IT部門担当者様必見

見直すなら今

セキュアで高効率なリモートアクセス環境の実現方法

～リモートアクセスのセキュリティ課題を解決～

ARTERIA

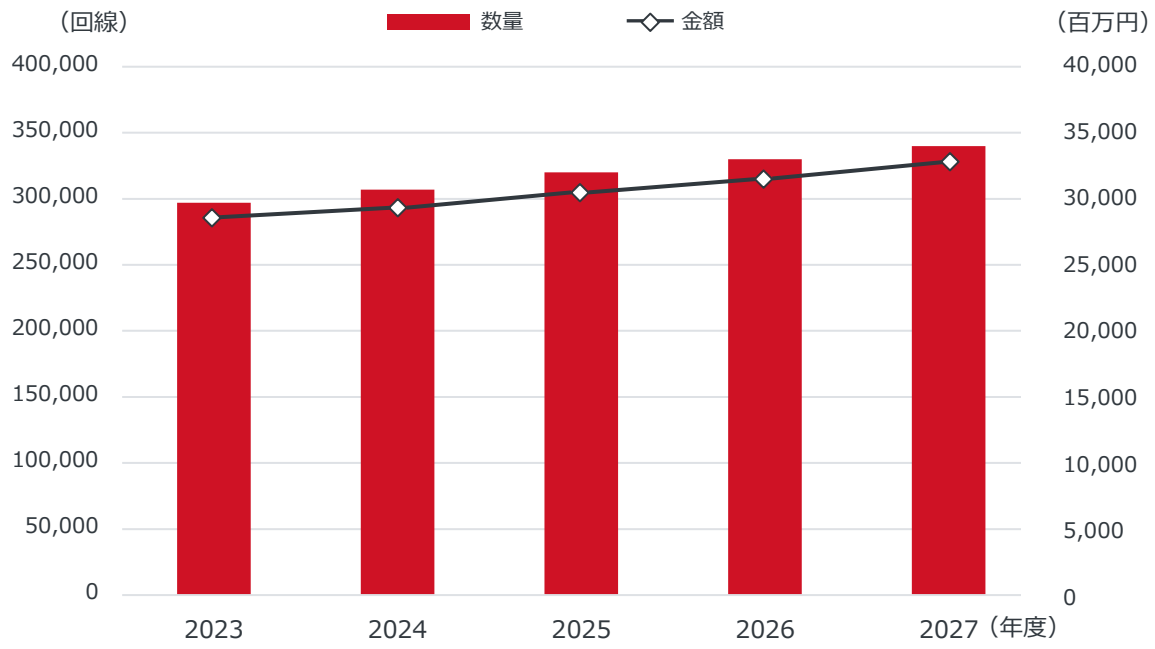
アルテリア・ネットワークス株式会社

目次

1. 働き方の変化にともない伸長する「インターネットVPN」市場

近年の働き方の変化にともない、リモートアクセスは今や企業のネットワーク要件になりつつあります。下に示す富士キメラ総研の「インターネットVPNサービス 市場規模推移／予測（2023～2030年度）」資料によると、インターネットVPNの市場は右肩上がりで伸長していることがわかります。

