IDC MarketScape

IDC MarketScape: Japan Managed Detection and Response 2025 Vendor Assessment

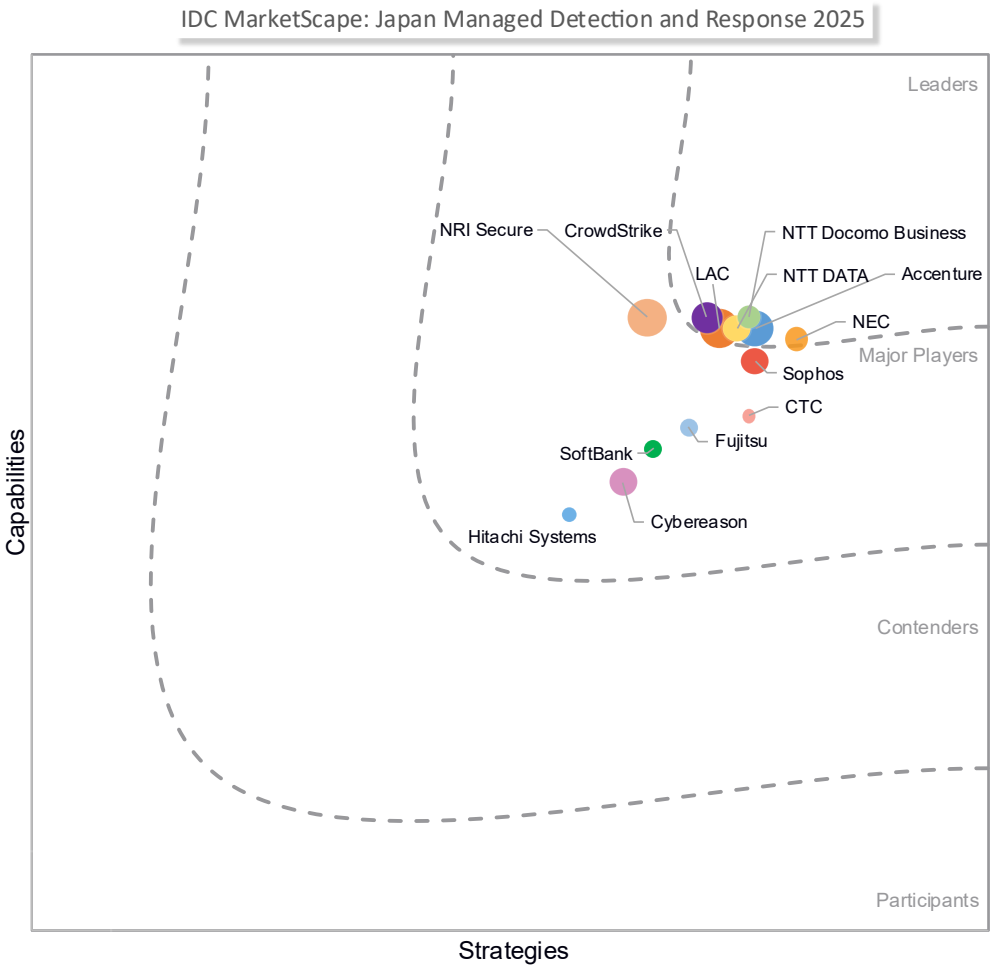
山下 頼行

THIS IDC MARKETSCAPE EXCERPT ACCENTURE AS LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Japan Managed Detection and Response Vendor Assessment



Source: IDC, 2025

November 2025, IDC #JPJ53015825e

詳細な調査方法、市場定義、評価基準については、「補遺」のセクションを参照していただきたい。

調査概要

本調査レポートは、『*IDC MarketScape: Japan Managed Detection and Response 2025 Vendor Assessment*（IDC #JPJ53015825、2025 年 11 月発行）』の Excerpt（抜粋）版である。

