「ネットワーク」と「セキュリティ」の実態と展望に関する市場調査レポート

アルテリア・ネットワークス株式会社

調査概要

ARTERIA
アルテリア・ネットワークス株式会社

調査目的	勤務先でのネットワークとセキュリティに関する導入意向や課題についての意識調査
調査対象	アイティメディアID会員
調査期間	2025年1月24日～2025年2月19日
調査手段	Web メディア掲載およびメール配信による オンラインアンケート
有効回答数	285件

※調査結果の統計データについては、個別の割合の小数点以下第2 位を四捨五入しているため、必ずしも合計が100%にならない場合があります。

調査結果サマリー

アイティメディアは、2025 年1 月から2 月にかけて、EDR（Endpoint Detection and Response）やSASE（Secure Access Service Edge）の導入状況アンケート調査を実施した。

本レポートはその結果をまとめたものである。集まった回答のうち、設問1（ネットワークインフラに関する回答者の立場）に「ネットワークインフラには関与しない」と答えた回答を除く285 件を有効回答とした。

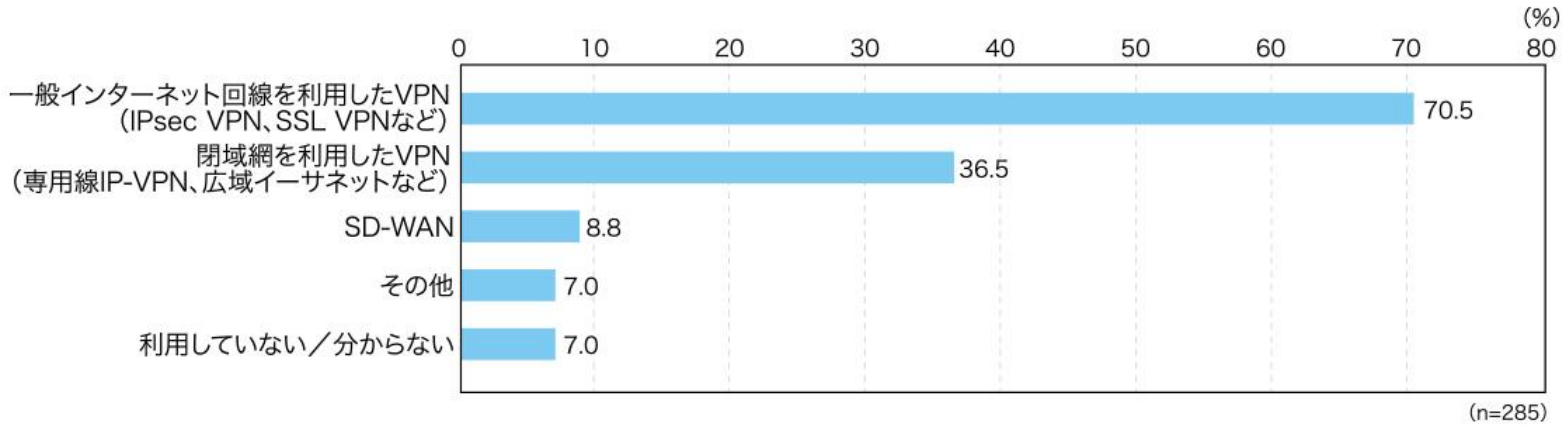
以下に、調査を通じて判明したことと推測されることを挙げる。

- 使用中のネットワーク技術としてはVPN（仮想プライベートネットワーク）が主流。SD-WAN（ソフトウェア定義WAN）を導入済みの企業はまだ少なく、初期段階にある。
- ネットワーク運用の主な課題はパフォーマンス低下、セキュリティの脆弱性、コスト増加の3 つ。
- 企業はランサムウェア、情報漏えい、人の不注意や悪意などを身近な脅威として捉えている。6 割以上が、セキュリティ対策としてのEDR の重要性を認識している。
- SASE を導入済みの企業は約1 割で、4 分の1 以上が導入についての意欲を示す。企業のSASE に対する理解が進んでいないことが、導入を妨げる一因になっている。
- 企業はSASE に対してセキュリティの向上、運用管理の効率化、コスト最適化といった効果を期待している。SASE にはネットワークの可用性やスケーラビリティの向上、パフォーマンス向上といった効果も見込めるが、今回の調査ではそこまで期待度は高くなかった。SASE への理解度を深め、自社の課題解決に役立つかどうかを判断することが重要だ。
- 人材不足や予算不足の解消、業務の省力化といったネットワークとセキュリティにおける主要な課題は、ベンダーを積極的に活用して解決するとよい。人材育成や外部人材の投入、SOC（Security Operation Center）のマネージドサービスなどが助けになる。

利用中のネットワーク技術の種別

ARTERIA
アルテリア・ネットワークス株式会社

お勤め先でご利用中のネットワーク技術の種別をお聞かせください。（複数選択可）



設問2 では、自社で利用しているネットワーク技術について質問した。選択肢はインターネット回線利用のVPN、閉域網利用のVPN、SD-WAN の3 つだ。

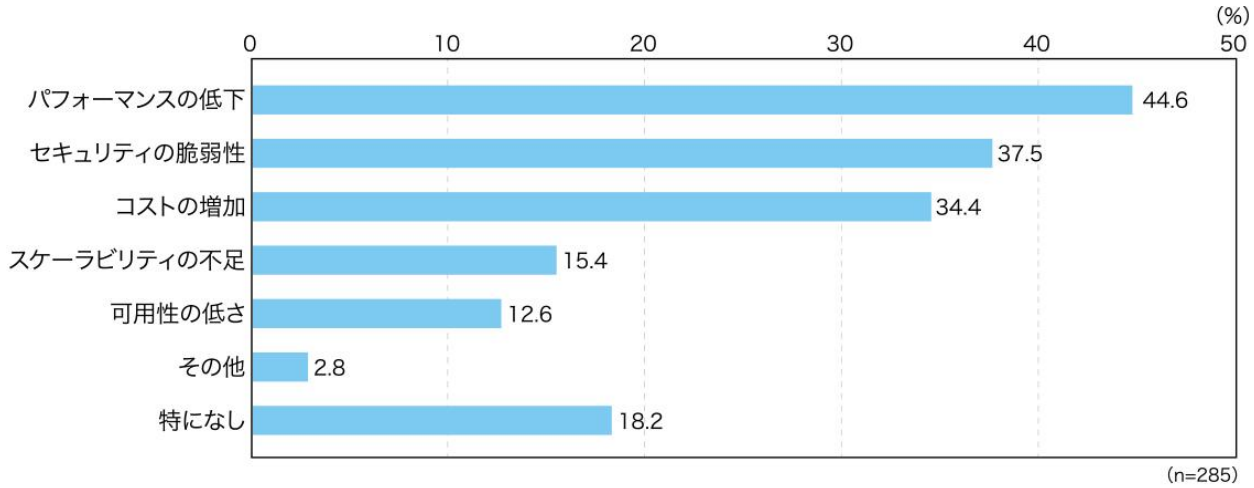
結果を見ると、インターネットVPN を使うとした回答が70.5%あるのに対し、閉域網VPN は36.5%と半分程度だった。閉域網VPN はセキュリティを重視する企業が主に利用するネットワークだが、利用料金もその分かさみやすい。比較的安価なインターネット回線を利用するインターネットVPNはコストパフォーマンスに優れており、テレワークやハイブリッドワーク（テレワークとオフィスワークの併用）時にセキュアな回線として使えるという利点もある。