インターネットVPNサービス・2024年度見込み、2025年度以降予測



左記資料からも、インターネットVPNサービスの市場規模推移は、これからも堅調に推移すると予想されています。

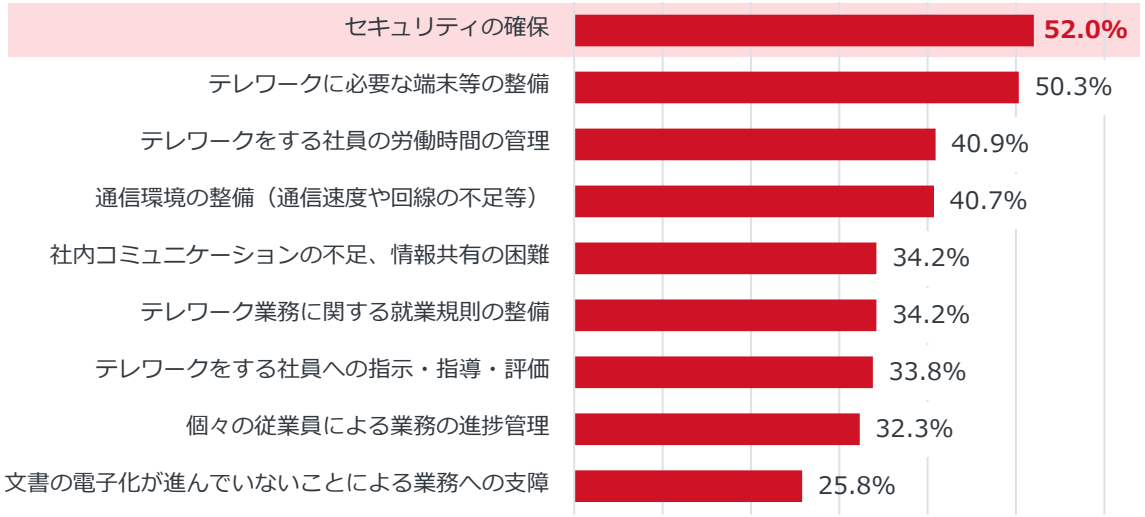
出典：富士キメラ総研「2024 コミュニケーション関連マーケティング調査総覧」
<インターネットVPNサービス・2024年度見込み、2025年度以降予測>

2. リモートアクセスを狙ったサイバー攻撃の増加

リモートアクセスの増加にともない、ニューノーマルな働き方を狙ったサイバー攻撃も増加しています。テレワークを行う企業では、自宅・カフェなど社外からのVPN接続におけるセキュリティ不安が増大しました。例えば、VPN機器の脆弱性を狙うサイバー攻撃により、個人情報が外部に漏洩するというインシデントが発生したり、VPNパスワードの管理不備による不正アクセスから、社内システムのウイルス感染などが多発しています。今や、VPNの情報セキュリティ対策は必須といえます。

課題 01　リモートアクセスの増加により企業のセキュリティの悩みも増加

テレワークの導入で課題となった点



企業向けテレワークセキュリティに関する実態調査（2024年）｜総務省

課題 02　ニューノーマルな働き方を狙った攻撃に対する運用課題が浮き彫りに

組織向け情報セキュリティ10大脅威2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

情報セキュリティ 10 大脅威 2025 「組織」向けの脅威の順位｜IPA

3. VPNのメリット・デメリット

自宅・カフェなどからのVPN接続はセキュリティに懸念が生じるケースも少なくありません。また、VPNはソフトウェアのバージョンアップなどにともなうシステム部門の運用負荷の増加や、通信の遅延といった課題も顕在化するようになりました。

VPN（特にインターネットVPN）のメリットとデメリット

メリット

- 低コストで導入ができるため、導入障壁も低い
- 暗号化により一定のセキュリティが担保できる

デメリット

- インターネットVPNはインターネット経由のため通信遅延が起きやすい
- インターネットVPNは閉域ネットワークなどに比べ、セキュリティが劣るため、不正アクセスや情報漏えいリスクがある
- 関連するソフトウェアのアップデートやその管理など、システム部門の業務負荷が高い（VPN全般にいえる）

