IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2020 Vendor Assessment

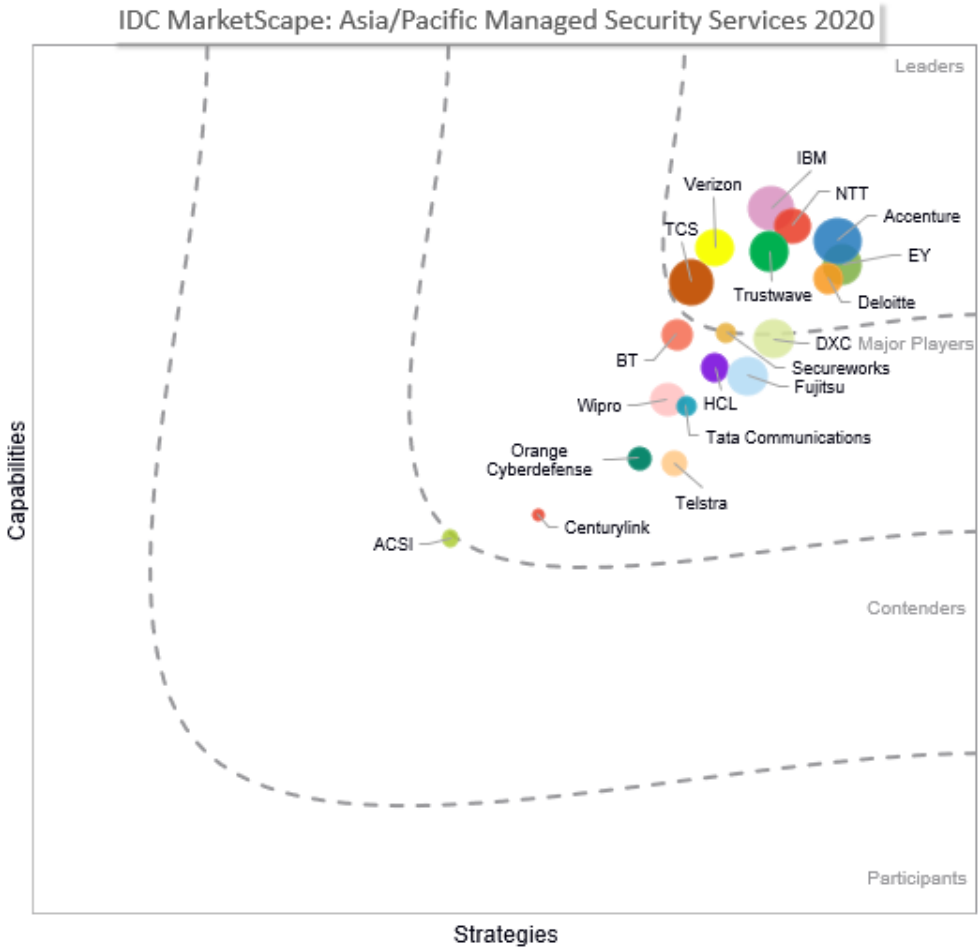
Cathy Huang James Sivalingam

THIS IDC MARKETSCAPE EXCERPT FEATURES: NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Asia/Pacific 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

February 2020, IDC #AP45547820e

IDC の見解

規制による圧力の高まりや、巧妙化する脅威という状況の下で、各業界のデジタルトランスフォーメーションが急速に進みつつある。多くの企業が、堅牢なセキュリティ体制を維持するのに苦心している。さらに重要な点として、サイバーセキュリティの重要性とインパクトが増大し、もはや単なる技術的な問題やコンプライアンス上の問題とはみなされず、経営レベルで検討すべきビジネス戦略上の事案になっている。全社的な対応策への認識不足、準備や覚悟の欠如は、事業活動および企業の社会的評価に深刻なダメージを及ぼしかねない。

それゆえに、CISO（Chief Information Security Officer）や IT セキュリティ責任者が経営会議に呼び出され、企業のセキュリティ戦略、セキュリティ投資の価値、サイバーリスクの最新動向などについて説明を求められるケースが増えつつある。多くの企業でセキュリティが単なるアドオン要素から戦略上の必須課題に昇格した結果、検知／レスポンスおよび脅威インテリジェンスなどをベンダーが提供するサービスの活用が検討され、マネージドセキュリティサービスに対する需要が増大している。こうした需要の増大は、各地域や各国におけるセキュリティ市場の成長と進化を促す。新規参入のプレイヤーが勢力拡大を試みる一方で、既存の市場リーダーが製品／サービスのさらなる拡充を図りつつある。アジア太平洋地域のマネージドセキュリティサービス（MSS）市場は、こうした新しい展開を背景に、活気のある競争の熾烈な市場になりつつある。同地域の企業にとって、そのメリットは非常に大きい。

