



SAシリーズ SSL VPN アプライアンス SA2500、SA4500、SA6500

製品概要

リモートアクセスソリューションの幅広い品揃えでSSL-VPN市場をリードするジュニパーネットワークスのSSL-VPN製品「Secure Access (SA)」。

次世代バージョンの新製品として、SA2500およびSA4500、そして、大企業・サービスプロバイダ向けに設計された高拡張性と冗長構成が可能なSA6500の3製品があります。

SAシリーズは、SSLのセキュリティ機能に加え、標準規格準拠のアクセス・コントロール機能、きめ細かいポリシー作成機能、卓越した柔軟性を備えています。

その結果、企業のあらゆる業務をカバーするユビキタス・セキュリティを実現します。

特に機密性の高いアプリケーションやデータについては、アクセス・コントロールを非常に厳格なレベルに設定して保護力を強化することも可能です。

ジュニパーネットワークスSAシリーズSSL VPNアプライアンスは、IPSecクライアントを使用する従来型ソリューションに比べてTCO（導入・運用に伴う総コスト）を削減できるうえ、独自のエンドツーエンドのセキュリティ機能も搭載しています。

製品説明

ジュニパーネットワークスの「SA2500」、「SA4500」、「SA6500」は、事業規模を問わず、あらゆる企業のニーズにお答えするSSL-VPN製品です。

また、SA6500は、SSL-VPN市場におけるジュニパーネットワークスのリーダーシップを証明する製品であり、実際の環境でのパフォーマンス試験に基づいた拡張性の高いソリューションとなっています。

SAシリーズ SSL VPNアプライアンスは、標準的なWebブラウザに必ず搭載されているセキュリティ・プロトコルのSSLを採用しています。

SSLの場合、クライアントソフトのプリインストールや内部サーバーの設定変更、コストのかかる継続的な保守の必要がありません。

また、ジュニパーネットワークス SAシリーズは、パートナーや取引先向けの高度なエクストラネット機能を搭載しており、インフラの変更、DMZ (Demilitarized Zone) の設定、エージェントソフトの使用に頼ることなく、ユーザー単位、グループ単位でアクセスを制御できます。

アーキテクチャと主要コンポーネント

SA2500 SSL VPNアプライアンスは、イントラネットはもちろん、リモートアクセスやエクストラネットでも経済的に安全な環境を実現できる中堅・中小企業向け製品です。

ユーザーは、標準のWebブラウザで社内のネットワークやアプリケーションにアクセスできます。

SA2500はシームレスなフェイルオーバーを実現する高可用性 (HA) をサポートしています。

また、SA2500は、上位機種種のSA4500およびSA6500と同じソフトウェアを使用するため、小規模な組織でも、同等の高いパフォーマンス、柔軟な管理機能、快適な使い心地を実現します。

SA4500 SSL VPNアプライアンスは、中規模～大規模の企業向けのSSL-VPN製品です。

出先にいる従業員や外部の納入業者は、Webブラウザを使用して、簡単にリモートアクセスできます。

豊富なアクセス特権管理機能を備えており、取引先・パートナー向けの安全なエクストラネット構築に威力を発揮します。

この機能を利用すると、社内のイントラネットに安全にアクセスできるため、従業員も来訪者も、会社全体のセキュリティポリシーを順守しながら、それぞれの立場に合ったリソースを利用できます。

あらゆるトラフィックタイプに対応する圧縮機能を内蔵し、パフォーマンスを向上させます。

また、きわめて厳格な条件が求められる環境向けとして、オプションモジュールによるSSLアクセラレーション (高速化) 機能も用意されています。

SA4500もシームレスなフェイルオーバーを実現する高可用性 (HA) をサポートしています。

SA6500 SSL VPNアプライアンスは、大企業・サービスプロバイダ向けのSSL-VPN製品です。

クラス最高のパフォーマンス、拡張性、冗長性を備え、膨大な量のセキュアアクセスや権限付与が必要な組織に最適です。

SA6500もシームレスなフェイルオーバーを実現する高可用性 (HA) をサポートしています。

また、SA6500は、ウェブやファイルの圧縮機能に加えて、ハイパフォーマンスなSSL高速化機能を標準で実装しており、CPUリソースを大量に消費する暗号化・復号化の負担を大幅に軽減します。

SAシリーズ SSL VPNアプライアンスは全機種で同じソフトウェアを使用しているため、どの機種を選んでも、ユーザーや管理者の快適な使い心地が損なわれることはありません。すべての機種において、最高クラスのパフォーマンス、安定性、拡張性を実現します。このため、組織のニーズにあった機種を選択するのも、同時接続ユーザーの数、そして冗長構成や大規模な高速化オプションがリモートアクセス・ユーザー数の増加に適應できるかどうかで簡単に決定することができます。

