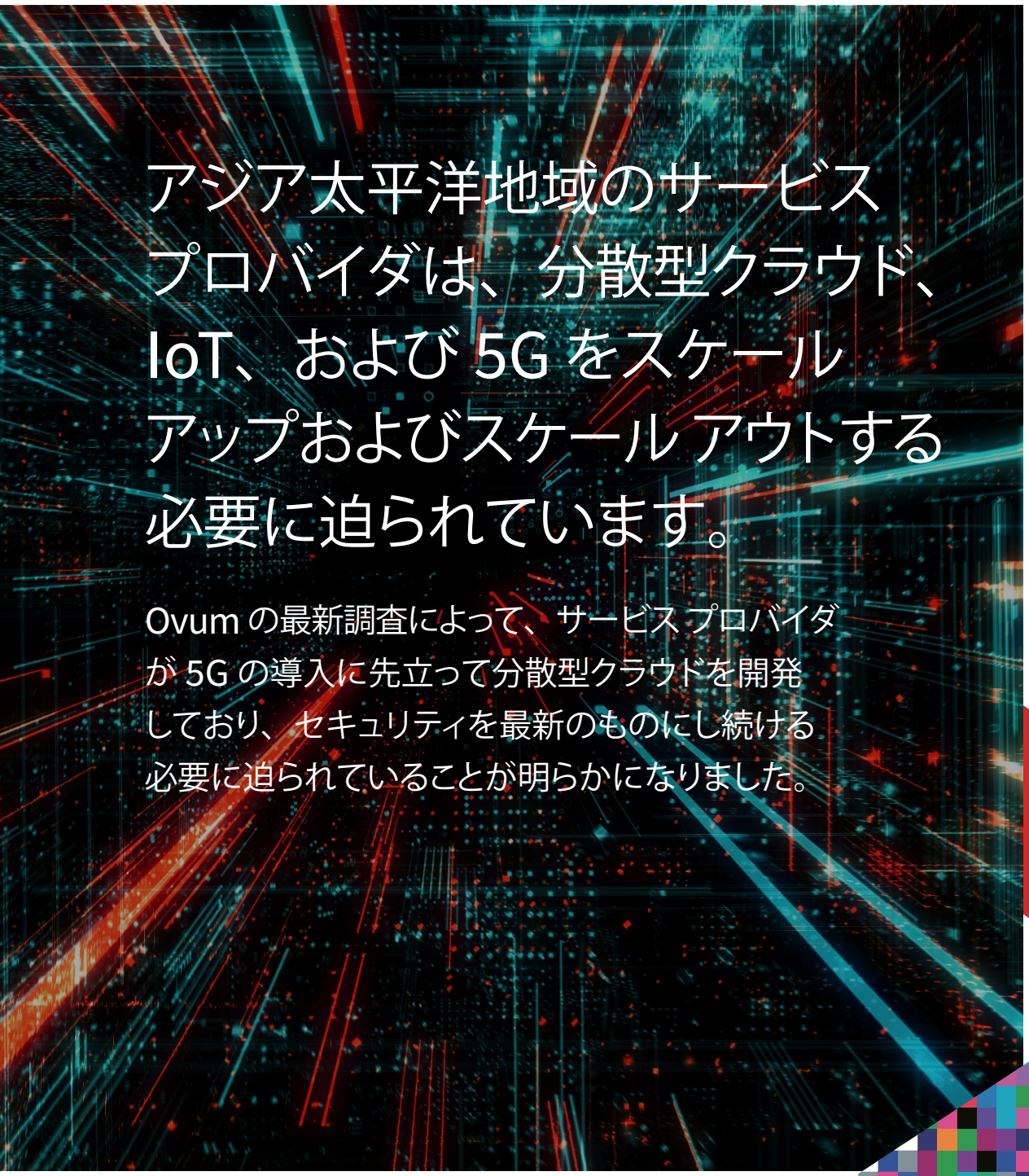


アジア太平洋地域のサービスプロバイダは、分散型クラウド、IoT、および 5G をスケールアップおよびスケール アウトする必要に迫られています。

Ovum の最新調査によって、サービス プロバイダが 5G の導入に先立って分散型クラウドを開発しており、セキュリティを最新のものにし続ける必要に迫られていることが明らかになりました。

