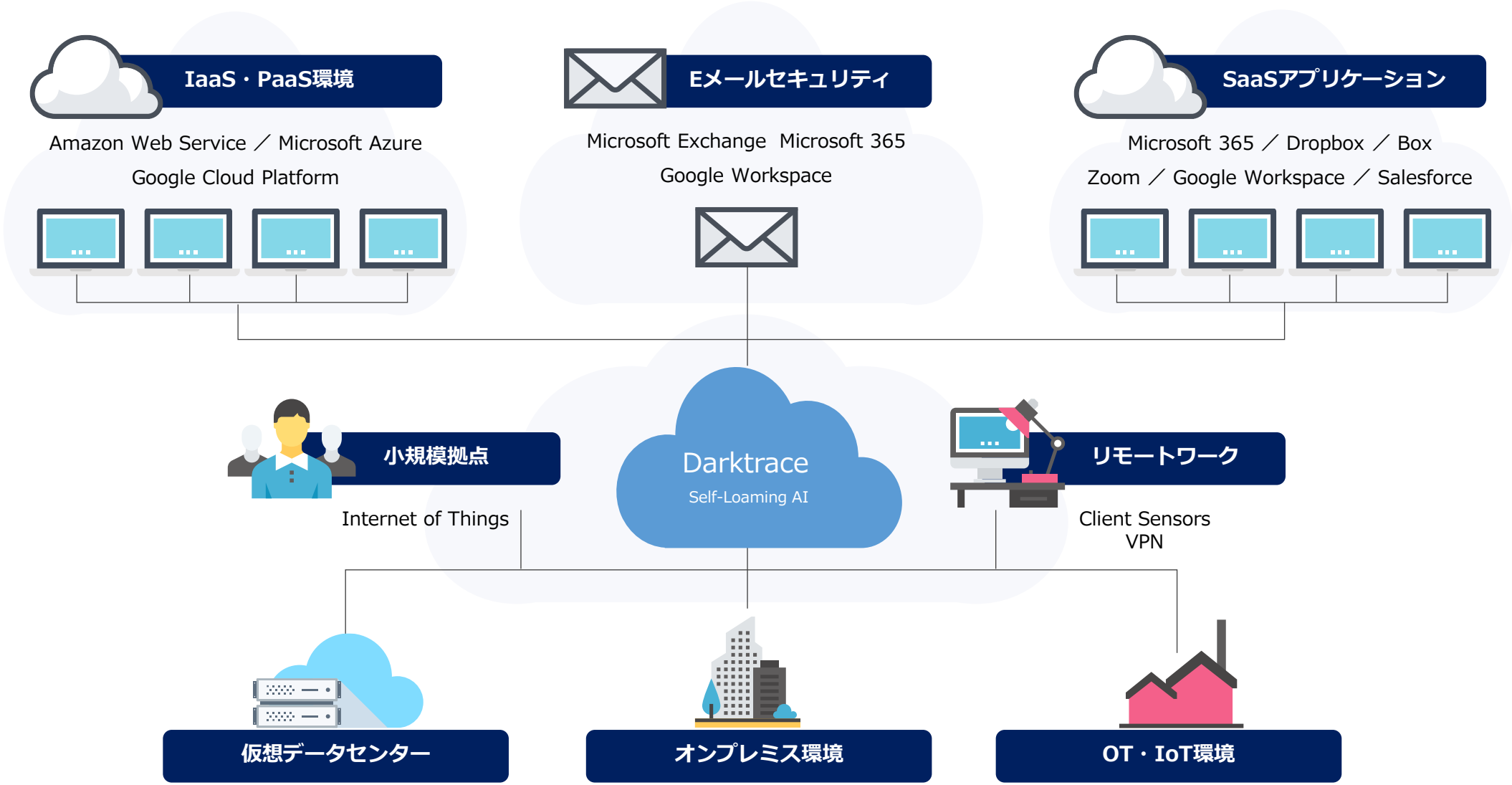
アラート対応件数の例
（監視対象1,000台規模の場合）



セキュリティ監視運用の例
1件あたり3分で確認完了



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



3． Darktrace サービスについて

DarktraceのNDRに加え、エムオーテックスによる人が行うサイバーセキュリティ運用支援

DARKTRACE × LANSCOPE Professional Service

最新の攻撃手法と最適な対応策を探求するセキュリティプロフェッショナルがサイバー攻撃などのリスクから組織を守ります。
Darktraceの検知と難関国家資格保有のセキュリティプロフェッショナルが運用・監視を行います。

