AIを搭載した サイバー攻撃監視支援システム

中村　信之　　八百　健嗣

サイバー攻撃は高度化・巧妙化し続け、情報流出事件とその被害は増える一方である。日本でも国家としてサイバーセキュリティへの対策を強化する動きがあり、企業にも対策を整備する責任が求められている。OKIは長年サイバーセキュリティに対する対策、運用を実施してきた実績があり、そのノウハウを活かしたソリューションとしてセキュリティ運用監視サービスを提供中である。さらに、増え続ける攻撃と、攻撃に関連する膨大なログを対象としたサイバーセキュリティ監視のために、AI技術を用いた次世代のセキュリティ対策への取組みを進めている。

本稿では、OKIが進めているAIを搭載したサイバー攻撃監視支援システムを紹介する。

OKIのサイバー攻撃への取組み

現在OKIでは、長年のサイバーセキュリティ対策の知見を元にしたSOC（Security Operation Center）のアウトソーシングサービスを提供している[1)]。本サービスは、セキュリティ監視センターからのリモート監視により、異常トラフィックやログの分析業務を請け負うものである。このような分析業務には、サイバーセキュリティに関する高度な専門知識が必要となるため、人材の確保が難しい。サイバー攻撃の増加・高度化に対応できるスキルを持った人材を確保することは、サイバーセキュリティ対策の大きな課題となっている。

この課題に対して、サイバー攻撃の監視にAI技術を活用する動きがある[2)]。サイバー攻撃の分析業務の目的は、ネットワークや機器から取得したログを分析し、実際に攻撃されたか否か、被害が発生したか否かを判断することである。このような分析業務の一部をAIに肩代わりさせることで、人材が不足している監視員の分析工数を削減することが期待される。サイバー攻撃監視へのAI技術の活用はOKIでも既に開始し、SOCで蓄積された知見をシステム化することに成功している。次章ではまず世の中の動向と課題を概説し、それ以降の章でOKIのシステムの概要と詳細を説明する。

サイバー攻撃監視の課題

一般にSOCでのマルウェア対策や情報漏洩（ろうえい）対策には、ネットワークログを収集して統合管理するSIEM（Security Information and Event Management）が用いられることが多い。既存のSIEMの多くは、危険なイベントの見落としを減らすために大量のアラートを出す傾向がある。それらのアラートは人手で確認することになるため、オペレーターの工数が増大してしまうという問題がある。一方、検知エンジンを絞り込むなどアラートを抑制すればサイバー攻撃を見落とす可能性が増える。このため既存のSIEMでは、設置環境に応じた検知エンジンのチューニングが課題となる。

AI技術を活用したサイバー攻撃監視にも同様の課題がある。AI技術を活用する攻撃検知システムでは、従来のシグネチャマッチングのようにウイルス自体を検知するだけではなく、機械学習器を用いて不審な振る舞いや未知のウイルスを検知する。具体的には、マルウェアの挙動を学習することで類似する挙動を疑いのある挙動として検知したり、通常状態を学習しそこからの乖離を検知したりできる。前者は既知の脅威を検知し、後者は未知の脅威を検知する。このようにAI技術を監視業務に活用することで、人手による監視業務を補完できる可能性がある。しかし、AI技術の活用では、見落としを減らすために安全側に倒したチューニングをする場合も多く、誤検知が増えるという問題がある。また、AI技術によっては中身がブラックボックスとなっているため、異常判定時にその根拠を説明できないという問題がある。これらの問題を解決し、高精度にサイバー攻撃を検知することでSOCを支援できる、サイバー攻撃監視支援システムを次章より説明する。

サイバー攻撃監視支援システムの概要

図1にサイバー攻撃監視支援システム（以下、本システム）の全体図を示す。本システムは、サイバー攻撃検知にネットワーク機器ログを対象とした分析環境を利用する。ネットワーク機器にはファイアウォール、メールサーバー、プロキシサーバーなどさまざまな種類がありその量は膨

大である。本章では、これら膨大なネットワーク機器ログに対してリアルタイムに分析処理するための分析環境を、更に分析環境上で動作する機能として、さまざまな種別のログを取り込むログ収集機能、異常検知エンジン、GUI・フィードバック機能を以下に説明する。