IDC は、2019 年～2020 年にアジア太平洋地域で MSS を提供する 19 社のベンダーについて、IDC MarketScape モデルに基づく評価を行った。この評価では、現在の市場需要および MSS を利用するユーザーの期待事項に対応する広範囲のパラメーターを参照し各社を調査した。具体的には、MSS 製品／サービスの対象範囲、ポートフォリオの利点、脅威ライフサイクル対応状況、クラウドセキュリティ、提供モデル、コスト管理、市場遂行、知名度、ソートリーダーシップ、イノベーション、顧客満足度、顧客アドボカシーが含まれる。一次調査、各ベンダーへの詳細なインタビュー、顧客の意見調査を通じて、IDC は市場における各サービスプロバイダー（SP）の強みと課題を明らかにした。この調査で浮き彫りになった注目すべきテーマは以下の通りである。

- **さまざまな成熟度、さまざまな目標**：アジア太平洋地域の市場は、さまざまな国、言語、文化で構成されており、非常に多様性の高い市場である。そのため、業界や業種、企業によってデジタル成熟度のばらつきが非常に大きい。企業が MSS プロバイダーとの関わりにおける目的や動機も、市場全体で見ると成熟度に応じて大きく異なっている。IDC は、規制要件が厳しい業界に属する企業を主とした成熟度の高い企業は、業界の置かれている状況や事情に詳しいプロバイダーの専門知識、IP（Intellectual Property）、フレームワーク、プロセスを活用し、社内のセキュリティ部門を補強したいという意向が強いことを本調査結果から確認した。対照的に、成熟度の低い企業は、セキュリティおよびコンプライアンス関連業務の全部ではないが大部分を MSS プロバイダーに外注委託する意向が見られる。したがって、エンドツーエンドの包括的なポートフォリオを備え、業種毎の専門知識を有するベンダーは、両方のカテゴリーの顧客を獲得するのに有利である。
- **顧客中心主義という共通点**：成熟度の違いによるこれら 2 つの顧客グループは、動機や目標がそれぞれ異なるとはいえ、サービスの設計、オリエンテーション／トレーニング、サービスの提供に関する限り、顧客中心主義を貫く必要がある点が共通している。顧客中心主義は、マネージドセキュリティサービスプロバイダーによる MSS-as-a-Service オプションなど、柔軟なサービス提供モデルに反映されている。複数のパブリック／プライベートクラウドへのワークロード移行が進むにつれ、こうした適応性に優れたクラウド化オプションは、顧客にとって特に重要である。長年に渡って企業内に蓄積されたセキュリティツールには、使われていないものや、部分的にしかインストールされていないもの、構成が不完全なものが多く見られ、これまでになく複雑な状況となっている。マネージドセキュリティサービスプロバイダーは、複雑性に対処すると共に、クラウドへの移行プロセスのリスクを取り除く必要がある。さらに重要なポイントとして、クラウド投資を最適化する必要があり、これには Infrastructure-as-a-Service（IaaS）サブスクリプションに含まれる組み込みのセキュリティツールや、セキュリティベンダー製のクラウドセキュリティツール

の活用が含まれる。調査に参加した多くの企業が、オンプレミスのセキュリティ情報イベント管理（SIEM：Security Information and Event Management）、クラウド型 SIEM を活用して、柔軟性のある顧客志向性の高い提案を提供できると IDC はみている。