概要

サービス プロバイダは、これまで以上に分散型クラウド テクノロジ、モノのインターネット（IoT）、および 5G テクノロジを採用しています。

これにより、容量の増大とパフォーマンスの大幅な向上を実現できるアーキテクチャの必要性が生まれています。新しいアーキテクチャを採用するサービス プロバイダは、新しい要件に合わせて変更できる機敏性を備えたセキュリティ体制を確保し、セキュリティがネットワーク パフォーマンスのボトルネックにならないようにしなければなりません。また、セキュリティ インフラストラクチャは、高まる容量要件に対応するためのスケール アップ、そして、エッジ分配のシグナリングおよびセッション需要の増加に加えて、IoT エンドポイント数の増加に対応するためのスケール アウト可能である必要性があります。

現在、分散型クラウドと IoT を導入するサービス プロバイダが増えています。これらの技術を採用すると、攻撃対象領域が大幅に拡大し、サイバーセキュリティが複雑になります。多くのサービス プロバイダは、新しいセキュリティ ソリューションに投資することで、このような新しい課題に対応しています。しかし、これにより新たな課題も生じます。より重要となる俊敏なネットワークや膨大な数のセキュリティ ツールの統合型ビューがさらに困難になるのです。

こうした背景の下に行われた Ovum の調査では次のことが判明しました。

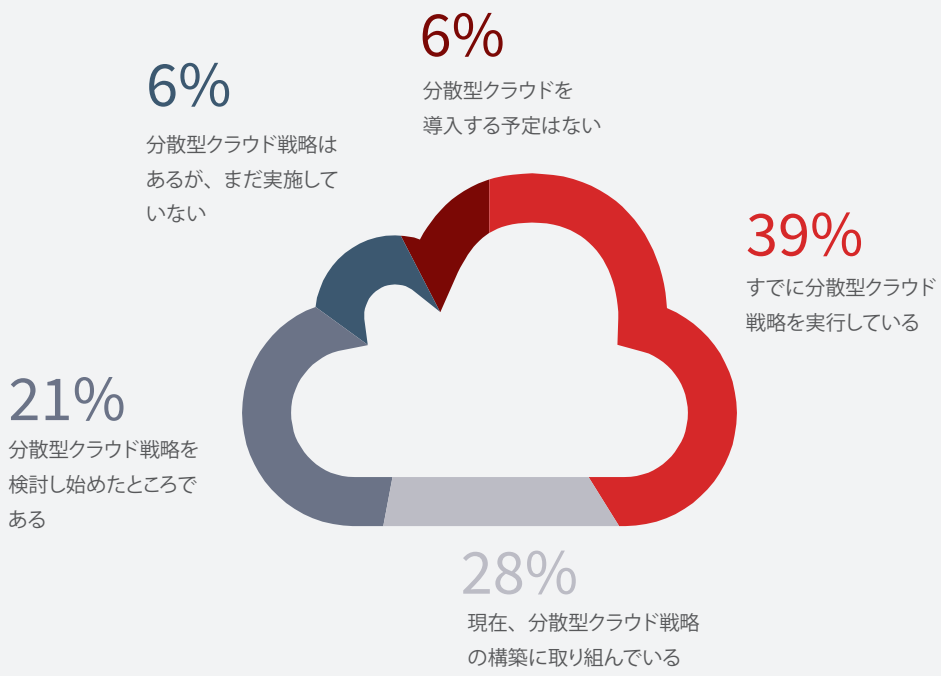
- サービス プロバイダは、5G の導入に先立ち、分散型クラウド アーキテクチャを開発している。
- 分散型クラウドと IoT は、新たなセキュリティの課題を生み出す。
- 5G の利用ではセキュリティがより複雑になり、分散型クラウドと IoT に関連する問題が難しくなる。
- サービス プロバイダは、分散型クラウド、IoT、および 5G 展開に応じて進化していく複数のネットワークの統合ビューが必要になる。
- サービス プロバイダは、セキュリティは確保しているが、セキュリティ体制を分散クラウド、IoT、および 5G の展開に対応できるものにする必要があると回答している。
- サービス プロバイダにとって、侵入検知システムは重点を置くべき分野である

サービス プロバイダは、5G の導入に先立ち、分散型クラウド アーキテクチャを開発している

サービス プロバイダは、俊敏性と運用効率を高めるためにネットワークを変革しています。分散型クラウド アーキテクチャは、計算リソース、ネットワーク、およびストレージ リソースが中央データ センター外の多くの場所に展開され、サービス プロバイダが導入を望む次世代のサービスにおいて重要な役割を果たすでしょう。分散型クラウドは新たな課題を生み出しますが、コストの削減や収益の拡大など、さまざまなメリットも約束してくれます。サービス プロバイダは、何年も前からオープンソース、仮想化、さらにはクラウド化とそれに伴う自動化へと移行している企業と同じように進歩し続けています。

