IDC MarketScape

IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment

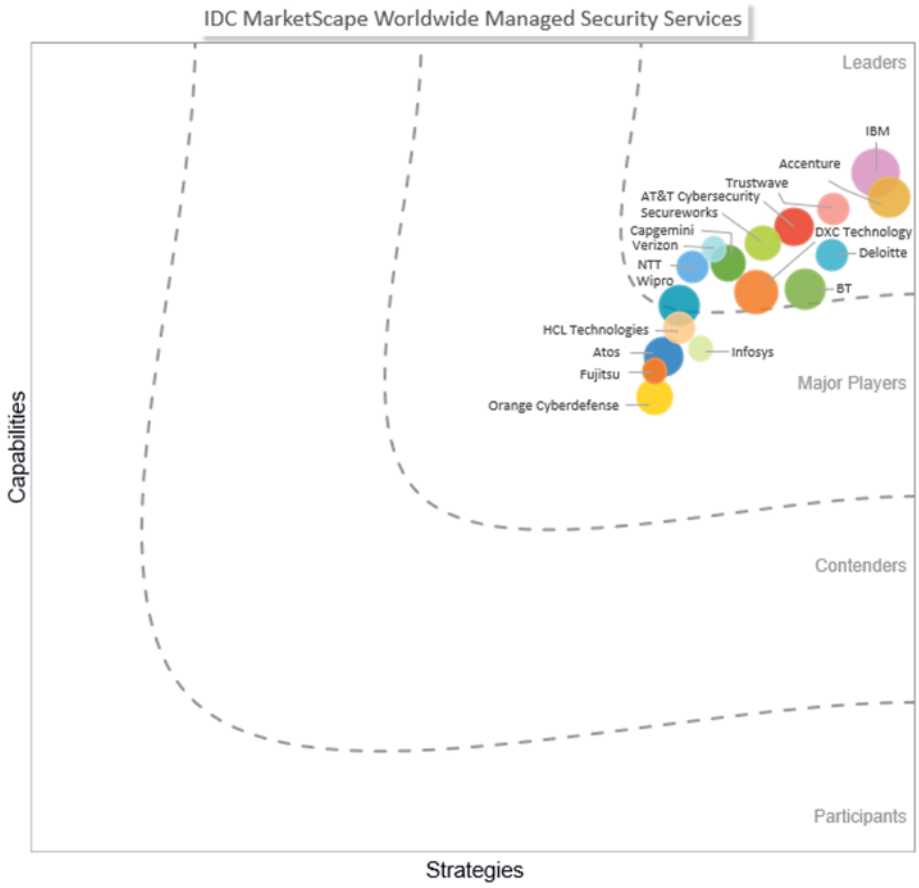
Martha Vazquez

THIS IDC MARKETSCAPE EXCERPT FEATURES NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Security Services Vendor Assessment



Source: IDC, 2020

Note: 詳細な調査方法、市場定義および採点基準については「補遺」のセクションを参照

September 2020, IDC #US46235320e

調査概要

本調査レポートは、『*IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment*（IDC #US46235320、2020 年 9 月発行）』の Excerpt（抜粋）版である。本 Excerpt には、Figure 1 に加え、「IDC の見解」「IDC MarketScape ベンダー選定の基準」「IT バイヤーへの提言」「ベンダープロフィール」「補遺／関連調査」「参考資料」のセクションのすべての内容、または一部が含まれる。

IDC の見解

マネージドセキュリティサービス（MSS）市場は、急速な進化を続けている。特にこの 1 年間は、社会や経済が混乱した時期にもかかわらず MSS プロバイダー（SP）各社は好調を維持している。IDC は 2020 年、企業における最新の攻撃への防御対策を支援するために、サービスプロバイダー各社がサービス、テクノロジー、手法、プロセスをどのように変化させているかを調査した。2020 年は COVID-19 パンデミックの影響によって非常に興味深い年となっており、IDC は現在のパンデミックに限定したプロバイダーの対応評価は行ってはいないが、世界中の企業のニーズが急速に変化していることから、評価の焦点に変化が生じていることは確かである。今回のパンデミックは、企業に対し、一歩下がって現行のセキュリティ機能を見直すと共に、新たに出現したリモートワークのサポートに必要なセキュリティ機能についての検討を促した。

パンデミック以前にも、サービスプロバイダー各社は企業のセキュリティに対する考え方を巡って重要な変化を経験し、検知と対応（Detection and Response）の機能を獲得する必要があった。もはや企業の関心は、セキュリティ製品の管理や、ポリシー、ルールセットの管理を求める、あるいはコンプライアンス規定の遵守だけを求める時代ではなくなっている。ただ、これらの機能が重要ではなくなったという意味ではない。その代わりに、企業はサービスプロバイダーに対し、インシデント対応時間の短縮や、最新の攻撃に対する改善対策の提供を求めている。さらに企業は、自社のセキュリティ成熟度やリスクの把握に悪戦苦闘している。サイバーセキュリティの成熟度向上に苦心する企業は、攻撃が発生した際にどのように備えておくべきかあらかじめ策を講じておくため、ビジネスや戦略の観点からもセキュリティを考えている。

セキュリティサービスプロバイダー各社は、さまざまな環境（例：マルチクラウド、エッジ、オンプレミス）から流入するデータを理解し分析できるサイバーセキュリティ専門家が不足していることから、脅威インテリジェンス、機械学習（ML）および AI（Artificial Intelligence：人工知能）、自動化、分析などのテクノロジー分野への投資を増やしている。こうした新分野への投資を組み合わせることで、人間よりも迅速に少ないエラーで処理できるスケーラビリティも企業にもたらしている。実際、IDC の調査レポート『*Key Findings: 2019 U.S. Managed Security Services Survey Results*（IDC #US45632819、2019 年 11 月発行）』では、セキュリティサービスのアウトソーシングに対する主なニーズは、高度なセキュリティ脅威からの保護、24 時間 365 日のサポート、可用性とパフォーマンスの向上につながるセキュリティ専門知識、新たなセキュリティテクノロジーの利用であるとしている。