- **SA2500**：SMB向けの経済的なソリューションで、単体または2台のクラスタ構成で最大100人の同時接続ユーザーをサポートします。
- **SA4500**：中規模～大規模の企業向けの製品で、単体でサポートする最大同時接続ユーザー数は1,000人です。また、高負荷状態でも最大のパフォーマンスを必要とする場合、ハードウェアベースのSSL高速化にオプションでアップグレードすることもできます。
- **SA6500**：大企業・サービスプロバイダ向けの製品で、クラス最高のパフォーマンス、拡張性、冗長性を備え、膨大な量のセキュアアクセスや権限付与が必要な組織に最適です。単体では最大10,000人の同時接続ユーザーを、4台のクラスタ構成では数万人のユーザーをサポートします。

SA6500の標準機能

- 二重のミラーリングされたSATA（Serial Advanced Technology Attachment）ハードドライブ（ホットスワップ対応）
- 二重ファン（ホットスワップ対応）
- ホットスワップ対応電源装置
- 4GB SDRAM
- Copper 10/100/1000インタフェースカード×4ポート
- Copper 10/100/1000管理インタフェース×1ポート
- ハードウェアベースのSSL高速化モジュール

SA6500のオプション機能

- DC電源装置、または二次電源装置
- 4ポート×SFP（Small Form-factor Pluggable）インタフェースカード

特長（機能）・メリット

SA6500 SSL VPNアプライアンスの高拡張性

SA6500では、急速に成長するエンタープライズ・ビジネスとサービスプロバイダ・ビジネスのニーズを満たすために、同時接続ユーザー数を柔軟に拡張できます。SA6500プラットフォームがサポートする最大同時接続数は次のとおりです。

- SA6500単体：最大同時接続ユーザー数10,000人
- SA6500 2台のクラスタ構成：18,000人
- SA6500 3台のクラスタ構成：26,000人
- SA6500 4台のクラスタ構成：30,000人

性能試験は、お客様のネットワークを想定し、実際の環境に近い条件で実施しています。コアネットワークでは、ウェブアプリケーションにアクセスが集中し、大量のHTMLファイルが書き込まれ、その都度、ポリシー評価が発生することを想定しています。

エンドツーエンドの階層型セキュリティ

SA2500、SA4500、SA6500は、エンドツーエンドの総合的な階層型セキュリティ機能を搭載しており、エンドポイントのクライアント、デバイス、データ、サーバーなどを階層型のセキュリティ制御機能で守ります。

表1：エンドツーエンドの階層型セキュリティの特長（機能）とメリット

特長（機能）	概要	メリット
UACとSA間の連携	SAシリーズのユーザーセッションをジュニパーネットワークス統合型アクセス・コントロール（UAC）へのログイン時にプロビジョニング、あるいは反対にUACセッションをSAシリーズのユーザーセッションにシームレスにプロビジョニングできます。ユーザーは、これらの環境に対して1回の認証のみでアクセスできるようになります。	リモート環境、ローカル環境を問わず、社内リソースへのシングルログインによるシームレスなアクセス権をユーザーに提供します。リソースは、UACかSAシリーズのアクセス・コントロール・ポリシーで保護します。さらにエンドユーザーの使い勝手も高まります。
SMSによる自動修復機能	社内のセキュリティポリシーを順守していないソフトウェア・アプリケーションを更新することで、ポリシーに適合しないエンドポイント端末を修復します。このようなエンドポイント端末でのソフトウェア・アプリケーションの更新は、MicrosoftのSMSプロトコルを使用して動的に行われます。	ソフトウェア・アプリケーションの定期更新時期を待たずに企業ネットワークにいつでもアクセスが可能となるため、リモートユーザーの生産性が向上し、社内のセキュリティポリシー要件も確実に満たされます。
ネイティブホストチェッカー	セッション開始時とセッション中にクライアント端末をチェックし、エンドポイント用セキュリティ・アプリケーション（アンチウイルス、パーソナル・ファイアウォールなど各種対策ソフト）のインストール状況や動作状況など、デバイスのセキュリティ状態について問題の有無を確認します。また、ネットワークポートの開閉状態の確認、ファイルやプロセスのチェックやMD5ハッシュ値のチェックサムによる同一性確認、レジストリ設定やマシン証明書などの確認をはじめ、各種カスタム仕様のチェックもサポートしています。	アクセス権を付与する前に、エンドポイント・デバイスが自社のセキュリティポリシー要件を満たしているかどうか確認し、必要に応じてデバイスを修復します。
ホストチェッカー API	エンドポイント環境を専門とする有力セキュリティベンダー各社とのパートナーシップの下で、開発しました。パーソナル・ファイアウォール、アンチウイルスなどセキュリティ関連クライアントを導入済みの管理対象PCや、検疫非対応のエンドポイントに対して、信頼性ポリシーを適用できます。	常に最新のセキュリティポリシーをリモート側のユーザーやデバイスに適用し、管理の手間を軽減します。
ホストチェッカーの Trusted Network Connect（TNC）対応	アンチウイルスソフトウェアのパッチ管理やコンプライアンス管理ソリューションなど、エンドポイントの多様なセキュリティ・ソリューションの相互運用性を保証します。	エンドポイントに配置した既存のサードパーティ製ソリューションを使用できます。
ポリシーベースの適用	カスタムAPIを実装したり、外部ユーザー（他のセキュリティ・クライアントを利用している顧客やパートナーなど）を締め出したりすることなく、API非準拠のホストの信頼性を確立できます。	自社とは異なるセキュリティ・クライアントを利用するパートナーからでも、エクストラネットのエンドポイントにあるPCなどのデバイスにアクセスできます。
堅牢性を高めたセキュリティ製品	専用OS	追加サービスの運用を一切認めない設計のため、悪意ある攻撃のリスクを最小限にとどめます。不正使用やハッキングなどのバックドアも心配ありません。
カーネルレベルのパケットフィルタリングと安全なルーティングを採用したセキュリティサービス	意図しないトラフィックは、TCPスタックで処理される前に遮断します。	異常パケットやDoS攻撃など不正な接続要求を確実に遮断します。
セキュア・バーチャル・ワークスペース（SVW）	リモートセッションのセキュリティを高めるために、独立したセキュアな仮想デスクトップ環境を作り、すべてのデータを暗号化して、プリンタやディスクドライブなどへのI/Oアクセスを制御します。	リモートセッションが完了した後は、キオスクなどの非管理対象エンドポイントから企業データを安全に削除できます。
キャッシュクリーナー	セッション中にインストールされるプロキシ経由のダウンロードファイルとテンポラリーファイルをすべてログアウト時に消去します。	機密情報が含まれている可能性のあるセッションデータをエンドポイントの端末に残しません。
データトラップとキャッシュ制御	キャッシュ不可能な形式でコンテンツをレンダリングします。	機密情報を含むメタデータ（cookie、ヘッダ、フォーム入力など）の漏洩を防止します。
統合型マルウェア防御機能	キーロガー、トロイの木馬、遠隔操作アプリケーションからユーザーやデバイスを保護するチェック機能がブラインストールされています。	エンドポイント封じ込め機能が利用できます。
協調型脅威管理	SAシリーズ SSL VPNアプライアンスおよびジュニパーネットワークスIDPシリーズ 侵入検知防御アプライアンスを組み合わせ、SSL-VPNのセッションIDとIDPシリーズの脅威検知機能を連動させることにより、万一ユーザーが攻撃を仕掛けるようなことがあっても自動的に対策を講じます。	リモートアクセスのトラフィック内に潜むネットワークレベルとアプリケーションレベルの脅威を発見、阻止、緩和します。

