Darktrace「Enterprise Immune System」+監視運用サービス 導入事例

THE NEW VALUE FRONTIER

KYOCERA

ソニーライフ・エイゴン生命保険株式会社　様

ソニーライフ・エイゴン生命

創業：2007年8月
住所：東京都渋谷区神宮前5-52-2
事業概要：生命保険会社

生年金

AIを活用したツールで情報漏えい対策を強化
内部不正も検知できる堅牢な環境を構築

ソニー生命保険株式会社と年金保険のリーディングカンパニーである蘭エイゴン・インターナショナルB.V.との合弁によって設立されたソニーライフ・エイゴン生命保険株式会社（以下ソニーライフ・エイゴン生命）。「個人年金を人生年金へ」というスローガンを掲げて年金保険を中心としたビジネスを展開している同社は、最新のデジタルテクノロジーを活用してビジネスを変革する「デジタル戦略」を推進中だ。その一環として、AI（人工知能）を活用した英ダークトレース社のセキュリティ免疫システム Darktrace「Enterprise Immune System（以下Darktrace）」を導入。京セラコミュニケーションシステム（以下KCCS）が、この導入と運用支援を担っている。

（左から）
ソニーライフ・エイゴン生命　情報システム部 ITセキュリティマネージャ　磯貝 徹 氏
同　情報システム部 システム業務課 統括課長　馬場 正晴 氏
KCCS　ソリューション営業統括部 東日本セキュリティ営業課　大関 慶
同　セキュリティ事業部 東日本インテグレーション課責任者　早坂 寿晃
同　セキュリティ事業部 セキュリティサービス課　西山 健太

【Darktraceの概要および特長】

- Darktrace は、**業務上の正常通信をAIと高等数学ベイズ推論を用いて自己学習**することで、**内部ネットワーク上の“異常”を検知**する製品です。
- スイッチのミラーポートに接続することで、流れる通信をキャプチャし、自動的に正常通信を学習するため、**細かな防御ルールの設定が不要**です。
- サイバー攻撃に加え、**正社員による不正行為やオペレーションミスなども検知**することが可能。**アラート発生の経緯、問題があった時間帯の通信内容を再現、分析が可能**です。

【画面イメージ】

Darktraceが提供するコンセプト（活用ステップ）

①正常業務上の通信を自己学習	接続元IP、接続先IP、データ送受信量、操作する時間帯などを自己学習し、正常な通信を学習します。
②異常通信を検知	Darktraceが正常な通信から外れるとみなした通信に関しては、異常としてアラートを上げます。
③通信内容を詳細に分析	検出されたアラートを確認し、対応が必要であれば関係各所へ連絡します。またセキュリティ対策製品へ設定を追加します。

背景・課題

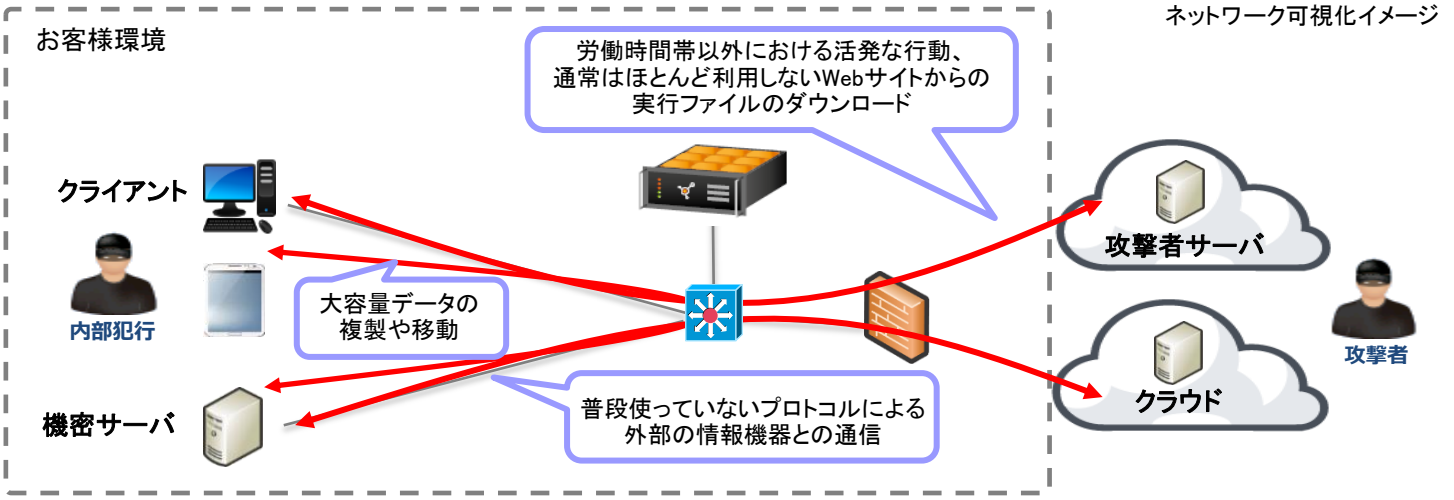
- 保険業として顧客情報の保護は最重要課題
- 企業の相次ぐ情報漏えい事故を背景に、サイバー攻撃や内部不正などの脅威を軽減するための対策が急務
- 限られた社内リソースでのセキュリティ運用