- AIによるネットワーク脅威検知「Darktrace」
- 難関国家資格取得者を中心としたサービス提供体制
- NDR×セキュリティプロフェッショナルによる細やかな支援

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

充実の提供実績

2015年~
多業種 への導入実績

Darktraceの日本進出時から、いち早く取り扱いを開始。製造業や金融業、重要インフラなど様々なお客様への導入により蓄積されたナレッジ・ノウハウが弊社の強みです。

自社でのフル活用

SOC
×
CSIRT

我々は単なるベンダーではありません。自社やグループ企業にDarktraceを導入し、SOC/CSIRTの観点から有効な運用方法を常に模索しています。得られた知見はアナリストや運用監視サービスへフィードバックされています。

弊社LANSCOPE製品とのコラボ

Endpoint Manager
×
Cyber Protection

弊社が提供するセキュリティ対策製品(エンドポイントマネージャー、サイバープロテクション)のログも併せての調査が有効です。インシデントかどうか判断できない場合、原因や影響の特定のため、 エンドポイントソリューションを有効活用します。

Darktraceサービスのメニュー 一覧

	名称	付帯サービス	概要
1	**Darktrace 3年間ライセンス**	製品保守	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスをご提供いたします。
2	**Darktrace 運用監視付(スタンダード) 3年間ライセンス**	製品保守 運用監視（スタンダード）	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスに加え、Darktrace 社提供の監視サービスをご提供いたします。
3	**Darktrace 運用監視付(アドバンスド) 3年間ライセンス**	製品保守 運用監視（アドバンスド）	Darktrace製品 のご利用に必要なアプライアンス・デバイスライセンス/保守サービスに加え、MOTEX 社提供の監視サービスをご提供いたします。

Darktrace製品のご契約と共に、お問い合わせ・製品保守サービスを標準でご提供します

■Darktrace製品に関するお問い合わせ

・Darktraceの操作方法

- Threat Visualizer
- Advanced Search

・機器の各種設定

- Config
- System Status

・機器が正常に利用できないなど

■その他保守

・ハードウェア故障対応（代替機器送付、サポート）

・Darktrace 最新情報のご案内

・ソフトウェアのアップデートモジュール提供/検証など

MOTEX Darktraceサポートセンター

お問い合わせ先：darktrace-support@motex.co.jp

受付：当社営業時間内（9:30～17:30）

◆安心の日本語サポート

◆1営業日以内に受付、3営業日以内に一次回答※

※ メーカ調査の状況により、お時間を頂戴する場合があります

※ 電話やオンサイトでのサポート対応は受け付けておりません。

※ モデル作成や運用方法、発生アラート等のお問い合わせはサポート範囲外です。別途メーカ提供のサポートサービスにて提供可能です。

※ 契約担当者様からのみ問い合わせを受付いたします。

※ 代替機器はメーカよりお客様先へ直送いたします。また、交換機着荷後の初期設定および機器設置は本サービスに含まれません。

４． Darktrace 運用監視付き メニューについて

監視運用サービスで、自社運用によるあらゆる 「不足」の解決をサポートします

自社運用の場合

日々発生する
セキュリティアラートに対し・・・

◆常時監視が出来ない
（**リソース不足**）

◆最新の攻撃に気づけない
（**情報不足**）

◆マルウェア感染か正常な通信か
分からない（**スキル不足**）

◆どのアラートを報告すべきか
分からない（**経験不足**）

検知 → 調査分析 → 報告

運用監視サービスの場合

検知 → 調査分析 → 報告

監視工数が大幅に削減

検知

・セキュリティアナリストによる定期監視
・情報による一次切り分け
※ アラート内容、検知条件、想定される脅威
・最新の脅威インテリジェンス情報による一次切り分け
※ 脆弱性情報、攻撃手法、マルウェア解析情報

調査・分析

・該当端末の特定、攻撃サーバーの調査・特定
・発生時系列の分析、影響範囲（感染）の調査
・発生前後の挙動及び操作情報の調査（原因特定）
・外部の脅威情報を踏まえた分析（接続先、ハッシュ値など）