TCO（Total Cost of Ownership）削減

SA2500、SA4500、SA6500は、エンタープライズ環境に対応したセキュリティ機能に加え、TCO削減につながる多彩な機能を搭載しています。

表2：TCO削減の特長（機能）とメリット

特長（機能）	概要	メリット
SSLの採用	アプリケーション層でのウェブ接続により、リモートユーザーから内部リソースへの接続を高信頼化します。	専用クライアントソフトのインストールや、既存サーバーの変更も一切不要でありながら、高信頼のリモートアクセスを実現します。ファイアウォール・プロキシやNAT（ネットワークアドレス変換）越えの問題とも無縁です。
業界標準のプロトコルとセキュリティ方式に準拠	ベンダー独自仕様プロトコルのインストールや設備が不要です。	SAは、多彩なアプリケーションやリソースで長期的に大きな投資効果が得られます。
大規模なディレクトリ統合と広範な相互運用性	社内ネットワークですでに稼働中の既存ディレクトリを認証・権限付与に活用し、ポリシーを作成し直すことなく、きめ細かい高信頼のアクセスを実現します。	インフラに変更を加えることなく、既存ディレクトリを有効活用できます。完全ネイティブあるいは内蔵の場合、ディレクトリ統合のAPIも不要です。
認証プラットフォームとID・アクセス管理プラットフォームの統合	SecurID、SAML（Security Assertion Markup Language）、PKI（公開キーインフラストラクチャ）/デジタル証明書に対応しています。	既存の認証方式を使用できるため、管理タスクを簡素化できます。
複数ホストネームのサポート	さまざまなバーチャル・エクストラネット用ウェブサイトを1台のSA SSL VPNアプライアンスで収容できます。	サーバー増設コストの節減、管理コストの軽減が可能で、複数のログインのURLを使い分けることで快適な使い心地を実現します。
カスタマイズ対応のユーザーインタフェース	完全カスタマイズ対応のサインオンページを作成できます。	ユーザーのロールに応じて画面構成をカスタマイズし、ユーザーの使い心地を向上させます。
Juniper Networks Network and Security Manager	単体のデバイスや単一クラスタ内のローカル環境、またローカルを越えたクラスタ環境の場合でも、SAシリーズアプライアンスの設定、アップデート、監視は、直観的なウェブベースのユーザーインタフェースから利用できます。	SAシリーズアプライアンスの管理、設定、保守が管理拠点などから一元的に実施可能です。
In Case of Emergency（ICE）	災害や伝染病が発生した場合、一時的にSAシリーズSSL VPNアプライアンスにユーザーを大量に追加するためのライセンスを発行します。	予期せぬ事態が起こった場合、生産性を損なわず協力関係はそのままに、また顧客へのサービスも停滞させることなく企業は業務を継続できます。
クロスプラットフォーム対応	Windows、Mac、Linux、携帯端末など、プラットフォームを問わずリソースにアクセスできます。	デバイスやOSの種別を問わず、社内リソースにアクセスできる柔軟性があります。

