2024 年 9 月 3 日

NTT コミュニケーションズ株式会社

# サイバー攻撃の脅威に迅速に自動対処しセキュリティ技術者を支援する「マネージド SOAR」にて、自動化と生成 AI を活用した新機能提供開始

## ～「Microsoft Sentinel」を活用した「マネージド SOAR」の新機能～

ドコモグループの法人事業ブランド「ドコモビジネス」を展開する NTT コミュニケーションズ株式会社(以下 NTT Com)は、「Microsoft Sentinel※1」を活用したセキュリティ自動化を実現するマネージドセキュリティサービスである「WideAngle プロフェッショナルサービス マネージド SOAR」（以下、本サービス）の新機能を 2024 年 9 月 3 日より提供開始します。

本サービスは、「Microsoft 365 E5 Security※2」のログを「Microsoft Sentinel」に転送し、ログ蓄積、ログ分析、アラート自動対処の機能を提供してきましたが、このたび、Zscaler, Inc.、Palo Alto Networks、Netskope などの提供するネットワークセキュリティ製品のログ※3 に対応します。また、生成 AI を活用したわかりやすい日本語アラート通知機能を実装するなど、新機能を提供開始します。

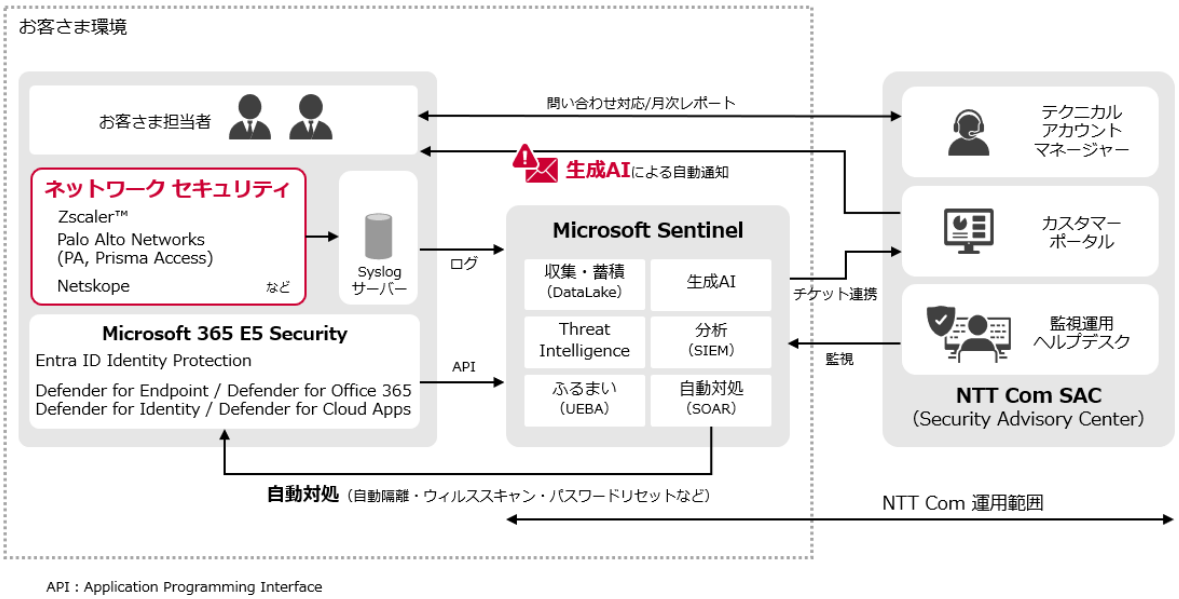
### 1.背景

サイバー攻撃の件数が増加するとともに攻撃手法が巧妙化する一方、被害の防止・復旧に対応できるセキュリティ技術者が社会的に不足しています。本サービスで採用する SOAR(Security Orchestration, Automation and Response)は、脅威を検知した際に自動的な対処・復旧を可能にする技術であり、サイバー攻撃への迅速な対応とともに、技術者のスキルによらず対応を平準化・高度化でき、セキュリティ対策を組織的に向上することが可能です。

一方 SOAR の導入には、脅威への自動的な対処方法を定義する Playbook と呼ばれるワークフローの設計と適用が必要なため、高度なセキュリティ技術が不可欠になります。本サービスは、NTT Com が蓄積した技術と専門知識を反映した Playbook をマネージドサービスとして継続的に提供し、SOAR の円滑な導入と運用を実現します。