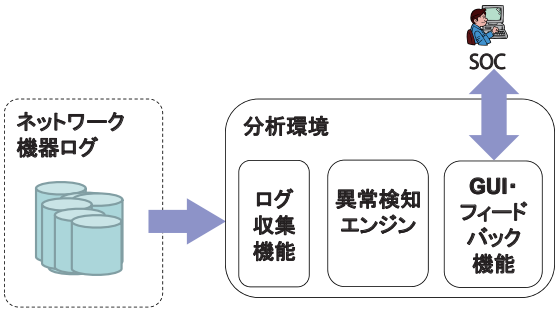

図１　システムの全体図

(1)分析環境

ネットワーク機器ログは、1イベントに対して1行生成されるものもあれば、1パケットに対して1行生成されるものもある。特にインターネット利用時に主に利用されるWebページへの接続を中継するプロキシサーバーでは、従業員数や利用方法にもよるが、1カ月のログの総数が数十億以上になることもある。

このような膨大なログを実時間で処理しようとすると、CPUやメモリを豊富に搭載したサーバーが必要となる。さらに、異常検知エンジンには、SOCの知見を元にした検知エンジン群（以下、個別AIと呼ぶ）が多数用意されているため、同ログを多数の個別AIで複数回処理する必要があり、単独のサーバーでは処理が間に合わない。

そのため、クラスター環境で並列処理することで実時間処理する構成とした。**図2**で示すように、複数のサーバーでHadoop/Spark*1) クラスターを構成し、処理すべきネットワーク機器ログはHDFS*1) 上に冗長性を持たせて配置し、個別AIは分散して動作させている。

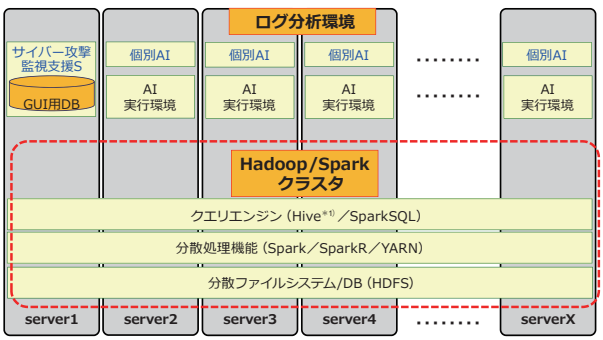

図２　分析環境構成図

この構成により、対象とするログの量が増えた場合や対象とするネットワーク機器が増えた場合、あるいは個別AIの数が増えた場合に、柔軟にリソースを追加して実時間処理することを可能としている。

(2)ログ収集機能

ネットワーク機器は、装置の種別やベンダーによって複数種類があり、更に分散配置されている場合には、多数のログを一様に扱えない状況が発生する。

図3はそのような二つのパターンを示し、ファイル転送後に処理するバッチ処理と、syslogで転送して処理するリアルタイム処理に分類している。

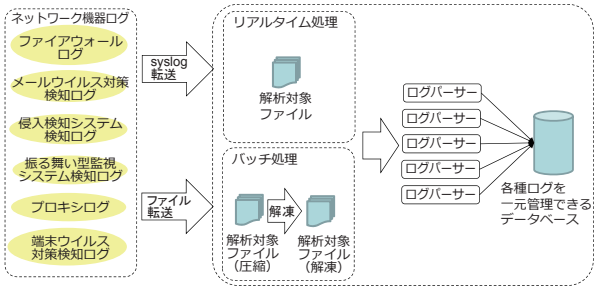

図３　ログ収集の概要

バッチ処理では、イベント発生からログがファイルとして書き込まれて転送されるまでにランダムな時間遅延が発生する。さらに、複数個所に分散配置されているネットワーク機器などの場合、それらのログの転送時間も含めると、ログがそろう時間を確定することが難しい。そのため、普段のログ転送時間を計測し、それから決めた一定時間経過後に処理する。

一方、リアルタイム処理では、データ転送量が膨大でない場合やネットワーク機器側にログを保存できない場合に有効であり、syslogでログを転送してログ収集サーバーで受信する仕組みを用いている。ネットワーク機器でイベントが発生してからログ収集サーバーで受信するまでのネットワーク遅延だけであるため、リアルタイム性が高い処理方法である。

これらの処理方法で収集されたログは、フォーマットも多種多様であるため、ログパーサーでログに含まれるパラメーターを切り出した後にフォーマットをそろえる必要がある。さらに、ネットワーク機器の種別によって保持するパラメーターが多様であるため、同種のネットワーク機器同士でパラメーターを統一して管理することが必要となる。これらの処理を経て、ネットワーク機器ログを一元管理できるデータベースを構築している。