- **主流化するクラウド**：すでに多くの企業が、クラウドベースのセキュリティサービスを採用し、クラウドセキュリティ市場が拡大している。これはマネージドセキュリティサービスプロバイダーのクラウドセキュリティサービスの機能が向上していることを示している。たとえば、本地域ではクラウドモニタリング、クラウドアクセスセキュリティブローカー（CASB）サポート（主として Software-as-a-Service の保護が目的）が勢いを増している。通信事業者のマネージドセキュリティサービスプロバイダーは、脅威の検出とレポートのために各種セキュリティ機能を自動化し、オーケストレーションを行う独自のセキュリティクラウドサービスを提供している。さらに、調査に参加した企業の多くが、自社のネイティブなクラウドセキュリティ能力を強化し、DevSecOps サービスなどをポートフォリオに加えている。
- **革新的なユーザーインターフェース（UI）、強化されたユーザーエクスペリエンス（UX）**：顧客中心主義の基盤には、インターフェースレベルのイノベーションもある。リーダーに分類された一部の企業は、ユーザーエクスペリエンス機能の点で明らかに他社の先を行っている。ソーシャルメディアに酷似した形で、Uber アプリのようなマッチング機能を通じて、インシデント発生時には自動的にアナリストの割り当てを行い、脅威に関する調査、アラート、更新の流れを示し、さらには音声認識のデジタルアシスタントに対応するインターフェースの出現も見込まれている。

IDC MarketScape ベンダー選定の基準

多数のサービスプロバイダーが、マネージドセキュリティサービスの機能やサービス内容などにおいて競合状況にある。本評価は、MSS の検討すべきプレイヤーをすべて網羅したものではなく、特定に始まり、防御、検知、対応、復旧に至るまでの脅威ライフサイクル全体にまたがる各種機能を提供している主なプレイヤーについて調査したものである。本 IDC MarketScape では、19 社のマネージドセキュリティサービスプロバイダーに関するデータを収集、分析した。IDC は以下の基準に基づき調査対象となるプレイヤーを絞り込んでいる。

- **MSS ポートフォリオ**：各サービスプロバイダーは、包括性の高い MSS ポートフォリオを有している必要がある。ポートフォリオの少なくとも 50%以上が、IDC の MSS の市場定義による分類（マネージド脅威インテリジェンスサービス、マネージド・ディテクション・アンド・レスポンスサービス、マネージドネットワークセキュリティサービス、マネージドエンドポイントセキュリティサービス、マネージドセキュリティ Web ゲートウェイサービス、クラウドポスチャー、コンプライアンスモニタリング、OT/IoT モニタリング）と一致していなければならない。
- **地域におけるプレゼンス**：各ベンダーは、アジア太平洋地域の 2 つ以上の地域において MSS を提供しているか、または、セキュリティオペレーションセンター（SOC）を有していなければならない。その地域は、北アジア（日本、韓国）、中華圏（中国、香港、台湾）、東南アジア（シンガポール、マレーシア、タイ、インドネシア、ベトナム、フィリピン）、南アジア（インド、パキスタン、スリランカ、バングラデシュ）、ANZ（オーストラリアおよびニュージーランド）である。
- **収益**：調査対象の企業は、アジア太平洋地域における 2018 年の総収益が 1,000 万米ドル以上でなければならない。
- **マルチポイント評価の完了**：調査対象となる各社は、この地域におけるマネージドセキュリティサービスの成功への貢献を基準に IDC が定義した計 29 に及ぶサービス機能と戦略に関するマルチポイント評価を完了している必要がある。

IT バイヤーへの提言

セキュリティベンダーの選択は極めて重要なビジネス／戦略上の決定事項であり、企業の全体的なビジネス目標に合致することが望ましい。ベンダーパートナーの選択に際して、IDC は企業が以下の点に留意することを推奨する。