## 2.本サービスの概要

<本サービスの提供イメージ>



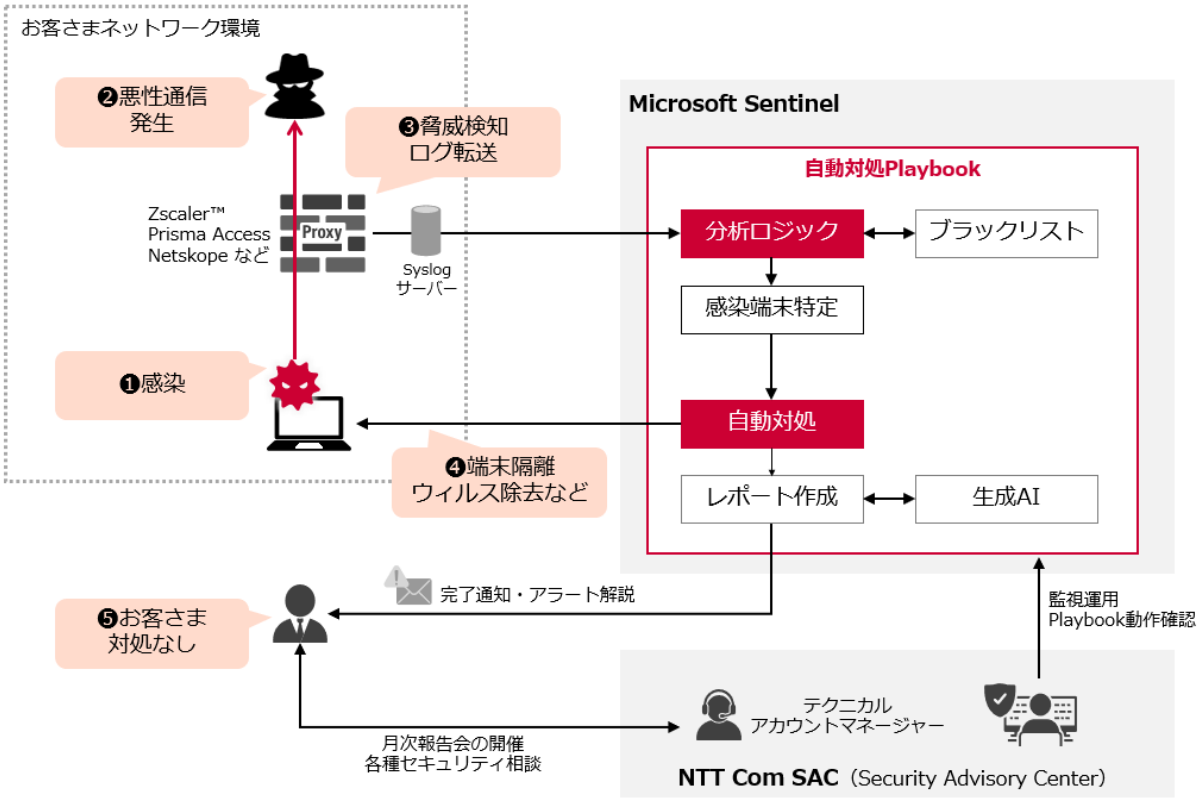

本サービスでは、「Microsoft Sentinel」を SIEM※4SOAR の基盤として採用、マイクロソフト製品に加え、ネットワークセキュリティ製品のログを分析することでセキュリティを強化します。さらに、脅威が発見された際は、SOAR を活用し、セキュリティインシデントに対して Playbook に従い自動的に対処・復旧まで行います。※5

## 3.本サービスの拡充する機能の特長

(1)サイバー攻撃への自動対処

マイクロソフト社の「Microsoft 365 E5 Security」製品に加え、Zscaler, Inc.、Palo Alto Networks、Netskope などの提供するネットワークセキュリティ製品のログにも対応します。これにより、マイクロソフト製品のログからの自動対処だけでなく、ネットワークセキュリティと、エンドポイントセキュリティ(「Defender for Endpoint※6」)を組み合わせた相関対処が実現可能になります。ネットワークセキュリティ製品で攻撃を検知した際、侵害された端末を自動的に特定し、ネットワークから隔離したうえでウイルススキャンなどを実行し、脅威を自動的に取り除き、復旧までを自動で行うことができます。お客さまは、セキュリティアラートが発生した場合でも、自動対処の結果を確認するのみとなり、稼働削減につながります。