ほとんどのサービス プロバイダは、クラウドベースのアーキテクチャおよび原則が増加し続けるデータ トラフィックを管理するうえで不可欠なものになると考えています。Heavy Reading 社による最近のサービス プロバイダに対するアンケートでは、回答者の大部分が、分散型クラウド戦略をすでに採用しているか、採用を計画していると回答しています。分散型クラウドを導入する各社の意向について、以下の図 1 に示します。

図 1：分散型クラウドの導入計画



分散型クラウドにより、サービス プロバイダは、モノのインターネット（IoT）に対応したサービスを提供できるようになるだけでなく、自社を、サードパーティー製アプリケーションをサポートする立場に位置づけ、隣接市場に参入して新たな収益源を開拓することができるようになります。このような新しいサービスは、5G を導入する前でも提供できます。ただし、5G を導入するには、分散型クラウド、つまりネットワーク変革を加速が必要になります。エンド ユーザーに近い場所での処理を必要とする低遅延サービスは、サービス プロバイダの 5G サービスポート フォリオの重要な部分になると期待されています。

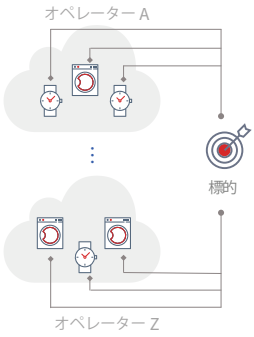
分散型クラウドと IoT は、新たなセキュリティの課題を生み出す

分散型クラウドと IoT を実装すると、悪意のあるハッカーが利用できる攻撃対象領域が大幅に拡大します。IoT の実装ごとに、それぞれ異なるセキュリティ ポリシーとそれに関連する要件が必要となるでしょう。その結果、これらの実装をセキュリティ保護する複雑さが増します。

図 2 に、IoT とエッジ コンピューティングによってもたらされるセキュリティ上の脅威を示します。

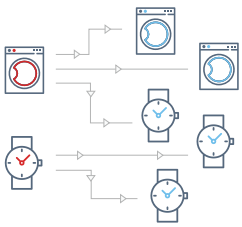
図 2：エッジ コンピューティングと IoT によってもたらされるセキュリティ上の脅威

感染した IoT デバイスからの DDoS 攻撃



- モノカルチャな「モノ（things）」のゾンビ マシン群
- 侵害されたデバイスが連携して大規模な攻撃を実行

IoT 標的ピア デバイス

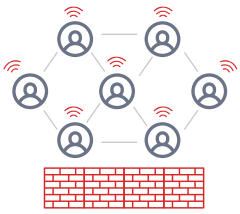


- 侵害されたデバイスが脆弱なピア デバイスを探し回る
- 感染したデバイスのトラフィックがネットワークのパフォーマンスに影響を与える

その他の悪意ある IoT イベント

- OTA 要求フラッド
- デバイス データが外部に露出
- 標的型攻撃
- IoT の破壊行為

予想外の IoT の混乱



- デバイス ローミングの大規模集中
- アクセス ネットワークやゲートウェイの過負荷

このように脅威の数が増加し、それによって引き起こされる損害の規模が大きくなると、サービス プロバイダはそのような課題に対処するために複数のセキュリティ ソリューションを購入しなければならなくなります。

IoT デバイスがネットワークのエントリ ポイントとして使用されるようになるにつれて、IoT デバイスが DDoS 攻撃を開始するための起点として利用されることが増えています。IoT デバイスから発生する脅威の種類は実に多様であり、これらすべてのリスクを管理する必要があります。

これまで、サービス プロバイダは、小規模の DDoS 攻撃であれば、既存の技術を使用して対処できました。しかし大規模な DDoS 攻撃になると、サービス プロバイダはオフラインにすることを余儀なくされ、サービスの中断を引き起こす傾向があります。DDoS 攻撃の頻度、規模、および洗練度が高まるにつれて、新しいソリューションが必要となっています。5G および IoT の時代には、サービス プロバイダは、今までより大規模にトラフィックをフィルタリングできる能力を持つ必要があります。これを実現するためには、サービス プロバイダの保護を自動化、インテリジェンス、機械学習の機能をした形で構築する必要があります。

