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

THE NEW VALUE FRONTIER

KYOCERA

国立研究開発法人理化学研究所 計算科学研究センター 様

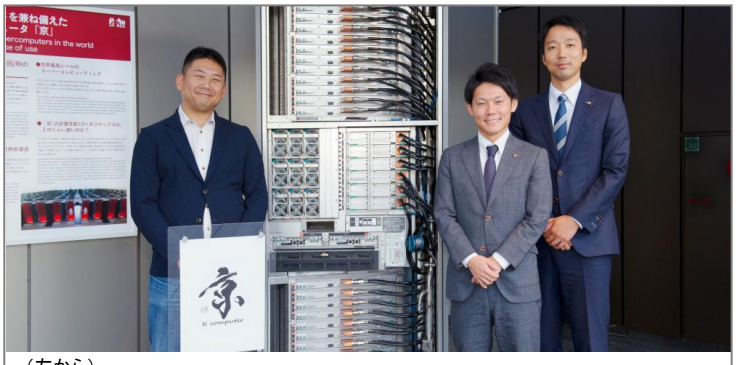
RIKEN R-CCS

設立：2010年7月
住所：兵庫県神戸市中央区港島南町7-1-26
研究所概要：計算科学および計算機科学の研究開発機関

提供：　理化学研究所

AIを活用したツールによる内部ネットワークの見える化と、タイムリーな分析結果を報告する監視運用サービスでセキュリティ対策を強化

日本で唯一の自然科学の総合研究所として、幅広い分野で研究を進めている国立研究開発法人理化学研究所（理化学研究所）。同研究所の中で、スーパーコンピュータ「京」を運用している計算科学研究センターが、セキュリティ対策強化のためにDarktrace「Enterprise Immune System」（以下Darktrace）と監視運用サービスを導入。APT（持続的標的型攻撃）にも対応できる体制を築いた。
京セラコミュニケーションシステム（KCCS）が、このシステムの導入と運用支援を担っている。



（左から）
理化学研究所 計算科学研究センター 運用技術部門 システム運転技術ユニット
岩本 光夫 氏
KCCS ソリューション営業統括部 セキュリティ営業部 西日本セキュリティ営業課責任者
原田 洋司
同 セキュリティ事業部 SecureOWL Center 西日本セキュリティサービス課 係責任者
東 伸二

背景・課題

- どんなに予防対策をしていてもAPTを防ぐことは困難
- 外部の人のネットワーク利用が多いため、事前予防として、ポリシー違反となる行動を検知したい

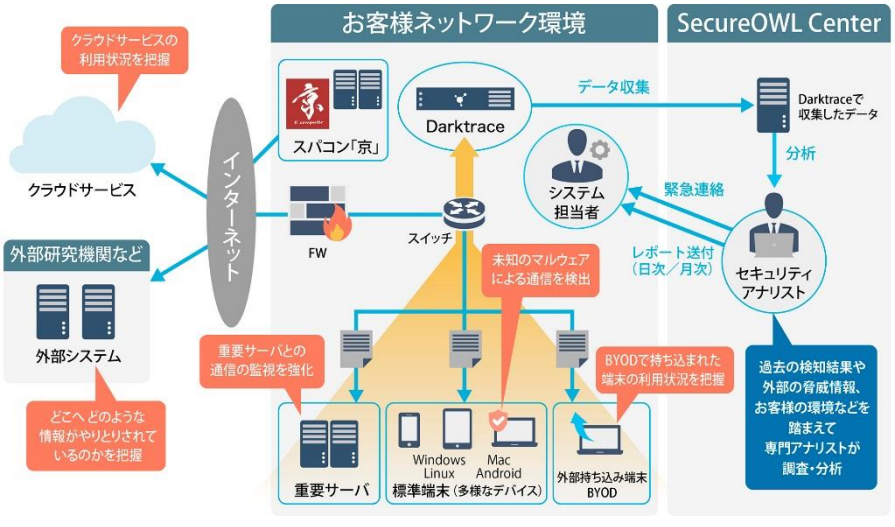
選定のポイント

- AI技術を利用し、イレギュラーな通信状況を検知することで、APTやポリシー違反をリアルタイムに検知
- 専門アナリストが、検知したアラートを調査・分析し、タイムリーに報告してくれる監視運用サービス

導入効果

- ポリシー違反となる行動やツールの稼動など、導入前は検知できなかった脅威を検知
- リアルタイムな調査・分析、原因・対処法のレポートにより、迅速な脅威の対処を実現

内部ネットワーク上で何が起きているか『見える化』の実現



理化学研究所　計算科学研究センターのネットワーク監視・運用イメージ

背景・課題　ネットワークの実態を把握する仕組みが必要に

全国に拠点を擁する理化学研究所では、組織全体のセキュリティ対策を本部（埼玉県和光市）が統括している。各拠点にはセキュリティ担当部署が配置されており、計算科学研究センターでは、運用技術部門がこの役割を担っている。

計算科学研究センターには、スーパーコンピュータ「京」や「HPCI共用ストレージ」といった共用設備があり、理化学研究所の外部の人がネットワークを利用する機会も多い。これは、ほかの拠点に比べて、セキュリティ対策のガバナンスが効きにくいことを意味する。理化学研究所の岩本氏は「内部ネットワーク上で何が起きているのかを『見える化』し、あらゆる事態に対応できる柔軟かつ効率的なセキュリティ対策へと強化したいと考えていました」と語る。