IDC の見解

本調査レポートは、国内マネージドセキュリティサービス市場において MDR（Managed Detection and Response）サービスを提供する主要ベンダーに対して、IDC MarketScape モデルに基づき「戦略（Strategies）」および「能力（Capabilities）」の評価を行い、その分析結果を報告するものである。

国内における MDR サービス市場は、2020 年頃から EDR（Endpoint Detection and Response）の普及を契機に拡大してきた。EDR の導入によって対応すべきアラート件数が増加し、企業における運用負荷が高まったことで、EDR の運用を支援する MDR サービスの需要が拡大したことがその背景にある。MDR サービスの提供形態は大きく 2 つに分類できる。一つは、EDR 製品ベンダーが自社で SOC（Security Operation Center）を運営し、MDR サービスを直接提供するベンダーSOC 型である。もう一つは、MSSP（Managed Security Service Provider）が自社の SOC と EDR 製品を組み合わせて提供する MSSP 型である。

当初、EDR ベンダーは国内 MSSP と連携し、MSSP 型で市場展開を進めていたものの、近年では、ベンダーSOC 型が増加している。大企業を中心に EDR の普及が一巡しており、EDR ベンダーが新たな事業機会を求めて自社の提供領域を拡大していることがその背景にある。こうしたことから、従来は補完関係にあった EDR ベンダーと MSSP の間に競争関係が生じる場合も出てきている。一方で、ID 管理など他のセキュリティ機能に注力し、SOC を自社で提供しない戦略をとる EDR ベンダーも存在する。こうしたベンダーは MSSP にとって連携しやすいことから、協業関係を強化する動きが見られる。

IT バイヤーによるベンダー選定においては、ベンダーSOC 型と MSSP 型の違いを理解し、自社の体制やニーズに応じて選定することが重要である。ベンダーSOC 型では、EDR 製品の開発元企業が運用するため、アラートやログの理解力や、分析力がより高いことを期待できる。また、MSSP 型を利用した場合に追加的な時間を要する原因となり得る、インシデント対応時のベンダーSOC への再問い合わせの必要もない。情報集約基盤として EDR ベンダーの SIEM（Security Information and Event Management）を利用すれば、EDR ベンダーが提供する AI（Artificial Intelligence）などを用いた最新の自動化機能を利用しやすい。一方で、MSSP 型では、ネットワーク機器や ID 管理機能のセキュリティ監視を含む包括的な運用支援が可能である。特に、社内にセキュリティ人材を十分に確保できていない企業にとっては、EDR を含む複数の製品においてベンダーSOC 型を利用すると、製品ごとに問い合わせ先が分かれることから情報集約の面で課題となり、運用負荷も高まる。また、オンプレミスのサーバーの障害監視やネットワークの利用状

況の監視などのセキュリティ以外の運用も MSSP に一元化することで、運用の効率化を図れる場合も多い。

ベンダー間の競争領域の観点では、独自の脅威インテリジェンスや自動化機能は、MDR サービスにおける主要な差別化要素となっている。MSSP も独自の脅威インテリジェンスの収集や自動化技術の開発に注力している。一部のベンダーは、独自に収集した脅威情報の外部販売や、情報セキュリティのコミュニティへの共有を行っている。これらの脅威情報は、購入などを通じて他のベンダーでも入手可能であるが、情報を自ら収集しているベンダーは、当該情報をいち早く活用でき、対処方法の検討にも迅速に着手できる利点がある。自動化機能の活用の観点では、以前からある SOAR（Security Orchestration, Automation and Response）のプレイブックなどを用いた対処ではベンダーの経験が成果に直結する。長年の運用経験に基づき、大規模なプレイブックを構築しているベンダーもある一方で、そうしたプレイブックを提供できないベンダーもある。Generative AI（生成 AI）や AI エージェントの活用の観点では、AI を活用した自動化に積極的に取り組み、SOC 業務の完全自動化を目指すベンダーもあれば、アナリストによる対処の補助としての文章作成の自動化などの活用に留まるベンダーもある。IT バイヤーによるベンダー選定において、こうした点の技術的優位性と MDR サービスへの適用状況を見極めることも重要である。