多彩なアクセス特権管理機能

SA2500、SA4500、SA6500には、アクセス特権を動的に管理する機能が搭載されており、インフラの変更、カスタム開発、ソフトウェア導入・保守が不要です。このため、安全なリモートアクセス環境のほか、安全なエクストラネットやイントラネットを簡単に構築・保守できます。ユーザーがSAシリーズ SSL VPNアプライアンスにログインすると、認証前の判定をパスした後、ネットワーク、デバイス、ID、セッションの各ポリシー設定を組み合わせたセッションロールに動的にマッピングします。さらに、リソースの許可に関しては、きめ細かいポリシーを設定できるため、セキュリティ規定に厳密に適合させることが可能です。

表3：アクセス特権管理の特長（機能）とメリット

特長（機能）	概要	メリット
ロールベースとリソースベースを融合したハイブリッド型ポリシーモデル	管理者がアクセス権を自由にカスタマイズできます。	刻一刻と変化する業務上の要件をセキュリティポリシーに反映します。
認証前の評価	ホストチェッカーやキャッシュクリーナーの有無、エンドポイント・セキュリティのスキャン結果、送信元IPアドレス、ブラウザのタイプ、デジタル証明書など、ネットワークとデバイスの属性を検証し、その結果を基にログインを許可します。	検証結果は、動的なポリシー適用判定に利用されます。
動的認証ポリシー	個々のセッション単位の動的認証ポリシーを作成できます。	ディレクトリやPKI、強固な認証技術など、既存の資産を活用できます。
動的ロールマッピング	ネットワーク、デバイス、セッションの属性を組み合わせ、3種類のアクセス方式の中から適切な方式を決定します。	個々のセッションごとに目的別のプロビジョニングが可能です。
リソースの許可	URL、サーバー、ファイルのレベルで非常にきめ細かいアクセス制御が可能です。	管理者がグループ別にセキュリティポリシーをカスタマイズし、必要なデータに絞ったアクセス権を付与します。
詳細な監査・ログ作成	セキュリティ業務や容量計画の目的に合わせて、ユーザー単位、リソース単位、イベント単位で設定可能です。	わかりやすい明快的なフォーマットで、詳細な監査・ログ作成が可能です。
カスタム表示	ロール定義・マッピングルールによる「セッション単位」の属性と、リソース許可ポリシーレベルを動的に組み合わせることができます。	ポリシーロールの細分化とカスタマイズを実現します。

ユーザーセルフサービス

SA2500、SA4500、SA6500には、総合的なパスワード管理機能が搭載されています。エンドユーザーの生産性を向上、多彩なユーザーリソース管理を大幅に効率化、ヘルプデスクへの問い合わせ件数の大幅削減などの効果があります。

表4：ユーザーセルフサービスの特長（機能）とメリット

特長（機能）	概要	メリット
制約付きの委任認証	ユーザーが、バックエンドサーバーへの委任認証が認められない信用情報を使ってSAシリーズにログインすると、SAシリーズ アプライアンスはActive Directoryインフラストラクチャからユーザーの代理としてKerberosチケットを取得します。このチケットは、セッション完了までSAシリーズ アプライアンス上にキャッシュされます。ユーザーが、Kerberosによって保護されたアプリケーションにアクセスすると、SAシリーズ アプライアンスはキャッシュされたKerberosの信用証明書を使用してユーザーのログインを行います。このとき、ユーザーはパスワードなどを入力する必要はありません。	固定パスワードの管理が不要となるため、管理にかかる時間とコストを節約できます。
強化されたシングルサインオン (SSO) 機能 — Kerberos SSO および NTLMv2 のサポート	SAシリーズは、ユーザー信用証明書を使用したKerberosまたはNTLMv2経由でアクセスするユーザーを自動的に認証します。	アプリケーションごとの信用情報の入力が必要となり、エンドユーザーの使い勝手が向上します。
パスワード管理の統合	ディレクトリストア（LDAP、Microsoft Active Directory、NTなど）のパスワードポリシーとの広範な統合を実現する標準準拠のインタフェースです。	既存のサーバーを使用してユーザーを認証できます。ユーザーはSAシリーズ インタフェースを使用してパスワードを管理できます。
ウェブベースのシングルサインオン (SSO) BASIC 認証、NTLM (NT LAN Manager)	他のアクセス管理システムの保護下にあるアプリケーションやリソースにも、ログインのユーザー名やパスワードを再入力することなく、アクセスできます。	ウェブベースのアプリケーションやMicrosoft系アプリケーションを利用するために何種類ものユーザー名やパスワードを入力・管理する手間を省くことができます。
ウェブベースのシングルサインオン フォーム方式、ヘッダ変数方式、SAML 方式	ユーザー名、信用情報のほか、管理者が独自に定義した属性を他の製品の認証フォームに渡したり、ヘッダ変数に含めたりすることができます。	ユーザーの生産性を向上させるとともに、カスタマイズによる最適な使い心地を実現します。

