パートナー
ロゴスペース

トップ10 SASEプロバイダに求めるべき10の機能

ボタンを1つ押すだけでネットワークアーキテクチャ全体を安全なクラウド環境に移行できる、そんな簡単な方法でSASEアーキテクチャへの移行を実現できるなら、それが理想的です。残念ながら、現実の世界ではそこまで簡単にはいきません。しかし、この複雑な移行作業を簡素化することは可能です。

SASEアーキテクチャに円滑に移行するためには、まず移行をサポートできる最適なプロバイダを見つける必要があります。既存の投資を活用しながら、貴社に最適なペースで、シームレスかつ安全にクラウド型セキュリティへの移行をサポートできる、経験豊富なプロバイダを選択しましょう。

1 統合ポリシー管理

オンプレミスとクラウドを問わず、あらゆる場所のセキュリティを単一のUIを使用してクラウドから管理

場所を問わずユーザー、デバイス、アプリケーションにポリシーを適用して安全なユーザーエクスペリエンスを確保するための統合ポリシー管理が必要です。

2 高度な脅威からの迅速かつ効果的な保護

見えない脅威、未知の脅威、暗号化された脅威から保護

静的および動的マルウェア検知により極めて高度で見つけにくい脅威さえも特定し、即座にほぼリアルタイムでブロックしてくれるクラウドベースサービスを選択します。

3 耐障害性と拡張性

物理ベース、仮想ベース、クラウドベースのセキュリティ環境に容易かつ効果的に対応可能な拡張性

エンドユーザーに気づかれることなく、またユーザーエクスペリエンスに一切悪影響を及ぼすことなく、大規模環境の運用を簡素化してセキュリティを確保する必要があります。

4 単一スタックアーキテクチャと単一ポリシーフレームワーク

既存の投資を土台として、ビジネスクリティカルなクラウドセキュリティサービスを実現

統合ポリシー管理により、ポリシー（ユーザーベースおよびアプリケーションベースのアクセス、IPS、アンチマルウェア、セキュアなWebアクセスなどを単一のポリシーに設定）を一度作成するだけで、そのポリシーをあらゆる場所に適用できます。

5 分散した従業員を保護するための一貫したセキュリティ

効果的な業務遂行に必要なアプリケーションやリソースにリモートワーカーが安全にアクセスできるようにする

ルールセットのコピーや再作成をせずにユーザー、デバイス、アプリケーションに適用できる、一貫したセキュリティポリシーが必要です。

6 ハイブリッド環境のサポート

オンプレミスか、クラウドか、その双方の組み合わせかを問わず、さまざまなインフラストラクチャに問題なくすべてに対応できるSASEプロバイダが必要

貴社に最適なペースで、シームレスかつ安全にSASEアーキテクチャへの移行をサポートできるプロバイダを選びましょう。

7 単一の情報源としてのアイデンティティ

あらゆるアイデンティティソリューションプロバイダとシームレスに統合

貴社のビジネスニーズに最適なアイデンティティソリューションプロバイダを自由に選択できるプロバイダを選びましょう。

8 ダイナミックユーザーセグメンテーション

場所を問わずに確実にユーザーを保護

ユーザーがどこにいても適用されるポリシーを適用し、きめ細かいポリシーを通じてリスクに基づき自動的にアクセスを制御することで、攻撃ベクトルとしてのサードパーティアクセスをブロックします。サードパーティアクセスに対応することで、エッジの攻撃対象領域をさらに縮小します。

9 検証済みのセキュリティの有効性

セキュリティの有効性が実証されているプロバイダを選択

クライアント側、またはサーバー側の悪用、ランサムウェア、ボットネット、DNSトンネリングなどの脅威から効果的に保護でき、脅威の現状という課題に真に取り組んで貴社のオンプレミス、またはクラウド環境に対する攻撃を阻止し、サービスとしてのセキュリティを提供しているプロバイダを選びましょう。