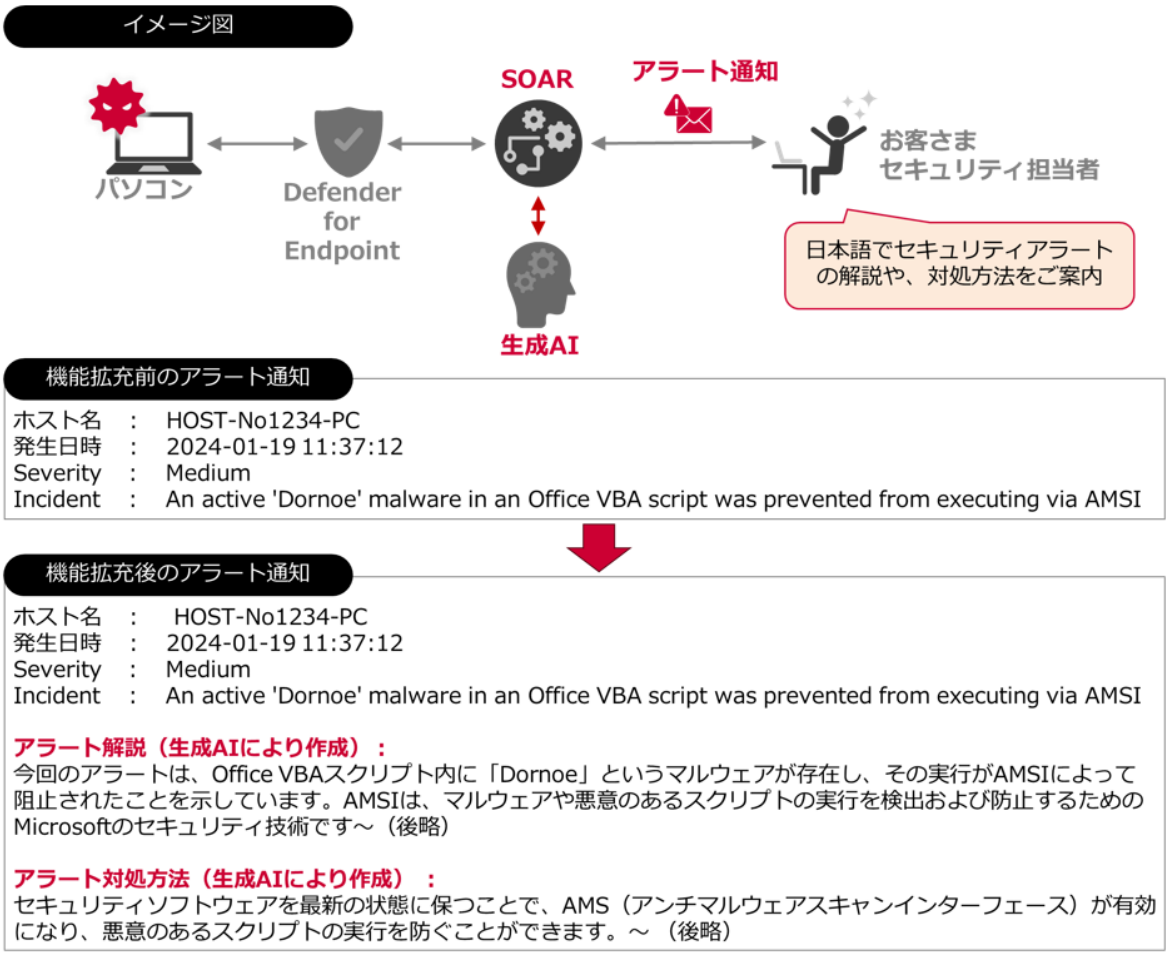
<サイバー攻撃へのネットワークセキュリティを利用した自動対処の提供イメージ>




(2)生成 AI によるアラート解説・対処方法のご案内

今回の機能拡充により、アラートの解説・アラート対処方法を、生成 AI を活用することで、わかりやすい日本語で生成し、お客さまへメール通知を行います。※7 お客さまは、何が起こったのか日本語で直感的にわかりやすく理解することが可能となり、アラート調査の稼働削減につながります。

