# AI機械学習による新たなサイバー防御ソリューション

Enterprise Immune Systemは、導入されている既存のセキュリティ・システムとは競合するものではありません。新たなセキュリティ強化オプションです。

DARKTRACE

**謹告：**

**情報システム防衛は入口対策・出口対策・エンドポイント対策では不十分であることが世界3,000以上のDarktraceユーザと48, 000を超える新たな脅威をDarktraceが検出したことで証明されています。**

# Enterprise Immune System

## 世界をリードするDarktraceのAI機械学習がサイバー防衛の流れを変えます。

**主な機能**

- 洗練された機械学習と数学に基づく新しい高度な脅威検知
- シグネチャを必要としないアプローチにより、これまでに出現したことのない新たな攻撃や標的型攻撃の検知が可能
- リアルタイムに機能し脅威の出現と同時に警告を出力
- あらゆるネットワーク機器を対象として可視化
  (PC, UTM, ルータ, 複合機, 仮想, クラウド, IoT等IP所有機器)
- 3D可視化画面で脅威を直感的に分析と調査が可能
- アプライアンスでの機能提供
- オプション機能Antigenaで脅威の検知だけでなく防御が可能


Darktrace アプライアンス

**DarktraceのAI機械学習は、「既に侵入してしまった悪意のプログラムの動態」をはじめ「内部不正利用・操作ミス等および全ての周辺機器の動態」も可視化し変化を検知・アラート通知**

ネットワーク境界およびエンドポイント防御をすり抜けて侵入する新しい種類のサイバー攻撃を検出し調査するためのネットワークソリューションです。高度な数学とAI機械学習を適用してエンタープライズ内の動作をモデル化することにより、社内のコンピュータ等の装置およびユーザの活動を監視して異常を検知します。数学的アプローチは、シグネチャやルールを必要としないため、これまでに知られていない新たな攻撃を検知することが可能です。　Darktraceは、内部ネットワーク から生のネットワークトラフィックを受け取るアプライアンスとして提供されます。アプライアンスを接続すると、様々な数学的アプローチを用いてネットワーク内部の各個別ユーザおよび機器の動作モデルの作成と機械学習を即座に開始し、導入初日からネットワーク上の異常動作を検知し始めます。機械学習は継続的に行い組織の変化に応じて常に更新されます。

ネットワーク上のあらゆる個人およびデバイスの「生活パターン」モデルを作成することにより、Darktraceは動作のほんのわずかな変化、たとえばユーザによる使い方、マシンのデータ アクセス パターン、または通信の傾向の変化などを検知することができます。これにより、ユーザの認証情報不正取得、デバイスの感染、あるいは不満を抱いた、または不注意な従業員の行為など、脅威となる可能性のあるイベントが多数見つかるかもしれません。 ネットワーク偵察やスキャン、 見慣れないインターネット・ドメインからの予期せぬダウンロード、イントラネットやファイルシステムのクローン化、新しいデバイスや場所、通常と違うアプリケーションやプロトコルからの機密性データへのログイン、または情報のアップロードのパターンの変化などは、すべて数学的モデリングを通じて検出可能です。これらの活動が通常の動作から著しく逸脱している場合には、調査が必要になります。

### Antigena

**Antigena**は、Enterprise Immune Systemのオプション機能です。検知した脅威通信を自動遮断します。例えば、ランサムウェアを検知するとDarktraceは社内ネットワーク内の疑わしい接続をリアルタイムで一時的に強制停止し、拡散を防止します。Antigenaが自動で行うことにより、データの損失や暗号化がされてしまう前にセキュリティチームが対策するための貴重な時間が得られます。Darktraceはデバイスがファイルへのアクセス、暗号化の試み、水平方向への他の接続可能なデバイスがないかスキャンしている異常性の高い挙動を検知して、WannaCry マルウェアの活動を特定することに成功しています。Antigenaは445 番ポートへの接続をブロックするTCP kill コマンドを送信することで即座に対応し、マルウェアがネットワーク内で水平に拡散して他のデバイスの暗号化を阻止します。

### Threat Visualizer

Threat Visualizerは、視覚的な対話型3Dインターフェイスで、プラットフォームの基盤である高度な数学を理解する必要なく、分析担当者が直感的にネットワークの動作を可視化し異常を調査することができます。ネットワーク全体にわたるデータフローや関係性をリアルタイムまたは履歴の任意の時点でのインテリジェンスに基づいた考察をユーザに提供します。異常が発生すると、異常発生までおよび発生中のイベントを表示し、疑わしい一連のイベント発生の様子を再生することができます。