- **Security by Design の採用**：デジタルトランスフォーメーション（ここではクラウドが重要なイネーブラーとなる）を開始したばかりのユーザー企業にとって、セキュリティを事前に考慮する「Security by Design」は、テクノロジーの新規採用やクラウドの導入に際して極めて重要である。これによって、最大のセキュリティと可視性を無理なく確保することが可能になる。
- **サイバーリスクモニタリングの組み込みと統合**：すでにマネージドセキュリティサービスプロバイダーを利用している場合、サービスレベル契約（SLA）の見直しを行い、サイバーリスク関連の評価基準を追加する必要がある。最新の調査レポート『*IDC FutureScape: Worldwide Security and Trust 2020 Predictions*』では、IDC の予測では 2021 年までに上場企業の 80%が、事業計画および四半期報告にサイバーリスクモニタリングを盛り込む予定であるとしている。継続的なサイバーリスクモニタリングは、企業間（B2B）関係に必要な最低限の基盤となり、投資家を惹き付け、信頼の構築に役立つ。このようなプロセスの確立は、より安全で信頼に値する企業への第一歩となる。さらに、テクノロジーリスクがそのままビジネスリスクとなるよう、企業の IT 戦略とビジネス戦略を一体化させることにもつながる。
- **業界専門知識による技術能力の強化**：マネージドセキュリティサービスプロバイダーの立場で、これは何を意味するのであろうか。高度なセキュリティ専門技術のみならず、ビジネスリスクに関する幅広い経験も要求され、サイバーリスク戦略サービスを提供する必要がある。効果的なサイバーリスク戦略を策定し、ビジネス目標に合致させるためには、業界に関する深い専門知識に加え、従来のインフラストラクチャの監視の範囲を超えた、業界固有の脅威モデルを開発する能力が要求される。調査対象のベンダー各社に関する IDC の評価では、本地域でサービスを提供しているベンダーの大多数が、各業界における実績とサービス提供能力において、一定程度の差別化に成功している。
- **継続的な見直しと評価**：厳しい規制要件のある業界に属さず、セキュリティへの投資実績にも乏しい企業の場合、現時点における自社のセキュリティニーズを見直すとともに、現在の環境またはセキュリティベンダーが現在と今後のニーズに十分対応できる能力を備えているかどうかを評価することが重要である。たとえば現在の SIEM システムのワークフローで生成されるアラートが過剰に発生していないか。誤検知率はどれくらいか。IoT デバイスなどの新しいソースを SIEM に追加することは可能か。レベル 1 タスク（例：ログのアセンブリ、トリアージなど）の自動化率はどれくらいか。SOC の分析生産性はどの程度か。インシデントの認識に要する時間、平均検出時間、平均軽減時間、平均復旧時間、自動応答率、アラートの精度などの主要な指標を用いて、現在の SOC 環境の有効性を評価する必要がある。さらに、重要インフラ企業であれば、マネージドセキュリティサービスプロバイダーと連携して IT-OT コンバージェンスを実現し、産業システムや OT/IoT 環境に対するサイバーリスクの増大に対処することが有益である。
- **新テクノロジーの導入と柔軟な活用**：人工知能（AI）／機械学習（ML）、自動化、脅威インテリジェンスアナリティクスを活用し、現行の SOC 業務の拡大と改善を図る必要がある。調査対象となった企業の多くが、アナリティクス、自動化、コンテクスト化を中心に、SOC/SIEM で提供される機能の大幅な向上を示している。マネージドセキュリティサービスプロバイダーの SIEM プラットフォームに各種のアナリティクスおよび AI/ML ツールが組み込まれた結果、誤検知率の低下と共にオーケストレーションと自動化が強化されている。さらに、クラウドサービス型 SIEM を始めとする柔軟性に富んだオプションを顧客に提供する必要がある。IT 環境要件が高度化し、AWS（Amazon Web Services）、グーグル、マイクロソフト、AliCloud といったクラウド企業によるセキュリティサービスが拡充されつつある現在、IT リソース不足や限られたセキュリティ予算の企業において、サービスとしてのセキュリティは今後さらに大きい影響力を持つことが予測される。こうし

た理由から、マネージドセキュリティサービス市場の需要増大が見込まれる今、クラウドベースのセキュリティサービスを含め、柔軟なオプションを用意する必要がある。

ベンダープロフィール（要約）

本セクションでは、IDC MarketScape でリーダーに位置付けられた NTT に関する IDC の主な所見を説明すると共に、同社の強みと機会について概要を述べる。

NTT

NTT は「*2020 Asia/Pacific Managed Security Services IDC MarketScape*」調査において、IDC による分析と顧客のフィードバックを総合した結果、リーダーの 1 社に選出されている。

NTT は 2016 年、NTT グループ会社で MSS に特化したすべてのリソース、提供プラットフォームを統合した後、2019 年に組織の再編成を行い、新事業会社 NTT Ltd に 28 社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。アジア太平洋地域に強力なプレゼンスがあり、17 か国で事業を展開している同社は、この地域最大のセキュリティサービスプロバイダーの 1 社である。