このように普及しているVPN に比べると、SD-WAN の導入率は8.8%と低い。SD-WAN の特徴は、複数の回線をソフトウェアで仮想化して一元管理することで、トラフィックの状況に応じて経路を最適化し、帯域幅（通信路容量）を効率的に活用できるようになることだ。ただし現時点では、多くの企業はインターネットVPN の省コスト性の方が重要だと考えていることがうかがえる。

利用中のネットワークインフラの課題

ARTERIA
アルテリア・ネットワークス株式会社

お勤め先における、現在のネットワークインフラの主な課題をお聞かせください。
（上位2つまで複数選択可）



設問3では、現在利用中のネットワークインフラに対して感じている課題を尋ねた。

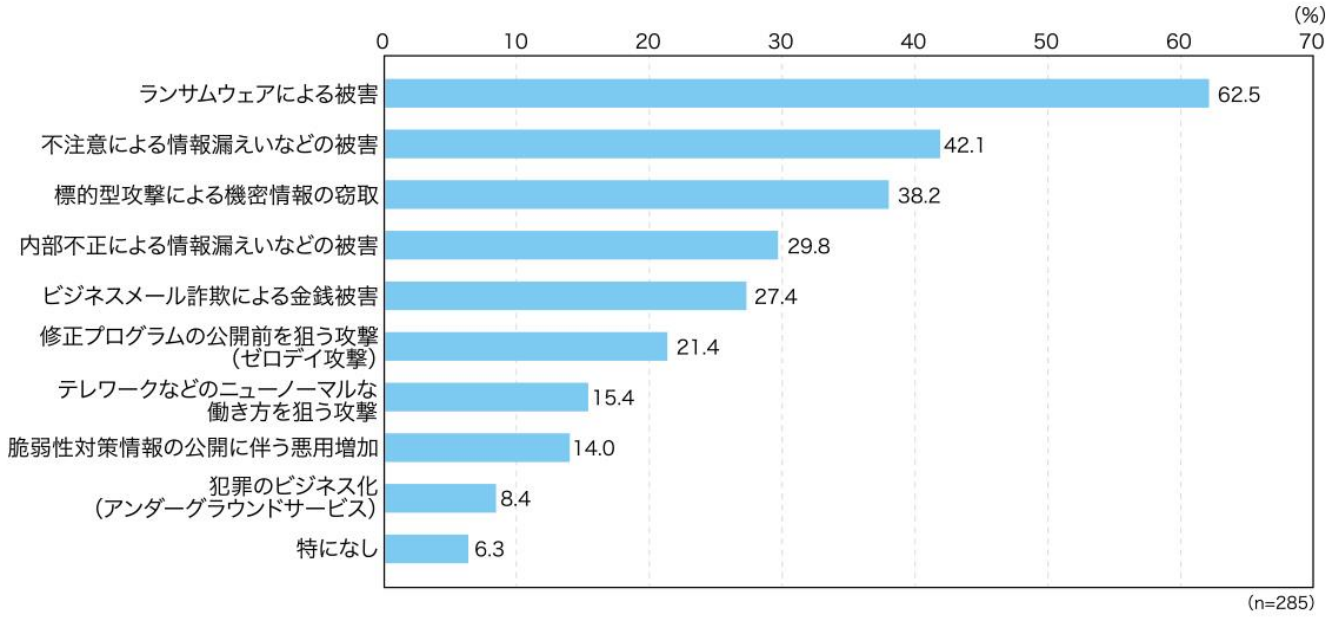
トップ3に挙がったのは「パフォーマンスの低下」「セキュリティの脆弱性」「コストの増加」で、いずれも回答者の3分の1以上が選択した。通信速度などのネットワークパフォーマンスの低下は、SD-WANによるインターネットブレークアウト（データセンターを介さずにインターネットに直接接続する技術）やSASEといった、最新のネットワーク技術を採用することで解決できる可能性がある。

「その他」と回答した人に対して、具体的な課題を設問4で聞いたところ、人材や運用体制の欠如、セキュリティ確保の難しさ、障害の原因特定と対処の迅速化などが挙がった。これらの課題を解決するには、セキュリティ対策や障害対処のための製品／サービスを導入したり、人材育成や運用管理の体制を見直したりすることが有効だ。

身近な脅威

ARTERIA
アルテリア・ネットワークス株式会社

お勤め先において、どのような脅威が身近に感じられるかをお聞かせください。
（上位2つまで複数選択可）



設問5 では、懸念している脅威の具体的な内容を質問した。

結果は、「ランサムウェアによる被害」が62.5%と最多だった。これに続くのが情報漏えい関連の脅威で、不注意によるもの（42.1%）、標的型攻撃によるもの（38.2%）、内部不正によるもの（29.8%）を懸念する人が多く見られた。人の注意力欠如や悪意によって発生する脅威（不注意、内部不正、ビジネスメール詐欺）を選んだ人もそれぞれ25%以上おり、比較的関心が高い。

これらの脅威に対抗するには、セキュリティ対策ツールによる技術的対策だけではなく、従業員の意識や業務プロセスの変革を促す人的対策も欠かせない。ベンダーが提供する人材育成や従業員教育のプログラムを活用したり、独立行政法人情報処理推進機構（IPA）などのセキュリティ機関が策定するセキュリティガイドラインを参照して実践したりすることが対策になる。