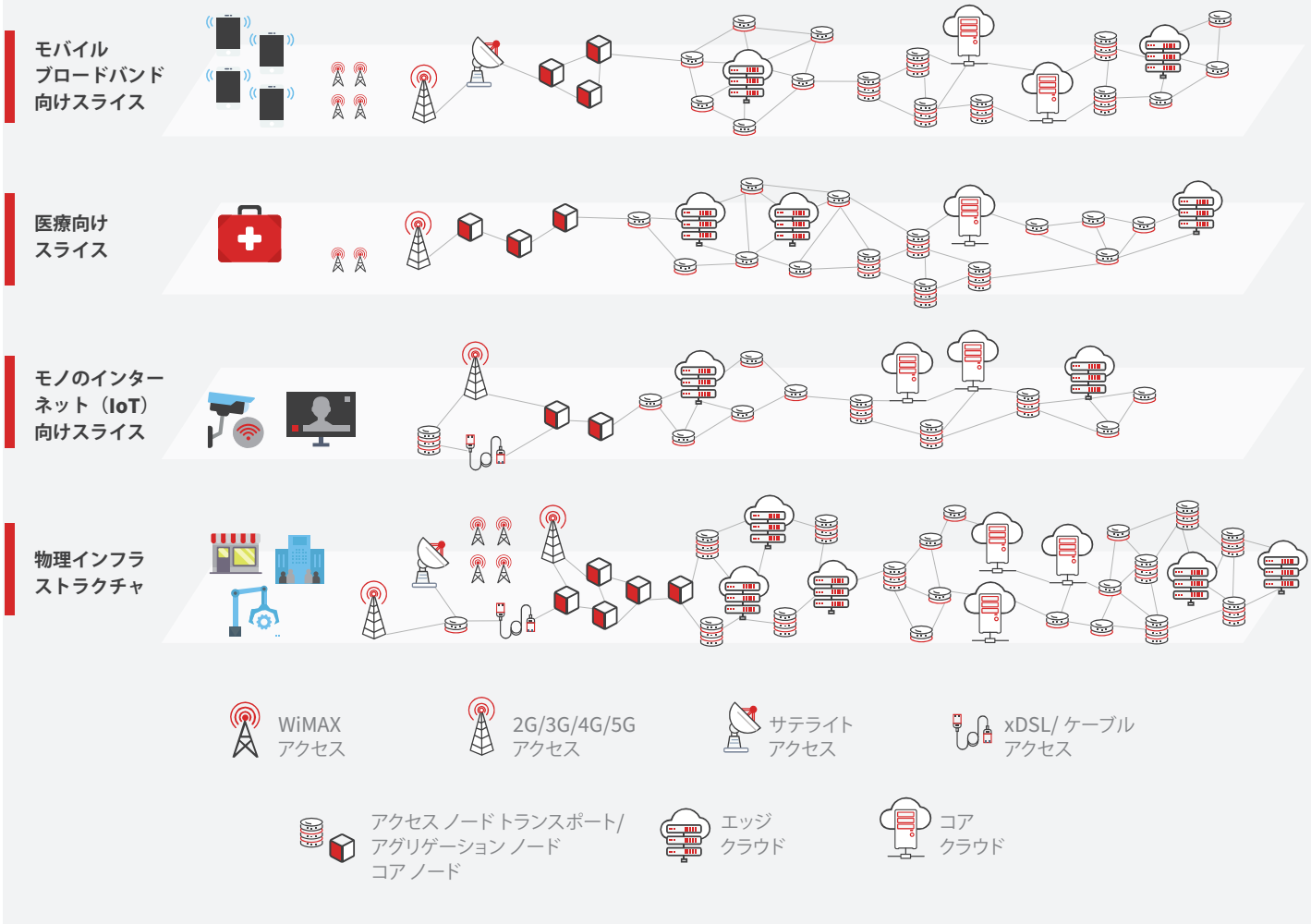
5G の利用はセキュリティを より複雑にする

5G によって、モバイル サービス プロバイダがネットワーク リソースを分割し、さまざまなユーザーの異なるパフォーマンスや機能要件を伴う、多様な使用事例に対応できるようになると期待されています。また、単一の物理インフラストラクチャで、こうした使用事例を多様化することもできます。