目的別のプロビジョニング

SA2500、SA4500、SA6500には、3種類のアクセス方式が用意されています。この中から、ユーザーのロールの一部としてアクセス方式を選択できるため、管理者は、会社のセキュリティポリシーに加えて、ユーザー、デバイス、ネットワークの属性を考慮したうえで、セッションごとに適切なアクセス権限を付与することが可能です。

表5：目的別のプロビジョニングの特長（機能）とメリット

特長（機能）	概要	メリット
クライアントレスのウェブアクセス（Core）	複雑なJavaScriptやXML、Flashベースのアプリケーション、Javaアプレットなど、ソケット接続が必要なウェブベースのアプリケーションに加え、標準準拠のメール（Outlook Web Accessなど）、WindowsやUNIXのファイル共有、telnet/SSHのホスティング・アプリケーション、シトリックスやウィンドウズのターミナルサービス、ターミナル・エミュレーションなどにWebブラウザ経由でアクセスできます。	携帯端末をはじめ、多彩なエンドユーザー端末からアプリケーションやリソースに最も簡単なアクセス方式を実現し、非常にきめ細かいセキュリティ制御が可能になります。ブラウザだけを使用するため、クライアント・ソフトウェアが不要になります。
Secure Application Manager（SAM）	JavaやWindowsベースの軽快動作のダウンロード機能を利用し、クライアント/サーバー・アプリケーションへのアクセスが可能です。	ウェブブラウザさえあれば、クライアント/サーバー・アプリケーションが可能です。事前にクライアント・ソフトウェアをインストールすることなく、ターミナルサーバー・アプリケーションにネイティブモードでアクセスできます。
Network Connect（NC）	自動プロビジョニングによるクロスプラットフォームのダウンロードでネットワーク層での確実な通信を実現します。Windows Logon/GINAの統合によるドメインのシングルサインオン（SSO）、管理者権限の必要性を軽減するインストーラー・サービスがあります。スプリット・トンネリング機能が利用できます。	ユーザー側で必要なのは、ウェブブラウザだけです。ネットワーク環境に応じて最高のパフォーマンスを引き出すために、Network Connectモジュールがバックグラウンドで2種類の伝送方式の中から自動的に選択されてVPNトンネルが接続されます。ジュニパーのインストーラー・サービスと組み合わせると、Network Connectのインストールや実行、アップデートに管理者権限が不要です。オプションでスタンドアロンのインストール方式も利用できます。スプリット・トンネリング機能により、サブネットまたはホストごとにトンネリングを適用する/しないを選択できるようになります。

製品オプション

SA2500、SA4500、SA6500製品には、各種ライセンスオプションが含まれており、機能拡張が可能です。

ユーザーライセンス

SA2500、SA4500、SA6500製品は、個別にアップグレードした機能を組み合わせているため、購入も簡単になりました。導入に必要なのはユーザーライセンスひとつだけです。システムがバージョン6.1（以降）のソフトウェアにアップグレードされているため、旧製品（ジュニパーネットワークスSA2000、SA4000、SA6000）を利用しているお客様も今回の変更によるメリットを得ることができます。

ユーザーライセンスは、リモートユーザー、エクストラネットユーザー、イントラネットユーザーのネットワークアクセスを可能にする機能を提供します。基本的な環境だけでなく、ユーザーや利用形態が多岐に渡る複雑な環境のニーズにも対応することができ、クライアント・ソフトウェア、サーバー変更、DMZ設定、ソフトウェア・エージェントの導入は、ほぼ必要ありません。また、ユーザーライセンス数の管理を容易にするため、各ライセンスはライセンスに指定した数のみが利用可能となり、また、追加方式を採用しています。例えば、最初に100ユーザーのライセンスを購入し、翌年に同時接続ユーザーが増えてライセンス数が不足した場合、100ユーザーライセンスをシステムに追加するだけで、最高200人の同時接続ユーザーのサポートが可能になります。このライセンスによって利用可能になる主な特長は次の通りです。

- SAMには、クライアント/サーバー・アプリケーションをクロスプラットフォームでサポートする機能があります。一方、NCのアダプティブ・デュアル・トランスポート方式を利用すると、ネットワーク層での完全なアクセスが実現します。このSAMとNCをクライアントレスアクセス機能に組み合わせることで、リモート環境やモバイル環境のユーザー、パートナー、顧客に至るまで、あらゆるユーザーが安全なアクセス環境を利用できるようになります。もちろん、多彩な端末に対応し、発信側ネットワークの種類も問いません。