IDC MarketScape ベンダー選定の基準

本調査レポートは、国内マネージドセキュリティサービス市場において MDR サービスを提供するベンダーを取り上げた。選定基準は以下のとおりである。

- 国内市場において MDR サービスを過去 12 か月以上提供している。
- 国内の当該サービス市場の売上額が 5 億円以上である。
- 当該サービスを、マネージドセキュリティサービスにおける主要な提供ソリューションの一つと位置づけている。

2025 年 9 月 10 日時点で一般に提供されている製品や機能を評価の対象としている。また、MDR サービスの定義は後述する。

IT バイヤーへの提言

本調査レポートのベンダー評価指標や評価内容を踏まえて、IT バイヤーが MDR サービスの選定時に考慮すべき項目を以下に示す。

- **EDR 製品と MDR サービスを連動して選定すべきである**：EDR 製品はベンダーごとに検知精度や対応機能に違いがあるため、自社のセキュリティ要件に合致した EDR 製品を注意深く選定することが重要である。加えて、候補となる EDR 製品を監視対象としてサポートする運用サービスの選定も併せて行うべきである。運用サービスの選定においては、ベンダーSOC 型と MSSP 型の違いや、MSSP によるサービス内容の違いを意識すべきである。軽微なトリアージ対応のみを求め、コスト効率を重視するのであれば、限定的な対応を安価に提供する MSSP 型でも十分な効果を得られる。一方で、高度な分析や迅速な対応を求める場合には、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を自社で提供できる MSSP 型や、ベンダーのセキュリティアナリストと直接対話できるベンダーSOC 型が適している。IT バイヤーによっては、セキュリティ以外の製品とのバンドル契約によるコストの最適化のみを重視し、セキュリティ機能の評価を十分に行わずに EDR の選定を進める場合も多い。セキュリティレベルの向上のためには、EDR 製品のセキュリティ機能に関して妥協できないポイントを見極め、そうした条件に合致する EDR 製品に対応可能な MDR ベンダーの中から、MDR サービスベンダーを選定すべきである。

- **監視範囲とサポートレベルが将来変わる可能性を前提に、運用範囲の拡張を見据えた選定を行うべきである**：MDR サービスの選定においては、現時点の要件だけでなく、将来的な監視対象の拡張や運用体制の変化を見据えた柔軟性のある選定も重要である。たとえば、現在は EDR 中心の監視であっても、ID 管理、クラウド、OT 環境などを将来監視対象に追加する可能性がある場合、統合的な監視体制を提供できる MSSP 型を選定しておく方が適している。一方、EDR ベンダーが提供する AI を用いた機能の進化を見据え、将来的に実現が見込まれる高度な機能をいち早く利用したい場合には、ベンダーSOC 型が有効であることも多い。IT バイヤーは、単に現在の要件に合致するかどうかだけでなく、「どこまで拡張可能か」「どこまで連携可能か」「どこまで進化するのか」といった将来の運用設計における柔軟性や、機能の拡張性を軸に、ベンダーを評価することが重要である。こうした観点で選定を行うことで、初期導入コストだけでなく、将来的な運用効率の向上や追加投資の適正化にもつながる。
- **海外拠点におけるサポートの現地対応力を評価すべきである**：近年発生しているセキュリティインシデントでは、管理が行き届きにくい海外拠点に起因するケースも多く存在する。海外拠点が存在する企業において、そうした拠点のセキュリティレベルを底上げし、グローバルで統一されたツールやポリシーを適用することは、全社的なリスク管理において不可欠である。特に、現地語での対応、現地時間での即応、法規制への理解といった現地対応力は、インシデント発生時の初動対応や継続的な運用において極めて重要である。ベンダーによっては、海外拠点におけるサポートレベルが限定的な場合もあり、現地に専門人材や SOC 拠点を持つかどうか、現地語でのサポートが可能か、現地の法規制や文化的背景に配慮した対応ができるかといった観点で評価する必要がある。また、グローバルで統一されたツールやポリシーの適用を進める際にも、現地の技術支援体制が整っていなければ、導入や運用が滞るリスクがある。IT バイヤーは、自社の拠点の展開状況に応じて、現地対応力のあるベンダーを見極めることが重要である。

