SRX 3400／SRX 3600 サービスゲートウェイ

製品概要

SRXシリーズ サービス・ゲートウェイは革新的なアーキテクチャに基づく次世代のセキュリティプラットフォームであり、高度な防御、パフォーマンス、拡張性、可用性、セキュリティサービスの統合を可能にします。処理能力やI/O能力の柔軟な拡張性、サービス統合に対応するカスタム設計により、SRXシリーズはデータセンターの統合やサービスの集約（アグリゲーション）に伴うセキュリティ要件を十分に満たしています。同様に、SRXシリーズに搭載されたJunos OSは業界屈指のオペレーティングシステムプラットフォームであり、データセンター向けに世界最大規模のネットワークの運用、管理、およびセキュリティ保護を可能にします。

Your ideas. Connected.™

製品説明

ジュニパーネットワークスのSRX3400サービスゲートウェイとSRX3600サービスゲートウェイは、高度な防御市場をリードするパフォーマンス、拡張性、サービスを中型サイズのモデルに統合して提供する次世代のサービスゲートウェイです。特に以下のような中～大規模な企業やパブリックセクターサービスプロバイダのネットワークに最適です。

- 企業のサーバーファーム／データセンター
- モバイル通信事業者のネットワーク環境
- 部門単位またはセグメント単位のセキュリティソリューションの集約
- クラウドおよびホスティングプロバイダのデータセンター
- マネージドサービスの展開

セキュリティについては、これらのプラットフォームは、アプリケーションセキュリティ、UTM（Unified Threat Management）、およびIPS（Intrusion Prevention System）などの次世代ファイアウォールサービスを提供します。Spotlight Secureによって統合される脅威インテリジェンスは、C&C（Command and Control）関連のボットネットに対する適応型脅威保護と、GeoIPおよび攻撃者フィンガープリント技術（後者はWebアプリケーション保護用）に基づくポリシー適用を実現します。これらはすべてジュニパーネットワークスが提供するフィードに基づきます。顧客は、高度なマルウェアやその他の脅威からの保護に独自のカスタムフィードおよびサードパーティフィードを利用することもできます。

革新的なミッドプレーン設計とジュニパーのダイナミック・サービス・アーキテクチャに基づいたSRX 3000シリーズは、企業やサービスプロバイダの環境における価格性能比の制約をリセットします。サービスゲートウェイにサービス処理カード（SPC）を1枚追加するごとに、ほぼ直線的に拡張性を増やすことができるため、SRX 3600では55Gbpsまでのファイアウォールスループットを実現します。SPCは広範囲のサービスに対応できるように設計されているので、将来最新の機能をサポートする際もサービス専用のハードウェアを追加する必要はありません。あらゆるサービスにSPCで対応するので、特定のサービスの使用によってアイドル状態のリソースが発生することはなく、ハードウェアが最大限に活用されます。

市場をリードするSRX 3000シリーズの柔軟性と価格性能比は、モジュール型アーキテクチャにより生み出されるものです。ジュニパーのダイナミック・サービス・アーキテクチャをベースとした本ゲートウェイは、I/Oカード（IOC）やネットワーク処理カード（NPC）、サービス処理カード（SPC）を柔軟に組み合わせて実装できるため、パフォーマンスとポート密度を理想的なバランスに保てるようにシステム構成をすることができます。つまりジュニパーネットワークスSRXシリーズのサービスゲートウェイを、特定のネットワーク要件を満たすようにカスタマイズできるのです。このような柔軟性を備えているため、ギガビットイーサネットまたは10ギガビットイーサネットポートを使用することで、100Gbpsを超えるインタフェースのサポートや、55Gbpsまでのファイアウォールパフォーマンスや特定のビジネスニーズに見合うサービス処理をサポートできるようSRX 3600を構成することができます。

SPCやNPC、IOCの拡張性は、SRX 3000シリーズで採用されているスイッチファブリックによって実現されています。スイッチファブリックのデータ転送能力は最大320Gbpsに達するので、どのような構成でも最大の処理およびI/O能力を実現できます。SRX3000シリーズは、このような最高クラスの拡張性と柔軟性によって、ネットワークインフラの拡張を容易にし、比類のない投資保護を提供します。