IDC は、以下の各分野が MSS 市場を牽引し、ベンダー各社のマネージドサービスを差別化し、より価値のある内容とする機会を提供すると考えている。

- 複雑化する IT 環境を広範囲にカバーするマネージドセキュリティサービス
- 巧妙化する脅威に対する可視性を高め、プロセスの自動化を促進する先進的なテクノロジーの利用
- 柔軟で満足のいく教育研修期間、手法、手順の提供
- マネージドサービスプラットフォームで提供される高レベルなオーケストレーション、自動化、製品／サービス間のオープンな連携機能

- さまざまな地域に偏りなく配置されたセキュリティオペレーションセンター（SOC）による、フォローザサン（FTS：follow-the-sun）体制での 24 時間 365 日でのグローバルなセキュリティサービスの提供
- マルチクラウド環境をシームレスに稼働させる、クラウド監視、可視性、管理機能の実現
- ハイレベルなカスタマーサポート、専門知識、満足度
- 顧客の要望に合わせたサービスのカスタマイズと柔軟な導入モデル
- 顧客の意向に沿ったサービス価格モデルの構築
- カスタマーポータルの機能拡充と、モバイルアプリや経営幹部向けのレポートテンプレートなどの強化
- 優秀なセキュリティ人材の獲得と維持

IDC MARKETSCAPE ベンダー選定の基準

IDC は 2020 年、IDC MarketScape モデルに基づき、MSS をグローバルに提供する 17 のサービスプロバイダーと、そのサービスを利用している 20 以上の顧客企業を対象に調査を行った。グローバルに MSS を提供するサービスプロバイダーは多数存在するが、今回の評価対象ベンダーは、グローバルでサービスを提供すると同時に、以下に示す特定のサービスと基準を満たすことを条件としている。

- **MSS ライフサイクル全体に渡るサービス提供能力**：各サービスプロバイダーは、フルサービスの MSS を提供する能力を有していること（MSS の説明は「補遺」のセクションを参照）。
- **売上高**：各サービスプロバイダーは、2019 年のグローバルにおける総売上高が 1 億 7,000 万ドル以上であり、世界各地に 5 拠点以上の SOC を配備していること。
- **地域におけるプレゼンス**：各サービスプロバイダーは、南北アメリカ、EMEA（Europe, the Middle East and Africa）、APAC（アジア太平洋地域）の 3 つの地域で、MSS の提供が可能であること。

IT バイヤーへの提言

マネージドセキュリティサービスの契約を検討している企業は、自社の IT 環境が流動的であることを認識しており、特に最近のパンデミック期においては環境が絶えず変化しているため、これまでにないビジネス課題が生じている。セキュリティ対策のアウトソーシング先となるプロバイダーを評価するに当たって、企業は自社の IT 要件に対応できるセキュリティサービスプロバイダーをさまざまな角度から慎重に把握する必要がある。

外部のサービスプロバイダー選択の際に、セキュリティサービス機能のポートフォリオ、専門知識とサービスのサポート、教育研修プロセス、ポータル機能、パートナーシップ、プラットフォームの開放性、導入オプション、価格設定の柔軟性など、確認すべき項目が多数ある。

今日のセキュリティ環境は刻々と変化しており、テクノロジーは急速に進化している。そのため企業は現在だけでなく今後を見据えたサービスの評価が必要である。将来的に提供されるサービスが、予測されるビジネスの変化やコスト予測に沿ったものかどうかを確認することが重要である。プロバイダーの乗り換えは、コストが高く混乱を招きやすいため、セキュリティサービスのアウトソーシングを行う際には、バイヤー側は最適なプロバイダーを慎重に見極める必要がある。顧客満足度調査、価格ベンチマーク、ユースケース、概念実証、ベストプラクティスを提供できるプロバイダーは、意思決定プロセスにも役立つ可能性がある。

2020 年、IDC では、通信事業者、クラウドプロバイダー、システムインテグレーター、付加価値再販業者（VAR：Value-Added Resellers）、セキュリティ製品サプライヤー、コンサルティング企業など、セキュリティサービスプロバイダーが、MSS プロバイダーとして、あるいはマネージド