EDRの導入状況

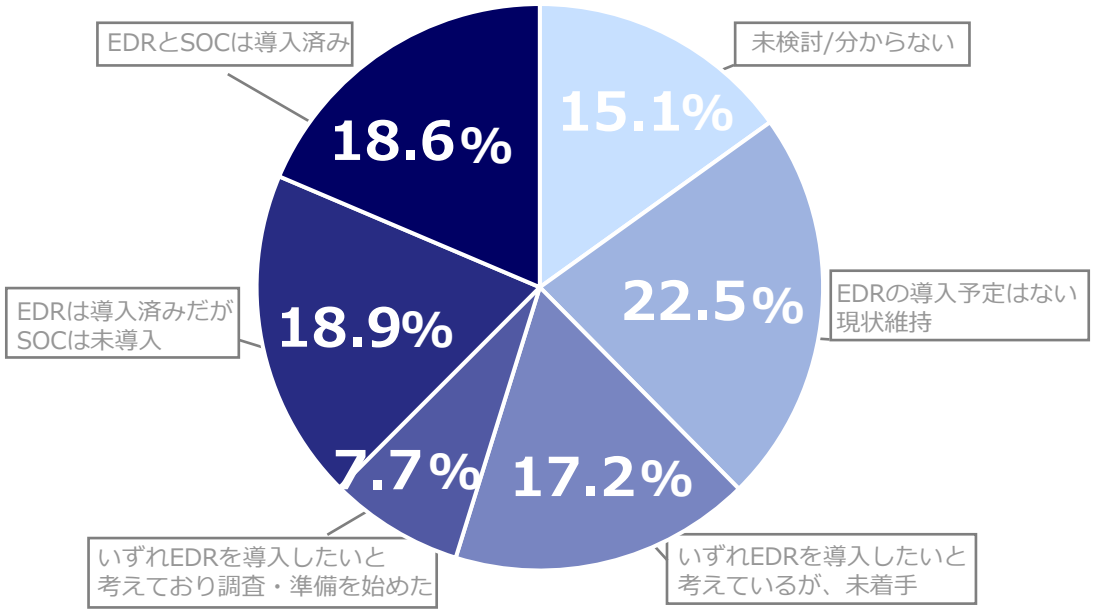
ARTERIA
アルテリア・ネットワークス株式会社

お勤め先における、EDRの導入状況をお聞かせください。

設問6 では、セキュリティの脅威に対抗するための技術的対策となるEDRとSOC の導入状況を調べた。

EDR を導入済みの企業は37.5%、導入の意向がある企業は24.9%あり、両者を合わせると6 割以上の企業がEDR の必要性を認識していることが読み取れる。EDR は従来のセキュリティ対策の延長線上にあり、従来のセキュリティの枠組みとして理解しやすい技術であるため、その重要性も認識しやすいと感じていることの表れだと考えられる。設問5 で懸念する脅威の具体例を聞いた際、ランサムウェアによる被害がトップになっていたことを踏まえれば、今後EDR の導入率はさらに高まると言える。

一方で、セキュリティの運用管理にSOC を利用していない企業は81.4%に上った。エンドポイントでマルウェアを検出して対処するEDR は大量のアラートを発するので、使いこなすには専門的な知見や24 時間365日の監視体制、インシデント対処プロセスが重要になる。EDR を活用したセキュリティ強化にはSOC が不可欠であるため、人材や運用の面で課題を抱えている企業は、外部SOC サービスを積極的に導入して、SOCをセキュリティ運用に組み込むことが望ましい。