理化学研究所　岩本氏

具体的には、重要サーバや特定デバイスの監視を強化するとともに、ネットワーク上で異常が発生した際に検知したいというものだ。利用を禁止しているツールやクラウドサービスの利用状況をチェックすることや、新しく導入された端末や外部から持ち込まれた端末の把握、マルウェア感染の疑いがある通信や不審なツールのダウンロードの検知といったことも課題に挙がっていた。ハードウェアおよびソフトウェアのアラート・ログを一元的に管理・分析するSIEM（Security Information and Event Management）は、ネットワークの調査分析には必要不可欠のツールである。しかし、岩本氏は、専門技術を要する人員が必要となることや検出ロジックの確立にも時間を要しリアルタイムな検出には限度があることから、同センターの課題改善の一つにネットワーク上をリアルタイムに監視する仕組みが必要だと考えていた。

選定のポイント　巧妙な標的型攻撃にも対応できるAI技術とサポート体制が決め手に

課題の解決に向けて、さまざまなソリューションを検討していた際に出会ったのが、英ダークトレース社が開発したDarktraceだった。このツールの大きな特長は、不正を検知する機能にAI技術の一種である機械学習を活用していることだ。ネットワーク内の全ての通信パケットを分析し、正常な状態（不正が発生していない状態）の通信パターンを自己学習する。学習後は流れるパケットをリアルタイムで監視し、正常な状態から外れた際に「異常が発生した」と判断し、アラートを発する仕組みだ。異常だと判断するしきい値を利用者が設定できるため、アラートをクリティカルな内容に絞ることも可能だ。

また、この仕組みの大きなメリットは、近年サイバー攻撃の大きな脅威として急浮上しているAPTの防御が期待できることだ。近年のAPTでは、初めにターゲットとなる組織の情報を収集する。攻撃対象が導入しているセキュリティツールの情報を取得し、そのツールでは検知されないマルウェアを作成するという。このため、マルウェアのパターンで検知するツールや振る舞い検知型のツールではすり抜けてしまう。これに対して、イレギュラーな通信状況を検知するDarktraceであれば、APTの検知が期待できる。

このような機能を評価して、岩本氏はDarktraceの採用を本格的に検討する。最終的に、このツールを選定する決め手となったのが、KCCSが提供する「Darktrace監視運用サービス」だったという。このサービスは、Darktraceが検知したアラートをKCCSのセキュリティ監視・運用センター「SecureOWL Center」で受け付け、専門のアナリストが調査し、利用者に通知するものだ。同センターでアラート内容を確認し、専門のアナリストが原因および影響を分析・調査して「アナリストレポート」を作成し、セキュリティ担当者に日次でメール報告する。緊急を要するものは、担当者に電話で連絡まで行う。また、その月のアラート状況や傾向、セキュリティに関するトピックをまとめた「月次運用報告書」も提供している。

監視運用サービスでは、顧客ごとにメインのアナリストが選定され、そのメインアナリストを中心に調査・分析を行っている。KCCSの東は、この体制の効果を次のように語る。「メインアナリストは、これまで培った知識や経験を基に、重要サーバをはじめお客様の環境を把握し、重点監視項目などを設定した上で調査・分析をしています。ですので、複数のお客様で同じようなアラートが発生しても、お客様ごとの状況を踏まえて原因や影響を分析し、報告します」。


KCCS　東

岩本氏は「Darktraceの検知アラートに迅速に対応するためには、専門アナリストが調査・分析を日次で行い報告してくれる、KCCSの監視運用サービスが必要不可欠です」と評する。

導入効果・展望　本格稼働後に脅威に結びつくような行動を検知

計算科学研究センターでは2018年3月にDarktraceを導入。1か月間の学習期間を経て、4月から本格稼働を開始した。稼働後も引き続き機械学習は継続するので、脅威に結びつくような行動を検知する精度は向上していく。

実際、同センターでは本格稼働後に、そのような行動をいくつか検知している。例えば、評判の良くないツールのダウンロードを検知したり、インストールを禁止しているツールが稼働していたのを発見したこともある。岩本氏は「ウィルス対策ソフトが検知できなかったウィルスに感染した端末を発見したこともありました。このようなケースは、Darktraceがなかったら気づくことは難しかったと思います」と語る。

さらに、監視運用サービスについても次のように高く評価する。

「アナリストの方が当センターの環境を熟知してくれており、重要サーバを重点的に監視するなど、こちらの環境を踏まえた上で調査・分析してくれるレポートがとても分かりやすく、期待以上でした。例えば、過去に発生したアラートが再発した場合に、どのような行動に起因しているかといった分析やその後の対処法についても掲載されています。セキュリティ対策の運用に本当に役立っています」。

KCCSの原田は「昨今、セキュリティ対策に取り組みたいが、自社内に運用できるノウハウやリソースがないことが企業の課題となっています。当社は自社内でもCSIRTを運用しており、そこでのノウハウをベースに、いかにお客様に安心して、負担を掛けずにセキュリティ対策に取り組んでもらうかということを第一に考えてサービスを企画・開発しています」と語る。KCCSでは、今後も計算科学研究センターのセキュリティ対策の支援をしていくとともに、セキュリティ対策に関する運用負荷を軽減するためのソリューションの幅を広げていく計画だ。


KCCS　原田

本事例の詳細は　⇒https://www.kccs.co.jp/secureowl/case/case10009.html

KYOCERA

京セラ コミュニケーションシステム株式会社

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 https://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

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

2018-12