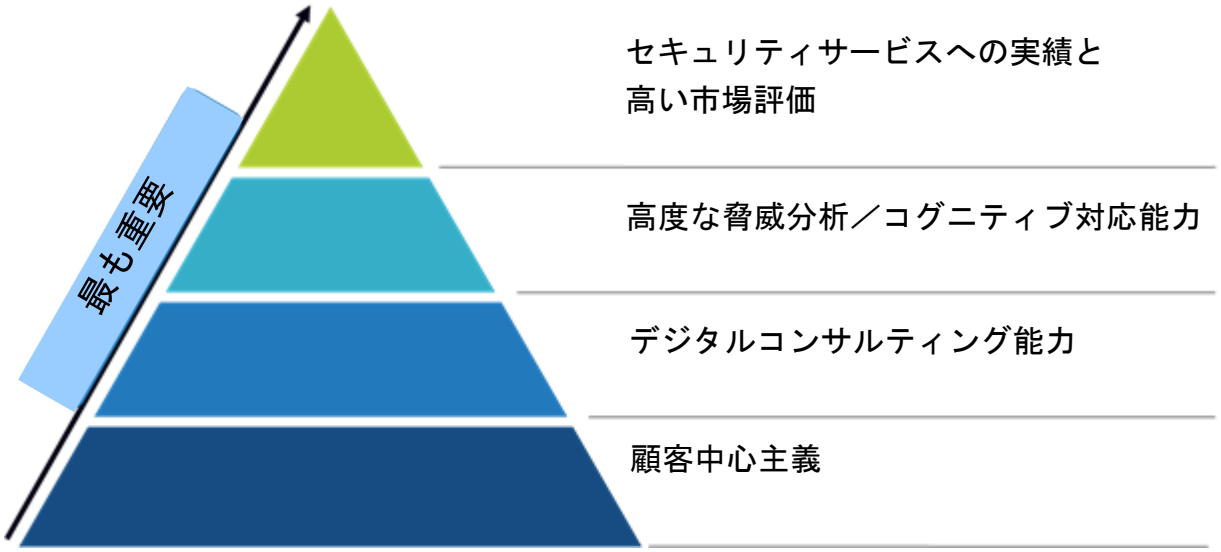
ディテクション&レスポンス（MDR）プロバイダーとして、MSS 市場に続々と参入する状況を確認している。これらのプロバイダーはいずれも、差別化された価値、サービス、サポートを提供している。企業が自社のアウトソーシングのニーズに合わせてプロバイダーを評価する際、選択肢の幅広さは適切なサービスプロバイダーを選ぶための評価プロセスに悪影響を及ぼしがちである。さらに、攻撃対象の拡大、リモートワーク、IT インフラストラクチャの複雑さなどを考慮して理解する必要がある。これらのセキュリティサービスのバイヤーは、セキュリティに関する戦略的な意思決定と、健全なセキュリティ態勢の維持に貢献するパートナーの選択に向けて、見識を養う必要がある。

IDC が 2019 年に実施したユーザー調査「*Managed Security Services Survey*」では、企業が MSS プロバイダーを選択する際に、高度な脅威に迅速に対処するために最も重視する要件を質問したところ、以下の 4 項目を挙げている。セキュリティサービスの提供を市場から高く評価され評判が良いこと、高度な脅威分析／コグニティブ対応能力、デジタル分野に強いコンサルティング能力、顧客志向である（Figure 2 を参照）。

FIGURE 2

次世代 MSS プロバイダーに求められる主な要件

Q.　　未来思考の MSSP に求められる要件とは?



n = 402

Source: IDC's Managed Security Services Survey, January 2019

適切なプロバイダーの選択は極めて重要であり、MSS のバイヤーは、プロバイダーを選択する際には、自社の IT 要件、地域、業種、全体的な戦略的ビジネス目標を考慮する必要がある。企業がパートナープロバイダーを選択する際、以下の点を留意することを IDC は推奨する。

- **MSS ポートフォリオの幅広さ**：ローエンドのサービスから、カスタマイズタイプのマネージドセキュリティサービスまで提供するなど、幅広いマネージドサービスプロバイダーが存在する。したがって、企業の IT 要件を満たす多様なサービスをすべて評価することが重要である。この市場でバイヤーは、ファイアウォール、IDS/IPS、セキュリティ情報およびイベント管理（SIEM）、脆弱性スキャン、セキュアメッセージングなど、従来のセキュリティ対策を探そうとしているのかもしれない。本調査レポートに掲載したプロバイダーはいずれも、これらのサービスをすでに提供している。しかし、これらのサービス

は、アイデンティティ／アクセス管理、脅威インテリジェンス、Webアプリケーションスキャン、マネージドディテクション&レスポンス、マネージドSOC、脆弱性管理／リスクモニタリングなど、より進んだサービスに拡張されている。さらに、MSSプロバイダーは、インシデントレスポンス（IR）、フォレンジック、その他のデジタルコンサルティングなど、セキュリティ対策を補うサービスの提供も開始している。したがって、企業のセキュリティ態勢に応じて、セキュリティ対策のさらなる強化を支援できるプロバイダーを選択することが望ましい（Figure 4を参照）。