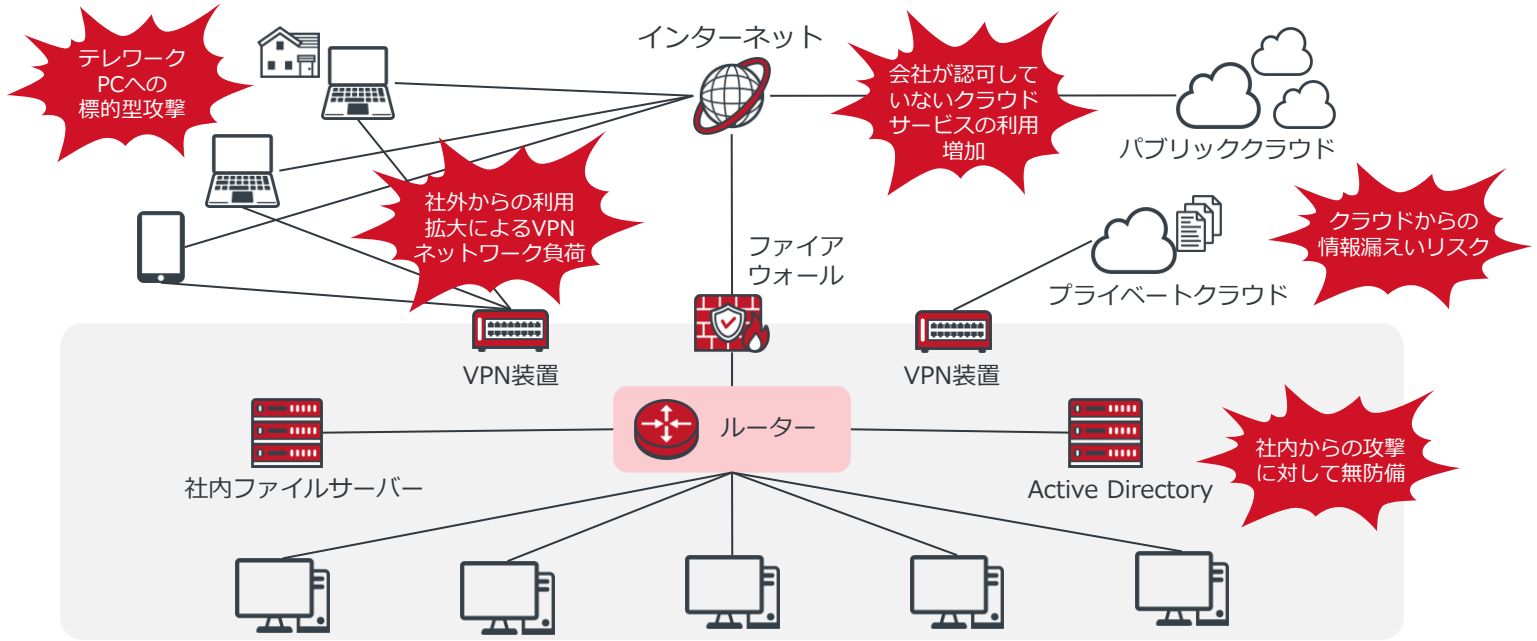
4. ゼロトラストの重要性の高まり

境界型セキュリティとゼロトラストモデルの違い

従来の境界型セキュリティでは、ネットワークの内外を境界で分けて、外部からの攻撃を防御します。ただし、一旦内部に侵入されると対応が困難になるというリスクがあります。

