IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2018 Vendor Assessment

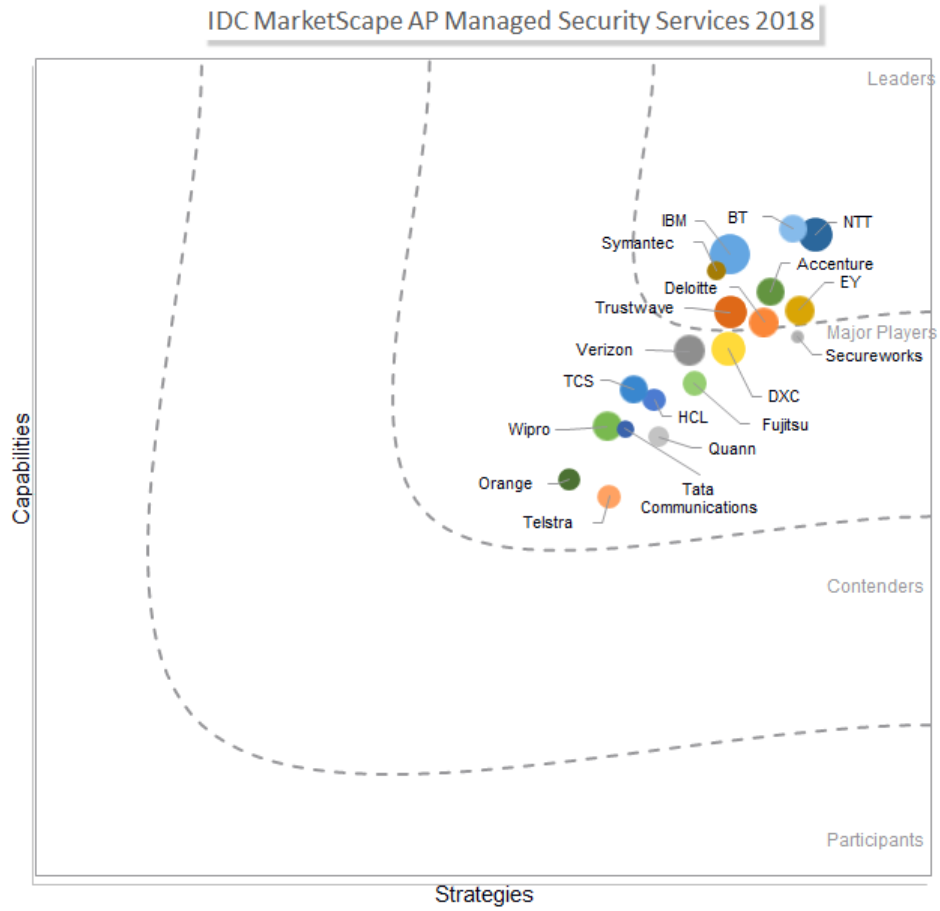
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES: NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape：アジア太平洋地域マネージドセキュリティサービスベンダー評価



Source: IDC, 2018

調査方法、市場定義、そして評価基準については「補遺」のセクションを参照のこと。

June 2018, IDC #AP42609818e

調査概要

本調査レポートは、『*IDC MarketScape: Asia/Pacific Managed Security Services 2018 Vendor Assessment*（IDC #AP42609818、2018 年 6 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 ベンダー選定基準」「IT バイヤーへの提言」「ベンダープロフィール概要」「補遺」「関連調査」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

IDC は、IDC MarketScape モデルを使用して、2017 年から 2018 年にかけて、アジア太平洋地域でマネージドセキュリティサービス（MSS）を提供する 19 の企業について調査を行った。ただし、参加企業の大半がこの地域以外にも世界規模でサービスを提供している。評価は、サービスの包括性、ポートフォリオの優位性、配信モデル、事業推進力、コスト競争力、プラットフォーム能力、マネージドセキュリティサービスに対する現在の需要と将来の市場ニーズに沿った顧客サービスなど、多数の項目に渡って行われる。本調査において IDC は、マネージドセキュリティサービス事業者（MSSP：Managed Security Service Provider）とその顧客に詳細なインタビューを行い、対象となる事業者を評価した。その結果、いずれの事業者もそれぞれに長所と短所を持つことが確認された。本調査の対象企業の選定は、市場で一定の存在感があり、差別化のための独自の取り組みを進めていること基準としている。独自の差別化を持つ一方、事業者の間でいくつかの共通の傾向も見られる。

