
DARKTRACE

ケース スタディ

# キッセイ薬品工業株式会社 様

明日の健康を見つめる キッセイ薬品

## 概要

### 業界

- 医薬品

### 課題

- 研究開発における機密データ、顧客に関わる情報を絶対的に保護する必要性
- 内部の通信を客観的、一元的に漏れなく把握したい

### 結果

- 端末間の関係性や異常発生の原因を客観的かつリアルタイムに把握・可視化
- セキュリティレベルの質向上、勤怠管理への応用

## ビジネスの背景

キッセイ薬品工業株式会社(以下、キッセイ薬品)は1946年8月に長野県松本市に「橘生化学研究所」として創業以来、「患者さんのために」を第一義に新薬開発に注力してきました。「研究開発なくして製薬企業にあらず」という信念のもと研究開発に注力し、独自の新薬の提供を目指して挑戦し続けています。

> Enterprise Immune System がもたらす100%の可視性によって、淀んで見えなかった内部ネットワークが透明度を増して、途端に目が行き届くようになったことで、一時的に仕事量が増えたものの自社のセキュリティレベルの質は間違いなく向上しました。これまでは思い込みでしかなかった安心感が、現実のものになりました。
>
> **キッセイ薬品工業株式会社 システム企画部 参与 小澤賢一様**

## 課題

知識集約型産業と言われている医薬品業界では、研究開発の過程で発生する様々な特許情報、安全性データ等を絶対的に管理・保護する必要があります。医食同源の考えのもとで、高齢者や腎疾患患者の方などに役立つ様々な食品の開発・自社通信販売も展開しているキッセイ薬品では、医薬品の機密データのみならず、顧客情報の保護も非常に重要です。従来のセキュリティ対策として、内部ネットワークに接続するデバイスやシステムにアクセスするために必要な ID とパスワードを設定・管理することはもちろん、次世代型のファイアウォール製品や URL フィルタリング製品を導入することで、外部の脅威対策に積極的な投資を続けてきました。一方で、内部対策としては、ネットワークトラフィックを日常的に監視していたものの、個々の通信の異常度や不正のレベルを客観的に理解できる環境ではなく、国内外で新たな脅威が次々と猛威を振るう中で、内部ネットワークを流れる通信を一元的に漏れなく把握できるツールの導入は急務でした。

## 解決策

大量のデータの転送などは、万一の情報漏えいリスクに備えて、業務上必要な範疇のものかどうかを即座に客観的に把握できる体制を整えることが理想です。システム毎に個別にログを確認するのではなく、内部ネットワーク全体を俯瞰することで通信元と通信先の挙動、それらの関係性をもリアルタイムに監視したいというニーズもあり、ポートミラーリングによって通信パケットを漏れなく収集することで、ネットワーク固有の通信パターンを AI が自動的に機械学習・可視化し続ける Darktrace の Enterprise Immune System をトライアル導入しました。

アプライアンス製品として提供される Enterprise Immune System は、L3 スイッチにミラーポートを設定してインストールすることで、パケットキャプチャによりそのネットワークに関わる個々のユーザー、デバイスの挙動やそれらの関係性を常時学習し、ネットワークの定常状態とは異なる通信を即座に検知するという、ルールやシグネチャに依存しない全く新しい脅威検知のアプローチであり、いかなる未知の脅威や内部不正も理論上、検知・可視化することができます。

VDI（仮想デスクトップ）環境を導入しているキッセイ薬品では、POV（※ 1）を開始した直後から1 台のサーバーに複数のユーザーが同時にアクセスしているトラフィックから個々のユーザーがどのサーバーのどのファイル、どのフォルダにアクセスしているかを漏れなくリアルタイムに可視化できる Threat Visualizer（Darktrace 独自の 3D インターフェース）が同社のネットワーク環境に最適なツールであるとすぐに実感しました。IP アドレス単位のみならず、ユーザー単位でログを深掘りできる点や、検知された異常や脅威を解析・評価し、対策を定期的にレポートする TIR（※ 2）によって、稀な通信が発生した際の因果関係をセキュリティ担当者でなくても分かりやすく一元的に理解できる点は、大きな安心感につながっています。

## 利点

キッセイ薬品では、現在 1,500 名を超える全従業員が業務で使用する端末およびサーバー類を含めた 6,700 近くのデバイスを Enterprise Immune System の監視対象にしています。情報漏えいにつながりかねない深刻な脅威はこれまでに検知されていませんが、万が一マルウェアやウイルスに感染しそうな事象が発生した際、異常度に応じて段階的にアラートを受け取ることで、これらを予兆レベルで把握できる体制を整えられたことは費用対効果に見合っていると感じています。また、定常状態を機械学習するにあたり、通信が行われる時間帯も異常度を判断する重要な要素であり、ポリシー違反ではなくても休日や業務時間外におけるデータのコピーや転送なども自動的に把握できるため、勤怠管理や働き方改革にも応用できます。また、POV 開始から実導入開始まで 3 か月程度で完結できたことは、社内ネットワークのコアスイッチに接続し、簡単な設定を行うだけで最短 1 時間程度で容易にインストールが完結する Enterprise Immune System の製品特性のおかげだと感じています。

（※ 1）Proof of Value: 4 週間の導入前検証。
（※ 2）Threat Intelligence Report: Enterprise Immune System が検知した異常や脅威を解析・評価し、対策をレポートするサービス。

**お問い合わせ**
東京: +81 (03) 5456 5537
大阪: +81 (06) 6133 4570
シンガポール: +65 6804 5010
米国: +1 (415) 229 9100
**japan@darktrace.com | darktrace.jp**
**@darktraceJP**