このようなフォーマンス プロファイルの多様性は、セキュリティ プロトコルの選択とポリシーの実装に直接影響します。たとえば、スマート シティ アプリケーションなどの使用事例におけるサービスでは、非常に長い寿命のバッテリー寿命が必要になる場合があり、これによりセキュリティ プロトコルが他の何らかの形で制約を受けます（頻繁な再認証の実行など）。あるいは、その用途がプライバシにきわめて敏感なものであり、きわめて処理が集中するセキュリティ手順（一時的な ID の頻繁な再割り当てなど）を必要とする場合などが考えられます。

図 3 は、5G がさまざまな用途やネットワーク スライスの提供につながることを示しています。

図 3 – ネットワーク スライシングと 5G の用途

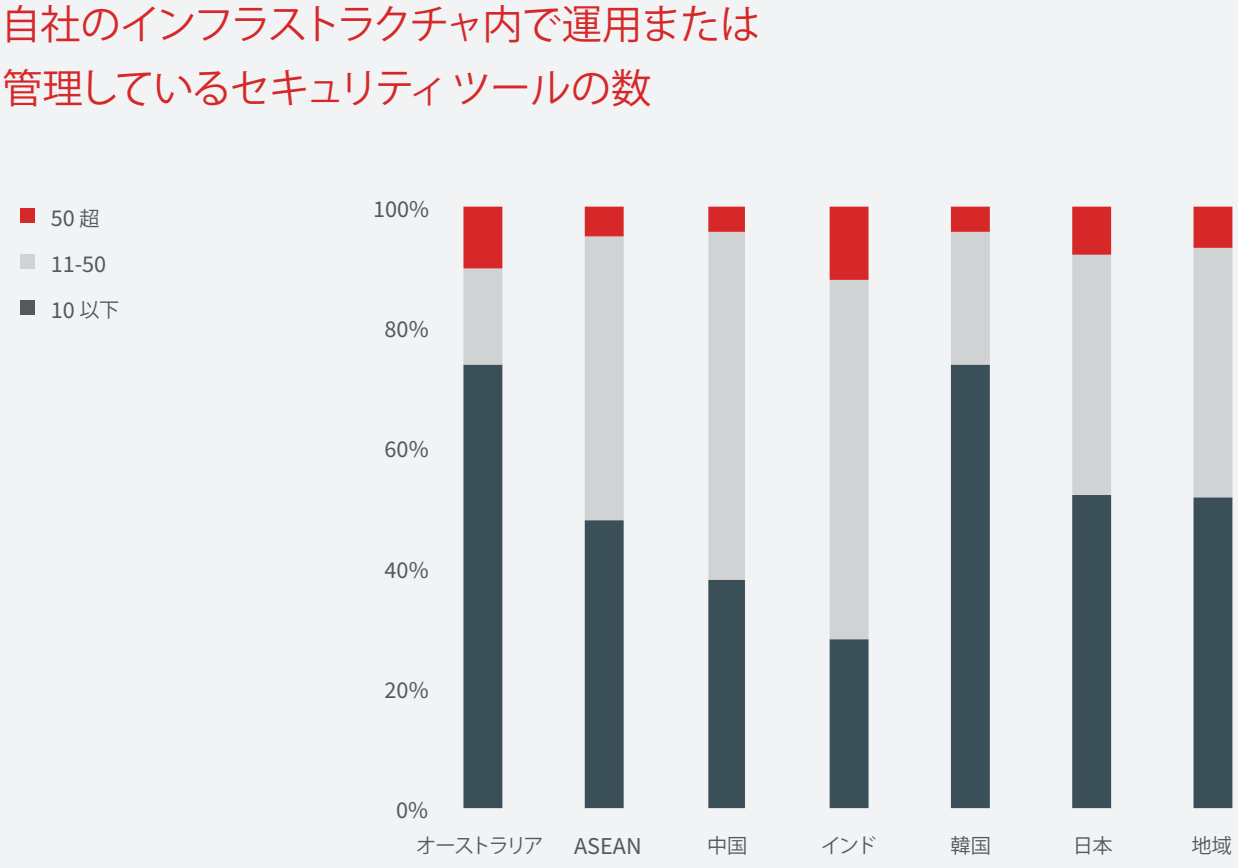


サービス プロバイダには、進化する複数のネットワークの統合ビューが必要

多くのサービス プロバイダの意思決定者は、分散型クラウド環境と IoT 環境の複雑性が高まり、既存のツールでは新たに出現する脅威をすべて検出できないという状況に、最新のセキュリティ ソリューションを複数導入することで対応しています。ところが、そのうちに、連携しないセキュリティ製品が増え、情報がそれぞれ独自のダッシュボードに表示されるという状況になってしまいます。サービス プロバイダは、通常、SIEM を利用してこのような管理上の課題に対処していますが、彼らは、サイバーセキュリティ スタッフが複数のコンソールを監視したり、別々の画面や異なるフォーマットの情報の間を相互に参照したりする課題に直面しないように、常に、セキュリティ アラートの一元的な表示を提供するようにしなければなりません。さらに、ダッシュボードが複数ある環境では、セキュリティ ポリシーの変更を適用するのは手間と時間がかかる作業であり、そうした状況自体がセキュリティ上の脅威となります。