- **プラットフォームのイノベーション**：相当数の MSSP が、AI（Artificial Intelligence：人工知能）や機械学習などの新しい技術を活用することによって、コアプラットフォームにおける自動化とオーケストレーションのレベルを向上させ、検出／対応時間の短縮を図っている。こうした MSSP のうち 2 社が、セキュリティ運用をよりいっそう効率化するために、RPA（Robotic Process Automation）とロボティクス活用の高度化を図っている。
- **柔軟性とポータビリティ**：自動化とオーケストレーションに加えて、柔軟性とポータビリティもコアプラットフォームの非常に重要な特性である。これによって、MSSP は、顧客のセキュリティ成熟度と能力が進化し、個々の要件に合わせた継続的なセキュリティサービスを通じて、顧客を次の段階にシームレスに移行させることができる。
- **統合**：一部の MSSP は、セキュリティ情報／イベント管理（SIEM：Security Information and Event Management）プラットフォームを脅威管理プラットフォームやインシデント対応プラットフォームなどの他の重要なプラットフォームと統合させることに長けている。その結果、セキュリティ面で大きな成果が得られると共に、クライアントの経験が大幅に改善した。
- **クラウドセキュリティ**：ポートフォリオの強化の一環として、今年、数多くの MSSP がクラウドセキュリティポートフォリオを導入、あるいは既存のクラウドセキュリティポートフォリオの拡張を図った。先行する MSSP の中には、早い段階からこの分野に投資していたか、あるいは市場を主導するクラウドセキュリティベンダーとの密接なパートナーシップによって先行しているところもある。MSSP によっては、自社のコアインフラストラクチャの大部分をパブリッククラウドに移行させ、独自のクラウドセキュリティアーキテクチャや製品／サービスを採用しているところもあり、クラウドセキュリティは多くのプロバイダーが注力している分野である。
- **IoT（Internet of Things）/OT（Operational Technology）セキュリティ**：クラウドセキュリティと同様に、IoT/OT セキュリティは、多くの MSSP の提供品目のロードマップで頻繁に言及されている。そうした MSSP の中には、わずかながら、OT セキュリティ監視機能のパイロットプロジェクトの実証に取り組んでいる企業もある。
- **顧客中心主義**：顧客中心主義は、MSSP を差別化する最も重要な要因の一つである。これは、地域内のローカルサポート、顧客ポータルの使いやすさ、レポートおよびサービスレベルアグリーメント（SLA）評価基準のカスタマイズ、プロジェクト管理、オンボーディングプロセス、専用アカウント／技術アカウント管理など、さまざまな要因に反映されている。実際、多くの企業は、顧客中心主義の観点から、小規模であっても、大手 MSSP よりも専門分野に特化したプレイヤーを選定している。
- **中堅企業向け市場**：より多くの MSSP、特に、従来大企業向け市場に焦点を合わせてきた MSSP が、中堅企業向け市場に目を向け始めたことは好ましいことである。MSSP によって

は、中規模の顧客を対象としたコンプライアンス管理を中心としたパッケージソリューションを開発しているところもあり、今ではそれが差別化の鍵となっている。

IDC MARKETSCAPE ベンダー選定の基準

IDC は、2018 年 IDC MarketScape アセスメントの一環として、マネージドセキュリティサービス事業者 19 社についてデータを収集、分析した。マネージドセキュリティサービスを提供している MSSP またはサービスベンダーの数はこれよりも多く、ポートフォリオの範囲と配信能力に大きな幅があるが、IDC は、以下の基準にしたがって対象とする企業を絞り込んだ。