- 目的別のプロビジョニングにより、ロールベースのアクセス制御だけでなく、アクセス要件に関わるセキュリティにおいて、適切、正確、かつダイナミックにバランスを取ることができます。
- 複数のルートCA・中間CA、OCSP（Online Certificate Status Protocol）、複数のサーバー証明書のインポート機能など、高度なPKI機能をサポート
- ユーザーセルフサービスにより、お気に入りのブックマークを設定してリモートで自分のワークステーションにアクセスしたり、期限切れになるパスワードを変更したりすることができます。
- 複数のホスト名（例えば、<https://employees.company.com>、<https://partners.company.com>、<https://employees.company.com/engineering>）に対応可能なため、ユーザーのニーズや希望に合わせて個別のログインページとカスタマイズした表示を設定し、自分達だけがそのシステムを使用しているように見せることができます。
- ユーザーや権限のある管理者の役割に応じてカスタマイズ可能なユーザーインターフェース
- ホストチェッカー、キャッシュクリーナー、セキュア・バーチャル・ワークスペースなどの高度なエンドポイントのセキュリティ制御機能により、リモートシステムが組織のセキュリティポリシーを順守する範囲でのみ、システムやリソースへのアクセスがユーザーにダイナミックに提供され、その後は、残されたデータがハードドライブから消去するため、エンドポイント端末には何も残されません。
- 最大240のVLANサポートを提供

Secure Meetingライセンス（オプション）

ジュニパーネットワークスSecure Meetingアップグレード・ライセンスは、SAシリーズ SSL VPNアライアンスの機能を拡張し、オンラインWeb会議や遠隔操作によるPCアクセスをいつでもどこからでも安全に実現します。Secure Meetingは、リアルタイムのアプリケーション共有を実現する機能で、許可を受けた従業員やパートナーであれば、直観的なウェブインタフェースを使って簡単にオンラインミーティングのスケジュールを設定したり、即座にミーティングを開始したりすることができます。このため、トレーニングや特別な環境は必要ありません。ヘルプデスクのスタッフや顧客サービス担当者の場合、ユーザー側のPCを遠隔操作しながら問題を解決することもできます。もちろんユーザー側のPCに特別なソフトウェアをインストールしておく必要もありません。クラス最高水準のAAA（認証・許可・アカウントिंग）機能を備えており、社内でも利用中の既存の認証インフラやポリシーをSecure Meetingに簡単に統合できます。ジュニパーのSSL-VPN製品のアーキテクチャは、市場で高い評価を集めており、Common Criteria認証取得済みで堅牢性にも優れています。また、あらゆるトラフィックに対してSSL/HTTPSのトランスポートを採用しており、常に社内の最高レベルのセキュリティ要件に確実に適合する形でウェブ会議や遠隔操作のソリューションを運用できるため、管理者に多大な安心感をもたらします。

Secure Meetingアップグレードは、SA2500、SA4500、SA6500に用意されています。

Instant Virtual Systemライセンス（オプション）

ジュニパーネットワークスのInstant Virtual System（IVS）オプションを利用すると、単一のデバイスまたはクラスタ内で、論理的に独立した240のSSL-VPNゲートウェイのプロビジョニングを管理者が実行できるようになります。例えば、サービスプロバイダは、単一のデバイスあるいはクラスタを利用して、複数の企業にネットワークベースのSSL-VPNマネージドサービスを提供できるだけでなく、複数のグループ間でSSL-VPNトラフィックを完全にセグメント化できます。IVSは、VLAN（802.1Q）タギングを利用してきめ細かいルールを作成することにより、利用企業ごとに完全に切り離し、それぞれのトラフィックを分離させることができます。たとえ別々の企業でIPアドレスが重複している場合でも、それぞれのエンドユーザーのトラフィックを安全に分離し、各社のリモート環境にいる従業員やパートナーなど、ユーザーごとにVLANを設定できます。

DNS（Domain Name Service）/WINS（Windows Internet Name Service）、AAA、ログ/アカウントング・サーバー、アプリケーション・サーバー（ウェブメール、ファイル共有など）は、各企業のイントラネットか、サービスプロバイダ側のネットワークに置くことができます。サービスプロバイダは、ユーザー企業単位で同時接続ユーザー総数を設定可能なため、リモート環境の従業員や納入業者、パートナーなどユーザーごとに柔軟に対応できます。SAシリーズでは、IVSの設定と管理のプログラム化機能が強化されます。これにより、サービスプロバイダは独自のオペレーション・サポート・システムにIVS管理機能を統合できるようになります。また、IVSを使用する企業は、XMLのインポート/エクスポート機能を活用した管理が可能となります。