報告

・適切な対処（NW隔離、AVスキャンなど）及び対策を支援
・自社・他社の監視実績を基にした報告アラートの選別

運用監視サービスの概要

	スタンダード	アドバンスド
提供元	**Darktrace**	**エムオーテックス（MOTEX）**
サービス特徴	・メーカーのアナリストによる標準サービス ・高危険度のアラートを調査 ・通知内容は発生した通信の情報のみ	・MOTEXのアナリストによる高付加価値なサービス ・高危険度で発生したアラートが調査対象 ・通知内容は通信内容に加え、原因・経緯まで含まれる ・顧客の環境に合わせた調査範囲のカスタマイズ提案可能
対応言語	**英語**	**日本語**
対応時間	**24時間365日**	**24時間365日** ※弊社営業日 9:30-17:30はMOTEXアナリストによる詳細解析/分析/通知を提供 それ以外の時間帯はDarktrace機器からのアラート自動メール通知とし、 MOTEXアナリストによる詳細解析/分析/通知は翌稼働日での対応となります。
報告タイミング	**随時** Darktrace社アナリストによる分析調査した結果、早急に調査が必要な事象と判断した時点で連絡します。	**定期** MOTEX社アナリストによる分析調査した結果を1日に2回、弊社営業日にて定期連絡します。 ① 9:30-15:00の発生アラート ⇒ 当日17:30までに報告 ② 15:00-翌9:30の発生アラート ⇒ 翌日12:00までに報告
検知後のアクション	・ Darktrace社アナリストによる分析調査 ・ 早急に調査が必要な事象と判断したものを報告 ・ 問題がなければ、報告せずクローズ	・ 弊社アナリストによる分析調査 ・ 弊社アナリストからお客様セキュリティ担当者にメール報告 ・ 問題がなければ、報告せずクローズ
カスタマイズ性	**不可** ※アラートの調査・分析はDarktrace機能で可能なもののみとし、他機器のログ調査などは含みません。	**可能** ※MOTEX提供のセキュリティ対策製品(エンドポイントマネージャー、Cylance、Deep Instinct)のログ調査
対象アラート数	**上限なし**	**詳細調査は15件/月を想定** ※調査対象のアラート件数を超える場合、翌月に超過分をご発注いただきます。
報告内容の問い合わせ	**問い合わせ対応なし** ※別途有償サービスを契約する必要あり	**Eメール**

Darktrace社による運用監視（スタンダード）の概要

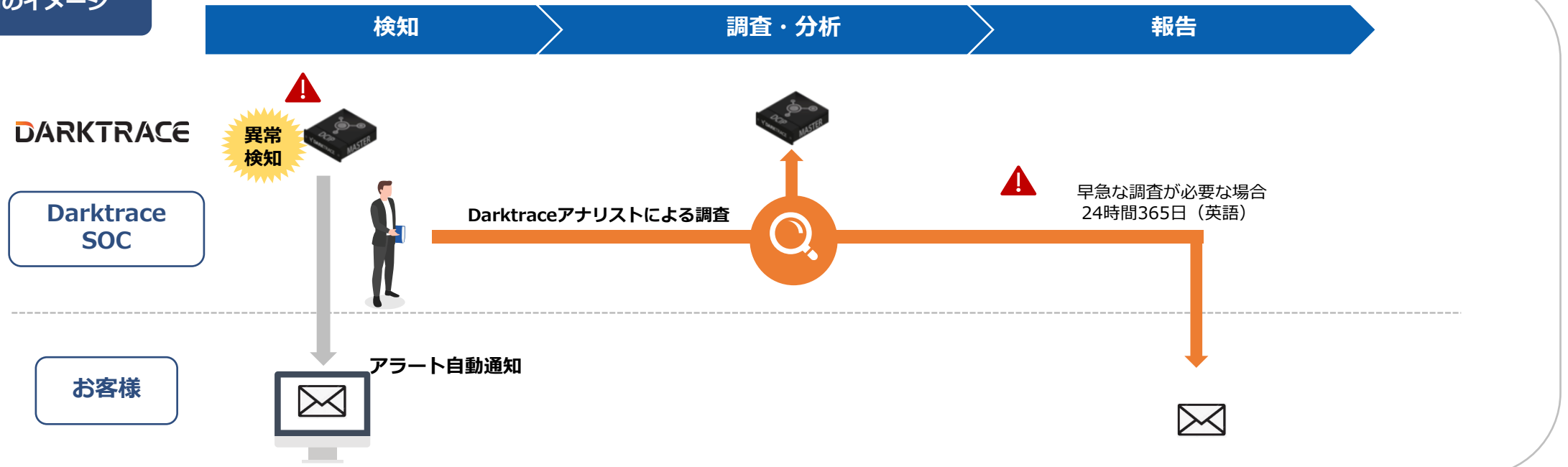
Darktraceのサイバーアナリストによって確認された、重大で影響が大きい可能性のあるアラートを
お客様へE-mail、SMS、もしくは、サポートチケットにて通知を行うサービスです