<生成 AI によるアラート解説・対処方法のご案内の提供イメージ>




(3)サポートの充実

①Playbook の継続的な最適化

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。従来は、セキュリティアラートの内容や対処方法をお客さま自身で調査し、適切な対処・復旧措置を実施しており、アラートに関する知識や対処に関するノウハウが必要となっておりました。どのアラートが出た時にどのような対処が必要なのか、NTT Com が蓄積した長年のセキュリティ対策運用ノウハウや知見を Playbook に適用し、自動対処を実現します。また、新しい脅威への対処やマイクロソフト製品の機能向上への対応など更新が必要となるため、最適化した Playbook を NTT Com がマネージドサービスとして継続的に提供し、SOAR の円滑な運用を実現します。

②テクニカルアカウントマネージャー(TAM)によるサポート

NTT Com のセキュリティアドバイザリーセンター(SAC)が、ヘルプデスク窓口としてお客さまの運用をサポートします。さらに、テクニカルアカウントマネージャー(TAM)として、専任の担当者をアサイ

ンし、月次報告会でセキュリティアラートの傾向や対策のご案内や、セキュリティ運用上の各種相談ができます。※8 テクニカルアカウントマネージャーを活用することで、お客さまのセキュリティ運用を支えます。

**4.セキュリティ監視対象**

本サービスでログを監視できる製品は以下の通りです。監視対象は選択でき、当初は小規模に導入し必要に応じて拡張することも可能です。

| 名称 | 提供開始日 |
|---|---|
| Microsoft 365 E5 Security 製品<br>・Entra ID P2 (Entra ID Identity Protection)<br>・Microsoft Defender for Endpoint (Plan 2)<br>・Microsoft Defender for Identity<br>・Microsoft Defender for Cloud Apps<br>・Microsoft Defender for Office 365 (Plan 2) | 2023 年 3 月 31 日より提供中 |
| ネットワークセキュリティ製品<br>・Zscaler™<br>・Palo Alto Networks PA Series/Prisma Access<br>・Netskope　など※3 | 2024 年 9 月 3 日より提供開始 |

**5.提供開始日**

2024 年 9 月 3 日

**6.利用料金**

月額　　：　44 万円～(税込)※9

初期構築費用　：115.5 万円～(税込)※9

詳細は NTT Com 営業担当までお問い合わせください。

**7.お申し込み方法**

NTT Com 営業担当までお問い合わせください。

**8.今後の展開**

NTT Com は、SOAR の積極的な活用を検討するお客さまをはじめ、セキュリティ対策のさらなる運用効率化・自動化を図るお客さま向けに、本サービスを適用できる製品の拡充や、さらなる自動化・効率化を目指し、サービスの拡充を進めていきます。

---

NTT ドコモ、NTT Com、NTT コムウェアは、ドコモグループの法人事業を統合し、法人事業ブランド「ドコモビジネス」を展開しています。「モバイル・クラウドファースト」で社会・産業にイノベーションを起こし、すべての法人のお客さま・パートナーと「あなたと世界を変えていく。」に挑戦します。

https://www.ntt.com/business/lp/docomobusiness/db2024_sol.html

※1：「Microsoft Sentinel」とは、クラウドネイティブの SIEM、SOAR 機能を提供し、サイバー攻撃の検出や可視化から脅威への対応までを包括的に対応するサービスです。

※2：「Microsoft 365 E5 Security」とは、マイクロソフト社のゼロトラストセキュリティを実現するクラウド型セキュリティサービスです。

※3：CEF 形式または Syslog 形式でログ転送が可能で、所定のログ項目(IP アドレス、ホスト名など)が転送ログに含まれる必要があります。なお、ネットワークセキュリティ製品のログを、「Microsoft Sentinel」へ転送するには、お客さまにて Syslog サーバーの構築が必要です。

※4：SIEM とは、ファイアウォールや IDS／IPS、プロキシーなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことで、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とした仕組みです。

※5：完全に脅威を取り除けない場合も存在します。

※6：「Defender for Endpoint」とは、Microsoft のクラウドベースのエンドポイントセキュリティソリューションです。

※7：生成 AI により作成された情報は参考情報となります。内容を保証するものではございません。また対象製品によりアラート解説・対処法が出ないものもあります。

※8：サポートの利用には、チケット制による追加の費用が発生する場合があります。また、テクニカルアカウントマネージャー(TAM)のアサインは有償となります。

※9：「マネージド SOAR」の料金であり、Microsoft 365 や、各種セキュリティデバイス、Microsoft Sentinel の費用は別途発生します。