2021 年 5 月 11 日

ジェノアテクノロジーズ株式会社
株式会社アドックインターナショナル
クレバースカイシステムズ株式会社

AI による画期的サイバー攻撃防御システムの実証実験
～サイバー攻撃検知トリガによりパケットキャプチャツールの膨大なデータ解析を容易に～

ジェノアテクノロジーズ株式会社（代表取締役：岡田　晃市郎、本社：東京都港区）と株式会社アドックインターナショナル（代表取締役社長：小林　常治、本社：東京都立川市）とクレバースカイシステムズ株式会社（代表取締役社長：手塚　啓一、本社：東京都杉並区）は、3社の強みと既存ソリューションを組み合わせ画期的な「サイバー攻撃防御システム」の構築を目指し実証実験を開始しその基本技術であるリアルタイム攻撃検知で成果があったことを以下に報告いたします。

1．実証実験の背景

近年「不正アクセス」、「DDoS 攻撃」等のサイバー攻撃による被害が急増しています。重要な官公自治体のホームページ・個人情報他の重要情報、企業のホームページ・個人情報他の重要情報等々、DDoS 攻撃によるサイバーテロの被害は急激に増加しています。IoT 時代の到来によりクローズであった生産ラインやシステム制御のネットワークもオープンなネットワークに接続されるようになりサイバー攻撃に脅かされてきています。サイバー攻撃はネットワークの NCP（Network Continuity Plan：ネットワーク運用継続性計画、クレバースカイシステムズが提唱）および健全な経済活動に深刻な影響を及ぼします。

2．実証実験の目標

公共機関・企業の BCP（Business Continuity Plan）実現のための一環である NCP を実現するために、AI による「サイバー攻撃防御システム」を実現することを目指します。

3．今回の実証実験（Step1）

・先ず実証実験の Step1 として、ジェノアテクノロジーズ、アドックインターナショナルのセキュリティ技術とクレバースカイシステムズのリアルタイムネットワーク診断技術を連携させ、リアルタイムサイバー攻撃検知のための実証実験を行いました。

・クレバースカイシステムズのネットワーク診断装置 TM2000 を利用して、実際にシステムへの「不正アクセス」、「DDoS 攻撃」等の模擬サイバー攻撃を行い、攻撃を受けている端末のリアルタイム検知ができるか検証しました。

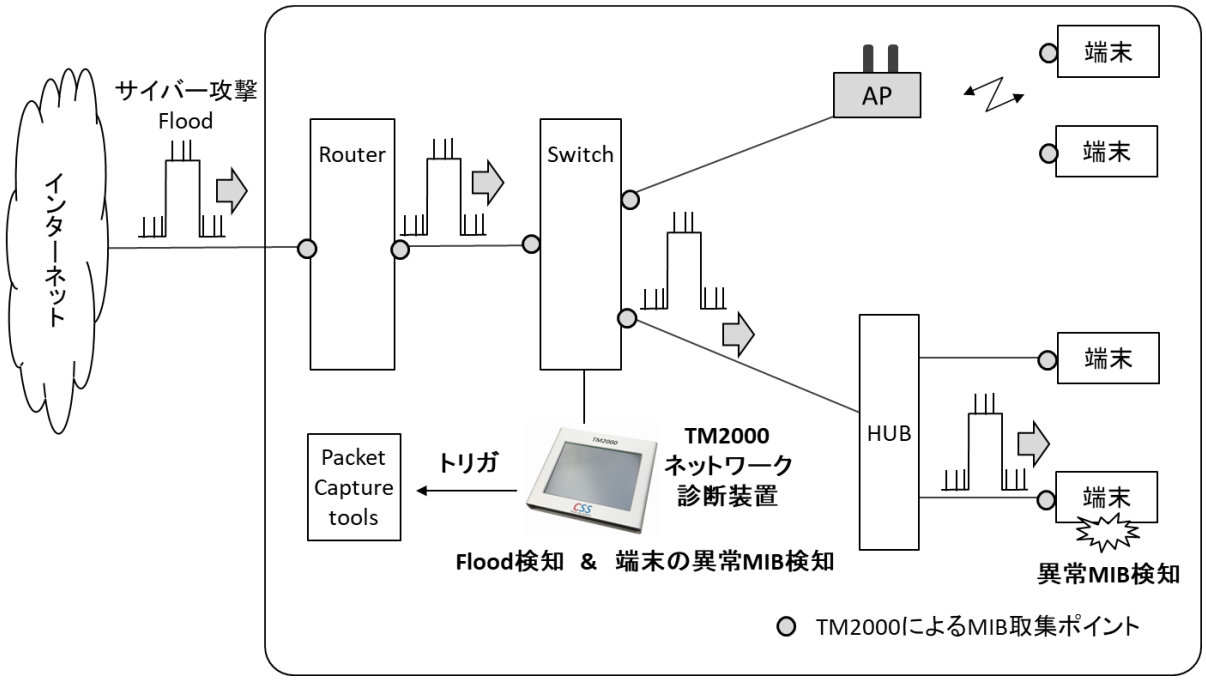

図1. サイバー攻撃のリアルタイム検知

4. 今回の実証実験による成果と意義

①サイバー攻撃を受けている端末をリアルタイム検知

ネットワーク診断装置 TM2000 により複数のネットワーク機器の MIB（Management Information Base）情報を SNMP(Simple Network Management Protocol)で同時収集し比較することでサイバー攻撃を受けている端末を容易にリアルタイム検知ができました。

②サイバー攻撃を行っている端末検知も可能

サイバー攻撃を受けている端末を容易に検知できるだけでなく、外部からのサイバー攻撃だけでなく内部のネットワークでサイバー攻撃を行っているアタッカー端末のリアルタイム検知も可能であることが分かりました。

