2026 年 11 月 26 日
株式会社 YCC 情報システム
NTT ドコモビジネス株式会社

YCC 情報システム、AI を駆使してサイバー攻撃の脅威を分析・自動対処する「AI SOC」を導入

株式会社 YCC 情報システム(以下 YCC 情報システム)は、NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、以下 NTT ドコモビジネス)が提供する、AI によるログ分析とセキュリティアラートの自動対処でサイバー攻撃の監視・対処を行う「AI SOC※1」(以下 本サービス)を導入し、2026 年 11 月から運用を開始しました。

1.背景

近年、サイバー攻撃は高度化・巧妙化しており、企業や自治体など組織の規模や業種を問わず、事業継続や情報資産を脅かすリスクが高まっています。特にランサムウェアによる被害は深刻化しており、被害は大企業だけでなく中小企業にも広がり、サイバー攻撃への対応は多くの組織にとって重要な経営課題となっています。

サイバー攻撃による被害の拡大を防ぐためには、従来の予防的な対策に加え、ネットワークや認証などの膨大なログから攻撃の兆候を早期に把握し、脅威を検知した際に迅速に対処することが重要となっています。一方で、こうした監視・分析を継続的に行うには専門的な知見が必要であり、セキュリティ人材の経験やスキルに過度に依存しない運用体制の構築も求められています。

このような状況の中、YCC 情報システムは 2026 年 4 月 2 日、内部ネットワークへの侵入によりファイルサーバーがランサムウェア攻撃を受け、ファイルが暗号化されたことにより、アクセスできない状態となりました。※2 これを受け、YCC 情報システムでは、ネットワークの監視・分析能力の向上や脅威検知後の迅速な対応など、セキュリティ運用体制のさらなる強化を進めてきました。

その強化の一環として、AI によるログ分析、自動対処、専門家による支援を組み合わせた「AI SOC」が有効であると判断し、NTT ドコモビジネスと検討を進め、2026 年 11 月から本格運用を開始しました。

2.本サービスの導入の効果

本サービスは、AI Advisor※3 による通信や認証などのログの分析と、マネージド SOAR※4 による自動対処を組み合わせ、高度化するサイバー攻撃に対して、AI を駆使した防御を実現するサービスです。

YCC 情報システムでは、本サービスの AI による高度な分析、自動対処、セキュリティの専門家による支援を一体的に活用することで、セキュリティ担当者の経験やスキルに過度に依存しない 24 時間 365 日の監視・対応体制の構築を実現しました。

本サービスの導入により、AI を活用して膨大なログを相関分析することで、従来は捉えることが難しかった攻

撃の兆候や脅威を早期に検知し、分析の高度化・迅速化を実現しています。さらに、Playbook※5を活用した自動対処により、被害の拡大防止につなげています。また、分析・対処・通知を自動化・標準化することで、属人化を排した運用体制を整備し、高度化・巧妙化するサイバー攻撃に対する継続的な対応力の強化につなげています。

3.今後の展開

YCC 情報システムは、本サービスを活用したセキュリティ監視・運用を継続するとともに、AI と専門家の知見を組み合わせたセキュリティ対策の高度化を進め、自治体や企業などのお客さまに安心・安全な IT サービスを提供できる体制の強化に取り組みます。

NTT ドコモビジネスは、AI Advisor による分析精度の向上や、マネージド SOAR による自動対処の適用範囲拡大などを通じて、さらなる機能拡充を図ります。これにより、高度化・巧妙化するサイバー攻撃に対して、お客さまの持続可能なセキュリティ運用を支援します。

※1：AI SOC の詳細は別紙をご確認ください。

※2：【重要】ランサムウェア攻撃に関するお知らせ（第五報） | 株式会社 YCC 情報システム

※3：AI Advisor とは、NTT ドコモビジネス独自開発のログ分析用の AI エージェントです。詳細は以下のサービス紹介サイトをご確認ください。

WideAngle AI Advisor サービス紹介サイト

※4：マネージド SOAR とは、Microsoft Sentinel の運用を NTT ドコモビジネスが提供するマネージドサービスです。詳細は以下のサービス紹介サイトをご確認ください。

WideAngle マネージド SOAR サービス紹介サイト

※5：Playbook とは、自動化対象とする脅威対処のワークフローを SOAR 上で実行できるようにしたプログラムです。

【別紙】

「AI SOC」詳細

「AI SOC」は、AI Advisor による通信や認証などのログの分析と、マネージド SOAR による自動対処を組み合わせ、高度化するサイバー攻撃に対して、AI を駆使した防御を実現するサービスです。

■サービスの特長

① AI Advisor によるログの分析

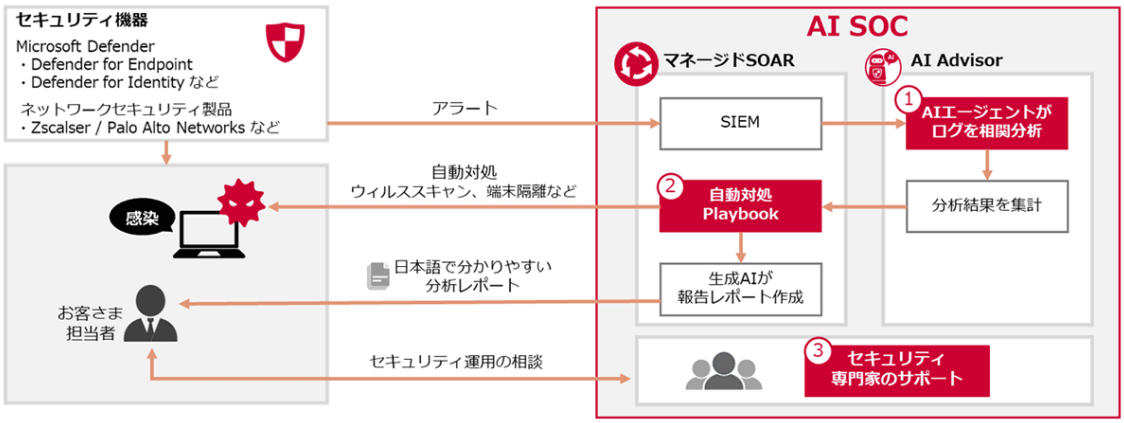
NTT ドコモビジネスが独自開発したログ分析用の AI エージェントである AI Advisor が、エンドポイント、ネットワーク、認証などの大量のログを横断的に分析することで、従来の人手中心の作業では 1～2 時間を要していた相関分析※別紙注 1 を約 10 分で行い、攻撃の全体像や影響範囲などを特定できます。

② マネージド SOAR による自動対処

脅威が検知された場合にはマネージド SOAR による自動対処を行うことで、対処を迅速化するとともに、セキュリティ担当者の経験やスキルによらない対処の平準化、および運用稼働の効率化を実現します。マネージド SOAR を組み合わせることで、セキュリティアラートへの対処の約 95%を自動化できます。

③ 専門家によるサポート

人手での対処が必要な場合や AI の分析結果に対する疑問などについて、NTT ドコモビジネスのセキュリティ対策の専門家がサポートすることで、専門知識をお持ちでないお客さまでも安心して導入いただけます。



<本サービスのイメージ>

※別紙注 1：相関分析とは、サイバー攻撃時に発生する複数のログや通信、端末の挙動などを関連付けて分析し、攻撃の全体像や原因、影響範囲を特定する手法を指します。