- **デジタルコンサルティング能力**：セキュリティ課題への対応を計画するに当たり、単に「最新の」「輝かしい」テクノロジーを実装するだけでは十分ではない。堅実なセキュリティ対策には、人、プロセス、テクノロジーの評価を含む包括的なアプローチが必要である。本調査レポートに掲載したプロバイダーの多くは、企業が、インベントリー、資産、データ、セキュリティプログラムへのアクセスを支援することが可能であるが、企業にとって重要なことは、現在何を保持しており、今後何が必要になるかを理解することである。多くのサービスプロバイダーが、補完的サービスとしてデジタルコンサルティングを提供しており、企業のデジタルな第3のプラットフォームテクノロジーのセキュリティへの活用や戦略的目標の達成について企業を支援する。IDCのユーザー調査「*Managed Security Services Survey*」（前出のFigure 2を参照）では、企業は、先進的なMSSプロバイダーは、強力なデジタルコンサルティング機能を提供すべきであると考えている。企業は現在のセキュリティ対策状況を評価し、ギャップを明らかにした上で、協力してセキュリティプロセスの構築を継続できるプロバイダーやベンダーを選択する必要がある。
- **マネージドディテクション&レスポンス**：IDCが2020年に実施したユーザー調査「*MSSP and MDR Survey*」では、回答者はサービスプロバイダーと提携する際に必要な5つの要因の一つとして、先進のセキュリティツールやテクノロジーの利用が可能であることを挙げている。そのため、MSSプロバイダーを探している企業は、セキュリティポジションを強化するために、プロバイダーがどのような先進的ツールを使用しているかを検討する必要がある。たとえば、エンドポイントの脅威検知（TD）ツール（EDR／クラウドネットワーク）、SIEM、脅威インテリジェンス（Threat Intelligence）、脅威ハンティング(Threat Hunting）、脅威対応とオーケストレーションの自動化、ビッグデータとアナリティクス、ML（Machine Learning）/AI（Artificial Intelligence）、インシデント分析、リモートインシデント対応などの機能が統合されたMDRがMSSの次なる進化形となっている（「市場定義」のセクションを参照）。レスポンス機能は、多くのサービスプロバイダーにとって差別化要因になると予測される。高性能のインシデントレスポンスを実行するには、時間とスキルが必要とされるが、多くの企業はそれらを持ち合わせていない。したがって、詳細な調査分析のためのさまざまなレベルのサポートに加え、封じ込め、修復、今後の軽減策に関する高度なガイダンスを提供できるプロバイダーを探すことが、評価に当たり重要な領域である。
- **脅威インテリジェンス、脅威ハンティングなど、その他の高度な機能**：サービスプロバイダーは既存のサービス内容を超え、脅威インテリジェンスなどの分野で深化している。脅威インテリジェンスは、すでにMDRなどの高度なサービスで重要なコンポーネントになっており、MSSやMDRサービスに統合されつつある。脅威インテリジェンスは、プロバイダーの専門知識やグローバルネットワークによって左右されるサービスである。多くのプロバイダーが深いレベルの共有機能（ネットワーク、エンドポイント、その他からの脅威データ分析）を提供することで、この分野の強化を続けている。業種や地域、攻撃ツール／戦術／手順に関する知見に富んだインテリジェンスが形成されており、単なるセキュリティ侵害インジケーター（IoC）を超えたものとなっている。分析を改善するため、サービスプロバイダーのデータセットを拡張し、最新の脅威を特定し、さまざまな既知のキャンペーンを把握する、より優れた方法が生み出されている。脅威インテリジェンスは、もう一つの重要な側面である脅威ハンティングの分野に組み込まれている。一部のサービスプロバイダーは、統合型の脅威インテリジェンスのフィードから、人間が主導する脅威ハンティングや自動化された脅威ハンティングを定常的に使用し、その結果に基づいてプロセスやプレイブックを作成している。
- **エンドポイント、ネットワーク、クラウドに広がる可視性を提供するプラットフォーム**：セキュリティパートナーは、コアプラットフォームだけでなく、先進テクノロジーの

利用についてもイノベーションを発揮することが求められる。インシデント発生時におけるディテクション&レスポンスのライフサイクルへの完全な可視性を提供できるベンダーを選ぶことが、企業にとって真の価値となる。サービスプロバイダーは、単一のプラットフォームにさまざまなタイプのデータをより多く取り込む機能を、コアプラットフォームに継続的に追加している。インフラのクラウドシフトによって複雑性が増しているが、IoT（Internet of Things）や OT（Operational Technology）、その他のテクノロジーも追加されており、考慮する必要がある。IoT および OT インフラの導入によって、新たな脅威がもたらされており、IT デバイスと IoT/OT デバイスでは、レスポンスやリスク緩和のための手法が大きく異なるため、CISO はこれらの課題に備えておく必要がある。脅威の増加と共に拡張されるセキュリティ機器からのデータの量が増加する現在、サービスプロバイダーは強化された AI/ML 技術を活用し、コグニティブサポートシステムを活用して、ディテクション&レスポンス機能のサービス向上に取り組んでいる。

- **オーケストレーション／自動化プロセスの統合**：サービスプロバイダーは、オーケストレーションツールや自動化ツールにいっそう注力し、セキュリティプラットフォームにこれらの技術を統合している。先進的な ML/AI と共に、オーケストレーションや対応の自動化などのテクノロジーは、サービスプロバイダー内 SOC の効率性を高め、アナリストによる脅威の優先度付け／分析／対応を迅速化している。自動化やオーケストレーションツールは、企業が従来よりもはるかに大きいキャパシティでの分析を可能にし、平均検出時間と平均応答時間（MTTR）の短縮につながっている。このような自動化の利用はサービス提供プロセスにも貢献し、それによって教育／トレーニングに必要な時間枠が短縮され、新しいサービス実装プロセスの標準化にも貢献している。
- **グローバル SOC の要件**：グローバル企業は、セキュリティプロバイダーのサービス詳細や SOC 運用が、自社の直接的な要件を満たすことを確認する必要がある。サービスプロバイダーは通常、MSS 機能を提供する SOC の数、所在地一覧を示すことで、マルチリージョン／グローバルなサービス提供能力を提示する。各 SOC の最初のシフト（業務引継ぎ）で、そのシフトの外部にある別の地域の IoC に対応できる方が、深夜を含む夜間シフトに頼ったインシデントの分析や対応を行うよりも、良い結果が得られる。これは 24 時間 365 日の「フォローザサン体制」を提供する上で重要なサービスである。
- **研究開発（R&D）への投資**：パートナーの選択に際しては、前述のように、先進のテクノロジーや進歩が極めて重要な部分である。先進的な考えを持ったセキュリティプロバイダーは、現在のサービスに投資するだけでなく、将来を見据えて、クライアントを何年にも渡って安全な状態に保つために何が必要かを検討し、研究開発のための予算を確保していなければならない。クラウドセキュリティ、IoT/OT インフラ、プレイブックの作成、自動化や平均応答時間の KPI 短縮に重要なテクノロジーに投資しているかどうかを確認する必要がある。OT と IoT のモニタリングと対応は、クラウドセキュリティの要件と共にいっそう重要になりつつあり、これらの分野におけるプロバイダーの現在と今後の投資について、評価する必要がある。
- **セキュリティの専門知識およびサポート**：プロバイダーのカスタマーエンゲージメントプログラムについて確認する必要がある。優れたセキュリティサービスプロバイダーは、サービスの実務を担当するサイバーセキュリティチームが、しばしば顧客のサイバーセキュリティチームの遠隔地のメンバーとみなされることを認めている。サイバーセキュリティチームの在職期間が、差別化要因として重要になりつつある。信頼されるセキュリティプロバイダーになるためには、人材維持と人材育成が重要である。バイヤーは、信頼のおけるパートナーとして、社内 IT チームの延長組織であるかのように行動することが可能なプロバイダーを選ぶ必要がある。顧客企業の IT 環境や課題をプロバイダーが理解していれば、推奨事項の提案や微調整を容易に行うことができ、セキュリティプロセスの各段階で継続的なガイダンスを示すことが可能になる。
- **クラウドセキュリティ戦略**：開発と機能拡張が継続的に進められている分野の一つにクラウドセキュリティがある。企業はかつてないスピードでクラウドに移行しており、プロバイダーによるクラウドセキュリティの統合に関する現状や、戦略から実装、運用までのライフサイクル全体にどのように統合されているかを確認する必要がある。マルチクラウドを前提とする柔軟なクラウドモデルを提供し、AWS（Amazon Web Services）、マイクロソ