ベンダープロフィール

本セクションでは、本調査レポートにおいて分析対象とした Accenture（アクセンチュア）に対して、IDC MarketScape モデルに基づいて「戦略」および「能力」の評価を行った結果をまとめている。また、評価基準に含まれない項目についてもベンダーの特徴を表している内容について言及している。

Accenture（アクセンチュア）

アクセンチュアは、「IDC MarketScape: Japan Managed Detection and Response Services 2025 Vendor Assessment」において、リーダー（Leaders）カテゴリーのポジションとなった。

アクセンチュアは、戦略立案などのビジネスコンサルティングを主軸とし、システムの実装、運用までを一貫して提供できる体制と併せて、ビジネスとテクノロジーの両面から企業の課題解決を支援するグローバルファームである。

アクセンチュアが提供している MxDR（Managed Extended Detection and Response）サービスは、構築が容易でありながらも多様な環境に対応することを目的としたモジュラー型の設計となっている。MxDR において運用サービスを提供する SOC を、東京を含む世界 23 か所に設置している。全世界で 3,500 人を超える検知、対応の専門家を有するほか、300 人を超えるサイバーインテリジェンスチームが、22 言語に対応する体制を整えている。世界中に設置した SOC によって、24 時間のサポートを実現しており、日本語によるサポートも選択可能である。

サービスメニューの観点では、個社ごとに要件を定めたプライベート SOC と、世界共通の標準化したサービスを提供している。標準化したサービスにおける情報集約基盤は Google SecOps を標準にしており、ほかに Splunk、Microsoft Sentinel などの複数の SIEM にも対応可能である。対応している EDR 製品は、CrowdStrike、Microsoft Defender、Cybereason などがあり、顧客側の要件に合わせて選択可能である。IT、OT（Operational Technology）、IoT（Internet of Things）を含むさまざまなテレメトリーに対応し、業界特化型のユースケースに関するコードや SOAR のプレイブックをまとめた Industry Content Library も提供する。インシデントレスポンスやデジタルフォレンジックに関しても、アクセンチュアは外部に依存せず、自社内に専門スキルを有する体制を整えている。感染源の特定や情報漏洩の分析など、法的証拠を伴わない実務的なフォレンジック対応を含め、緊急時の初動から復旧支援までを一貫して提供可能である。

AI に関する取り組みとして、アクセンチュアは 2024 年に、NVIDIA が提供するカスタム生成 AI モデルの構築プラットフォームである NVIDIA AI Foundry、NVIDIA AI Enterprise、NVIDIA Omniverse 上に、自社で開発した AI フレームワークである Accenture AI Refinery を構築した。Accenture AI Refinery を用いて、企業はドメイン固有の要素を持つカスタム LLM（Large Language Model）を構築して独自のビジネスニーズを反映できる。Accenture AI Refinery は、セキュリティ領域では AI エージェントを用いたワークフローの実現に役立ち、ペネトレーションテストや Web アプリケーション評価などの主要なセキュリティ業務の自動化や効率化を図ることが可能になる。

また、アクセンチュアは AI エージェントを用いたセキュリティサービスの自動化にも取り組んでいる。たとえば、脅威インテリジェンスにおいて現状では脅威情報のアップデートを定期的に行っているが、AI エージェントを用いて、更新のプロセスを自動化することによってリアルタイムで行うことを目指している。こうした機能の開発においては、パートナーとの協業に加え、インド、イスラエルなどの拠点において自社開発も行っている。セキュリティ運用における AI エージェントの活用の観点では、まずは初期対応者が行う難易度の低い業務を完全自動化することを目指している。具体的には、AI