- **より幅広い MSS ポートフォリオに渡ってサービス能力を有していること**：サービス事業者が、アジア太平洋地域でかなり包括的な MSS ポートフォリオとデリバリー機能を備えていること。たとえば、セキュリティインフラストラクチャ管理、セキュリティモニタリング、セキュリティ運用強化、コンプライアンス管理、アイデンティティ／アクセス管理、分散型サービス妨害（DDoS）攻撃緩和、リテーナベースのインシデントレスポンスサービス、脅威情報サービスなどを提供していること。
- **地理的プレゼンス**：すべてのベンダーは、北アジア（日本、韓国）、大中華圏（中国、香港、台湾）、ASEAN（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）、オーストラリア／ニュージーランドの各アジア太平洋地域のうち最低 2 つ以上の地域で、国内 MSS 配信能力を有していること。国内セキュリティサービス配信能力が、ベンダーの現地パートナーシップを通じて活用されていてもよい。
- **収益**：参加企業は 2016 年と 2017 年のアジア太平洋地域での MSS の収益の総額が 2,000 万ドルを上回っていること。この MSS の収益は、セキュリティ製品の再販収益を除いたものでなければならない。ただし、前述の 2 つの基準（幅広いポートフォリオと地理的プレゼンス）を満たすと同時に、市場で一定の存在感とその地域での成長戦略を明示できる MSSP は、この収益要件は適用されない。

IT バイヤーへの提言

アジア太平洋地域の MSS 市場は競争が激しく、多くの MSSP が顧客獲得を巡りしのぎを削っている。さらに重要なことは、この分野は企業統合が頻繁に行われるため、バイヤーは適切な MSSP を選択するのに多くの困難と複雑さに直面することになる。IDC は、バイヤーに対し、それぞれの評価プロセスにおいて複数の情報源を活用することを奨励している。具体的には、使用事例、概念実証、価格ベンチマーク、MSSP の顧客満足度調査、さらに、IDC MarketScape や、発行予定の脅威ライフサイクルサービスの IDC MarketScape 調査などのサードパーティによるベンダー評価がある。脅威ライフサイクルサービスの IDC MarketScape 調査では、セキュリティ評価、サイバー範囲、インシデントレスポンス、フォレンジックサービスなど、専門的なセキュリティサービスに力点を置いている。

さらに IDC は、テクノロジーバイヤーに対し、以下のように提言している。

- **システム保護からサイバーリスク低減へのシフト**：企業がセキュリティの成熟度と能力を向上させるにつれて、堅牢なリスク管理能力を活用して情報セキュリティ対策の指針を策定し、テクノロジーとプロセスおよび従業員の間の強い相互作用を実現する取り組みを我々は目にしてきた。さらに重要なのは、これらの企業が、自社のセキュリティ対策（目的、セキュリティへの投資、採用されたセキュリティ管理など）とビジネス戦略との間に良好な相互連携を構築できるという点である。多くの企業の資産がデジタル化され、あらゆる活動がデータの形を取ることによって、逆にサイバー犯罪者や攻撃者によるデジタル資産の窃盗を誘因するというこのデジタル時代においては、これは特に重要である。さらに、組織がこれらの新しい手段を使って顧客との間で双方向のやり取りを行う際に、デジタルチャネルやオンライントランザクション、モバイルトランザクションなどが爆発的に増加するため、サイバーセキュリティインシデントと不正行為との重なりから生じるリスクも顕著になっている。こうしたことから、重要な資産の保護と、サイバーリスクの低減は、デジタル企業にとって最重要課題である。