フト、グーグルなどのプロバイダー環境で動作する能力は、企業ニーズの観点から重要である。これらの多様な IT 環境を移行、活用するための支援や、企業へ向けた提案を行えるサービスプロバイダーかどうかを評価する必要がある。

- **ポータルのレポーティングと機能**：顧客エクスペリエンスとサポートを強化する手段として、ポータルが引き続き利用されている。企業はポータルを確認し、各プロバイダーのさまざまな差別化要因についてデモを通じて確認する必要がある。先進的な考えを持ったサービスプロバイダーは、チケット処理やワークフロー分析をリアルタイムで提供し、エンドユーザーにとってベネフィットとなるモバイルアプリに投資を行っている。信頼性の高い可視化と分析ツールの提供に加え、強化されたレポート機能、リスク指標、セルフサービス、ライブサポート、認証は、いずれも快適な顧客エクスペリエンスを促進する。

ベンダープロフィール

ここでは、IDC MarketScape 調査で得られた特定のベンダーに関する IDC の主な調査結果について簡単に説明する。「補遺／関連資料」のセクションに示す各基準を用いて、すべてのベンダーを評価したが、ここでは各ベンダーの強みと課題を要約する。

NTT

NTT は、IDC MarketScape 全世界のマネージドセキュリティサービスに関する 2020 年度ベンダー評価において、リーダーに位置づけられた。

NTT は 2016 年、NTT グループ企業各社に分散していた MSS に特化したすべてのリソースと配信プラットフォームを統合した後、さらに 2019 年に組織再編成を行い、NTT Ltd という新しい事業体に 28 のブランドを統合した。2019 年 7 月に完了したこの統合によって、NTT Ltd は 4 万人を超える従業員を擁する 110 億米ドル規模の企業となった。

NTT は、SOC を 12 か所（APAC に 6 か所、欧州に 3 か所、米国に 3 か所）に展開している。これらの SOC は 24 時間 365 日体制であるが、すべてが一律のサービスを提供しているわけではない。所在地ではなく、主として提供する機能によって、ワークフローモデルが決定されている。一部の SOC は、脅威検知サービスに特化し、このサービスを 24 時間 365 日体制で提供する。それ以外の SOC は、脅威検知を必要とする地域内の顧客に対応しているが、SOC によるサポートは通常の営業時間内に限られ、時間外は 24 時間 365 日体制のいずれかの脅威検知 SOC にサポートが引き継がれる。一部の SOC には脅威検知能力がなく、クライアントはその次に担当する SOC からのサービスを受ける。このアプローチは、セキュリティデバイス管理、エンタープライズセキュリティモニタリング、脆弱性管理などの他のサービスにも適用されている。一部の SOC は、これらのサービスに特化して 24 時間 365 日でサービスを提供可能だが、その他の SOC は、サポートが通常の営業時間に限られ、その後は 24 時間 365 日体制のいずれかの SOC に引き継ぐ。

NTT は過去数年間で多くの企業を買収したが、現在はこれらのリソースおよびプラットフォームを 1 つに統合している。同社の MSS サービスは、個別のビジネス目標に合わせたものであり、サービスのライフサイクル全体の基盤となるものである。NTT は共通のサービス提供モデルと構造を通じて、すべてのサービスを可能な限り一元的に提供し、必要に応じてローカライズしている。NTT は、脅威検知、脆弱性管理、エンタープライズセキュリティモニタリング、デバイス管理の各サービスをモジュール化して提供している。このモジュール方式によって、顧客の要件に合わせた調整が可能であり、最終的に顧客に価値がもたらされる。また、NTT の MSS は、IT と OT のハイブリッド環境をサポートする。同社の高度な分析エンジンは、文字通り「藁の中から針」を検知する。これは「ブロックされたアラート」へのフォーカスを減らし、「不審な許可イベント」にフォーカスを移すことによって実現している。同社の高度な分析エンジンは、脅威インテリジェンスの相関、脅威ハンティング、機械学習フレームワークなどのコンポーネントで構成されている。

NTT によると、脅威検知サービスの拡張とイノベーションによって、脅威と確認済みのインシデントを明らかにする可視性と能力がもたらされている。この脅威検出は、常に攻撃者の一歩先を行き、顧客のセキュリティ態勢とリスクプロファイルをプロアクティブに管理するという NTT の価値提案を支えている。NTT の脅威検知は、顧客のサイバーレジリエンス、セキュリティ運用の成熟度、レスポンス能力を向上させるための効率化を実現し、同社の MSS サービスとの差別化を図っている。