**Threat Visualizer画面例**
(ブラウザでログイン)

## 共存して補完

Enterpise Immune System は、既存のセキュリティ インフラおよびアプローチを補完するよう設計されています。適切に設定されたネットワーク境界防御およびホスト防御は非常に重要ですが、外部、内部を問わず意思を持った攻撃者に対しては限定的な効果しかありません。シグネチャを必要としない監視および検知機能を追加することにより、新しい攻撃や組織を狙った標的型の攻撃に対して、対応することが可能になります。

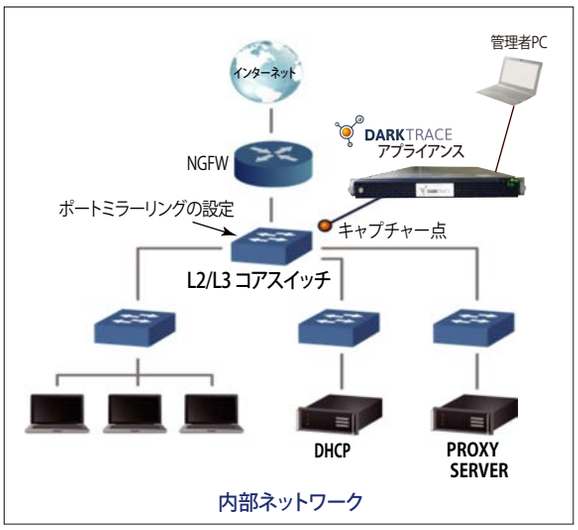
既にSIEMを導入している環境では、Darktrace は、Splunk, QRadar, ArcSightを含む、業界標準のCEF(Common Event Format)およびLEEF(Log EventExtended Format)をサポートするすべての主要なSIEMと共存することができます。Darktraceがリアルタイムに検知した脅威情報をSIEMに与えることで、SIEMの膨大なログ解析が短時間に容易に行えるので、SIEMの価値を高めることになります。SIEMに未だ投資をしておらず、データベースに大量の履歴ログを集積する必要のない組織においては、Darktraceがリスク軽減およびリアルタイムに脅威を検知にすることで、多くのリソースと長い期間が必要なSIEMプロジェクトに着手する必要性を解消することができます。

## データの秘匿性

Enterprise Immune System は、すべての処理をアプライアンス内で行います。収集するパケットはヘッダーのみでペイロード(データ本体)は収集されません。分析のために使用する Threat Visualizer 画面のパケット情報もペイロードを含まないためセキュリティは確保されています。

## 設置イメージ

組織内のコアスイッチにミラーポートを設定してアプライアンスを接続することで、トラフィックの収集と機械学習を継続的に実行し脅威や異常をリアルタイムに検知して警告を出力します。




## Darktraceアプライアンスの仕様

| モデル名 | キャプチャースループット | 最大監視デバイス数 |
|---|---|---|
| DCIP-S | 300Mbps | 1000台 |
| DCIP-M | 2Gbps | 8000台 |
| DCIP-X2 | 5Gpbps | 36000台 |

## 数学的基盤

この新しい数学的手法のポイントは、データ内の意味ある関係性を特定することのみならず、そのような推論にかかわる不確実性を定量化することにあります。不確実性を理解することにより、多数の結果をベイズ確率解析という一貫したフレームワークに基づいてまとめることが可能となります。Darktrace 製品の中心となるのは、革新的な再帰的ベイズ推定（Recursive Bayesian Estimation）を含む様々な数学的アプローチを駆使した4 つの数学エンジンです。最初の3 つのエンジンは、各個人と彼らの使用するデバイスおよび彼らが属するエンタープライズ全体の動作モデルを生成します。これら3 つのエンジンの1 つまたはそれ以上で通常と異なる動作が検出されると、警告の候補が「包括的」エンジンである Threat Classifier(脅威分類) に送信されます。Threat Classifier は、全時間にわたる全モデルからの出力を見渡し、誤検出をフィルタにより排除し、かすかな兆候であっても調査に値する純粋な異常を報告します。 Threat Classifier が行う複数のベイズ理論アプローチを独自の組み合わせで関連付けと調整により、Darktrace はエンタープライズ規模での異常検出を非常に高精度に行うことができます。



株式会社ピーエスアイ
〒160-0022 東京都新宿区新宿5-5-3　建成新宿ビル4F
TEL: 03-3357-9980 FAX: 03-5360-4488
大阪営業所
〒532-0011 大阪府大阪市淀川区西中島3-21-13 新大阪日新ビル4F
TEL: 06-4805-9601 FAX: 06-4805-9610


問い合わせ先:



2017/08