

報道関係各位

伊藤忠テクノソリューションズ株式会社

## 日本マイクロソフトと連携し、生成 AI を活用したセキュリティ分析サービスを開発 脅威インテリジェンスとアナリストの知見を用いて分析業務の高度化を実現

伊藤忠テクノソリューションズ株式会社(代表取締役社長:柘植 一郎、本社:東京都港区、略称:CTC)は、日本マイクロソフト株式会社(代表取締役 社長:津坂 美樹、本社:東京都港区)と連携し、CTC のセキュリティ・オペレーション・センター(CTC-SOC)における生成 AI を活用したセキュリティ分析サービスを開発します。マイクロソフトが提供する生成 AI サービス「Azure OpenAI Service」、インターネット上からサイバーセキュリティに関する脅威情報を収集して分析する「Microsoft Defender Threat Intelligence(以下:Microsoft Defender TI)」、セキュリティ監視基盤「Microsoft Sentinel(以下:Sentinel)」を活用します。CTC-SOC サービスやセキュリティアナリストの知見と膨大な脅威情報を生成 AI の学習データとして利用することで、分析の精度、品質の向上につなげ、今後さらに増え続けるセキュリティ脅威に対する分析業務の高度化を実現します。

CTC では、2014 年に、お客様のシステムを 24 時間 365 日遠隔監視する CTC-SOC を開設し、インターネット上の脅威動向を調査、分析してセキュリティ対策に活かすマネージドセキュリティサービスを、国内外の多くの企業に提供してきました。近年、より高度化・複雑化する脅威に対応するため、脅威情報と生成 AI を活用したサービスを開発し、更なるセキュリティ監視能力の強化を図ります。

CTC-SOC では、サイバーセキュリティに関する脅威を検知した際に、お客様向けにセキュリティインシデントの発生をメール、電話、カスタマーポータルなどで通知しています。通知する内容の作成には、脅威情報の収集と要約、初動対応の内容、被害の発生を未然に防ぐ対処方法の検討、文章の作成・校正など、様々な作業があります。今回開発するサービスでは、Azure OpenAI Service を通じた大規模言語モデル、Microsoft Defender TI が持つ膨大な脅威情報、Sentinel のセキュリティ監視機能を活用し、不正アクセスやマルウェア感染などの脅威が発生した際の分析品質を向上します。CTC-SOC の長年の運用で培ってきたセキュリティアナリストの知見と膨大な脅威情報を組み合わせて、生成 AI の精度向上に努め、セキュリティ監視能力の強化につなげます。

Azure OpenAI Service は、AI の開発を行う OpenAI 社の技術を、マイクロソフトが企業向けに提供する生成 AI サービスの1つです。GPT-3.5 や GPT-4 モデルなどの大規模な言語モデルをマイクロソフトのクラウドプラットフォーム Microsoft Azure 上で利用できます。OpenAI 社が提供する無料公開サービスとは環境が異なり、Microsoft Azure のセキュリティとコンプライアンス基準に準拠し、データの暗号化、アクセス制御、監査ログなどのセキュリティ機能が提供されます。

Microsoft Defender TI は、インターネット上からサイバーセキュリティ上の脅威となり得る様々な情報を収集・分析する脅威インテリジェンスサービスです。マルウェア、不正アクセス、ハッカーによる新たな攻撃手法や攻撃対象となった脆弱性情報などの脅威情報を提供し、攻撃の発生を早期に検知することで、適切な対策を講じることにつながります。Sentinel は、クラウド型のセキュリティ監視基盤(SIEM: Security Information and Event Management)です。ネットワーク機器などの IT インフラやソフトウェアから出力されるログを一元的に集約、分析して、サイバー攻撃やマルウェア感染などの脅威を検出します。

CTC は、マネージドサービスやセキュリティサービスを含めたハイブリッドクラウド支援サービス「OneCUVIC」を提供しており、CTC-SOCを含めて企業のセキュリティを支える総合的なサービスを展開しています。また、生成 AI の導入について検討から実装までをカバーするコンサルティングサービス「生成 AI アドバイザリサービス」の提供も 5 月に開始しました。

CTC は今後も、AI の利活用における姿勢をまとめた CTC グループの「AI 倫理原則」を遵守し、AI の有効な活用方法、技術に対する正しい理解、倫理面への配慮を推し進め、お客様ビジネスや社会への貢献に努めていきます。

#### ■ CTC のハイブリッドクラウドへの取り組み「OneCUVIC」

CTC は、複雑化、高度化するシステム運用の負荷低減や、セキュリティ強化を支援するオープンハイブリッドクラウド統合基盤サービスを「OneCUVIC」というブランド名で展開しています。今回の検証に基づき、セキュリティ関連サービスの拡充や、システム運用業務の効率化につなげ、お客様システムを安心して利用できる環境を整えていきます。

今回のプレスリリースにあたり以下のコメントをいただいています。

日本マイクロソフトは、CTC 様が Security SoC サービスにおいて、Azure OpenAI Service 並びに Microsoft Defender Threat Intelligence を活用したサービス開発を開始いただいたことを心より歓迎致します。

昨今のサイバーセキュリティの複雑化によるセキュリティニーズの高まりに対し、CTC 様はセキュリティ領域に関する深い知見やアプローチを活かし、最先端の技術力やサービス化の迅速さを実現されていると考えております。既に Microsoft Sentinel による SoC サービスをリリースいただいている中、Azure OpenAI Service 及び Microsoft Defender Threat Intelligence との連携による新たなサービスを市場にリリースされることで、より高いセキュリティの向上と効率化された運用の提供にて日本のお客様のデジタルトランスフォーメーションの推進に大きく貢献いただくことを期待しております。

日本マイクロソフト株式会社

執行役員 常務 パートナー事業本部長 浅野 智

- ※ Microsoft、Microsoft Sentinel、Microsoft Defender、Azure は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- ※ 記載されている商品名などの固有名詞は、各社の商標または登録商標です。
- ※ 掲載されている情報は、発表日現在の情報です。最新の情報と異なる場合がありますのでご了承ください。

以上

<報道機関からのお問い合わせ先>  
伊藤忠テクノソリューションズ株式会社  
広報部  
E-mail: [press@ctc-g.co.jp](mailto:press@ctc-g.co.jp)