NTT の脅威インテリジェンス機能は、社内外のソースに基づいており、これは企業が自前で構築することは難しいと NTT は考えている。このイノベーションの一例として、脅威検知分析エンジンは、脅威検知に用いられる独自仕様のカスタム IoC に基づいている。エンドポイントのディテクション&レスポンステクノロジーを強化する目的で特別に開発されたこの分析エンジンは、エンジンが持つネイティブの技術だけでなくカスタム IoC を使用することによって、インシデントを 70%の確率で検出する。多くの場合、これらの IoC は、ネットワークとエンドポイントのログイベントの高度な相関関係に基づいて開発される。管理下のデバイスによっては、エンドポイントフォレンジックや、疑わしいセグメントの封じ込めや隔離など、インシデントに関する高度な可視性を提供する追加のアクティビティを実行可能である。

NTT は 200 社を超えるテクノロジーパートナーと提携し、戦略的パートナーとの緊密な協力を通じて、共同イノベーションや新しい製品／サービスの共同開発を進めている。さらに NTT は、自社の能力を拡張して DevSecOps サービスなど新しいサービスを推進する目的で、WhiteHat Security を買収したほか、ShieldX などの革新的な企業に戦略的投資を行っている。

強み

顧客のフィードバックによると、NTT は最も分かりやすく、最も容易に提携できるベンダーの 1 社である。顧客の立場から見て、NTT の脅威インテリジェンスにおける専門性と高度な知識、および正確な検知能力は注目に値する。

NTT はグローバルな運用モデルと、ローカルな地域の特性に合わせた運用モデルでプレゼンスを確立している。NTT はセキュリティサービスのライフサイクル全体に対応した広範な MSS を提供している。顧客企業のセキュリティ態勢の構築を支援するために、MSS のコンポーネントをモジュール化して提供している。NTT は現在、脅威検知や OT など特定のニーズをターゲットにしたサービスパッケージを提供し、単一のサービスで IT と OT の両方に対応している。また、自動車業界向けに特化した SOC サービスなど、特定の業種に対応するサービスパッケージも提供している。価格モデルは柔軟性に富み、さまざまなサービスレベル、デバイスの種類、手法、ディスカウントが考慮され、提供される。ロードマップの観点では、NTT は価格モデルを効率化し、顧客にとってシンプルなものにすることを検討している。

NTT は継続的に研究開発に投資し、独自のツールやプラットフォームを開発している。同社は今後も引き続きプラットフォームに投資し、先進のテクノロジーの導入と、プラットフォームへのマルチベンダー統合のためのオープン API（Application Programming Interface）を導入し連携性を高め、自動化、オーケストレーションのレベル向上に取り組む計画である。

課題

NTT のマネージドセキュリティポータルには非常に優れた機能があるが、高度な分析と可視化のためのツールが不足している。コンプライアンスレポートに関しては、現時点ではまだ利用できないもののロードマップにはすでに含まれており、12～18 か月以内に顧客に提供される見通しである。さらに NTT は、脅威分析と可視化機能をポータルで強化することを示唆している。

どのような場合に NTT を検討すべきか

中～大規模の多国籍企業が、充実したローカルサポートを提供するグローバル通信事業者を希望する場合、MSS の要望を満たすために NTT を検討するとよいであろう。

補遺／関連資料

IDC MarketScape Graph の読み方

この分析の目的を考慮し、IDC では成功の尺度として重要と思われる要素を、機能と戦略の 2 つの基本カテゴリーに分けている。

Y 軸上の位置は、ベンダーの現在の能力、サービスメニュー、さらにベンダーの顧客ニーズへの適合度など、機能を中心に評価を反映している。機能カテゴリーは、会社と製品の現在の能力が中心である。このカテゴリーにおいて、IDC のアナリストは、ベンダーが選択した戦略を市場で実行できるようにするための機能をどこまで適切に構築、実現しているかをみている。

X 軸、すなわち戦略軸上の位置は、ベンダーの未来戦略と、顧客が今後 3 年ないし 5 年以内に要求する内容との整合度を示す。戦略カテゴリーは、ハイレベルな意思決定と、オファリング、顧客セグメント、今後 3〜5 年の間のビジネスマーケットプランについての基礎的な前提にフォーカスしている。

IDC MarketScape で、個々のベンダーを示すマーカーの大きさは、評価対象の市場セグメントにおけるベンダーのマーケットシェアを表す。

IDC MarketScape 調査方法

IDC MarketScape の基準の選択、重み付け、およびベンダースコアは、十分な調査に基づく、IDC の市場と個々のベンダーに関する判断を示す。IDC のアナリストは、市場リーダー、市場参入ベンダー、およびエンドユーザーとの体系化した議論、調査、取材によって、ベンダーの測定基準となる特性の範囲を調整している。市場の重み付けは、市場ごとに、ユーザーの取材、購買者調査、それぞれのテクノロジー市場を担当する IDC のエキスパートからの情報に基づいて行われる。IDC のアナリストは、詳細な調査やベンダー取材、公開されている情報、エンドユーザーの体験に基づいて個々のベンダースコアのベースとし、最終的に IDC MarketScape におけるベンダーの基本的な位置を設定して、各ベンダーの特性、行動、能力に関する正確で一貫性のある評価を行う。