(3)異常検知エンジン

異常検知エンジンは、**図4**のように個別AIと総合AIの二段で構成されている。個別AIではSOCの知見をAI化した検

*1)Hadoop、Hive、Spark、HDFSは、The Apache Software Foundationの米国及びその他の国における商標または登録商標です。

知エンジンを複数用意してさまざまな観点からの判定結果を出力する。一方、総合AIでは個別AIの出力を元に結果を集約して特徴量を作成し、サイバー攻撃の有無を判定する。

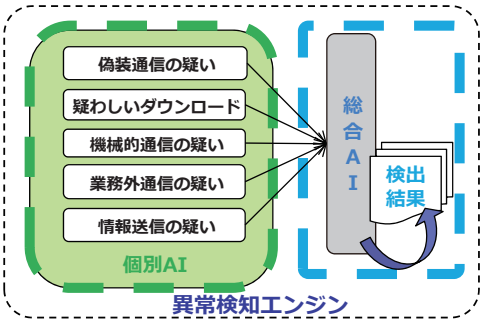

図 4　異常検知エンジンの構成

このニ段構成のシステムにより、総合AIで異常検出した結果に対して、どの個別AIが異常と判定したかを特定できるため、SOCで異常原因の分析をする際に、どこから分析に着手するかを情報として提供することができる。よって、AIで異常と判定された原因が分からないというブラックボックス問題を解決することができる構成である。

①個別 AIの動作

個別AIは、システムの一段目の機能であり、SOCの知見を元にした検知エンジン群である。図4のように、偽装通信の疑い、疑わしいダウンロードなどを検知する。個別AIは、ネットワーク機器の種別に応じて異常判定のパラメーターや知見が変わるため、ネットワーク機器に応じた検知エンジンをそれぞれ多数用意して動作させる。個別AIは上述のように分析環境上で分散して実行され、各個別AIの異常判定結果は総合AIへ出力される。

②総合 AIの動作

総合AIは、個別AIの異常判定結果を束ねて特徴量を生成する。さらに、**図5**のようにニつのAIを持ち、別々に動作する。一つはログ単位での異常判定であり、もう一つは要素単位（ユーザーIDやPCのIPアドレス）での異常判定である。

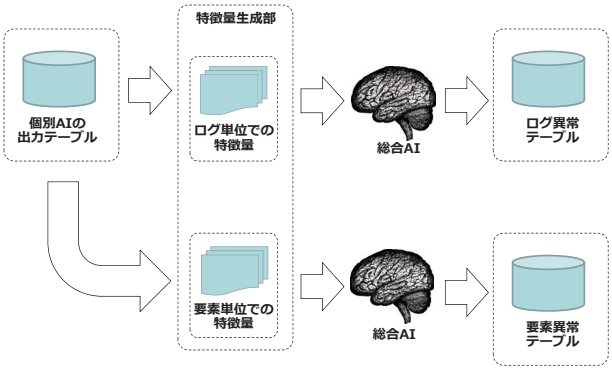

図 5　総合 AI の動作

ログ単位で異常判定する総合AIは、ログに対する個別AIの出力結果を特徴量として、正常ログと異常ログを学習する。判定時は、正解となる特徴量との近さを元に異常度を評価している。この総合AIは、ログ単位での異常が示せるという特徴を持つ。

一方、要素単位で異常判定する総合AIは、SOCの初動を重視して、SOCが分析する必要がある異常なユーザーIDやPCのIPアドレスを抽出して見せることを重視している。そのため、例えばユーザーIDごとに特定の時間の個別AIの出力を集計し、ユーザーの振舞いを特徴量として生成し、異常度を評価している。要素単位の総合AIとログ単位の総合AIとを相互に補完的に利用することで、SOCを支援するシステムとしている。

（4）GUI・フィードバック機能

前述した総合AIの出力を**図6**及び**図7**に示す。SOCでは、まず要素単位の総合AIにより**図6**のようにバブルチャートで表示される異常度の高い要素を確認し、分析すべきユーザーやIPアドレスに焦点を絞る。特定の要素を選択すると、個別AIの異常度の時系列変化を参照できるため、攻撃の状態を視覚的に把握し、緊急性や分析の優先度を決めることができる。