のアドバイスを受けることで、誰もが熟練作業者並みの高度な業務の実施が可能になる取り組みなどである。将来に向けて、AI による支援を前提とした次世代型 SOC の構築を目指している。

M&A の観点では、アクセンチュアは過去 9 年間にセキュリティ専門企業を 18 社買収しており、その中には MNEMO Mexico、Innotec Security、Navisite、6point6、Sentor、Openminded、Morphus、Real Protect などが含まれる。2020 年にはサイバーセキュリティコンサルティング会社の Context Information Security や、IT および OT 分野の評価やテスト、システム運用サービスを提供する Revolutionary Security を買収した。また、同年にシマンテックからはサイバーセキュリティサービス部門を買収し、人的資源を強化している。

強み

MDR ソリューションとビジネスコンサルティングを組み合せることで、セキュリティ対応を企業の業務や経営戦略と整合させるアプローチを取っていることが強みである。CISO（Chief Information Security Officer）支援、GRC（Governance, Risk, and Compliance）強化、セキュリティ投資の優先順位づけなど、戦略的な支援を通じて、セキュリティ施策の位置づけを技術領域に留めず、組織全体のリスク管理やレジリエンス向上と結びつけることを志向している。さらに、AI の活用においては、AI エージェントを用いた脅威ハンティングや初動対応の自動化などの取り組みを進めている。また、グローバルで多くの拠点に展開している SOC から多言語のサポートを行う体制を整えることで、特に海外拠点を持つ大企業に対しては、MDR に加えて IT ガバナンス強化の支援を強みにつなげている。

課題

価格競争への対応が課題となり得る。高付加価値型サービスを志向する一方で、価格競争が激化する市場においては、コスト面での柔軟性が必要な場面がある。

補遺／関連資料

IDC MarketScape Graph の読み方

本分析に当たって、IDC では潜在的な主要な指標を能力と戦略の 2 つのカテゴリーに分けている。

Y 軸は、サービスメニューや顧客ニーズへの貢献度合いといったベンダーの現在の能力を示す。この能力は、現在の組織や製品の能力に関するものである。このカテゴリーに基づき、IDC アナリストは、市場戦略を遂行する上で、こうした能力をどのように築き上げ発揮しているかを分析する。

X 軸は、ベンダーが 3〜5 年後の将来に顧客からの要求に応えられる度合いを示す戦略軸である。この戦略軸は、高度なレベルの意思決定や製品／サービス提供、顧客セグメント、事業に関する計画、3〜5 年後の顧客への製品／サービス提供計画に関するものである。

バブルの大きさは、2024 年におけるベンダー各社の国内 MDR サービス市場における売上を基に、相対的な大きさを算出し、かつ、グラフの見やすさを考慮して総合的に指標化したものである。

IDC Marketscape 調査方法

IDC MarketScape の評価基準、重み付け、ベンダースコアは、市場やベンダーに関する十分な調査に基づいた IDC の判断によって設定されている。IDC アナリストは、標準特性の範囲を定め、その基準に基づき、市場のリーディングベンダー、市場参入ベンダー、エンドユーザーとのインタビュー、分析、調査を通して、ベンダーの評価を行っている。市場の重み付けは、各市場に関するユーザーインタビュー、バイヤー調査、IDC の専門家で構成される委員会のレビューに基づき行われている。IDC のアナリストは、詳細な調査、ベンダーインタビュー、公開情報、エンドユーザーからの情報、個々のベンダーのスコア、ポジショニングの分析結果に基づき、正確で一貫性のあるベンダー評価を行っている。