図 4 は、サービス プロバイダを含むアジア太平洋地域組織がどれだけの数のツールを利用しているかを示しています。

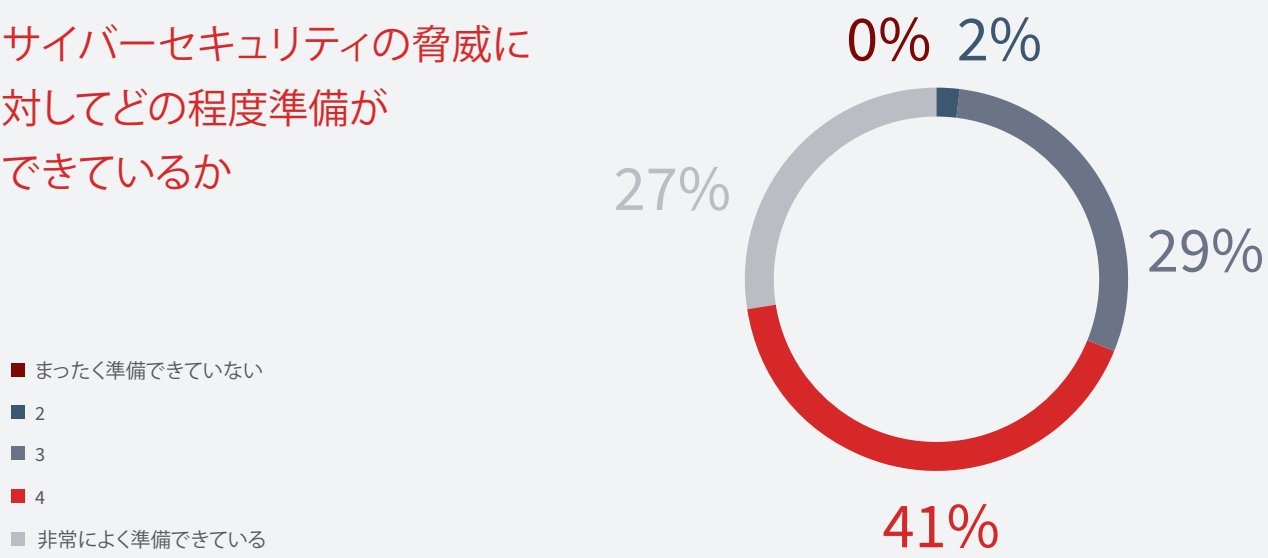
図 4：アジア太平洋地域の大規模な組織で使用されるセキュリティツールの数



サービス プロバイダは、自社のセキュリティ体制を分散型クラウド、IoT、および 5G の展開に対応できるものにする必要がある

インタビューを受けたサービス プロバイダは、サイバーセキュリティの脅威に対して十分準備ができていると回答しています。サイバーセキュリティの準備状況に関する 5 段階の自己評価を依頼したところ、3 分の 2 以上のサービス プロバイダが、自社のサイバーセキュリティの脅威に対する準備を「よく準備できている」か「非常によく準備できている」と回答しています。
以下の図 5 に、サービス プロバイダの認識を示します。

図 5：サイバーセキュリティの脅威に対する準備状況の認識



サービス プロバイダが分散型クラウド、IoT、および 5G テクノロジを採用するにつれて、セキュリティには、スケール アップのための物理インフラストラクチャのアップグレードと、スケール アップとスケール アウトの両方のための仮想インフラストラクチャのアップグレードが必要になるでしょう。パフォーマンスを高めるためにこのような投資を行わなければ、セキュリティがネットワーク パフォーマンス全体のボトルネックになってしまいます。