10 貴社のペースでクラウド型セキュリティにシームレスに移行

SASEアーキテクチャへの移行は各社のペースで行うべきもの

単一の管理UI、統合ポリシー、直感的な導入ウィザードを使用して、貴社のペースでクラウド型セキュリティアーキテクチャにシームレスに移行できます。ポリシーサービスのオーケストレーション、プロビジョニング、管理を、サービスの場所を問わず簡単かつ効果的に行うことができます。

11 ボーナスポイント：セキュリティアシュアランス

ポリシールールを安心して変更でき、その変更を確実に適用

従来のファイアウォールポリシーであれ、サービスとして提供されるポリシーであれ、ルールを適切な順序で配置して効果が発揮されるようにする必要があります。ITチームがこれらのルールセットを理解し、重複したルールやシャドウルールを有効化される前に自動的に特定するのをサポートしてくれるSASEプロバイダを選びましょう。

SASEへの移行プロセスは各企業によって異なります。また、新しいSASEアーキテクチャをどのように設計、構築、維持することで、ユーザーエクスペリエンス、サービス、必要な際の必要なデータを最適化するのかは、最終的には各企業の選択に委ねられます。ただし、どのようなプロセスを選択しても、いつでも相談でき、SASEの実装をプロセス全体を通じて全面的にサポートしてくれるプロバイダの存在が不可欠です。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.JUNIPER
（888.586.4737）
または+1.408.745.2000
FAX：+1.408.745.2100
www.juniper.net

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

日本
ジュニパーネットワークス株式会社
東京本社
〒 163-1445 東京都新宿区西新宿 3-20-2
東京オペラシティタワー 45 階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒 530-0001 大阪府大阪市北区梅田 2-2-2
ヒルトンプラザウエストオフィスタワー 18 階
https://www.juniper.net/jp/jp/

Juniper Networks | Driven by Experience™

PART NO：3050168

トップ10 SASEプロバイダに求めるべき10の機能

ボタンを1つ押すだけでネットワークアーキテクチャ全体を安全なクラウド環境に移行できるというような、そんな簡単な方法でSASEアーキテクチャへの移行を実現できるなら、それが理想です。しかし残念ながら、現実の世界ではそこまで簡単にはいきません。それでも、この複雑な移行作業を簡素化することは可能です。

SASEアーキテクチャに円滑に移行するためには、まず移行をサポートできる最適なプロバイダを見つける必要があります。既存の投資を活用しながら、貴社に最適なペースで、シームレスかつ安全にクラウド型セキュリティへの移行をサポートできる、経験豊富なプロバイダを選択しましょう。

1 統合ポリシー管理

オンプレミスとクラウドを問わず、あらゆる場所のセキュリティを単一のUIを使用してクラウドから管理。

場所を問わずユーザー、デバイス、アプリケーションにポリシーを適用して安全なユーザーエクスペリエンスを確保するための統合ポリシー管理が必要です。

2 高度な脅威からの迅速かつ効果的な保護

見えない脅威、未知の脅威、暗号化された脅威から保護。

静的および動的マルウェア検知により極めて高度で見つけにくい脅威さえも特定し、即座にほぼリアルタイムでブロックしてくれるクラウドベースサービスを選択します。

3 耐障害性と拡張性

物理ベース、仮想ベース、クラウドベースのセキュリティ環境に容易かつ効果的に対応可能な拡張性。

エンドユーザーに気づかれることなく、またユーザーエクスペリエンスに一切悪影響を及ぼすことなく、大規模環境の運用を簡素化してセキュリティを確保する必要があります。

4 単一スタックアーキテクチャと単一ポリシーフレームワーク

既存の投資を土台として、ビジネスクリティカルなクラウドセキュリティサービスを実現。

統合ポリシー管理により、ポリシー（ユーザーベースおよびアプリケーションベースのアクセス、IPS、アンチマルウェア、セキュアなWebアクセスなどを単一のポリシーに設定）を一度作成するだけで、そのポリシーをあらゆる場所に適用できます。