サービスの特長

サイバーアナリストが
脅威を検知・サポートします

Darktraceのアナリストがアラートを調査します。
早急に調査が必要な事象と判断した場合、24時間365日、メールやSMNなどで管理者へ通知を行います。

運用のイメージ

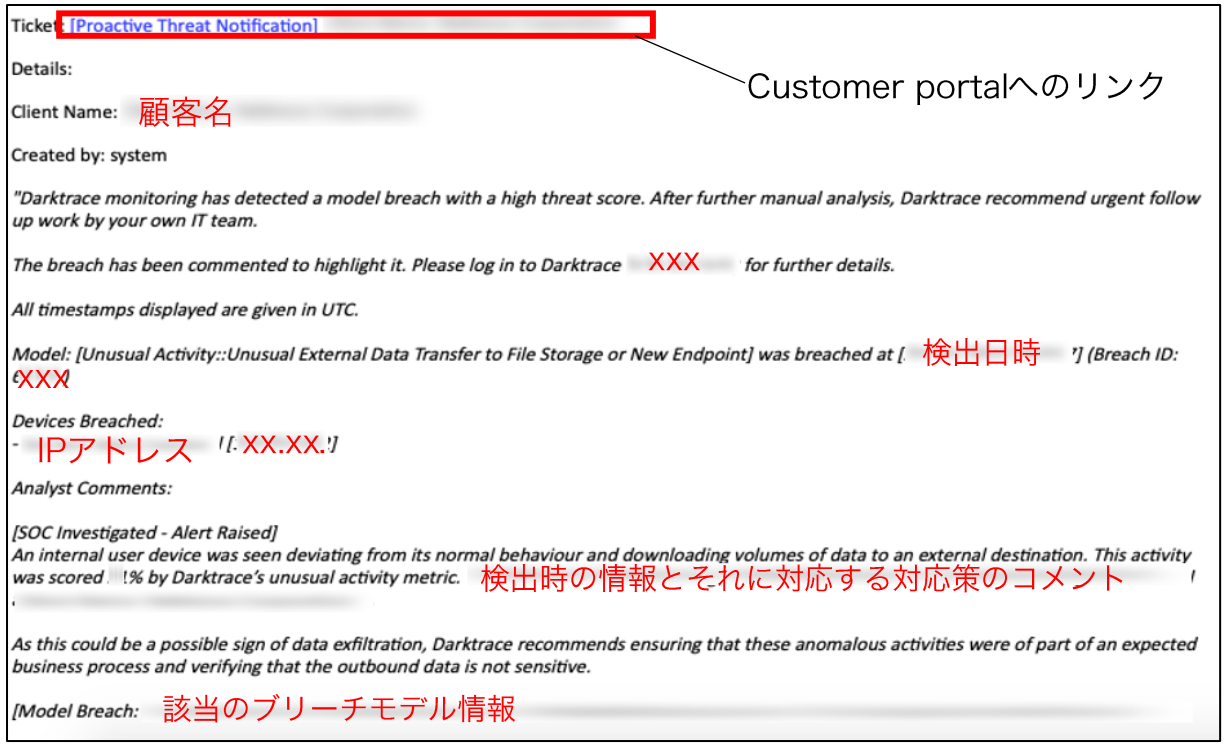


アラート報告イメージ

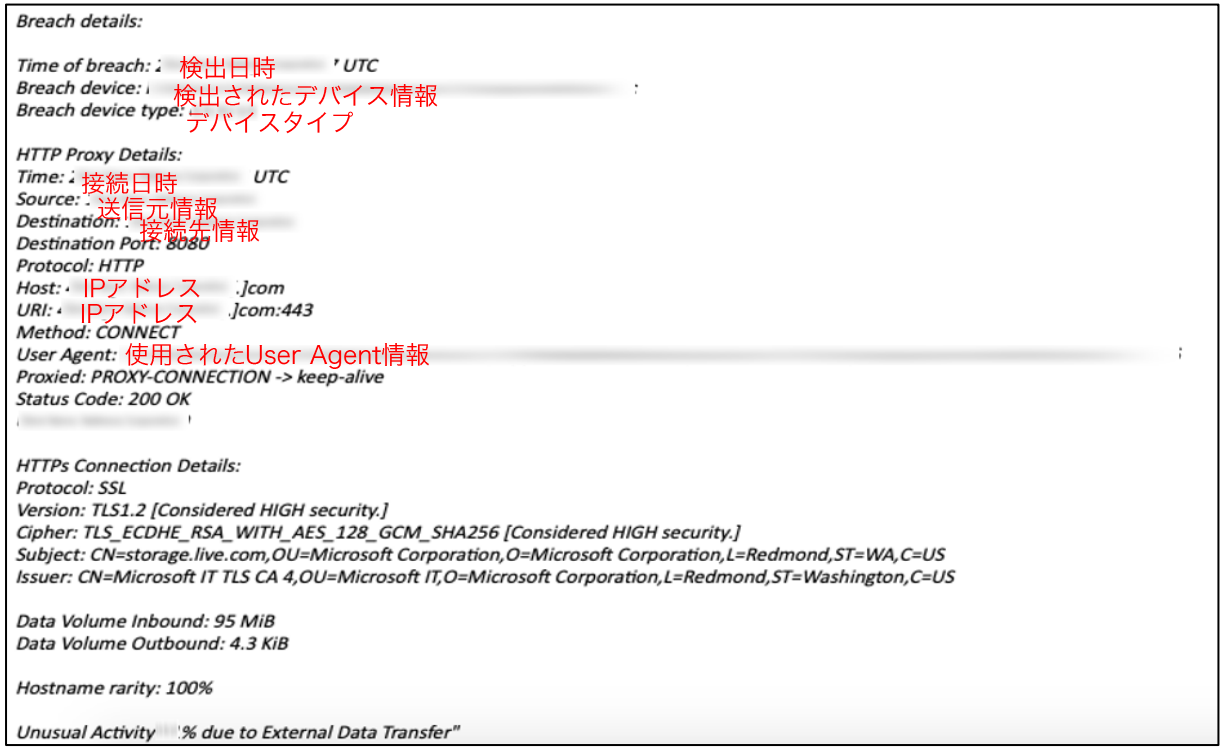
報告内容

- 検知日時