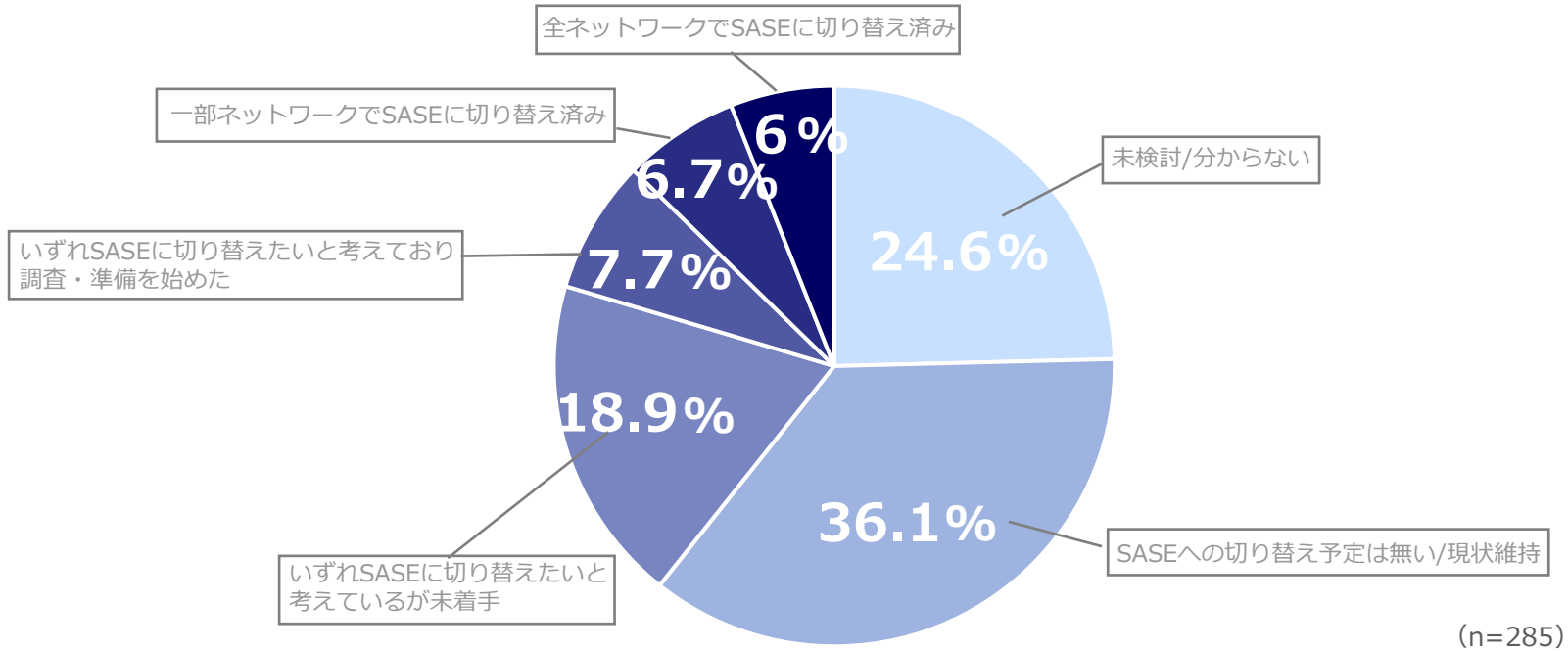


（n=285）

SASEの導入状況

ARTERIA
アルテリア・ネットワークス株式会社

お勤め先における、SASEの導入状況をお聞かせください。



（n=285）

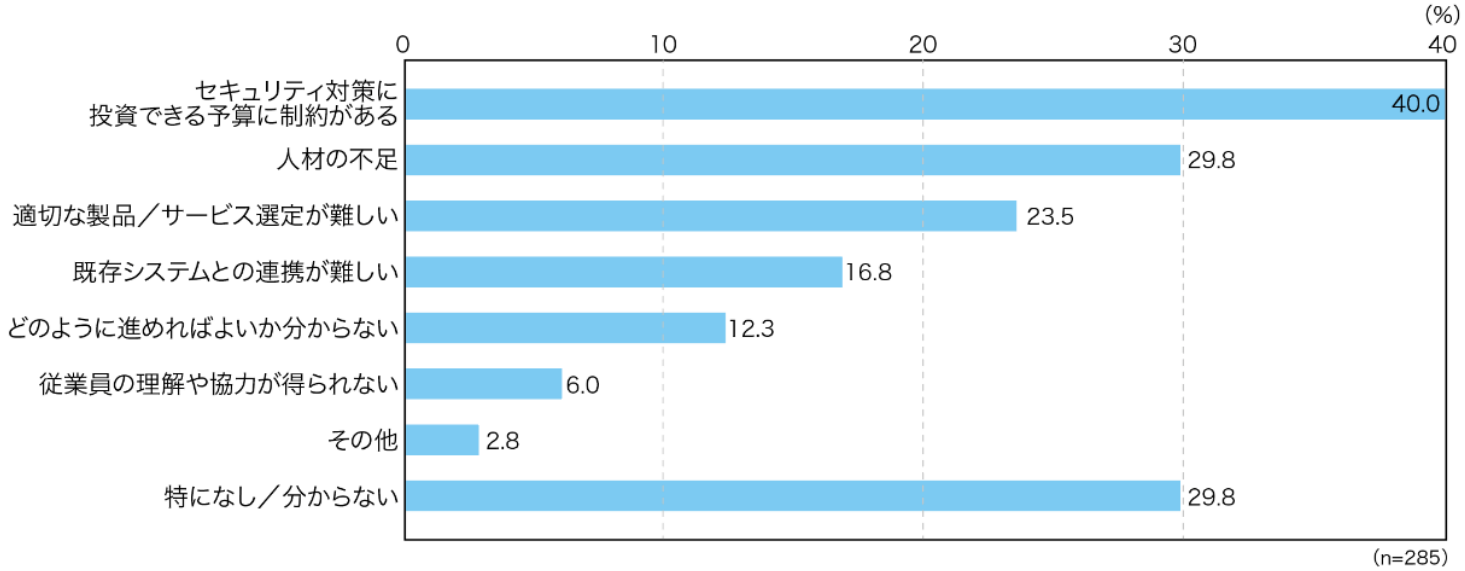
ネットワークセキュリティを包括的に強化するアプローチとしてはSASEがある。SASEはSD-WANなどのネットワーク機能と、CASB（Cloud Access Security Broker）、SWG（Secure Web Gateway）などのセキュリティ機能を統合し、クラウドサービスとして提供するアーキテクチャだ。設問7 では、企業のSASE 導入状況を調べた。

ネットワークの全部または一部をSASE に切り替え済みと回答した企業は1 割以上あった。一方で、「いずれSASE に切り替えたいと考えており、調査・準備を始めた」「いずれSASE に切り替えたいと考えているが、未着手」を合わせると、4 分の1 以上の企業がSASE の導入を検討中であることが分かる。

SASE導入の障壁

ARTERIA
アルテリア・ネットワークス株式会社

お勤め先における、SASE導入の主な障害をお聞かせください。（上位2つまで複数選択可）



設問8 は、SASE 導入の妨げになっている要因を問う質問だ。

注目したいのは、「既存システムとの連携が難しい」という技術的な理由を挙げた回答が16.8%にとどまっていることだ。設問7（SASE の導入状況）で、「将来はSASE に切り替えたいが調査には未着手」と答えた企業が18.9%とやや多かったことを考慮すると、SASE の導入検討自体を始めている企業がまだ少ない状況だと言える。

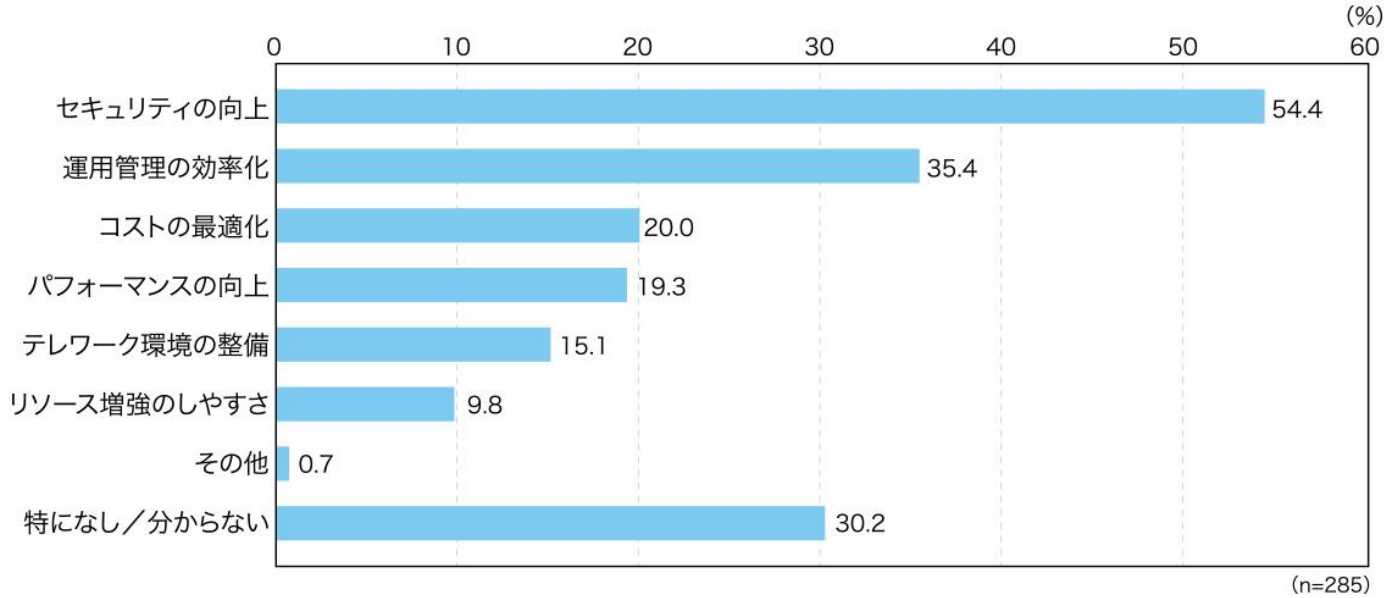
上位の回答を見ると、予算制約（40%）、人材不足（29.8%）、製品選定の難しさ（23.5%）などの理由が並ぶ。このことから、SASE を理解できていないために製品選定が難しく、SASE を使えるセキュリティ人材が少ないという企業の現状が浮かび上がる。SASE の理解が進んでいないことは、「特になし／分からない」の回答が29.8%あることからもうかがえる。

これらの課題を乗り越えるためには、自社のネットワークやセキュリティの運用における課題の特定から製品／サービスの選定、導入、実運用、人材育成といった一連のプロセスでベンダーの力を借りることが一助になる。特に専門人材が不足している場合、ネットワークやセキュリティのマネージドサービスを導入することは効果的だ。

SASEに期待する効果

ARTERIA
アルテリア・ネットワークス株式会社

SASEにどのような効果を期待されているかをお聞かせください。（上位2つまで複数選択可）



設問9 では、企業がSASE に期待している効果を尋ねた。

突出しているのは「セキュリティの向上」（54.4%）だ。設問5（脅威の具体例）で「ランサムウェアの被害」が最大の懸念事項に挙がっており、その脅威を緩和する効果をSASE に期待していると考えられる。これに次ぐのが、「運用管理の効率化（35.4%）だった。