市場定義

この調査の目的を考慮し、IDC はマネージドセキュリティサービス（MSS）を「リモートのセキュリティオペレーションセンター（SOC）から提供される、IT セキュリティ機能の 24 時間体制のリモート管理またはモニタリング」と定義している。この中には、顧客施設に導入されたセキュリティソリューションを監視するか、それとも顧客施設の外部にあるデータセンターでホスティングされるソリューションを監視するかを問わず、すべての MSS が含まれる。従来のマネージドセキュリティソリューションの枠を超えた新しいサービスが、MSS プロバイダーによって続々と提供されている。多くの場合、これらのサービスを利用する主な理由は、マネージド SOC などのさまざまなセキュリティ技術分野と、マネージドレスポンスサービスなどのさまざまなフェーズを含めて、セキュリティ運用を管理することである。

Figure 3 に、サービスプロバイダーを利用する最も重要な理由として、回答者が挙げた上位の回答を示す。IDC が 2020 年に実施したユーザー調査「*MSSP and MDR Survey*」では、セキュリティサービスプロバイダーを利用する顧客にはさまざまなニーズがあるが、最も多く挙げられている要因は、パフォーマンスと効率性の向上、検知および対応に要する平均時間の短縮、先進のセキュリティツール／テクノロジーの利用、すべてのセキュリティコントロールに広がる可視性の獲得、コンプライアンス要件への準拠であるとしている。

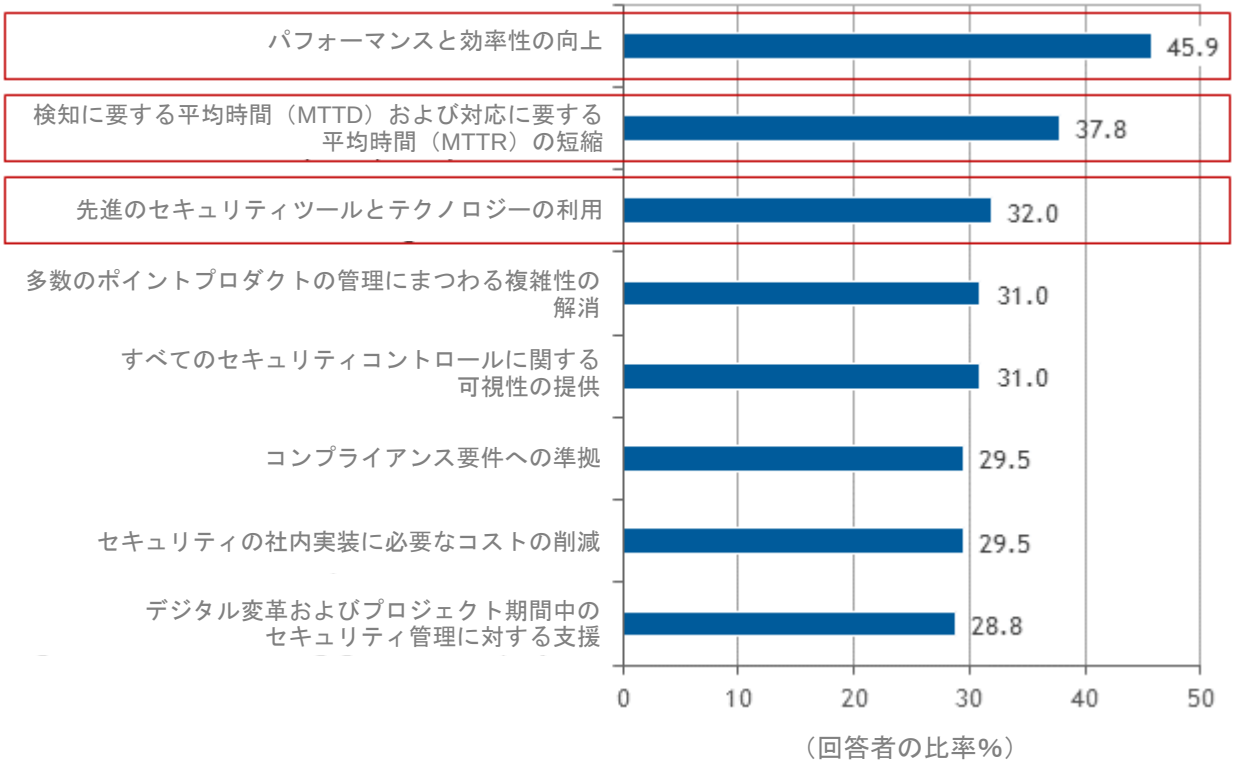
IDC が定義するマネージドセキュリティサービスとは、サードパーティが運営するセキュリティオペレーションセンターのリモートスタッフによって提供される、24 時間体制の IT セキュリティ機能のリモート管理／モニタリングである。パッチ管理、マネージドエンドポイント／ウイルス対策、マネージドファイアウォール／統合脅威管理（UTM）、マネージドセキュリティ情報／イ

ベント管理（SIEM）などの活動が、クラウドおよびマネージドオンプレミスデバイスで実行される。

FIGURE 3

セキュリティサービスプロバイダーを利用する主な理由

Q.　セキュリティサービスプロバイダーを利用する最も重要な理由5つを選択してください。



n = 410

基数 = 全回答者

Notes:

- この調査は、IDC Quantitative Research Group の管理下で実施された
- データの重み付けは行っていない
- 複数回答可
- サンプルサイズが小さい場合、解釈に当たって留意すべきである

Source: IDC's *MSSP and MDR Survey,* May 2020

企業におけるサイバーセキュリティプログラムの強化を支援するために、非常に多くのプロバイダーがマネージドディテクション&レスポンス（MDR）の提供を試みている理由を十分に理解するには、マネージドセキュリティサービスを提供するベンダーが、長年に渡ってどのように機能を進化させてきたかを知る必要がある。IDC は、さまざまな機能を分類した結果、MSS には現時点で 3 つのレベルがあると認識している。次項では、これら 3 つを説明する（『*MDR: The Next Generation of Managed Security Services*（IDC #US46427920、2020 年 6 月発行）』を参照）。