IVSアップグレードは、SA4500とSA6500に用意されています。

高可用性ライセンス（オプション）

ジュニパーネットワークスでは、万一のシステム障害時でも冗長性を確保してシームレスなフェイルオーバーを実現するため、SAシリーズ向けに多彩な高可用性（HA）クラスターリング・オプションを開発しています。こうしたクラスターリング・オプションは、パフォーマンス面の拡張性向上にも効果があるため、過酷な利用状況にも的確に対応できます。SA2500/4500はクラスタペア構成、SA6500はマルチユニット型クラスタ構成とクラスタペア構成が用意されており、完全な冗長性と圧倒的なユーザー収容力を実現します。マルチユニット型クラスタ構成、クラスタペア構成ともに、LANやWAN上でのステートフル・ピアリングとフェイルオーバーに対応しているため、万一、1台のユニットに障害が発生した場合でも、システム構成（認証サーバー、許可グループ、ブックマークなど）、ユーザープロファイル設定（ユーザー定義ブックマーク、cookieなど）、ユーザーセッションはすべて保持されます。フェイルオーバーはシームレスなため、ユーザーや組織全体の生産性低下やダウンタイムが発生することもなく、ユーザーが再度ログインする必要もありません。マルチユニット型クラスタ構成は、自動的に「アクティブ/アクティブ」モードになります。一方、クラスタペア構成は、「アクティブ/アクティブ」モードか「アクティブ/パッシブ」モードのいずれかを選択できます。

高可用性ライセンスにより、1台のSAシリーズ アライアンスのライセンスを別の1台または複数台のSAシリーズ アライアンスと共有することができます（該当するプラットフォームによる）。また、同時ユーザーライセンスへの追加方式ではありません。例えば、100ユーザーライセンスを搭載したSA4500が1台あり、その後、100ユーザークラスターライセンスを搭載したSA4500を1台購入したとします。この場合、合計100人のユーザーを両方のデバイスで共有することになります。単一デバイスごとの個別サポートではありません。

HAオプションは、SA2500、SA4500、SA6500に用意されています。

ICEライセンス（オプション）

SSL-VPNは、台風・地震、テロ攻撃、交通機関のストなど、予測不能な状況下でもユーザー同士をつなぎ、企業や組織の正常な運営を支援します。リスクとコストの適正なバランスを追求したジュニパーネットワークスSAシリーズ用ICEオプションは、リモートアクセス需要が急増する状況に対応するタイムリーなソリューションを提供します。災害発生時でも業務の継続性を確保します。ICEオプションには、SAシリーズSSL VPNアライアンスに一時的に大量のユーザーを追加するためのライセンスが用意されています。ICEオプションには、次の特長があります。

- ・ いつでもどこからでもアプリケーションにアクセスできる態勢を整え、生産性を維持します。
- ・ 24時間いつでもリアルタイムにアプリケーションやサービスにアクセスできる環境でパートナーシップを維持します。その際、リソースのセキュリティを確保し、保護します。
- ・ オンラインのコラボレーションによる顧客やパートナーに卓越したサービスを中断することなく提供します。
- ・ 不測事態・業務継続計画（COOP）に対する日本政府・自治体の遵守通達、ISMSなどの事業継続計画に合致します。
- ・ リスクや拡張性を重視する一方、コストと導入の手間にも配慮した最適なバランスを追求します。

ICEライセンスは、SA4500とSA6500に用意されており、下記の各機能が搭載されています。

- ・ Base機能
- ・ Secure Meeting



仕様

	SA2500	SA4500	SA6500
寸法・電源仕様			
寸法（高×幅×奥行）	4.4×43.8×36.8 cm	4.4×43.8×36.8 cm	8.8×43.8×45 cm
重量	6.6 kg（標準）	7.1 kg（標準）	12 kg（標準）
ラックマウント対応	○（1U）	○（1U）	○（2U、19インチ）
電源（A/C）*	100-240 VAC、50-60 Hz、2.5 A 最大200W	100-240 VAC、50-60 Hz、2.5 A 最大300W	100-240 VAC、50-60 Hz、2.5 A 最大400W
内蔵バッテリー	CR2032 3V （コイン型リチウム電池）	CR2032 3V （コイン型リチウム電池）	CR2032 3V （コイン型リチウム電池）
MTBF（平均故障間隔）	75,000時間	72,000時間	98,000時間
ファン	3×40mmボールベアリングファン 1×40mmボールベアリングファン （電源部）	3×40mmボールベアリングファン 1×40mmボールベアリングファン （電源部）	2×80mmホットスワップ対応 1×40mmボールベアリングファン （電源部）
パネルディスプレイ			
電源LEDランプ、HD動作状況、 ハードウェアアラート	○	○	○
HD動作状況、フェールLED （ドライブトレイ）	×	×	○
ポート			
トラフィック	2×RJ-45 Ethernet - 10/100/1000 （全二重または半二重） （オートネゴシエーション）	2×RJ-45 Ethernet - 10/100/1000 （全二重または半二重） （オートネゴシエーション）	4×RJ-45 Ethernet （全二重または半二重） （オートネゴシエーション） 内部スイッチに対するリンク障害時の 冗長性実現用 SFPモジュール（オプション）
管理	—	—	1×RJ-45 Ethernet - 10/100/1000 （全二重または半二重） （オートネゴシエーション）
ファーストイーサネット	IEEE 802.3u準拠	IEEE 802.3u準拠	IEEE 802.3u準拠
ギガビットイーサネット	IEEE 802.3zまたは IEEE 802.3ab準拠	IEEE 802.3zまたは IEEE 802.3ab準拠	IEEE 802.3zまたは IEEE 802.3ab準拠
コンソール	1×シリアルコンソールポート （RJ-45）	1×シリアルコンソールポート （RJ-45）	1×シリアルコンソールポート （RJ-45）