- **ハイブリッドな環境におけるセキュリティ管理**：企業がデジタルトランスフォーメーションに取り組み、まったく新しい（net-new）IT サービスを獲得するか、既存の IT サービスを新たなサービスに転換すると、企業はクラウドファーストアプローチをとることになる。「クラウド経由のセキュリティ」を評価した IDC の調査では、地域内の組織の約 45%が、クラウドベースのソリューションへの移行に伴い、今後 3 年間で、オンプレミスセキュリティがセキュリティ全体に占める割合（フットプリント）が 15%低下する見通しであると回答している。最新の 2018 年のアジア地域（日本を除く）セキュリティサービスソーシング調査では、「ハイブリッドな環境全体を網羅するセキュリティ管理」が、どの市場でも主要なセキュリティ課題に挙げられている。この難題に取り組むために、IDC はテクノロジーバイヤーに次の点の検討を推奨している。
  - **「設計段階からのセキュリティ」の適用**：プライベートクラウド、パブリッククラウド、マネージドパブリッククラウド、マルチクラウドなど、新しいタイプの非オンプレミス環境に「設計段階からのセキュリティ」を適用すべきである。すべてのビジネス／デジタルトランスフォーメーションイニシアティブにおいて、各事業部門（LOB）が、IT 組織と協力し、それぞれの設計／概念実証段階にセキュリティ要素を組み入れる必要がある。
  - **既存のセキュリティソリューションの見直し**：新しいセキュリティソリューションに投資する前に、既存のセキュリティソリューションを見直すべきである。既存のセキュリティソリューションを改めて評価または合理化する。マネージドセキュリティサービスや、予算上の制約がある場合には、特に有用なサービスオプションとしてのセキュリティなど、柔軟性に富んだ消費モデルを検討すべきである。
  - **飛躍的/革新的ソリューションの検討：**物理的オンプレミス環境から仮想環境、クラウド／マルチクラウド環境に至る多様な環境を通じてさまざまなセキュリティ機能のオーケストレーションと最適化を行える飛躍的／革新的ソリューションを検討すべきである。
- **サービスレベルアグリーメント評価基準**：従来の MSS サービスレベルアグリーメント（SLA）は、可用性と対応時間などの契約の効率に重点を置いている（一般に使用されている SLA コンポーネントの例については Table 1 を参照）。そのような評価基準が重要であることは変わらないが、それらによってセキュリティサービスの有効性を測定することは到底できない。多くの場合、IT 管理者やセキュリティ管理者は大量の警報や誤検出に圧倒されているのが現状である。IDC は、セキュリティ基盤のコンポーネントの可用性と信頼性に着目した主要な SLA 評価基準を維持することは重要ではあるが、企業が、数を絞って直感的な SLA 評価基準も開発することを推奨している。たとえば、ユニット当たりのリスク低減度（すなわち、セキュリティに 1 ドル投じるごとにそのリスク低減で「節約」できる金額をドルで表した正規化収益率）などが考えられる。そうした結果は、事業に及ぼす影響は明らかであり、それを各事業部門にフィードバックすることができる。それには、関与する MSSP がサービスを提供する相手先についての深い理解と、その相手先に業界標準の能力を提供できることが必要である。

TABLE 1

サービスレベルアグリーメント

SLA コンポーネント	これまでに集積されたサービス事業者の対応に基づいて広く受け入れられている対応時間範囲
顧客へのセキュリティインシデントアラート通知	重大度 1 のインシデントに対しては 15 分
1 つのインシデントの平均解決時間（MTTR）	重大度 1 のインシデントは 3 時間
インシデント発生後フォレンジック分析を完了し報告するまでの時間	優先度 1 のインシデントについては通知から 1 時間以内
顧客から発せられるサービス依頼に対する平均対応時間	緊急依頼の場合 2 時間

Source: IDC, 2018

ベンダープロフィール概要

このセクションは、IDC の主要な所見を簡単に説明し、IDC MarketScape においてそれぞれのベンダーがどのような地位を占めているかを報告する。「補遺」のセクションに記載した各基準に照らして各ベンダーを評価しているが、ここではそれぞれの強みと課題を簡単に説明している。

NTT

IDC の分析と顧客からのフィードバックでは、NTT は、2018 年のアジア太平洋地域のマネージドセキュリティサービス調査でリーダーの一つに位置付けられている。

NTT は、NTT セキュリティ、ディメンションデータ、NTT コミュニケーションズ、NTT データなど多くの企業を擁している。2016 年 8 月 NTT は、ソリューショナリー、NTT コムセキュリティ、ディメンションデータ、NTT コミュニケーションズ、NTT データ、NTT イノベーションインスティテュートなどの NTT グループ会社のすべての MSS 関連リソースと配信プラットフォームを、「グローバルマネージドセキュリティサービスプラットフォーム」（GMSSP）と呼ばれる 1 つの包括的なプラットフォームとして立ち上げた。

このプラットフォームは、独自開発のセキュリティ情報／イベント管理に基づいており、グローバル脅威情報プラットフォームと NTT セキュリティ脅威インテリジェンスデータベースと緊密に連携している。これは、NTT グループが年間 20 億米ドルをセキュリティに投資している結果である。GMSSP は、複数の地域に渡って一貫したサービスを提供する上で重要なコンポーネントであり、企業全体のセキュリティモニタリングと管理、脆弱性ライフサイクル管理、カスタムマネージド検知／分析にとって特に重要である。

