2023 年 3 月 27 日

Microsoft 365 導入企業へのサイバー攻撃に自動対処しセキュリティ技術者を支援、脅威への迅速な対応を可能にする新サービスを開始

～Microsoft Sentinel を活用した「マネージド SOAR」の提供開始～

NTT コミュニケーションズ株式会社(以下 NTT Com)は、「Microsoft 365」※1の導入企業を対象に、サイバー攻撃への対処を自動化する法人向けサイバーセキュリティ対策サービス「マネージド SOAR」(以下 本サービス)を、2023 年 3 月 31 日より提供開始します。

本サービスにより、サイバー攻撃への対処や復旧を自動化・迅速化できます。また、悪質化を続ける攻撃手段への最新の対処方法を NTT Com がお客さまへ継続的に提供し、多くの企業で常態化しているセキュリティ技術者の不足という課題を解決します。

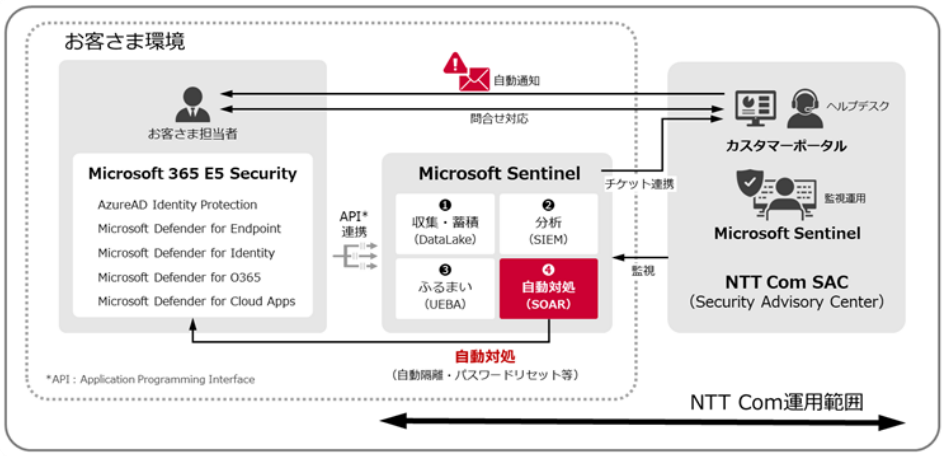
1. 背景

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・回復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>



NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation Public Relations Office
〒100-8019　東京都千代田区大手町 2-3-1　大手町プレイスウエストタワー
OTEMACHI PLACE WEST TOWER 2-3-1 Otemachi, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

本サービスは、多くの企業でマイクロソフト社製品が採用されていることを考慮し、「Microsoft Sentinel」を SOAR の基盤として採用、同社セキュリティ製品群のログを分析することでセキュリティを強化します、なお「Microsoft Sentinel」を SOAR として活用し、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・復旧まで行うマネージドサービスは、本サービスが国内初※2 となります。

3. 本サービスの特長

(1) サイバー攻撃への対処

本サービスの導入により、以下に挙げるようなセキュリティ対策が可能になります。

① エンドポイントセキュリティにおける自動対処

攻撃を検知した際、侵害された端末を自動的にネットワークから隔離したうえでウイルススキャンを実行し、脅威を取り除くことができます※3。

<自動対処イメージ>

② アカウント乗っ取りに対する自動対処

アカウント乗っ取りのアラートを検知した場合、侵害されたアカウントに対し、自動的にセッション断をおこなったり、パスワードリセットを実行したりすることができます。

③ ログの長期保存

セキュリティインシデント発生時のログの調査や定期的な監査に対応するため、通常は 90 日間(Azure AD Premium P2 の場合)が保存期間であるセキュリティアラートなどのログを、「Microsoft Sentinel」上で最大 2 年間(アーカイブは最大 7 年間)保存可能です。

(2) Playbook を継続的に最適化

Playbook 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。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テンプレート化します。

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。

(3) 容易な導入が可能

本サービスの導入に際して、「Microsoft Sentinel」のセットアップ(ログ収集設定、分析設定、Playbook 設定)を NTT Com のエンジニアが一括して提供するため、お客さまは特に設定作業を行うことなく容易に導入※4できます。

(4) ヘルプデスクによる運用サポート

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※5。Playbook の更新、バグ対応、アラートが発生した際の対処、各種設定変更作業など、本サービスを円滑に運用しお客さまのセキュリティをより高めることができます。

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マイクロソフト社の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	機能
Azure AD Premium P2 (Azure AD Identity Protection)	クラウド側の統合認証基盤
Microsoft Defender for Endpoint (Plan 2)	エンドポイントセキュリティ(EDR)
Microsoft Defender for Identity	オンプレミス AD の脅威検知
Microsoft Defender for Cloud Apps	クラウド(SaaS)の脅威検知
Microsoft Defender for Office 365 (Plan 2)	メールの脅威検知

5. 提供開始日

2023 年 3 月 31 日

6. 利用料金※6

月額　　：　44 万円～(税込)

初期構築費用　：115.5 万円～(税込)

7. お申し込み方法

NTT Com 営業担当者までお問い合わせください。

8. パートナーからのコメント

日本マイクロソフト株式会社　パートナー事業本部　業務執行役員　戦略アライアンス担当
小滝 亮太郎氏

このたびの NTT コミュニケーションズによる「マネージド SOAR」のリリースを心より歓迎いたします。多くの、また幅広いお客様に対してセキュリティ監視サービスを提供してこら

れた経験とノウハウを、当社「Microsoft Sentinel」と連携・統合していただくことにより、これまでにない自動化オペレーションを実現されましたことをたいへん喜ばしく思い、また、今後の両社連携・協力の主軸ソリューションの一つとして大いに期待しております。

9．今後の展開

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マイクロソフト製品の拡充や、同社以外のセキュリティ製品を対象とする各種サービスの提供を進めていきます。

NTT ドコモ、NTT Com、NTT コムウェアは、新ドコモグループとして法人事業を統合し、新たなブランド「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.html

NTT Com は、事業ビジョン「Re-connect X®」にもとづき、お客さまやパートナーとの共創によって、With/After コロナにおける新たな価値を定義し、社会・産業を移動・固定融合サービスやソリューションで「つなぎなおし」、サステナブルな未来の実現に貢献していきます。

https://www.ntt.com/about-us/re-connectx.html

※1：「Microsoft 365 E5 Security」が対象です。
※2：2023 年 3 月現在、NTT Com 調べ。
※3：完全に脅威を取り除けない場合も存在します。
※4：「Microsoft 365」の設定は本サービスに含まれません。
※5：SAC 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。
※6：「マネージド SOAR」の料金であり、Microsoft 365、Microsoft Sentinel の費用は別途発生します。