市場定義

MDR（Managed Detection and Response）サービスは、現在、一般的なものとなっている高度かつ迅速なサイバー攻撃から組織を保護するために、統合サービスとして提供するものである。MDR サービスの提供事業者は、顧客がすでに保有している機能と、サイバーセキュリティパートナーが提供するツールやサービス、ならびに自社の知的財産を組み合わせて MDR サービスを展開することが可能である。

一部のプロバイダーは、MDR サービスの技術的要素としてサードパーティの XDR（Extended Detection and Response）プラットフォームを活用し、それに自社のサイバーセキュリティ専門家による実務的なサービスを組み合わせることで、MXDR（Managed XDR）サービスとして提供している。また、MDR サービスは、プロバイダーの訓練されたサイバーセキュリティスタッフによって、24 時間 365 日体制のリモート SOC（Security Operation Center）から提供するものである。

MDR サービスの利用形態は組織によって異なり、特に大企業と中小企業の間で大きな差異が存在する。大企業では、MDR を共同管理型で利用する傾向がある。この形態には、MDR サービスの提供事業者が Tier 1 および Tier 2 の機能を提供し、顧客が Tier 3 のサポートを担当するケース、あるいはその逆に顧客が Tier 1 および Tier 2 を担当するケース、または対応をライフサイクル全体で混在させるケースなどを含む。

参考資料

関連調査

- *国内セキュリティサービス市場予測、2025 年～2029 年：AI とプラットフォーム化がもたらす構造的転換*（IDC #JPJ52496025、2025 年 5 月発行）
- *IDC FutureScape: Worldwide Security and Trust 2025 Predictions - Japan Implications - Positioning for Success - Opportunities for Tech Sales and Marketing Leaders*（IDC #JPJ52159025、2024 年 12 月発行）

- *2025 年国内 MDR 市場動向：セキュリティ製品のプラットフォーム化と AI のセキュリティサービスへの影響*（IDC #JPJ52496124、2025 年 1 月発行）
- *IDC Market Glance: Japan Managed Security Services, 4Q24*（IDC #JPJ52496424、2024 年 11 月発行）

Synopsis

本調査レポートは、国内 MDR（Managed Detection and Response）サービス市場における主要ベンダーに対して、IDC MarketScape モデルに基づいて「戦略」および「能力」の評価を行い、その分析結果を報告するものである。

国内 MDR 市場は、2020 年頃から EDR（Endpoint Detection and Response）の普及を契機に急速に拡大してきた。EDR 導入によってアラート対応の負荷が増加し、企業の運用支援ニーズが高まったことが、MDR サービスの需要を押し上げた一因である。国内 MSSP（Managed Security Service Provider）が自社の SOC（Security Operation Center）サービスとセキュリティ製品ベンダーの EDR 製品を組み合わせて提供するケースに加え、現在では EDR ベンダー自身が SOC を構築し、直接サービス提供を行うケースが増加している。

「IT バイヤーは、MSSP が SOC を提供する MDR と、EDR ベンダーが SOC を提供する MDR の違いを理解し、自社の体制やニーズに応じてベンダーを選定すべきである。その際、脅威インテリジェンスの収集能力や、AI（Artificial Intelligence）による自動化機能に重点を置いて評価することが重要である」と、IDC Japan、Infrastructure & Devices のリサーチマネージャーである山下 頼行は述べている。

IDC 社 概要

International Data Corporation（IDC）は、IT、通信、コンシューマー向け IT 分野に関する調査／分析、アドバイザリーサービス、イベントを提供するグローバル企業です。1964 年の設立以来、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。現在、110 か国以上を対象として、1,300 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査／分析および市場予測を行っています。IDC は、IDG（インターナショナル・データ・グループ）の系列会社です。

IDC Japan

IDC Japan（株）〒 150-6139 東京都渋谷区渋谷二丁目 24 番 12 号
81.3.6897.3812
Twitter: @IDC
blogs.idc.com
www.idc.com