- 検出脅威（アラート名、アラートレベル等）
- 検知内容（対象端末、通信先）
- 確認事項（対応策のコメント）

● 検出ブリーチ概要の通知



● 検出ブリーチ詳細情報の通知



エムオーテックスによる運用監視（アドバンスド）の概要

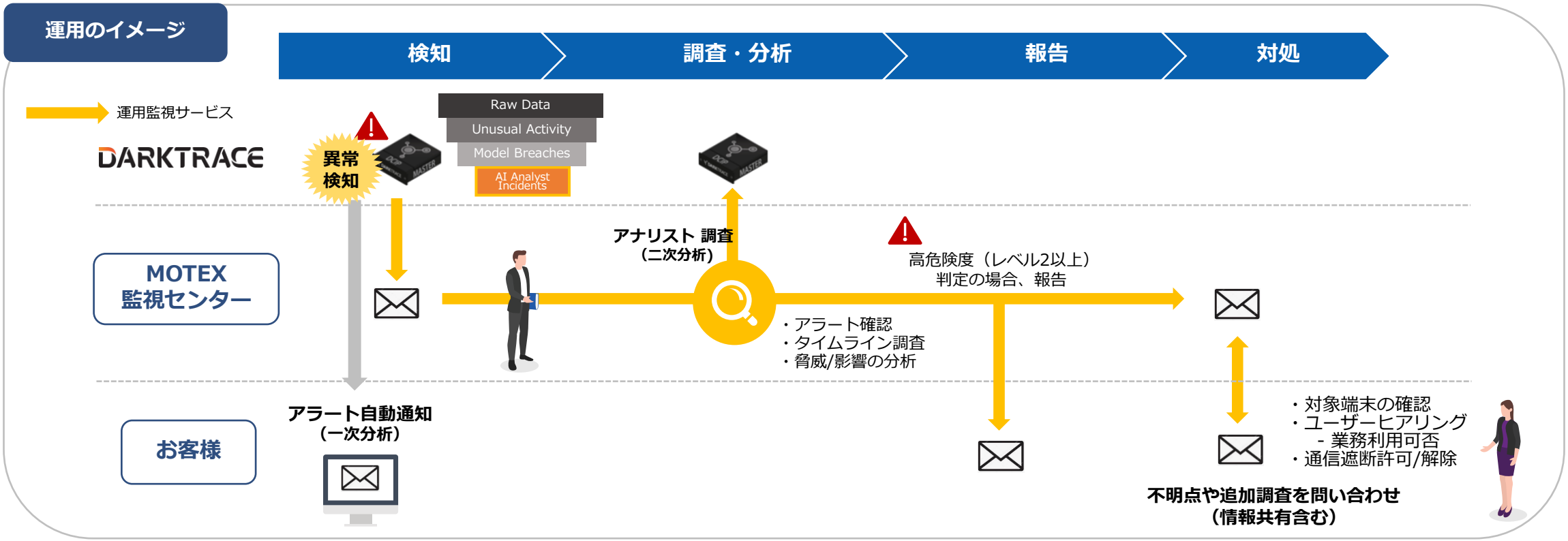
Darktraceの各種機能によるNWフォレンジックの観点からのアラート調査や、外部脅威情報(OSINT)を踏まえた分析により、精度の高い調査結果をご提供します