一方、ゼロトラストモデルは、すべての通信を信頼しない前提で、内部外部問わず厳格な認証と検査を行うモデルです。

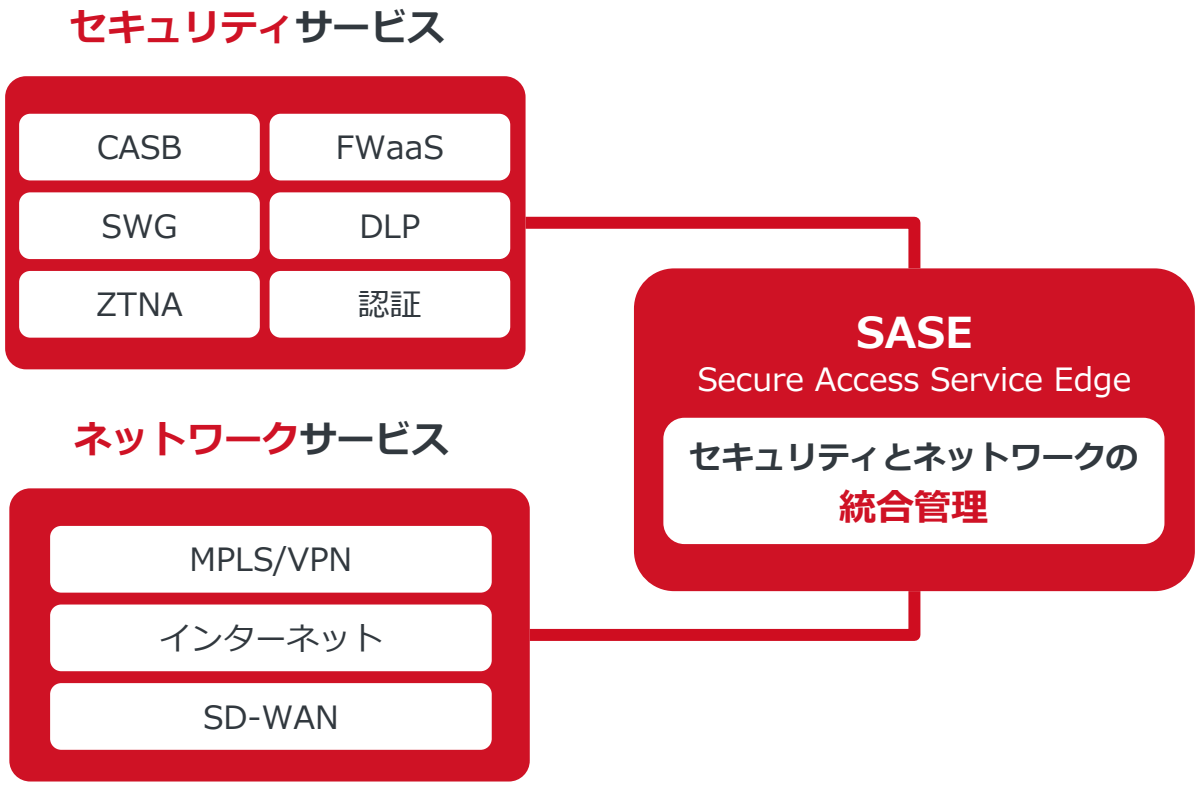
リモートアクセスにより、社外から社内のシステムにアクセスする端末やその頻度が増加したため、境界型セキュリティでは、VPNの認証を通ってしまった後のセキュリティが担保しきれなくなりました。そのためゼロトラストの重要性が高まっているのです。



従来の境界型セキュリティの課題

- 社内からの攻撃に弱い
- クラウドからの情報漏えい
- スケーラビリティ（VPNゲートウェイの処理能力）
- 端末紛失・盗難などの物理的リスク
- 管理・運用負荷などの増大

5. 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。

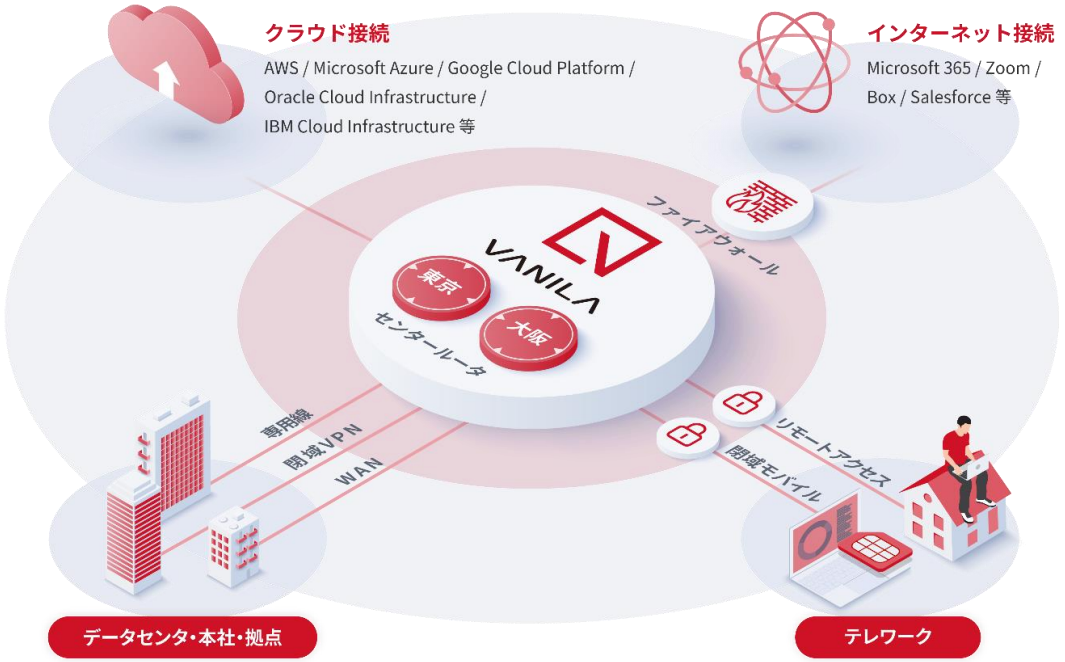
ゼロトラストやSASEの実現のための第一歩として
「VANILA」と「vSecureAccess」の活用がおすすめです！