この高度に専門化されたセキュリティ会社の発足は、投資を集中させ、セキュリティコンサルティング、システムインテグレーション、サポートサービス、マネージドセキュリティサービスなどの幅広いセキュリティポートフォリオをサポートすることを目指したものである。ディメンションデータ、NTT コミュニケーションズ、NTT データなどの代表的グループ会社が今後、それぞれの分野の専門知識を活用して、インシデントの検出と対処、リスク管理、セキュリティコンサルティング、ソリューションサポートサービス分野で地域や国内の要件にクライアントが対応できるように支援する。それには、それぞれの国内状況について深い理解と地域全体への配信能力が必要となる。

2017 年以来、NTT は、リアルタイム分析に UEBA（User Entity Behavior Analytics）とダーク Web への潜入機能を組み入れ、強化してきた。その結果誤検出が非常に少なくなり、顧客はより正確な「クリ

ティカルアラート（緊急警報）」対応を経験している。NTTは、世界のインターネットトラフィックの40%（NTTの電気通信バックグラウンド、23か国に渡って1,200か所以上でハニーポットを導入している実績から推定される数字）をカバーし、脅威の重大度をリアルタイムで検証するクオリティアナリストのチームを擁している。NTTは、高度なアナリティクス能力によって、こうした比類のない脅威インテリジェンスとCASB（Cloud Access Security Broker）技術と機械学習技術を組み合わせることで、セキュリティ実績とクライアントの経験を大幅に改善している。

NTTは2018年、SD-WAN（Software-Defined Wide Area Network）、OT/IoT環境、といった多くの使用事例に対応したセキュリティ製品／サービスも充実させた。たとえば、NTTは、最新の技術革新の一つである、IoTとオペレーティングテクノロジー（OT）をサイバー攻撃から守るためのデセプション技術を採用している。NTTは、クラウド向けセキュリティ（たとえば、CASB、EDR：Endpoint Detection and Response、脅威インテリジェンスなどのさまざまな分野に渡る統合クラウドセキュリティサービス）だけでなく、AWS（Amazon Web Services）やNTT独自のエンタープライズクラウド2.0といったクラウドも有効に活用してマネージドセキュリティサービスを提供している。今では、顧客は、クラウドベースのコントロールパネルからサービス指示を実行し、UTM（Unified Threat Management）設定を変更できるようになった。

市場開拓という観点から見ると、NTTは、アジア太平洋地域で、14を超える市場に直接参入し、この地域の6か所でセキュリティオペレーションセンター（SOC）を開設している。NTTは、2018年初めにシンガポールのSOCを改修し、頻繁にSOC施設（シンガポールSOCだけでなくその他のSOCでも）を使って、顧客を招待し、最新鋭のセキュリティアナリティクスサービスと脅威ハンティングについて解説し、高度な自動化とAIの活用を紹介している。

強み

ビジネスが成長するにつれ、丁寧なサービスを提供することが課題になる。長い応答サイクルと依頼するまでに複数のタッチポイントが必要となる他の大手MSSPに比べて、NTTは統合されていながら効果的なタッチポイントを提供しており、顧客から高い評価を得ている。これは、顧客エクスペリエンスの観点から見てNTTの大きな強みとして、しばしば取り上げられる。さらに、スムーズなセットアッププロセス、丁寧な配信、業界標準のサービスの提供なども、優れた顧客エクスペリエンスに挙げることができる。

NTTの脅威検出能力は、特にその精度の高さについて顧客から高く評価されている。さらに、インシデント探索やコンプライアンスの照会時に役立つデータログも、クラウドベースで検索可能であり、NTTの持つ優れた機能として高く評価されている。

従業員のリテンションマネジメントの面では、脆弱性情報リサーチ、リアルタイムアナリスト、脅威情報リサーチチームという3つのアナリスト／リサーチグループが交代で分析やリサーチに当たることによって、より広くより深い知見を獲得し、また、常に高いモチベーションを維持している。

さらにNTTは、ソートリーダーとしての地位を確立すべく努力を継続している。毎年発行されている「*Global Threat Intelligence Report*」は徐々に市場で影響力を拡大している。