サービスの特長

MOTEXのアナリストが分析調査
日本語でサポートします

エムオーテックスのアナリストが分析調査した結果を1日に2回、定期連絡します。
調査分析レポートは日本語で行われ、通信内容に加え、原因・経緯までを報告します。
アラートに関してQ&A対応も可能で、安心してご利用いただけます。

運用のイメージ



弊社アナリストが、脅威度が高いアラートと判断した場合、日次レポート（メール）にてご連絡します

報告内容

- 検知日時
- 検出脅威（アラート名、アラートレベル等）
- 検知内容（対象端末、通信先）
- 調査内容（OSINTでの調査結果）
- 確認事項（推奨対処）

● 日次レポート例 ~マルウェア感染事例~

【検知日時】 ： 20XX年▲▲月◆◆日 16:35:12
【検出脅威】 ： Unusual Incoming Data Volume（73%）
【検知内容】
対象端末より、普段接続しない通信先に対して繰り返し行われる通信が検知されました。
C&C サーバとの通信である可能性があります。
- 対象端末 ： 10.150.120.XX
- 通信先 ： panisdar[.]com（5[.]188.60.XX）
【調査内容】
通信を確認したところ、通信先のポート番号443（SSL）に対して9:29～10:01、
13:05～17:06の時間帯に通信が発生していました。通信先は C&C サーバとして報告されています。
また、以下のファイルをダウンロードすることが報告されており、対象端末は16:07:00にアクセスを行っていました。
・http://XXXXXXXXX [.]org/img/sm/story.rar
※アクセスすると、マルウェアに感染する恐れがあります。
VirusTotal上では複数ベンダーが脅威ファイルであると判定しています。
VirusTotalの結果:https://www.virustotal.com/gui/file/xxxxx（ハッシュ値）
【確認事項】
マルウェア感染などの被害が拡大する恐れがあるため、該当する端末をネットワークから至急隔離してください。なお、通信先情報より、最近確認されている不審メールを開封した可能性があります。
以下、参考URLとなります。
・https://www.jc3.or.jp/topics/v_log/201902.html#d20190218b
※情報窃取型不正プログラム「URSNIF」に関連

該当する端末を確認し、不審なメールに添付されたファイルを開いていないか、
不審ファイルが検知されていないかを確認してください。
また、ウイルス対策ソフトによるスキャンを実施することを推奨します。