NTT Ltd は包括的な MSS ポートフォリオを強みとして持ちサービスを提供している。顧客ニーズに適切に対応するため、同社は業種や地域の違いに応じてサービスの再編成を行った。アジア太平洋地域における NTT の最大の収益源としては、脅威検出（Threat Detection）、マネージドネットワークサービス（Managed Network Services）がある。NTT の脅威検出は、独自の分析エンジンである Advanced Analytics を利用し、「ブロックされたアラート」から「不審な許可イベント」に分析対象をシフトすることで、まさにことわざ「干し草の中から針を探す」のように高度な脅威検知能力を提供する。この分析ツールは、独自の機械学習、行動分析、ネットワークデータなど複数の分析手法を用いて効果的な検知を実現する。

NTT はネットワーク、データセンター、クラウドで培った実績とネットワーク資産、専門知識を生かし、ビジネスのサイバーセキュリティライフサイクル全体に戦略的な価値を提供すると共に、顧客がセキュリティ・バイ・デザインを実現できるよう支援している。NTT は、同社のグローバルスレットインテリジェンスセンター（GTIC：Global Threat Intelligence Center）で運用されるサイバースレットインテリジェンス（CTI：Cyber Threat Intelligence）フレームワークを通じて、インテリジェンス主導型の脅威ライフサイクル機能を構築できるように顧客をサポートしている。GTIC は CTI を収集し効率的に情報を共有し連携するために、人、プロセス、テクノロジープラットフォームで構成される統合型構造を持つ。

現在、NTT 顧客企業の約 80%が NTT のクラウドセキュリティ機能を利用している。このことはクラウドベースのセキュリティサービス、マネージドクラウドセキュリティにおける同社の実績が評価されていることを物語っている。一例を挙げると、NTT Enterprise Cloud は、脅威検知およびレポートのためのさまざまなセキュリティ機能の自動化／オーケストレーションを行うと共に、FW、IDS/IPS、ウイルス対策、URL フィルタリング、アプリケーションフィルタリングなど、各種のセキュリティ機能をクラウド環境に組み込んでいる。

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、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、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い、サービスポートフォリオを拡張し DevSecOps サービスなどの新サービスを推進している。

強み

NTT はオープン／ディープ／ダークウェブ全般に渡り、あらゆるサイバーインシデントに関する詳細かつ包括的に把握しており、独自ハニーポットに直接アクセスし、新たに出現した脅威について早期にデータを収集することが可能である。顧客中心、サービス主導、成果ベース、イノベ

ーションを主導する企業としてのビジョンを実現するため、NTT は R&D に継続的な投資を行い、独自のツールおよびプラットフォームを開発している。NTT 独自の SIEM エンジンは、こうした R&D 活動による成果の一つである。2018 年 8 月、Dimension Data（現 NTT Ltd.）は、IoT、バイオセンサー／ウェアラブル、仮想現実／拡張現実、セキュリティ、暗号化など、さまざまなイノベーションテクノロジーとソリューションの紹介を目的とした新しいクライアントイノベーションセンターをシドニーで開設した。

NTT はさらに、グローバル MSS プラットフォームの統合と展開を行った後、「ライトソーシング」モデルの推進に努力を続けてきた。つまり、大量のボリュームや高度なスキルを集中し、可能な限りスケールメリットを追求すると同時に、ローカル言語の使用や顧客中心主義の価値を通じて、顧客にとって身近な存在になることである。顧客からのフィードバックによると、NTT の提供サービスは継続的に改善されており、NTT との関係性は、単なるサービスプロバイダーと顧客の関係を超えて戦略的ビジネスパートナーシップに進化している。また、NTT のセキュリティ専門技術者の質の高さについても満足度が高い。

NTT はデータ主導型アプローチとペルソナに基づくマーケティングを通じて、すべての顧客エンゲージメントにオムニチャネル戦略を採用し、見込み客、新規顧客、既存顧客を対象に、顧客維持、アップセル、クロスセルを行っている。それに加えて、NTT は Global Threat Intelligence Center のデータと実際の顧客データを基に、Global Threat Intelligence レポートを発行している。グローバルと各地域のセキュリティ脅威状況を伝えるこのレポートは、各地域における NTT のソートリーダーシップへの取り組みの主要な成果であり、セキュリティ業界における NTT の信頼性を高める役割を果たしている。