選定のポイント・導入効果（お客様の声）

ネットワーク全体の可視化

ログを見ても把握できなかった社員の行動が可視化でき、リアルタイムに異常を検知できるようになりました。
万が一、情報が流出するようなインシデントが発生した場合でも、その後の対処を迅速に進められます。
（ソニーライフ・エイゴン生命　馬場氏）

ネットワーク可視化イメージ



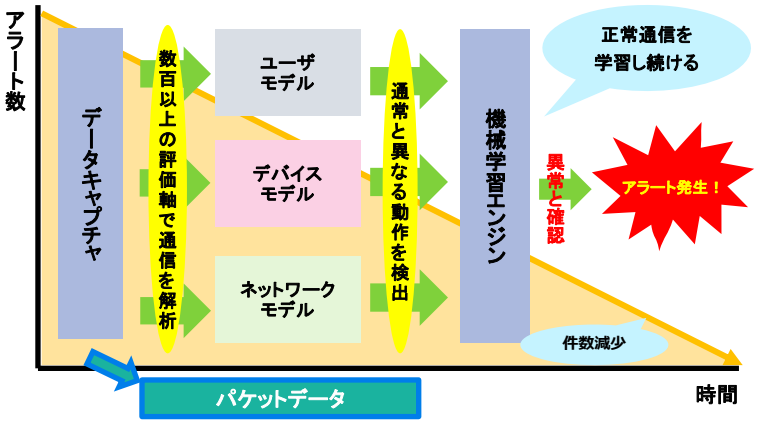
AIによる機械学習で異常通信を検知、運用省力化

機械学習によって正常な状態を学習し、そうでない場合は危険度によってアラートを上げてくれます。不正を判断するルールを人間が設定・変更する必要はありませんので、運用の省力化という要件にマッチしました。また、異常を検知した後の分析・調査には大きな手間が掛かりますが、アナリストレポートを含め、24時間365日の監視運用をKCCSに任せたことで生産性が大きく向上していると感じます。（ソニーライフ・エイゴン生命　磯貝氏）

導入が容易

SIEM製品では“不正の可能性がある”と判定するルールは人間が決めなければいけません。厳しいルールにすればアラートの数が膨大になり、緩やかなルールでは不正を見逃す恐れがあります。さらに、新たな手口のサイバー攻撃が登場した場合にはルールを変更する必要があり、運用が容易ではありません。その点、Darktraceは導入も運用管理も容易でした。
（ソニーライフ・エイゴン生命　馬場氏・磯貝氏）

アラートが減少するイメージ



Darktraceと他社SIEM製品比較表

カテゴリ	Darktrace	ログ分析製品（SIEM）
検知対象	通信	ログ
検知手法	顧客固有の正常動作を自己学習し、正常動作と異なる挙動を検知	各種ログの出力内容を定義されたルールと比較し検知
標的型攻撃（マルウェア）	○ 正常動作と異なる挙動を検知	△ 既知は可能 未知（新種）は困難
内部不正（情報の不正利用）	○ 正常動作と異なる挙動のため、内部の不正な通信を検知	△ 細かなルール定義が必要
構成変更	不要（ミラーポートに接続）	必要
ルールの定義	不要	必要

本事例の詳細は　⇒　https://www.kccs.co.jp/secureowl/case/case10008.html

京セラ コミュニケーションシステム株式会社

随時セミナー開催！
詳しくは　https://www.kccs.co.jp/secureowl/events/

KCCSカスタマーサポートセンター
フリーコール 0120-911-901
携帯電話・PHS・IP電話など 050-2018-1827
受付時間 平日9:00～17:00
（17:00以降のお問い合わせは自動応答になります。）
KCCSホームページ http://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

2017-05