エムオーテックスによる運用監視（アドバンスド）のアラート報告イメージ

事前に報告基準を取り決めた上で、脅威度の高い通信を検知した場合のみ、ご報告します

例えば「Level2」 以上を報告対象とし、Level 1以下は対象外となります

緊急度高

緊急度低

報告対象

レベル	報告	定義	具体例
Level 3	日次メール (詳細報告) 及び 月次レポート	**【緊急対応】** 被害が確認でき、 セキュリティインシデントが 発生している可能性が極めて高い	**【攻撃関連】** ・ウィルス感染による通信が発生していると判断した場合（C＆C通信、内部NWからの攻撃通信） ・ウィルス感染によって、データ転送など、情報漏えいの可能性があると判断した場合
Level 2	日次メール (詳細報告) 及び 月次レポート	**【詳細調査】** 被害は確認できず、 セキュリティインシデントが 発生している可能性が高い	**【攻撃関連】** ・ウィルス/スパイウェアのダウンロードを検知したが、端末に影響があると判断できた場合 ・スパイウェア感染による通信が発生していると判断した場合 【内部不正】 ・ポリシー違反によって、データ転送など、情報漏えいの可能性があると判断した場合
Level 1	日次メール (簡易報告) 及び 月次レポート	**【経過観察】** 被害は確認できず、 セキュリティインシデントが 発生している可能性が低い	**【攻撃関連】** ・ウィルス/スパイウェアのダウンロードを検知したが、ウィルス対策ソフトなどによって、端末に影響がないと判断した場合 **【内部不正】** ・ポリシー違反によって、クラウド利用を検知した場合
Level 0	日次メール (簡易報告) 及び 月次レポート	**【通常通信】** 通常通信を過検知している 可能性が高い	**【攻撃関連 / 内部不正】** ・マルウェアの影響や攻撃通信、ポリシー違反に該当する通信でない場合 ・業務利用や軽微な私的利用

運用監視（アドバンスド）におけるカスタマイズ例：LANSCOPE / Cylance/ Deep Instinct ログの活用

Darktraceで取得可能な情報に加えMOTEXのセキュリティ製品のログ情報も踏まえた深堀調査を提供

検知

詳細調査・影響確認

追加調査 エンドポイント

<検知フェーズ>

・外部への不審なデータ送信を検知
↓
・検知情報から普段アクセスのない宛先であることを確認

<絞り込みフェーズ>

・アラート検知前に外部へ送信したデータとほぼ同量のデータを内部ファイルサーバーからダウンロードしていることを確認
↓
・不審なEXEをダウンロードしており、ファイル名からデータ転送ツールであることを確認

<詳細調査フェーズ>

・操作ログから以下を確認。
-ファイルサーバーからデータをダウンロードしリネーム
-データ転送ツールをインターネットからダウンロードし実行

・検知/隔離情報から脅威を確認
- 不審ファイルの詳細/脅威度 など

DARKTRACE

<検知フェーズ>

・アラート検知

・検知内容確認（通信先、データ量、時間、ユーザー等）

<絞り込みフェーズ>

・影響範囲絞り込み（アラート前後の通信内容、関連する端末、ユーザー）

LANSCOPE Endpoint Manager

<詳細調査フェーズ>

・該当時間の操作内容確認
（操作ログ）

CylancePROTECT　deep instinct

<詳細調査フェーズ>

・導入端末の情報確認※
（カテゴリ、検知状況、脅威スコア）

※マルウェア感染が疑われる挙動が確認された場合や、その他インシデントの可能性がある場合、アナリストにて Cylance/Deep Instinct上での検知状況を確認

５．　サービス提供について

Darktrace ライセンス形態

標準ライセンス	オプション
筐体課金：モデル　S、M、X2	**追加モジュール課金** ・テレワーク（エンドポイント対策） ・クラウド（各種SaaS） ・メール環境　他
＋	
デバイス課金：デバイス数	

※標準ライセンスのモデルのスペックの詳細は「Darktrace スペック表 」をご確認ください

※標準ライセンスのデバイス課金のデバイス数は、Darktrace機器で観測、計測したデバイス数を指します

サービス導入までの流れ

	導入フェーズ			設計・構築フェーズ			運用フェーズ
イベント				★Darktrace 機器発注及び導入作業ご発注		★Darktrace サービス契約開始	★運用監視サービス 開始
期間		4週間		12週間			
内容	**Step1** **PoV** Darktraceの評価を行います	**Step2** **監視対象検討** PoVの結果を踏まえて監視対象とするネットワークセグメントを検討します	**Step3** **設置場所検討** 監視対象のトラフィックを収集できる設置場所を検討します	**Step4** **運用設計** 運用に関する取り決め(アラート報告件数やタイミング等)を検討します	**Step5** **設定・構築** 機器の設定と設置作業を行いトラフィックの収集を開始します	**Step6** **チューニング** トラフィックの学習が進行しますアラートの検知状況を確認してチューニングを行います	**Step7** **運用開始** 正式に運用を開始します
ライセンスのみ	○	○	○		○	○	○
ライセンス Darktrace監視	○	○	○		○	○	○
ライセンス MOTEX監視	○	○	○	○	○	○	○