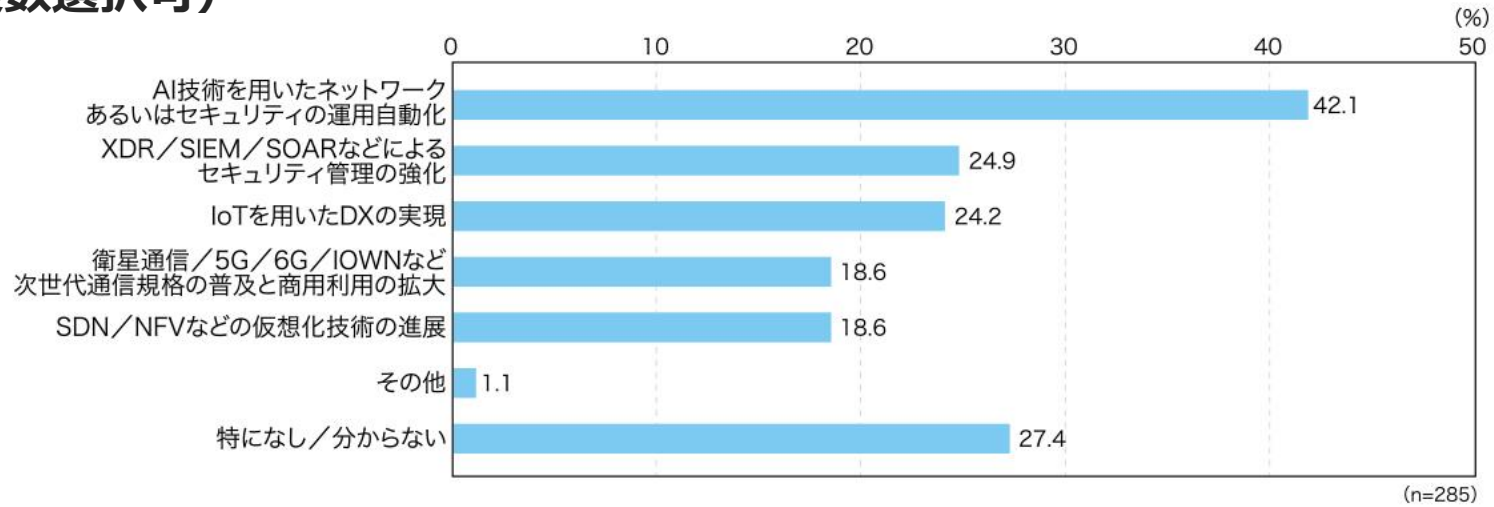
少し離れて「コストの最適化」（20.0%）と「パフォーマンスの向上」（19.3%）が続く。この2 つは、設問3（ネットワークインフラの課題）で第3 位となった「コストの増加」と、第1 位の「パフォーマンスの低下」の2つの課題に対応する効果だ。

企業がパフォーマンス向上効果をそれほど高く評価していない理由として考えられるのは、SASEの主要な価値を「セキュリティとネットワーク機能の統合」だと認識していることだ。SASE はトラフィックの経路最適化やインフラのスケーリングなどによって、ネットワークのパフォーマンス向上に貢献し得る。

関心のあるネットワーク分野の動向

ARTERIA
アルテリア・ネットワークス株式会社

ネットワーク分野において、現在関心をお持ちの動向をお聞かせください。
（上位2つまで複数選択可）



設問10 では、ネットワーク分野で関心を持っている技術動向を質問した。

最も多かったのは「AI 技術を用いたネットワークあるいはセキュリティの運用自動化」（42.1%）だ。セキュリティ管理の強化（24.9%）とDX の実現（24.2%）に役立つ技術への関心も高い。

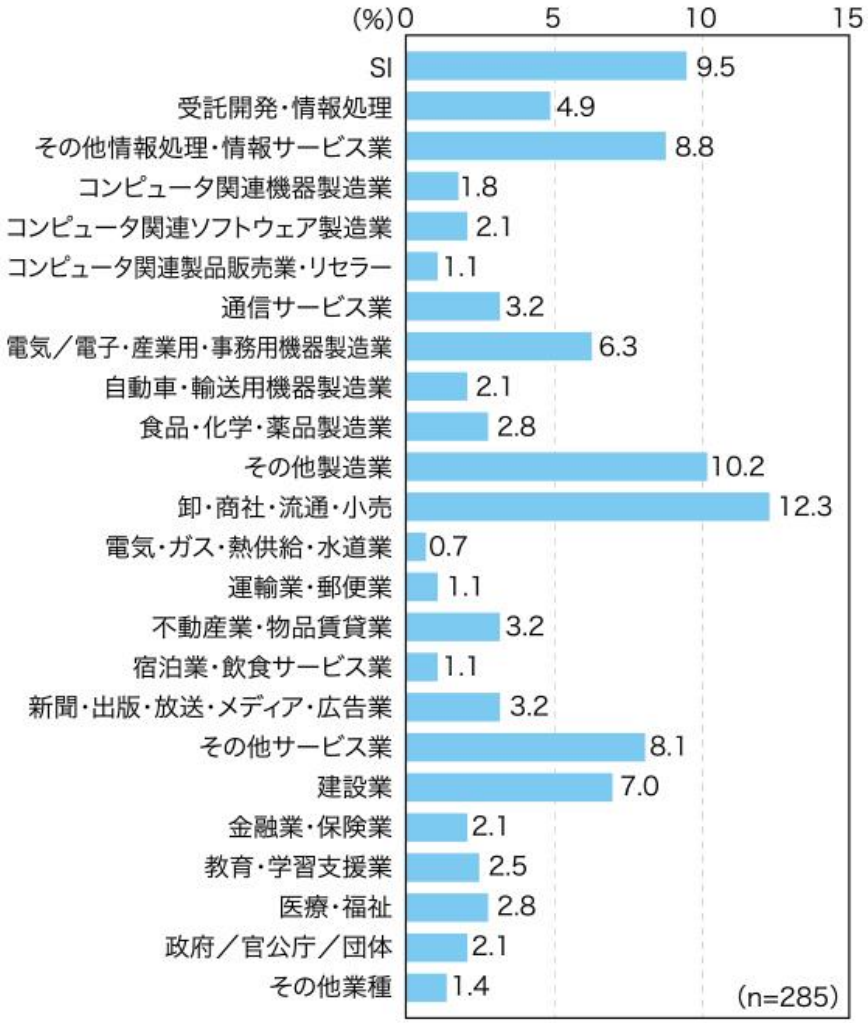
最新のネットワーク技術（衛星通信／ 5G ／ 6G ／ IOWN など）やネットワーク仮想化技術（SDN ／ NFVなど）に対する関心（共に18.6%）は、その他の項目と比べてあまり高くない。自動化、効率化といった実務的、即効性のある技術革新に期待が集まる一方、DX 推進などの長期的な進展や通信技術に対する期待は相対的に低いことが分かる。

