つなごう。驚きを。幸せを。

2025 年 10 月 1 日
NTT ドコモビジネス株式会社

多様なセキュリティデバイスのログを集約し、高度なセキュリティ分析を行う「WideAngle マネージドセキュリティサービス SIEM＆MDR」を提供開始

～NTT 独自の高度なセキュリティ分析により、サイバー攻撃によるビジネスリスクを最小化～

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）は、「WideAngle※1 マネージドセキュリティサービス SIEM＆MDR」(以下 本サービス) を、2025 年 10 月 1 日より提供開始します。本サービスは、多様なセキュリティデバイスのログを集約し、AI 活用を含む独自の高度な脅威分析や被害を最小化する対処、脅威ハンティング※2 により、サイバー攻撃によるビジネスリスクを最小化します。

1. 背景

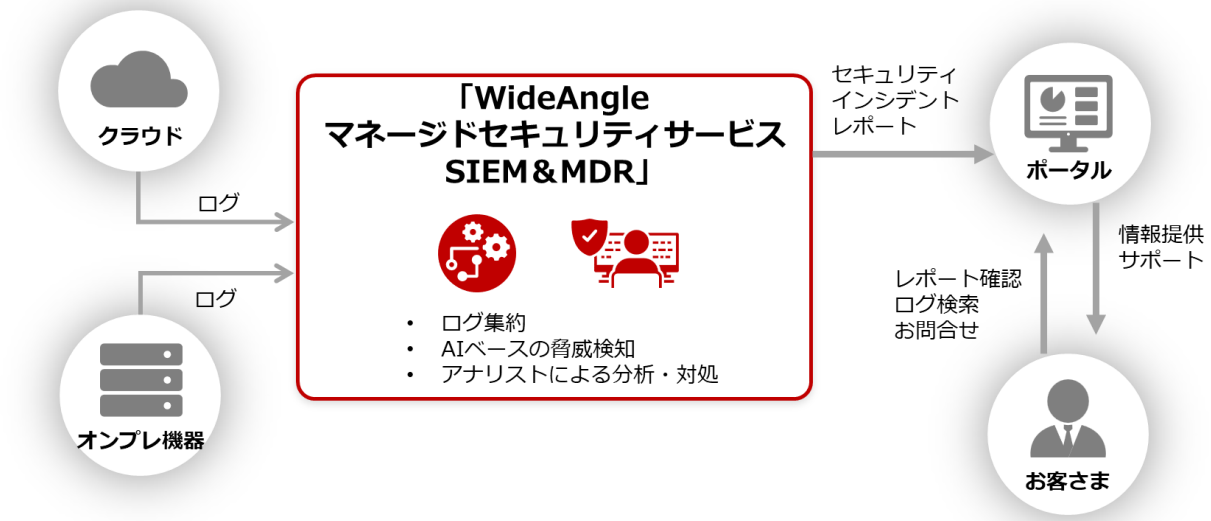
近年、サイバー攻撃の件数が増加するとともに、AI による攻撃も顕在化し、サイバーリスクは経営リスク、サプライチェーンリスクの一つとして捉えられています。そのような中、経済安全保障の強化、個人情報や機密情報などの電子データの取り扱いへの規制、能動的サイバー防御、業界ガイドラインなどに見られるように、国内外においてサイバーリスクマネジメントは転換期を迎えています。このような転換期において、サイバー攻撃のビジネスリスクを最小化するためには、セキュリティオペレーションセンター※3 (以下 SOC) による高度なセキュリティ監視・運用が求められます。そのためには、SIEM※4 などの分析に必要な仕組みの設計・構築・運用、専門人材(セキュリティアナリスト)の確保、運用体制の確立などが必要となります。増大する運用負荷を解消しつつサイバー攻撃の被害拡大を防ぐため、SIEM を活用し、検知したサイバー攻撃の対処も行う MDR※5 サービスが求められています。

2. 本サービスの概要と特長

本サービスは、お客さまに代わり、「WideAngle」のアナリストが SIEM を活用して高度なセキュリティ分析などを行う MDR サービスを提供します。具体的には、お客さまの多様なセキュリティデバイスのログを収集し、集約されたログをもとに「WideAngle」のアナリストが分析・対処を行います。その後、脅威とその影響の検証、および潜在的な侵害に関連する情報を特定し、セキュリティインシデントレポートを作成して、お客さまへ提供します。