③検知トリガーをパケットキャプチャツール等に送信

検知トリガーをパケットキャプチャツール等に送信することができますので、パケットキャプチャ装置はこのトリガーを受けることにより、膨大なデータ解析が容易になります。

従来は大掛かりなパケットキャプチャ装置で膨大なデータを分析することでサイバー攻撃を検知していましたが、今回の方法ではネットワーク診断装置 1 台と既存のネットワーク機器に一般的に搭載されている SNMP 機能を利用することで比較的安価にできることがわかりました。この方法により「ネットワーク診断レベルでの監視」と「サイバー攻撃検知」の両方を実現します。

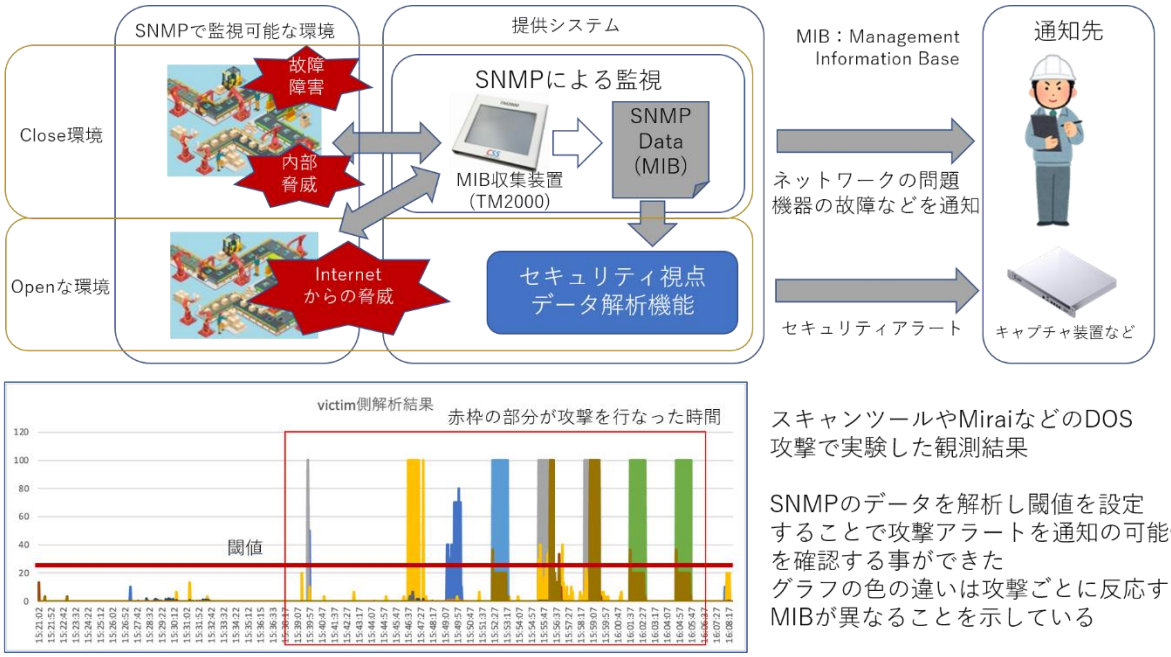

図2. SNMP による DDoS 攻撃など検知実証実験の結果

5. 今後の計画

5. 1. AI を使ったサイバー攻撃検知の実証実験（Step2）

AI を利用することによるサイバー攻撃検知率の向上、新たなサイバー攻撃への対応、アタッカーの分析等きめの細かい分析を可能にし、「サイバー攻撃防御システム」のための実証実験を予定しています。

5. 2. 商品化

・Step1商品化：「サイバー攻撃検知システム」の商品販売　　販売開始　2021 年 8 月予定

・Step2 商品化：「サイバー攻撃防御システム」の商品販売　　販売開始　2021 年末予定

【ネットワーク診断装置 TM2000】

ネットワーク診断装置 TM2000

・クレバースカイシステムズ株式会社が商品化した装置

・MIB 情報収集に特化したアプライアンス型ネットワーク診断装置

・最大 1,000 台、10,000 項目の MIB 収集が可能

・秒単位の MIB 収集が可能

【各社の説明】

◆ジェノアテクノロジーズ株式会社について

＜実証実験の役割＞

マルウェアを用いたサイバー攻撃に関するノウハウ提供およびサイバー攻撃模擬のためのノウハウ提供

＜会社事業内容＞

・ネットワークセキュリティに係る企画・設計・開発のコンサルティング

・サイバーセキュリティ製品開発・ソリューション開発

・サイバーセキュリティに係る教育

◆株式会社アドックインターナショナルについて

＜実証実験の役割＞

・商品化に向けての営業マーケティングの担当

＜会社事業内容＞

・ネットワーク、システム基盤を中心とするエンジニアリングサービス

・ソフトウェアテスト、業務効率化に関連するプロダクト販売およびコンサルティングサービス

◆クレバースカイシステムズ株式会社について

＜実証実験の役割＞

ネットワーク診断装置 TM2000 提供およびサイバー攻撃検知のための MIB 収集ノウハウ提供

＜会社事業内容＞

・ネットワークシステムの診断コンサル・診断サービス

・ネットワーク診断装置 TM1000/TM2000 の販売

・ネットワークシステム構築に係わる企画・設計・開発のコンサル

・ネットワークシステムの運用・管理の受託

【本件に関するお問い合わせ先】

ジェノアテクノロジーズ株式会社

Mail： info@jnoah.co.jp

URL： https://www.jnoah.co.jp/

株式会社アドックインターナショナル

Mail： info@adoc.co.jp

URL： https://adoc.co.jp/

クレバースカイシステムズ株式会社

Mail： info@cleverskysystems.com

URL： https://www.cleverskysystems.com/