5G の採用により、利用可能な帯域幅が増え、侵害された接続デバイスからの攻撃トラフィック生成に対してネットワークがさらに堅牢になります。高ボリューム型 DDoS 攻撃の頻度、規模、および洗練度が高まるにつれて、アウトオブバンドのスクラビング センターや手動による介入などの従来の防御は、不十分で、かつ費用がかかりすぎるものとなっています。

高ボリューム型攻撃の場合、疑わしいトラフィックをスクラビング センターにリダイレクトすると、遅延が増え、大きな経済的負担がかかります。攻撃防御のコストはデータ トラフィックの量と直接結びついているためです。サービス プロバイダは、よりインテリジェントでコスト効率の高い検出および攻撃防御プロセスを自動化するための、AI、リアル タイム分析、テレメトリを含む、DDoS 攻撃に対する新しい防御アプローチの採用を検討する必要があります。

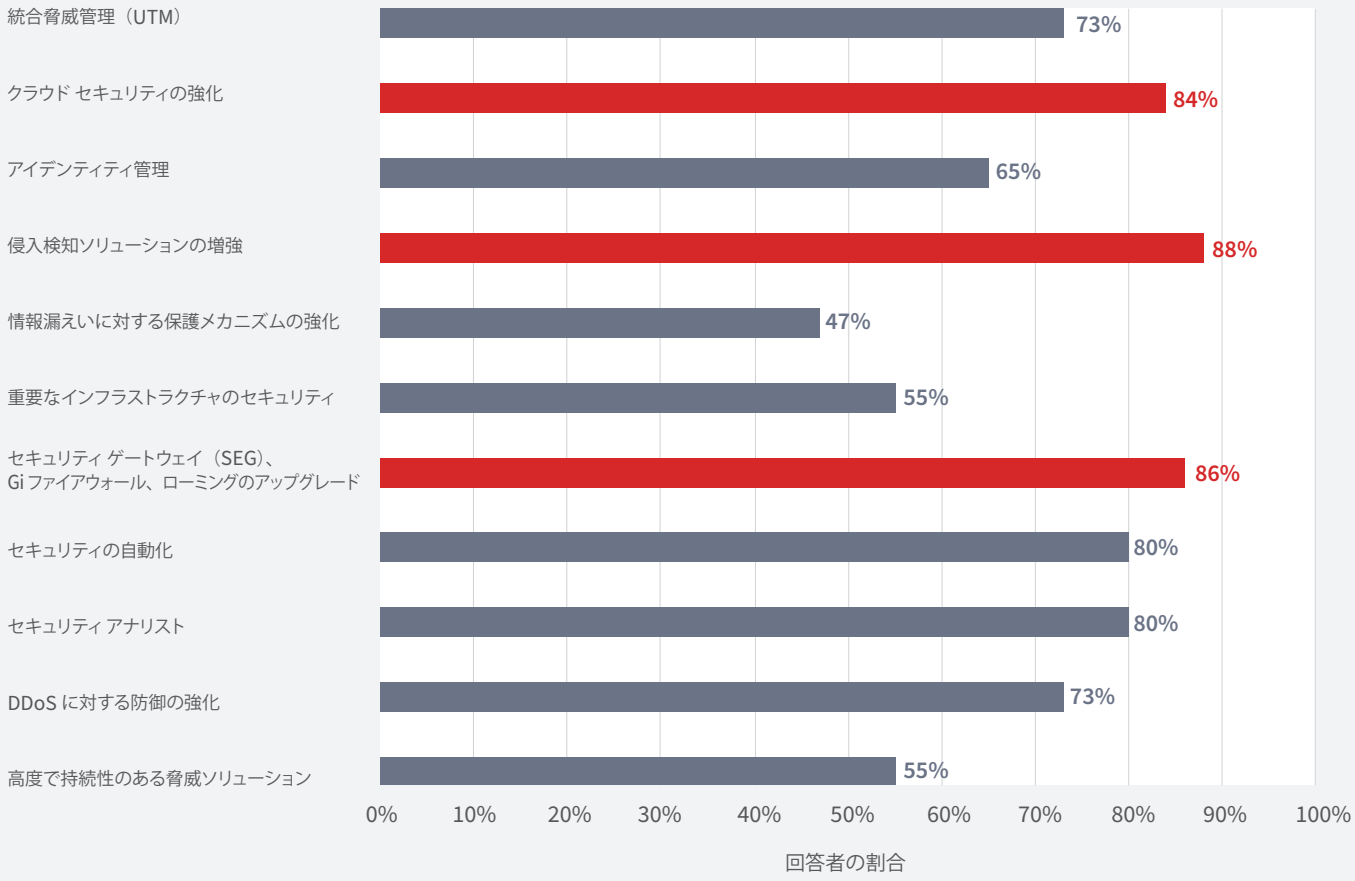
セキュリティ運用では、パフォーマンスだけでなく、物理ネットワーク機能（PNF）および仮想ネットワーク機能（VNF）を備えた分散型 Telco クラウド環境も拡張し、サポートしなければなりません。それには物理ドメインと仮想ドメインの両方を管理し、それらのドメインの統合ビューを提供する、統合セキュリティ管理システムが必要です。つまり、セキュリティ管理では、システム全体を包括的に可視化する必要があります。この戦略のもう 1 つの要素は、プログラム可能なセキュリティ ポリシーを通じて自動化されたポリシー オーケストレーションを活用して、サービス品質保証契約（SLA）を満たす信頼性の高い安全なネットワークを確保することです。