6. 柔軟なネットワークを実現する「VANILA」

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



ARTERIA

7.「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

8. リモートアクセスをセキュアにするVANILA「vSecureAccess」

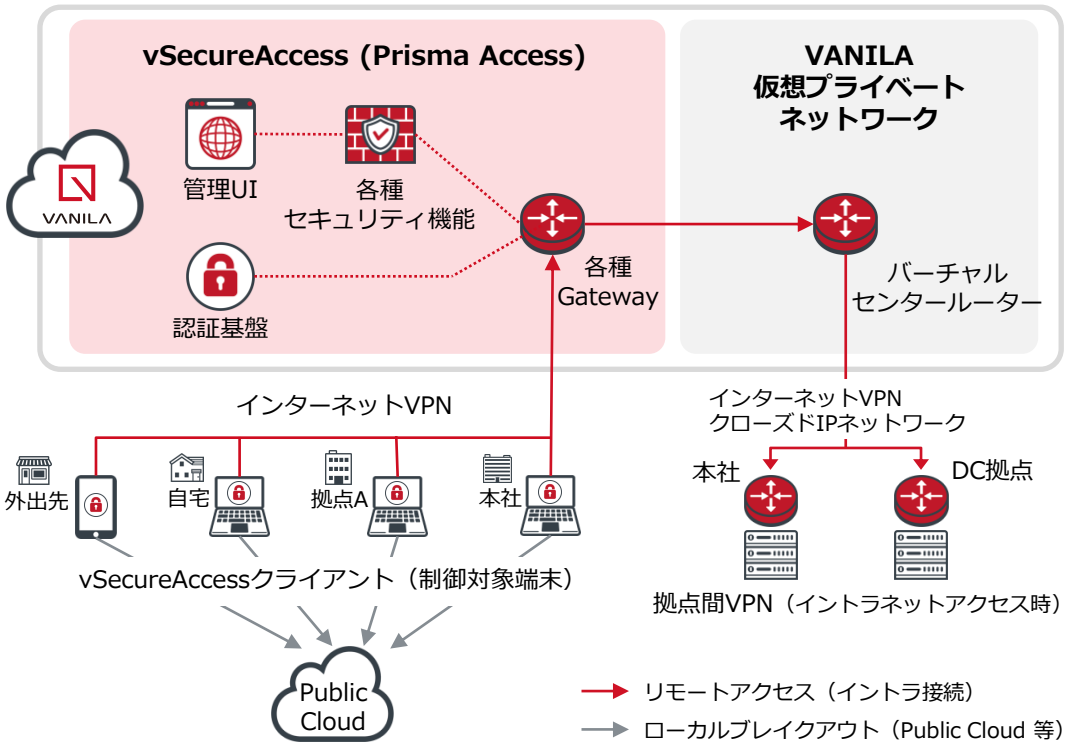
VANILAサービス基盤とvSecureAccess機能の基盤※1を組み合わせることにより、リモートアクセスにおける強固なセキュリティを実現しました。ネットワークの境界を問わず、全てのデバイス・ユーザー・通信ネットワークを監視し、適切なレベルで認証・認可を行うゼロトラスト環境を実現します。また、本サービスを利用することで、ローカルブレイクアウト※2 、複数PoP※3指定による最短経路接続等、ユーザーへの最適な通信制御が可能になります。