「特になし／分からない」と回答した企業が27.4%あることを見ると、多くの企業が日常の運用管理業務に追われ、新技術の評価や導入検討に十分な時間を割けていない可能性がある。このような状況にある企業は、ベンダーやコンサルタントなど専門家の支援を受け、自社の課題やニーズに合う製品／サービスについての知見を得ることが有効だ。

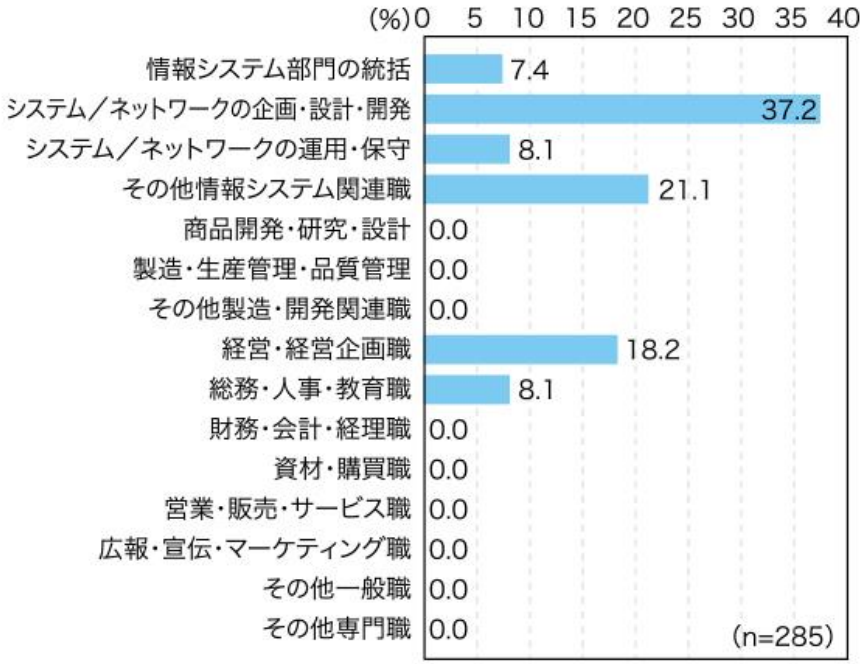
回答者属性

ARTERIA
アルテリア・ネットワークス株式会社

職種



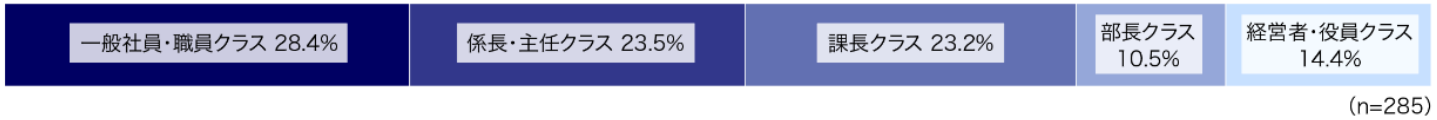
職務内容



回答者属性

ARTERIA
アルテリア・ネットワークス株式会社

役職クラス

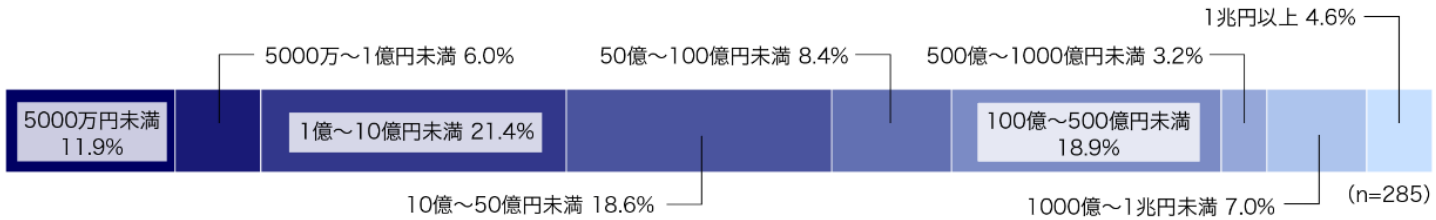


(n=285)

従業員数

(n=285)

年商規模

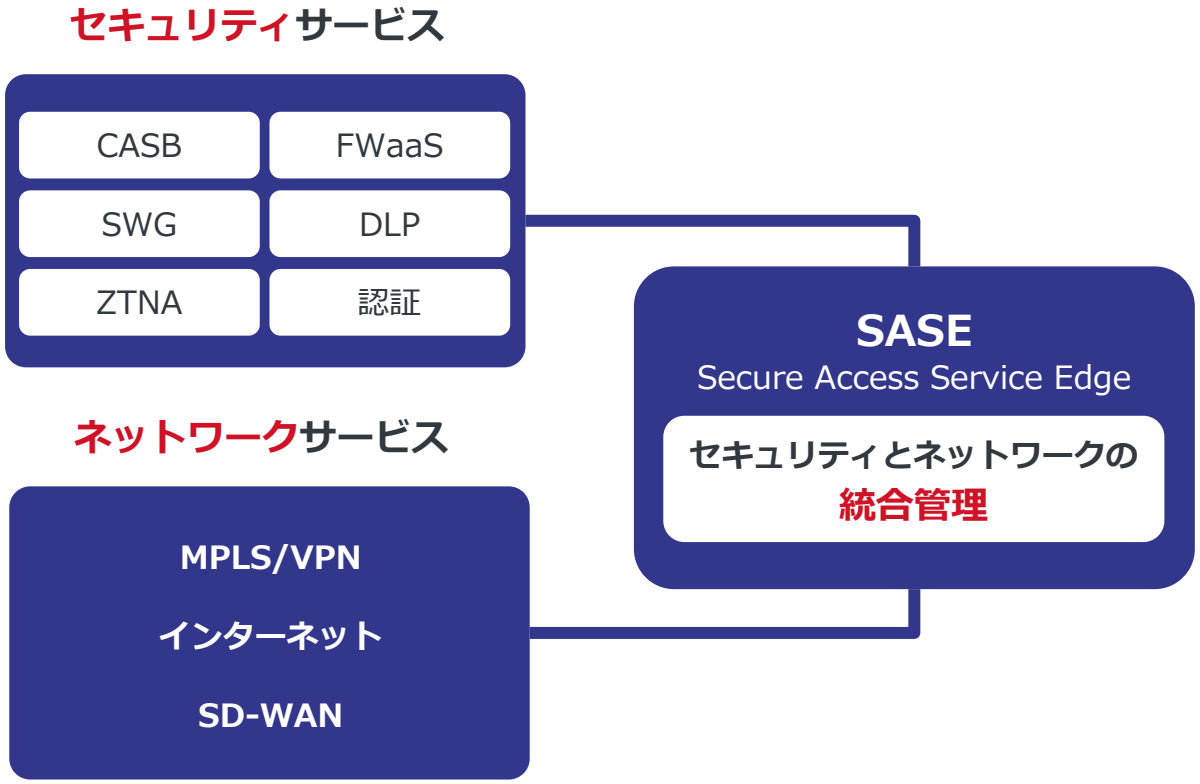


(n=285)