課題

顧客エクスペリエンスは総じて、NTTの顧客から高い評価を得ているものの、地域全体として見ると、顧客エクスペリエンスと配信には、依然一貫性に欠ける点が見受けられる。たとえば、デバイス管理では、顧客サイドからの長々とした文書の提供が必要であり、それが満足度を下げる要因となっている。

NTTのグローバルマネージドセキュリティサービスプラットフォームが能力の強化と豊富な機能性を約束するものであるとしても、プラットフォームの移行は顧客の解約や一時的な不満につながった面もある。とはいえ、NTTが信頼関係を築いてきた多くの顧客に対して、プラットフォームの移行による影響は出ていないように思われる。

補遺

IDC MarketScape Graph の見方

この分析の目的のために、IDC では、成功のための重要な尺度を、能力（capability）と戦略（strategy）の 2 つの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。能力カテゴリーは、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は、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能力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、ベンダーの将来に向けての戦略と、顧客が 3 年ないし 5 年以内に求めるニーズ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根底にある考え方に焦点を合わせている。

IDC MarketScape では、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 の方法論

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、バイヤー調査、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

本調査の目的に即して、IDC は、マネージドセキュリティサービスを、セキュリティオペレーションセンターから配信される各種セキュリティソリューションとセキュリティ活動の常時管理／モニタリングと定義している。IDC では、そのサービスが顧客のオンプレミス内に配置されたセキュリティソリューションの管理を対象としている場合も、あるいは顧客の施設の外部にあるデータセンターやクラウドにホストされているソリューションの管理を対象としている場合を含め、すべての MSS を調査対象に含めている。

MSS 事業者が提供する新しいサービスは着実に大きな流れとなり、従来のマネージドセキュリティサービスの枠を超えて広がろうとしている。これらのサービスの多くが求められる最大の理由は、成長し続ける複雑な環境のセキュリティ要素をより効率的に管理するための支援をクライアントが求めていること点にある。

参考資料

関連調査

- *Enhancing Security Proficiency and Addressing Challenges Brought by Cloud: A Perspective on Manufacturers and Retailers in Asia*（IDC #AP42610518、2018 年 3 月発行）
- *IDC's Worldwide Security Products Taxonomy, 2018*（IDC #US43535614、2018 年 2 月発行）
- *IDC FutureScape: Worldwide Security Products and Services 2018 Predictions*（IDC #US43286117、2017 年 12 月発行）

Synopsis

本調査レポートでは、IDC MarketScape モデルを使って、マネージドセキュリティサービスを提供する事業者について、ベンダー評価を行う。この評価は、ポートフォリオの利点、配信モデル、市場執行、コスト競争力、プラットフォーム能力、マネージドセキュリティサービスに対する現在の需要と見込まれる IT バイヤー（IT ユーザー企業）のニーズを定める顧客サービスなどの多数の項目に渡って行われる。本調査において IDC は、マネージドセキュリティサービス事業者（MSSP）とその顧客に詳細なインタビューを行い、ベンダーを評価し、その結果、同業他社と比較するといずれの事業者もそれぞれに長所と短所を有していることが確認された。

「成熟度に大きな幅があり、同質的でないというこの地域の特性を背景に、マネージドセキュリティサービス市場には、多種多様な事業者が参入している。本調査の対象企業の選定は、市場で一定の存在感があり、差別化のための独自の取り組みを進めていること基準としている。徹底した評価と選択プロセスを実行するには時間が要するが、IT バイヤー企業にとっては、信頼でき、高い価値を提供してくれる適切なセキュリティサービス事業者を選定することは重要なテーマである。IT バイヤーは適切な MSSP を活用して、それぞれのセキュリティオペレーションを強化、最適化すべきであるのはもちろんであるが、さらに重要なことは、それぞれのビジネス戦略にさらに合致するようにセキュリティ対策の転換を図ることである。同時に、このような要望が、巧妙化した膨大な脅威に曝されている現状と相まって、セキュリティサービス事業者に、自身のセキュリティ革新戦略／サイバー防衛戦略を強化、加速させ、サイバー犯罪から事業者自身そしてそのクライアントを守らせる要因となっている」と、IDC Asia Pacific セキュリティサービスのシニアリサーチマネージャーである Cathy Huang は述べている。

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

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