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。

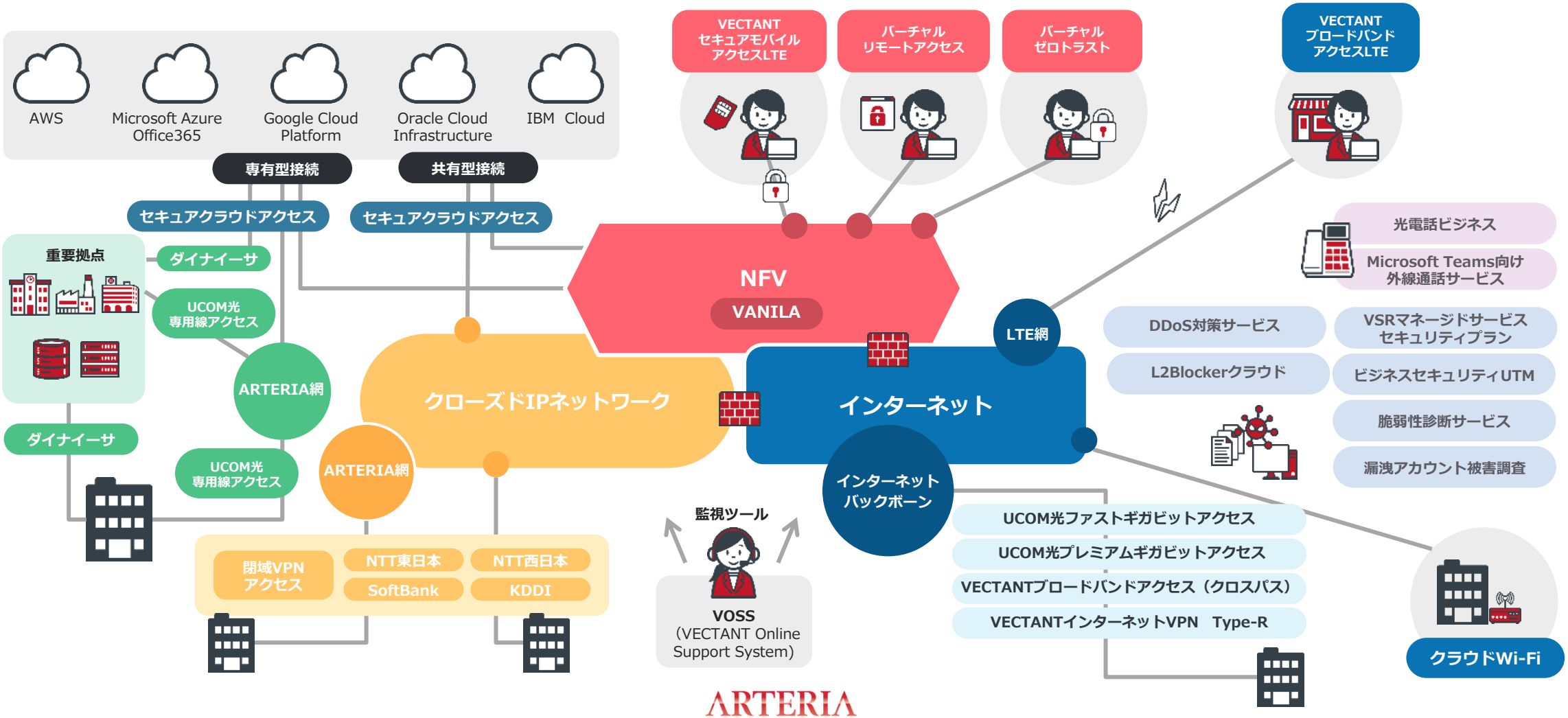
※1 本サービスはパロアルトネットワークス株式会社のPrisma　Accessを利用した提供となります。
各種提供仕様については同社仕様に準拠いたします。
※2 各拠点のルーターなどで特定の宛先向けのトラフィックを識別し、センター拠点を経由せずに直接インターネットから特定の宛先へ接続させることで、センター拠点へのトラフィック負荷を分散する設計です。
※3 「Point of Presence」の略。ユーザーのリモート接続を行う最寄りの接続サイトを示します。

サービスイメージ



9. 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。



お問い合わせ・ご相談

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