勤務地

(n=285)

SASEによるリモートアクセスの セキュリティ確保を実現するためには



SASE（Secure Access Service Edge）とは、セキュリティとネットワークを統合したモデルのことです。ゼロトラストを含むセキュリティ対策の考え方と、ユーザーの利便性や運用最適化まで含めた概念を指します。

VPNやリモートアクセス、SD-WANなどのネットワーク、ファイアウォールやIDS／IPS、ウイルス対策などのセキュリティ機能をクラウド上で包含的に行う考え方です。

ゼロトラストやSASEの実現のための第一歩として
「VANILA」と「vSecureAccess」の活用がおすすめです！

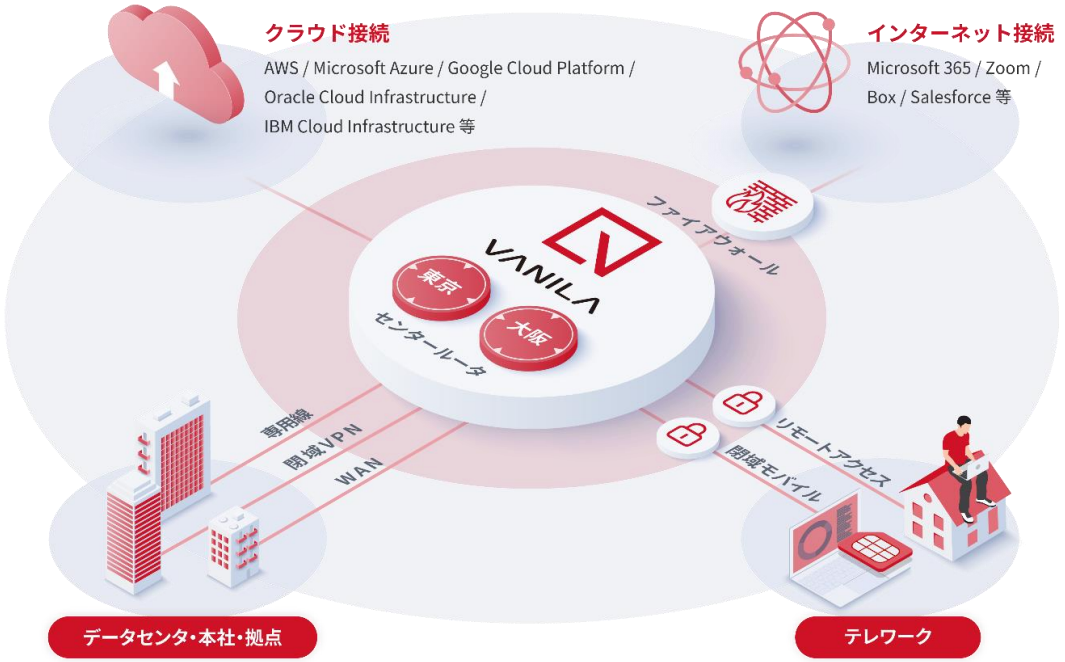
柔軟なネットワークを実現する「VANILA」

ARTERIA
アルテリア・ネットワークス株式会社

VANILAは、NFV（Network Functions Virtualization）技術を活用したサービスです。アルテリア・ネットワークスのIP網内に接続するだけで様々なネットワーク機能が利用できる次世代ネットワークサービスです。物理的投資が必要ないため、ミニマムスタートが可能であり、あらゆる変化に柔軟に対応することができます。

『VANILA』：Virtualized ARTERIA Networks Immaculate Layered Applications

『VANILA』のイメージ



「VANILA」３つの特徴

「VANILA」はお客様拠点からのVPNを終端とするセンタールーター機能を提供します。また、お客様のトラフィックや拠点数に応じたサイジングの最適化が可能です。標準的なセンタールーター機能である「Shared」とカスタマイズ性を重視した「Dedicated」からご選択いただけます。

『VANILA』の３つの特徴

	内容	詳細
特徴１	柔軟なカスタマイズ性	● 運用コストを抑えた「Shared」と、お客様の要件に適した各種カスタマイズが可能な「Dedicated」をご用意 ● お客様のご要望にあわせてシングル構成/冗長構成や、ご利用ロケーションを東日本Regionと西日本Regionから選択可能 ● クラウド型サービスのため、お客様が必要とする機能だけを選択して利用することができる
特徴２	高いスケーラビリティ	● クラウド型サービスのため、お客様拠点での設備投資が不要。機器の購入費用や設置作業といったコストの削減が可能 ● お客様のトラフィック利用量や拠点数に応じたスケールアップ、各種機能リソースを必要な分だけ利用できる
特徴３	セキュリティの向上	● 最短15営業日から利用開始が可能なファイアウォール ● 自宅や外出先といった通信速度やセキュリティに不安がある環境からも、快適かつセキュアなリモートアクセスが可能 ● 接続先やクライアント端末の利用場所を問わない、統一されたセキュリティポリシーを実現

リモートアクセスをセキュアにするVANILA「vSecureAccess」

ARTERIA
アルテリア・ネットワークス株式会社

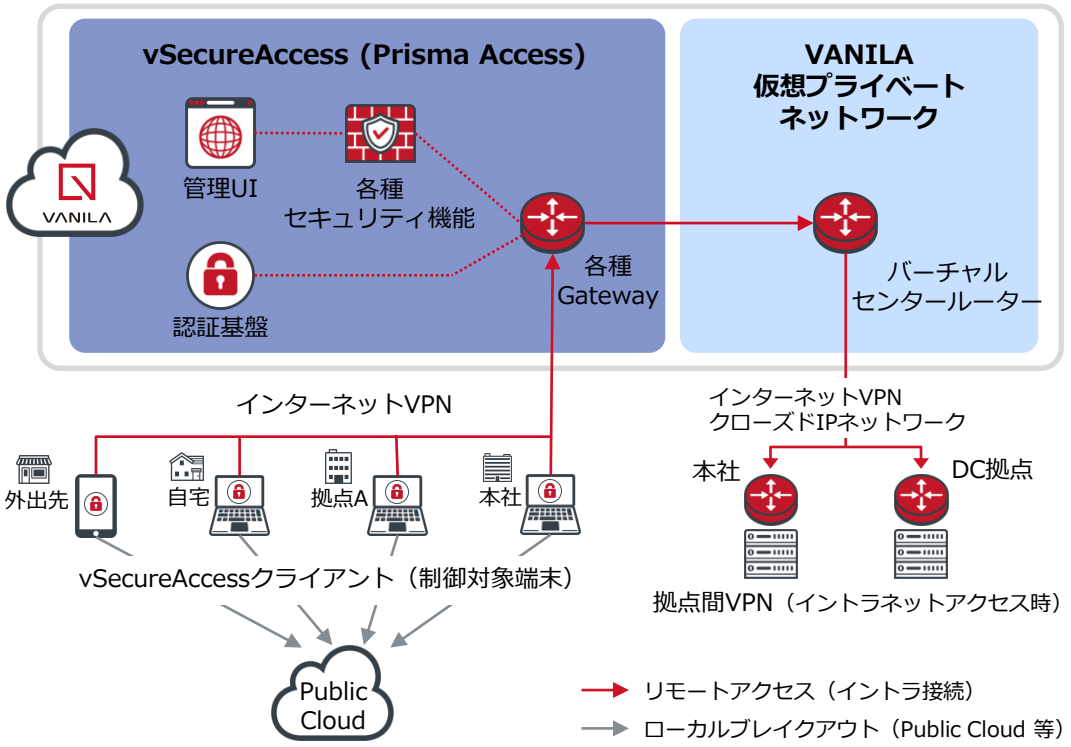
VANILAサービス基盤とvSecureAccess機能の基盤※1を組み合わせることにより、リモートアクセスにおける強固なセキュリティを実現しました。ネットワークの境界を問わず、全てのデバイス・ユーザー・通信ネットワークを監視し、適切なレベルで認証・認可を行うゼロトラスト環境を実現します。また、本サービスを利用することで、ローカルブレイクアウト※2 、複数PoP※3指定による最短経路接続等、ユーザーへの最適な通信制御が可能になります。