課題

同社は NTT ブランドの下で従来のすべての企業ブランドを再確立する必要に迫られている。各ブランドの既存顧客に、提供するサービスが従来と同等か、より良いサービスが提供されることを確信してもらう必要がある。また、新生 NTT Ltd にとって、アジア／太平洋地域が今後も主要なハブであり続ける安心感を与えることも重要である。

補遺

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とサービスメニュー、さらにベンダーが顧客ニーズにどの程度合致しているかを示す。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 年から 5 年以内に要求するものがどの程度合致しているかを示す。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

IDC は本調査において、マネージドセキュリティサービス、すなわち MSS の定義を、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 24 時間体制のセキュリティソリューション／アクティビティの管理と監視としている。この中には、顧客施設内に導入されたセキュリティソリューションを監視、または顧客施設の外部にあるデータセンターまたはクラウドでホスティングされているソリューションの監視が含まれる。

参考資料

関連調査

- *IDC FutureScape: Worldwide Security and Trust 2020 Predictions – APEJ Implications*（発行予定）
- Acceleration of Outcome-Driven Managed Security Services in the Asia/Pacific Region（IDC #AP45395519、2020 年 1 月発行）
- *Security Investment Priorities and Requirements by Verticals: BFSI, Manufacturing, and Retail in Asia/Pacific*（IDC #AP44700819、2019 年 12 月発行）
- *IDC FutureScape: Worldwide Security and Trust 2020 Predictions*（IDC #US45582219、2019 年 10 月発行）
- *Distributed Denial-Of-Services Attacks Are Increasingly Used to Negatively Impact*
- *in Asia*（IDC #AP44718419、2019 年 7 月発行）
- *Lessons Learnt from the SingHealth Case – Effective Incident Response Strategy and Consideration of Zero Trust Security Framework*（IDC #AP43913219、2019 年 2 月発行）
- *IDC MarketScape: Asia/Pacific Managed Security Services 2018 Vendor Assessment*（IDC #AP42609818、2018 年 6 月発行）

Synopsis

本調査レポートでは、アジア太平洋地域でマネージドセキュリティサービスを提供する 19 社のベンダーを評価した。調査対象のベンダー各社について、29 の市場決定基準に照らし合わせて評価を行った。具体的には、MSS 製品／サービスの対象範囲、ポートフォリオの利点、脅威ライフサイクル対応状況、クラウドセキュリティ、提供モデル、コスト管理、市場遂行、知名度、ソートリーダーシップ、イノベーション、顧客満足度、顧客アドボカシーなどが含まれる。IDC はベンダーとその顧客企業を対象に、一連のインタビューおよびマルチポイント評価を実施し、各ベンダーの差別化要因、強み、課題を総合的に捉えた。包括的かつ綿密な分析を行った後、専門アナリストで構成される IDC の内部委員会による審議を経て、最終的に IDC MarketScape の図に示される各社の位置付けを決定している。

「トップに位置付けられたマネージドセキュリティサービスプロバイダー各社は、専門技術および脅威ライフサイクル管理能力に優れているだけでなく、サイバーリスク戦略とサービス提供における幅広い経験がある。マネージドセキュリティサービスプロバイダーが効果的なサイバーリスク戦略を策定するには、ビジネス目標に合致するものにしなければならない。業界の深い専門知識に加え、従来のインフラストラクチャの監視サービスを超えた、業界固有の脅威モデルを開発する能力が要求される」と、IDC Asia/Pacific Services and Security のアソシエイトリサーチディレクターである Cathy Huang は述べている。

「企業を取り巻くサイバー脅威の状況は相変わらず猛烈なスピードで進化し続けており、セキュリティプロバイダーは常に、悪意のある者よりも一歩か二歩、先を行く必要がある」と、IDC Asia/Pacific Services and Security のリサーチディレクターである James Sivalingam は警告する。さらに、「アジア／太平洋地域のようにデジタル化が急速に進んでいる地域では特に、国や業種によって企業の成熟度にばらつきがあり、状況は困難を極める。しかし、今回の調査で明らかになったように、この地域でサービスを提供している主要セキュリティベンダーはすべて、当面の課題に十分対応できるサービス体制を整えている。アジア／太平洋地域の顧客に真の価値を提供するには、強力なサービス機能、テクノロジー、幅広いリスク要因への対応能力に加え、顧客がセキュリティ・バイ・デザインを実現できるよう支援する戦略的パートナーとしての地位を確立する必要がある」と述べている。

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。

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.