つなごう。驚きを。幸せを。

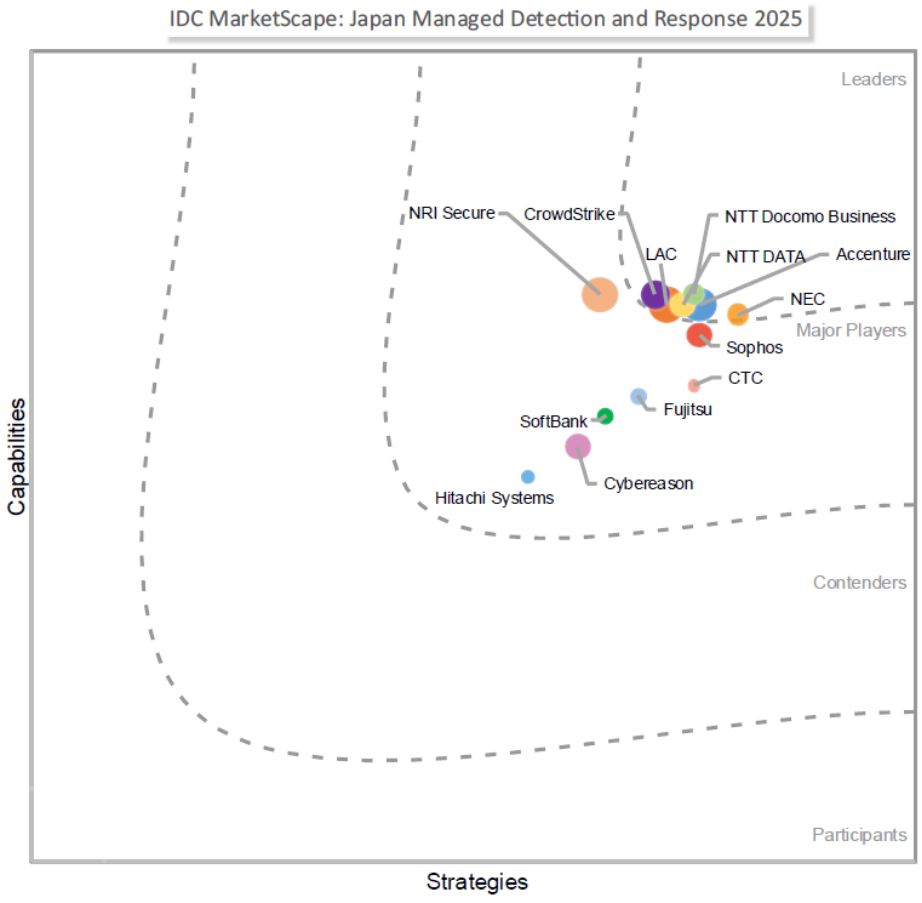
2025 年 11 月 20 日

NTT ドコモビジネス株式会社

NTT ドコモビジネス、米 IDC 社の「IDC MarketScape : Japan Managed Detection and Response Services 2025 Vendor Assessment」においてリーダーに選出

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、米 IDC 社のレポート「IDC MarketScape : Japan Managed Detection and Response Services 2025 Vendor Assessment」（IDC#JPJ53015825, November 2025、以下 本レポート）において、最も高い評価であるリーダー（Leaders）のポジションに位置付けられました。

NTT ドコモビジネスは、組織のセキュリティ監視を行う運用サービス「Managed Detection and Response※1 Services (以下 MDR サービス)」において、長年の運用経験にもとづく高度な自動化のノウハウや、多様な顧客ニーズに応える豊富なサービス戦略が評価されました。



PDF ダウンロードはこちら

1. 本レポートについて

IDC 社が実施する「MarketScape」とは、特定の市場における ICT サプライヤーの競争力の適応度を把握する分析モデルです。

IDC MarketScape ベンダー分析モデルは、特定の市場におけるテクノロジーおよびサプライヤーの競争力の概要を提供するように設計されています。この調査手法は定性的および定量的な基準にもとづいた厳格な採点方法を使用し、特定の市場における各サプライヤーの位置づけを単一のグラフィカルな図で表現します。「能力（Capabilities）」スコアは、短期的な、ベンダーの製品、マーケティング戦略、事業遂行力を測定したものです。「戦略（Strategies）」スコアは 3～5 年の期間における顧客要件とサプライヤー戦略の整合性を測定したものです。ベンダーの市場シェアは、円（バブル）の大きさで表されます。