サービス プロバイダにとって、侵入検知システムは重点を置くべき領域である

クラウド、IoT、および 5G テクノロジがもたらす新たなサイバーセキュリティの課題に対処するため、サービスプロバイダーは複数のソリューションに投資しています。最も重点を置くべき領域としては、侵入検知システムの増強、クラウド セキュリティおよびファイアウォールのアップグレードが挙げられています。

クラウド、IoT、5G の新たな課題への対処

新たな 5G、IoT、クラウドに関する脅威に対してどのように対処する予定か



サービス プロバイダが管理する攻撃対象領域が大幅に増えていることを考えると、インテリジェンスと機械学習をより広範囲に利用する必要があります。現在、サービス プロバイダのセキュリティ システムは、既知の脅威と比較的小規模の DDoS 攻撃に対処するうえで十分な機能を備えているのが普通です。大規模な DDoS 攻撃と洗練された攻撃に対処すると同時に、サービスの中断を最小限に抑えるには、自動化、人工知能、機械学習をより広範に活用するしかありません。

推奨事項

本調査は、サービス プロバイダは、新しいテクノロジの展開に関連するリスクを管理する必要があることを示しています。特に、分散型クラウド、IoT、および 5G テクノロジでは、現在のセキュリティ体制に対する大きな変更が必要になります。

サービス プロバイダは、分散型クラウド、IoT、および 5G テクノロジを採用するにあたって、資産を保護するために以下のアプローチを取る必要があります。

- 分散型クラウド、IoT/ エッジ コンピューティング、5G への移行に合わせて、セキュリティ インフラストラクチャをスケール アップおよびスケール アウトする。
- セキュリティ パフォーマンスを評価して、セキュリティ ソリューションがネットワーク インフラストラクチャ上での需要の増加にとってのボトルネックにならないようにする。
- 侵入検知システムを最新のものにする。脆弱な侵入検知システムが、DDoS 攻撃の増加につながります。侵入検知システムで人工知能と機械学習を利用して、未知の脅威による異常なネットワーク アクティビティを検知して対処できるようにします。
- サービス プロバイダは、物理ドメインと仮想ドメインの両方を管理でき、それらのドメインの統合ビューを提供する、統合セキュリティ管理システムを用意する必要がある。

調査方法

ジュニパーネットワークスは、Ovum にアジア太平洋地域のサービス プロバイダの IT 意思決定者 50 人に対するアンケートを依頼しました。この調査で得られたデータは、Heavy Reading が実施した、100 人のサービス意思決定者に対するグローバルなアンケートで得られたデータと共に利用されました。

著者

アンドリュー・ミルロイ
アジア太平洋地域、顧問サービス責任者
andrew.milroy@ovum.com

Ovum のコンサルタント サービス

本分析が貴社に有用な情報をもたらし、ビジネス上の創造的な意志決定にお役に立てば幸いです。ご不明な点などがありましたら、Ovum のコンサルタント チームが回答いたします。Ovum のコンサルタント サービスについて詳しくは、consulting@ovum.com 宛てに直接ご連絡ください。

著作権の表示と免責条項

お問い合わせ

www.ovum.com
askananalyst@ovum.com

各国のオフィス

北京
ドバイ
香港
ハイデラバード
ヨハネスブルク
ロンドン
メルボルン
ニューヨーク
サンフランシスコ
サンパウロ
東京

900061-JP-001 2019 年 11 月