5 分散した従業員を保護するための一貫したセキュリティ

効果的な業務遂行に必要なアプリケーションやリソースにリモートワーカーが安全にアクセスできるようにする。

ルールセットのコピーや再作成をせずにユーザー、デバイス、アプリケーションに適用できる、一貫したセキュリティポリシーが必要です。

6 ハイブリッド環境のサポート

オンプレミスか、クラウドか、その双方の組み合わせかを問わず、さまざまなインフラストラクチャに問題なく対応できるSASEプロバイダが必要。すべてに対応できることが肝要。

貴社に最適なペースで、シームレスかつ安全にSASEアーキテクチャへの移行をサポートできるプロバイダを選んでください。

7 単一の情報源としてのアイデンティティ

あらゆるアイデンティティソリューションプロバイダとシームレスに統合。

貴社のビジネスニーズに最適なアイデンティティソリューションプロバイダを自由に選択できるプロバイダを選んでください。

8 ダイナミックユーザーセグメンテーション

場所を問わずに確実にユーザーを保護。

ユーザーがどこにいようと適用されるポリシーを取り入れ、きめ細かいポリシーを通じてリスクに基づき自動的にアクセスを制御することで、攻撃ベクトルとしてのサードパーティアクセスをブロックします。サードパーティアクセスに対応することで、エッジの攻撃対象領域をさらに縮小します。

9 検証済みのセキュリティの有効性

セキュリティの有効性が実証されているプロバイダを探す。

クライアント側/サーバー側の悪用、ランサムウェア、ボットネット、DNSトンネリングなどの脅威から効果的に保護でき、脅威の現状という課題に真っ向から取り組んで貴社のオンプレミス/クラウド環境に対する攻撃を阻止し、サービスとしてのセキュリティを提供しているプロバイダを選びます。

10 貴社のペースでクラウド型セキュリティにシームレスに移行

SASEアーキテクチャへの移行は各社のペースで行うべきもの。

単一の管理UI、統合ポリシー、直感的な導入ウィザードを使用して、貴社のペースでクラウド型セキュリティアーキテクチャにシームレスに移行できます。ポリシーサービスのオーケストレーション、プロビジョニング、管理を、サービスの場所を問わず簡単かつ効果的に行うことができます。

11 ボーナスポイント：セキュリティアシュアランス

ポリシールールを安心して変更でき、その変更を確実に適用。

従来のファイアウォールポリシーであれ、サービスとして提供されるポリシーであれ、ルールを適切な順序で配置して効果が発揮されるようにする必要があります。ITチームがこれらのルールセットを理解し、重複したルールやシャドウルールを有効化される前に自動的に特定するのをサポートしてくれるSASEプロバイダを選びましょう。

SASEへの移行プロセスは組織によって異なります。また、新しいSASEアーキテクチャをどのように設計、構築、維持することで、ユーザーエクスペリエンス、サービス、必要な際の必要なデータを最適化するのかは、最終的には各組織の選択に委ねられます。ただし、どのようなプロセスを選択するにしても、いつでも相談に乗ってくれるとわかっており、SASEの実装をプロセス全体を通じて全面的にサポートしてくれるプロバイダの存在が不可欠です。

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.JUNIPER
（888.586.4737）
または+1.408.745.2000
FAX：+1.408.745.2100
www.juniper.net

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.0.207.125.700
FAX：+31.0.207.125.701

日本
ジュニパーネットワークス株式会社
東京本社
〒 163-1445 東京都新宿区西新宿 3-20-2
東京オペラシティタワー 45 階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒 530-0001 大阪府大阪市北区梅田 2-2-2
ヒルトンプラザウエストオフィスタワー 18 階
https://www.juniper.net/jp/jp/

Juniper Networks | Driven by Experience™

3050168-001-JP 2023年8月