Darktrace スペック表

機種	DCIP-S	DCIP-M	DCIP-X2
寸法(縦幅)	1ユニット	1ユニット	2ユニット
容積（cm）	W44×D37×H4.4	W44×D74.5×H4.4	W44×D74.5×H8.8
重量	6kg	15kg	23kg
搭載可能ラック	19インチ	19インチ	19インチ
インターフェイス※①	10/100/1000　BASE-T　1つ	10/100/1000　BASE-T　1つ	10/100/1000　BASE-T　1つ
収集用ポート	10/100/1000　BASE-T　3つ	10/100/1000　BASE-T　3つ	10/100/1000　BASE-T　1つ 10　GBASE-T　2つ
SFP ＋ポート	該当なし	10Gbe/1Gbe SFP+2つ	10Gbe/1Gbe SFP+2つ
ピーク時のスループット	300Mbps	2Gbps	5Gbps
最大監視デバイス数	1.000	8.000	36.000
最大コネクション数	2.000	50.000	100.000
電源	260W IEC 13C 120/240V(1本)	750W IEC 13C 120/240V(2本)	1110W IEC 13C 120/240V(2本)
電力消費量 （1時間あたり）	Idle時:26W 稼働率85%時:89W 最大：105W	Idle時:120W 稼働率85%時:359W 最大：418W	Idle時:128W 稼働率85%時:365W 最大：426W
拡張可能モジュール※②	以下のうち、最大1つ利用可能 ・2-port 1G/10G SFP＋ ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T	以下のうち、最大1つ利用可能 ・2-port 1G/10G SFP＋ ・2-port 10G RJ45 10000 BASE-T ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T	以下のうち、最大3つ利用可能 ・2-port 1G/10G SFP＋ ・2-port 10G RJ45 10000 BASE-T ・2-port 1G RJ45 1000 BASE-T ・4-port 1G RJ45 1000 BASE-T

※①インターフェイスは「admin port」「Remote management port」の2種となります。
※②拡張可能モジュールは別売りとなります。

導入事例：　フリュー株式会社 様

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インフラの整備を実現

業種	サービス業	従業員数	495名（2023年3月時点）

導入経緯・課題

安全と生産性を両立したセキュリティ対策

ユーザーから預かった**会員情報や画像情報などの個人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。データ保護の観点から、外部への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多層的に行っていた。また、業務プロセスにおいても、**外部へのアクセスが必要になるクラウドサービスなどは、基本的に使用禁止**としていたため、「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いた」という。

2015年の上場を機に、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目指して整備。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・可視化するツールを検討、NDRであるDarktraceを導入した。

導入効果

工数を掛けずに早期発見・早期対応

Darktrace導入の魅力は**「経路と原因が追跡できる」「カバー範囲が広いネットワーク型」「運用負荷の軽減」**の3点。

「経路と原因が追跡できる」点として、内部ネットワークへの侵入を前提とした対策として早期発見・早期対応できる仕組みがあり、従業員が加害者になることを避けることに貢献できている。

「カバー範囲が広いネットワーク型」として、エージェントインストールなどの従業員の利用端末への負荷をかけずPC以外にもネットワークに繋がっている複合機なども網羅的に監視できている。**「運用負荷の軽減」**としては、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するため、管理者が細かい設定をする必要がなく、運用の負担が軽減した。

導入効果

社内ネットワークのリスクを網羅的に対策

4人体制で管理者権限を細かく設定して運用しているものの、Darktraceをほぼ標準設定からの微調整レベルで運用できている。

さらにIT資産管理・ログ管理のLANSCOPEエンドポイントマネジャーと併用することで、ネットワークで察知した異常をリスクの起点として、エンドポイントのプロセスを組み合わることでスピーディーに追跡・解析ができている。結果、全ての通信を把握できており、**何かあったときには早期検知・対応できる体制を構築できていることでセキュリティ監査等にも役立っている**。

これまでのファイアウォールやプロキシによる境界防御から、Darktraceによる内部ネットワーク監視へシフトしたことで、**ネットワーク利用の体感値が上がったという副次的効果も得られている。**