さらに、ログ単位の異常を確認する画面が**図7**である。この画面では全体を俯瞰（ふかん）しつつ、要素単位の総合AIで判定されたユーザーやIPアドレスを、ログ単位の総合AIの判定を用いて、マルウェアのダウンロードや情報漏洩の疑いがあるログを絞り込む。

絞り込みと調査が終わったログや要素は、これらのGUIの詳細画面から正常／異常のフィードバックをかける。二つの総合AIそれぞれに対して、正解データをフィードバックすることにより、総合AIが再学習される。このフィードバックの仕組みを運用し続けることにより誤検知と攻撃の見落としの少ないサイバー攻撃監視支援システムを実現する。

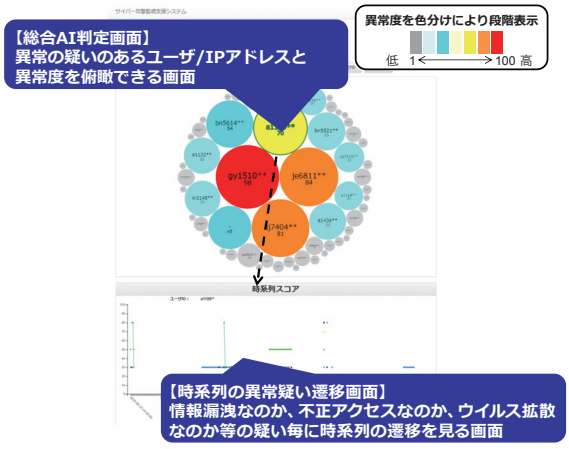

図 6　要素単位の GUI

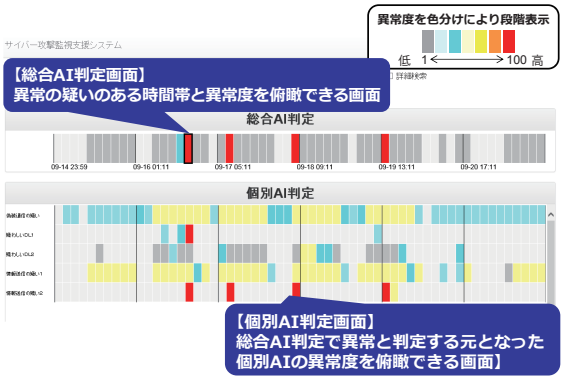

図 7　ログ単位の GUI

SOCでの活用と今後の方針

従来、SOCでのログ監視はネットワーク機器ログに対してオペレーターの知見でログを検索して、異常性の高いログを検知していた。本システムを運用することにより膨大なネットワーク機器ログに対してオペレーターの持つ知見が網羅的に適用されるため、攻撃の見逃しを低減できる。現在までに、個別AIでのサイバー攻撃の評価を実施し、スパイウェアによる情報漏洩の疑いのある通信を多数検出している。よって、従来検出しきれていない疑わしい通信を抽出できていることが確認できている。さらに、それぞれの個別AIの抽出結果には多数の誤検知とサイバー攻撃が含まれているが、それらを再学習してサイバー攻撃だけを検出することが期待できる。今後は、SOCでの運用を通じて学習データと知見を蓄積し、サイバー攻撃監視支援システムとして製品化を目指す。

まとめ

本稿では、OKIの次世代のサイバーセキュリティ対策への取組みとして、AIを用いたサイバー攻撃監視支援システムを紹介した。本システムは、SOCの運用の中で正解データをフィードバックすることにより、誤検知と攻撃の見落としが少ないサイバー攻撃監視を実現するものである。また、二段構成のAIを採用することにより、異常判定時の原因を特定できるという特徴を持つため、異常の原因説明やSOCでの対策立案に貢献できる。

今後は、SOCでの運用を通じて総合AIの検出精度を向上させると共に、個別AIのラインナップも拡充し、監視業務の高度化を目指す。◆◆

■参考文献

1) 松原大樹、森田達也：サイバー攻撃監視技術、OKIテクニカルレビュー第230号、Vol.84 No.2, pp.38-41, 2017年12月
2) 総務省サイバーセキュリティタスクフォース：IoTセキュリティ総合対策 別紙、p10、2017年10月

●筆者紹介

中村信之：Nobuyuki Nakamura. 経営基盤本部 研究開発センター スマートネットワーク技術研究開発部
八百健嗣：Taketsugu Yao. 経営基盤本部 研究開発センター スマートネットワーク技術研究開発部