これらにより、お客さまのセキュリティオペレーションを軽減するとともに、サイバー攻撃によるビジネスリスクの最小化を実現いたします。

<本サービスの提供イメージ>



本サービスの特長は、以下 4 点です。

(1) 独自の分析による精度の高い MDR サービスおよび脅威ハンティングの提供

セキュリティ製品の関連技術、フィッシングサイト検知などの AI ベースの脅威検出機能、および「WideAngle」のアナリストによる独自の高度分析を組み合わせることで、MDR サービスとして、より迅速で精度の高い分析と被害を最小化する対処を行います。さらに、「WideAngle」のアナリストの独自調査や NTT 研究所での研究成果などの NTT のグローバルな脅威インテリジェンス※6、および最新の脅威情報やセキュリティ動向を活用した精度の高い脅威ハンティングを提供します。

(2) 多様なセキュリティデバイスのログを集約

本サービスの分析対象外のセキュリティデバイスのログもまとめて、SIEM に集約できます。これにより、お客さまのログの統合的な参照、検索が可能になります。

(3) 充実のポータルサイト

本サービスのポータルは、「WideAngle」が発行するインシデント通知状況の確認、アナリストへの問い合わせ機能に加えて、取り込んだログの検索機能やダッシュボード機能が搭載されています。これにより、本サービスに集約したデータを使い、お客さま自身によって、簡易分析やエグゼクティブレポートを作成することができます。

(4) 高度な分析サービスをグローバルで均一に提供

日本と欧州(スウェーデン）に同じ仕様のプラットフォームをそれぞれ有しています。これにより、欧州のプラットフォームを選択すると、ログの集約場所が EU 圏内となるため GDPR※7 にも対応できます。

3. 提供開始日

2025 年 10 月 1 日

4. 利用料金

NTT ドコモビジネス営業担当までお問い合わせください。

5. お申し込み方法

NTT ドコモビジネス営業担当までお問い合わせください。

6. 今後の展開

今後、本サービスで対応するセキュリティ製品の拡充や閉域接続への対応など、お客さまのより幅広いニーズに柔軟に対応できる機能拡充をします。

また、AI の活用をさらに推進し、さらなる分析の高度化・効率化、お客さまのオペレーション支援などを行います。

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 DX のプラットフォーマー」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つなごう。驚きを。幸せを。
docomo Business https://www.ntt.com/about-us/nttdocomobusiness.html

※1：「WideAngle」とは、NTT コミュニケーションズが提供する総合リスクマネジメントサービスで、オンプレミス、クラウド、ハイブリッドなど、さまざまな ICT 環境に対し、SOC による専門家が総合的なセキュリティソリューションを提供します。
https://www.ntt.com/business/services/security/security-management/wideangle.html

※2：脅威ハンティング(Threat Hunting）とは、サイバーセキュリティの専門家が積極的にネットワークやシステムを監視して潜在的な脅威や攻撃を探し出すプロセスです。

※3：セキュリティオペレーションセンター(SOC)とは、サイバー攻撃の検知や分析を行い、対策を講じる専門組織のことで、各種セキュリティ装置やネットワーク機器、サーバーの監視や、それらから出力されるログの分析、サ

イバー攻撃を受けた場合の影響範囲の特定、サイバー攻撃を阻止するためのセキュリティ対策の立案などを担います。

※4：SIEM(Security Information and Event Management)とは、ファイアウォールや IDS／IPS、プロキシ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：MDR(Managed Detection and Response）とは、近年、巧妙化しているサイバー攻撃に対し、侵入されないセキュリティだけではなく、侵入された脅威を迅速に検知し、いち早く対応するためのセキュリティサービスです。

※6：脅威インテリジェンスとは、サイバー攻撃に関するあらゆる情報を収集して、整理・分析したものです。

※7：GDPR(General Data Protection Regulation）は、2018 年 5 月に施行された欧州連合の法令です。個人のプライバシー保護の強化、およびデータの収集や処理に対する透明性を高めることを目的としています。