* 日本向けに出荷される製品付属のAC電源コードは100V専用です。

仕様（続き）

	SA2500	SA4500	SA6500
動作環境			
動作時温度範囲	5～40℃	5～40℃	5～40℃
保管温度	-40～70℃	-40～70℃	-40～70℃
相対湿度（動作時）	8～90%（結露しないこと）	8～90%（結露しないこと）	8～90%（結露しないこと）
相対湿度（保管時）	5～95%（結露しないこと）	5～95%（結露しないこと）	5～95%（結露しないこと）
高度（動作時）	最大3,048m	最大3,048m	最大3,048m
高度（保管時）	最大12,192m	最大12,192m	最大12,192m
準拠規格			
安全規格	EN60950-1:2001+ A11、 UL60950-1:2003、 CAN/CSA C22.2 No. 60950-1-03、 IEC 60950-1:2001	EN60950-1:2001+ A11、 UL60950-1:2003、 CAN/CSA C22.2 No. 60950-1-03、 IEC 60950-1:2001	EN60950-1:2001+ A11、 UL60950-1:2003、 CAN/CSA C22.2 No. 60950-1-03、 IEC 60950-1:2001
電磁波適合規格	FCC Class A、EN 55022 Class A、 EN 55024 Immunity、EN 61000-3-2、 VCCI Class A	FCC Class A、EN 55022 Class A、 EN 55024 Immunity、EN 61000-3-2、 VCCI Class A	FCC Class A、EN 55022 Class A、 EN 55024 Immunity、EN 61000-3-2、 VCCI Class A

高性能がもたらすサービスとサポート

ジュニパーネットワークスは、高性能な製品によってサービスとサポートをもたらすリーダーであり、高性能ネットワークの促進や拡張、最適化の実現に向けたサービスを提供しています。これらのサービスでは、オンラインで迅速に収益創出能力を提供することにより、生産性の向上や、新しいビジネスモデルおよびベンチャー事業の迅速な展開、市場参入の拡大などを実現するとともに、より高いレベルの顧客満足度を達成します。また、ネットワークを最適化することで、必要な性能レベルや信頼性、可用性を維持し、オペレーショナル・エクセレンス（卓越した運用）を保証しています。

詳細については、<http://www.juniper.net/jp/jp/products-services/>をご参照ください。

ジュニパーネットワークスについて

ジュニパーネットワークスは、ハイ・パフォーマンス・ネットワーキングのリーダーです。サービスおよびアプリケーションの一元化されたネットワークにおける展開を加速するのに不可欠な、即応性と信頼性の高い環境を構築するハイ・パフォーマンスなネットワーク・インフラストラクチャを提供するジュニパーネットワークスは、お客様のビジネス・パフォーマンスの向上に貢献します。ジュニパーネットワークスに関する詳細な情報は、以下のURLでご覧になれます。

<http://www.juniper.net/jp/>

日本

ジュニパーネットワークス株式会社

東京本社
〒163-1035
東京都新宿区西新宿3-7-1
新宿パークタワーN棟35階
電話 03-5321-2600
FAX 03-5321-2700

西日本事務所
〒541-0041
大阪府大阪市中央区北浜1-1-27
グランクリュ大阪北浜

<http://www.juniper.net/jp/>

米国本社

Juniper Networks, Inc.

1194 North Mathilda Ave
Sunnyvale, CA 94089
USA

電話 888-JUNIPER
(888-586-4737)
または408-745-2000
FAX 408-745-2100

URL <http://www.juniper.net>

アジアパシフィック

Juniper Networks (Hong Kong) Ltd.

26/F
Cityplaza One
1111 King's Road,
Taikoo Shing, Hong Kong

電話 852-2332-3636
FAX 852-2574-7803

ヨーロッパ、中東、アフリカ

Juniper Networks Ireland

Airside Business Park
Swords, County Dublin
Ireland

電話 35-31-8903-600
FAX 35-31-8903-601

Copyright© 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks、JUNOS、NetScreen、ScreenOS、Juniper Networksロゴ、およびJUNOSelは、米国およびその他の国におけるJuniper Networks Inc.の登録商標または商標です。また、その他記載されているすべての商標、サービスマーク、登録商標、登録サービスマークは、各所有者に所有権があります。ジュニパーネットワークスは、本資料の記載内容に誤りがあった場合、一切責任を負いません。ジュニパーネットワークスは、本発行物を予告なく変更、修正、転載、または改訂する権利を有します。

1000220-003 JP May 2009