2. NTT ドコモビジネスが提供する MDR サービス

NTT ドコモビジネスが提供する MDR サービスは、「マネージド SOAR※2」と「マネージドセキュリティサービス(SOC)」の 2 つがあります。

① マネージド SOAR

マネージド SOAR とは、自動化を活用した、Microsoft Sentinel※3 の運用サービスです。Microsoft、Zscaler, Inc.、Palo Alto Networks などの提供するセキュリティ製品のログを自動で分析し、攻撃を検知した際には、NTT ドコモビジネスの開発した Playbook に従って、端末のネットワーク隔離の実行やウイルススキャンによる脅威の除去など、復旧まで自動的に行います。昼夜を問わずサイバー攻撃への迅速な対応を実現するとともに、お客さまの対応稼働を軽減し、セキュリティ対策を組織的に向上することが可能です。

② マネージドセキュリティサービス（SOC）

マネージドセキュリティサービスとは、お客さまのセキュリティ機器のログを SOC（Security Operation Center）の SIEM※4 に送信し、SIEM エンジンによる分析に加えアナリストが潜在的なリスクを含めて高度な分析を行うサービスです。アナリストはセキュリティ機器ごとの単体の分析でなく、EDR※5、UTM※6、プロキシーなど複数のデバイスのログを相関して分析します。また、極めて重大な攻撃を検出した際には、アナリストの判断で、端末のネットワーク隔離の実行や、ネットワークセキュリティ機器にブロックリストの投入を行います。

3. 本レポートにおける評価ポイント

本レポートにおいて、NTT ドコモビジネスは以下のように評価されています。

「NTT ドコモビジネスの強みは、長年にわたるセキュリティ運用経験を通じて蓄積したノウハウを生かし、マネージド SOAR において大規模なプレイブックを提供できる点にある。このプレイブックを基盤に、エージェンティック AI による自動化機能を拡充することで、中小企業向けには低価格サービス

を、大企業向けにはインシデントレスポンスやデジタルフォレンジックなどのより高度な機能を提供できるようになる。また、2024 年には生成 AI を活用したセキュリティ運用支援サービスである「AI Advisor」を開始し、従来型の自動化機能に加えて、生成 AI を用いた運用支援を実現している。さらに、通信事業者としてネットワークを含む運用サービスを提供できる点や、海外に複数の SOC を構える点も差別化要素となっている。海外に製造拠点のある製造業へのサービス提供などを中心に、統合的な運用やグローバルなセキュリティ運用のニーズに応えている。」

4. IDC Japan 山下頼行アナリストのコメント

MDR サービスにおける主要な差異化要素は、AI や SOAR を用いた自動化機能や、脅威インテリジェンス、海外拠点におけるサポートの現地対応力である。同社は、AI や SOAR を活用した自動化機能に加え、完全自動化 SOC の開発を進めるなど、運用効率化に向けた取り組みを強化している。また国内外に複数の SOC を展開し、グローバルなセキュリティ運用ニーズに応える存在感を示している。

「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：Managed Detection and Response(MDR)とは、サイバー攻撃を 24 時間 365 日監視し、脅威を検知したら迅速にアラートの対処をするセキュリティ運用サービスです。

※2：SOAR(Security Orchestration, Automation and Response)とは、サイバー攻撃を検知した際に、Playbook と呼ばれるワークフローに従い、自動的にアラートの対処を可能にする技術です。

※3：Microsoft Sentinel とは、マイクロソフト社が提供する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。

※4：SIEM（Security Information and Event Management）とは、サーバーやネットワーク機器などから得られるログを一元的に収集・管理し、それらを分析する基盤です。

※5：EDR（Endpoint Detection and Response）とは、パソコンやサーバーなどのエンドポイント端末を監視し、サイバー攻撃の兆候を検知して対処を行うセキュリティ製品です。

※6：UTM（Unified Threat Management）とは、ファイアウォール、アンチウイルス、アンチスパム、Web フィルタリングなど、複数のセキュリティ機能を 1 台の機器に統合した製品です。

IDC MarketScape について：IDC MarketScape ベンダー評価モデルは、特定の市場における IT サプライヤー、サ

ービスプロバイダーの競争力の概要を提供するように設計されています。
この調査では、定性的および定量的な基準に基づく厳密な採点方法を用いて、特定の市場内における各企業のポジションを単一のグラフィカルな図で表現します。
IDC MarketScape は、IT ベンダーの製品・サービス、能力、戦略、現在および将来における市場での成功要因を有意義に比較できる明確なフレームワークを提供します。
また、このフレームワークを利用することで、IT バイヤーは、対象ベンダーの現在および将来に渡る強みと弱みを 360 度で評価できるようになります。