MSS 1.0

MSS の最初の導入は、境界またはエンドポイントのレベルで攻撃を阻止したいという、企業の初期の考え方を体現している。ファイアウォール設定の管理や、各種デバイスからのログの収集は、MSS プロバイダーやマネージド SP による初期のサービスの特徴である。ファイアウォールが統合脅威管理アプライアンス（UTM：Unified Threat Management）に置き換わるにつれ、サービスプロバイダーは、これらのデバイスで提供可能なアンチウイルス、侵入検知／防御、コンテンツフィルタリングなどの管理も担うようになった。その他に提供されるサービスとしては、パッチ管理、デバイスヘルスチェック、脆弱性スキャンなどの従来の MSS 機能も提供されている。

MSS 2.0

企業がデジタルトランスフォーメーション（DX）に着手し、ハイブリッド（クラウドとオンプレミス）の IT 環境への移行が進むにつれ、より先進的なサイバーセキュリティ機能の必要性が明確になった。セキュリティサービスプロバイダーは、サイバー犯罪者と対峙するための新しいセキュリティテクノロジーの採用を加速する必要に迫られた。ML/AI、ビッグデータとアナリティクス、自動化、オーケストレーションなどの先進的な技術は顧客を支援し、巧妙化する脅威を阻止するための技術的基盤を提供する。

一部の MSS プロバイダーが MSS 2.0 に深化するにつれ、侵害管理、アーキテクチャ／設計の評価、フォレンジック、インシデントレスポンスなど、補足的なセキュリティサービスが加わった。プライバシー／セキュリティ規制が厳格化する情勢の中で、政府やサードパーティによるコンプライアンス追跡に必要なコンプライアンスサービスが、サービスプロバイダーのメニューに加わっている。

MDR サービスによって成立する次世代の MSS 3.0

絶えず進化するサイバーセキュリティ市場で競争力を維持するため、詳細かつ先進的なディテクション&レスポンス機能の提供を巡って、サービスプロバイダー各社がかつてないほどの競争を繰り広げている。競争の激化に伴い、コンサルタント企業、インテグレーター、セキュリティ専業ベンダー、通信事業者、クラウド／ホスティング事業者など、さまざまな企業が続々と市場に参入している。これらの異種プロバイダーはいずれも、パートナーシップまたは独自技術の開発によって時代を先取りしている。市場が進化した結果、従来の MSS プロバイダーが果たす役割が成熟し、IDC がマネージドディテクション&レスポンスのプロバイダーやサービスと捉えている、次世代の MSS（MSS3.0）の領域まで拡大している。MSS のサブセットとしての MDR は、各種ツール、テクノロジー、手順、手法を組み合わせ、企業向けの完全なサイバーセキュリティライフサイクル機能を提供する。サービスプロバイダーは、クライアントの既存機能を、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、独自の知的財産と併用することによって、MDR サービスを展開できる。MDR サービスは、SOC 内のトレーニングを積んだプロバイダーのサイバーセキュリティスタッフによる遠隔サポートによって、24 時間 365 日体制で提供される。IDC は、本 IDC MarketScape のフォローアップレポートを発行し、マネージドディテクション&レスポンス機能を提供するこれらのプロバイダーについて検証する予定である。MDR に関する IDC MarketScape は、2021 年第 2 四半期に発行予定である。

参考資料

関連調査

- *Data Security and Threat Detection/Response Top of Mind in Both MSSP and MDR Evaluation*（IDC #US46762320、2020 年 8 月発行）
- *COVID-19 Implications for Security Services*（IDC #US46192319、2020 年 4 月発行）
- *Key Findings: 2019 U.S. Managed Security Services Survey Results*（IDC #US45632819、2019 年 11 月発行）

Synopsis

本調査レポートは、マネージドセキュリティサービス（MSS）を提供する全世界のプロバイダーについて、IDC MarketScape モデルによるベンダー評価を示すものである。評価では、MSS に対する現在の市場需要と予測される購買者のニーズを定めるための質と量、両方の特性を精査している。各ベンダーが同業者と比較してどこまで達成しているかを評価する。そして、包括的かつ厳密なフレームワーク、さらに短期的および長期的に、MSS 市場で成功するために最も重要と思われる主要な要因を明らかにするフレームワークに基づいて評価を行っている。

「企業は絶えることなく発生するセキュリティ脅威の管理／監視に加え、セキュリティ部門で入手した、増える一方の各種ツールの完全な実装／統合をサポートできるセキュリティ専門性を求めて悪戦苦闘を続けている。その結果、マネージドサービスと補足的サービスを含むセキュリティ専門性を提供し、今後の攻撃への準備、検知、対応を支援する MSS プロバイダーに企業の関心が集まっている。これらのサービスプロバイダーは、絶えず進化するサイバーセキュリティ市場で競争力を維持するため、詳細かつ先進的なディテクション&レスポンス機能の提供を巡って競争を繰り広げている。これらの多様なプロバイダーはいずれも、パートナーシップまたは独自技術の開発によって時代を先取りしている。市場が進化した結果、従来の MSS プロバイダーが果たす役割が成熟し、IDC が「MSS 3.0」と呼ぶ MSS の進化形に発展している。この中に、マネージドディテクション&レスポンスが必然的に含まれる。競争を繰り広げるこれらのプロバイダーが、どのようにして時代の先端を走り続け、セキュリティ環境における差別化要因を示し続けるかを見るのは興味深い」と、IDC インフラストラクチャサービスのシニアリサーチアナリストである Martha Vazquez 述べている。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・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。50 年にわたり、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、1,100 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 は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com