主な提供機能

セキュリティ機能	詳細
Next Generation Firewall	従来のFirewall機能に加え、ポート番号やプロトコルに依存せず、アプリケーションの識別によりトラフィック制御を行います。
IPS/IDS (脆弱性防御)	弱性を悪用した不正なアクセスや攻撃を検知・防御し、端末やサーバを保護します。
アンチウイルス	マルウェア等悪意のあるソフトウェアをウイルスとして検出し、当該通信のブロックを行います。
DLP	Webトラフィックを検査し、機密データを自動的に検出・監視・保護し、データ漏洩を防止します。
CASB	SaaSアプリケーションへのアクセスの可視化・制御・監視を行います。

※1 本サービスはパロアルトネットワークス株式会社のPrisma　Accessを利用した提供となります。
各種提供仕様については同社仕様に準拠いたします。
※2 各拠点のルーターなどで特定の宛先向けのトラフィックを識別し、センター拠点を経由せずに直接インターネットから特定の宛先へ接続させることで、センター拠点へのトラフィック負荷を分散する設計です。
※3 「Point of Presence」の略。ユーザーのリモート接続を行う最寄りの接続サイトを示します。

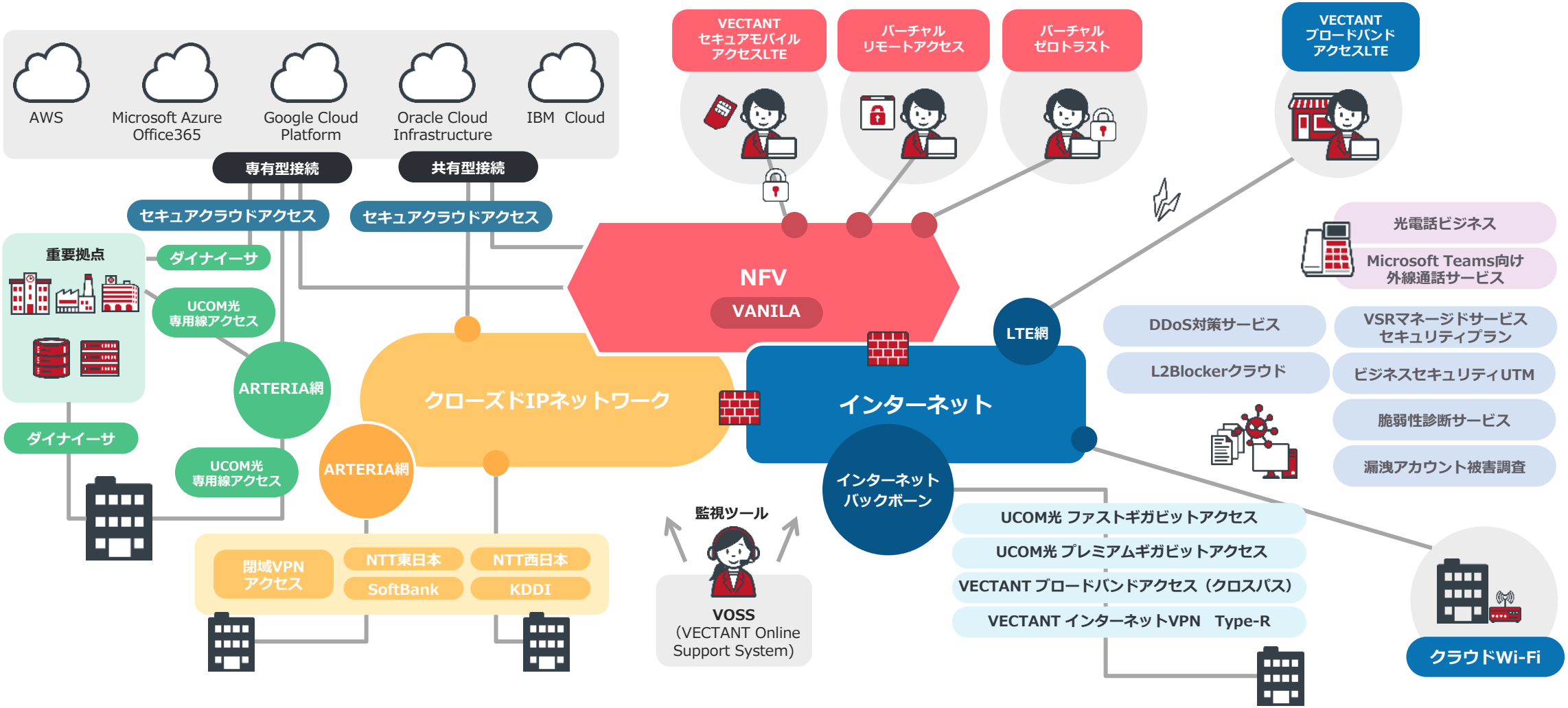
サービスイメージ



アルテリア・ネットワークスが提供するサービス

アルテリア・ネットワークス株式会社

アルテリア・ネットワークス株式会社では、今回ご紹介したVANILA以外にも、法人向けにさまざまなネットワークソリューションを提供しています。貴社にとって最適なネットワークをトータルでご提案、構築が可能です。



サービスの詳細や不明点など、下記のフォームによりお問い合わせください。

お問い合わせフォームはこちら

ARTERIA
アルテリア・ネットワークス株式会社

www.arteria-net.com

本　社	〒105-0004　東京都港区新橋六丁目9番8号 住友不動産新橋ビル
名古屋事業所	〒461-0002　愛知県名古屋市東区代官町35番16号 第一富士ビル5階
大阪事業所	〒541-0053　大阪府大阪市中央区本町二丁目1番6号 堺筋本町センタービル9階
福岡事業所	〒812-0016　福岡県福岡市博多区博多駅南一丁目3番6号 第三博多偕成ビル5階