SRX 3000シリーズの柔軟性は技術革新やダイナミックなサービスアーキテクチャに効果をもたらすばかりではありません。SRX 3000シリーズの前面と後面にSPCを実装することで、市場をリードする柔軟性と拡張性を備えたミッドプレーン設計が実現されます。必要とされるラックスペースの半分に従来の2倍の枚数のSPCを実装することができるようになり、SRX3000シリーズは斬新な内部構造と革新的な外観上のデザインを両立しています。

SRXシリーズのサービスゲートウェイの緊密なサービス統合を支えるのがジュニパーネットワークスのJunos®オペレーティングシステムです。SRXシリーズのサービスゲートウェイは、Junos OSに蓄積されたルーティング技術とScreenOS®に蓄積されたセキュリティ技術を組み合わせることによって、ファイアウォール、侵入防御システム(IPS)、VPN(IPsec)、サービス拒否(DoS)、アプリケーションセキュリティ、ネットワークアドレス変換(NAT)、UTM(Unified Threat Management)、サービス品質(QoS)などの豊富な機能を提供します。また、複数のネットワーキング/セキュリティサービスが1つのOSに組み込まれていることによって、プラットフォームを通過するトラフィックフローが大幅に最適化されます。ジュニパーのキャリアクラスのルーターとスイッチでは、1つのOS、そして1つのアーキテクチャが採用されており、Junos OSを搭載したSRXシリーズもそのメリットを十分に活かしています。

SRX3600

SRX 3600サービスゲートウェイは、市場をリードするセキュリティソリューションであり、最大55GbpsのファイアウォールやIPS、また15GbpsのIPsec VPNに加えて新規接続数を1秒当たり最大270,000コネクションもサポートしています。必要なセキュリティサービスをすべて備えたSRX 3600は、中～大規模企業のデータセンター、ホスティングまたはコロケーション型のデータセンター、次世代の企業システムサービス/アプリケーションなどのセキュリティ保護に最適です。マルチテナンシーを実現する必要があるクラウドプロバイダのインフラと、モバイル通信事業者のネットワーク環境のセキュリティ対策にも対応します。サービスゲートウェイには拡張性と柔軟性が確保されているため、密度の高いデータセンターで従来のセキュリティ機器を統合するのに理想的です。また、サービスの密度も高く、クラウドまたはモバイルプロバイダにとっても理想的です。

SRX3400

SRX 3400サービスゲートウェイは、SRX 3600と同じSPC、IOC、およびNPCを使用し、最大30GbpsのファイアウォールやIPS、また8GbpsのIPsec VPNに加えて新規接続数を1秒当たり最大150,000コネクションもサポートできます。SRX 3400は、企業のデータセンターおよびネットワークインフラのセキュリティ保護とセグメント化や、複数のセキュリティソリューションの集約に最も適しています。ゾーン単位で固有のセキュリティポリシーをサポートする機能やネットワークの拡張に柔軟に対応できるので、小中規模のサーバーファームやホスティングサイト、モバイル通信事業者の配備に適しています。

SRX 3000シリーズのサービス処理カード*

SPCは、SRX 3000シリーズのサービスゲートウェイをコントロールする「頭脳」として、プラットフォームで提供するすべてのサービスを処理するように設計されています。特定のサービスや機能を提供するための専用ハードウェアを必要としないので、一部のハードウェアに負荷が集中して、他のハードウェアがアイドル状態になる、という状況は起こりません。また、複数のSPCを一緒にプールできるSRX3000シリーズにSPCを増設すれば、これらのサービスゲートウェイの性能と処理能力を高め、管理のオーバーヘッドと複雑さを大幅に低減することも可能になります。SRX 3600とSRX 3400は、どちらも同じSPCをサポートしています。(注:システムを適切に機能させるための最小構成として、1枚のNPCと1枚のSPCが必要です。)

SRX 3000シリーズのI/Oカード*

SRX 3000シリーズはカッパーイーサネットインタフェース用、Small Form-factor Pluggable (SFP)トランシーバ用、および高可用性(HA)用のポートを理想的な組み合わせでサポートしていることに加えて、同等クラスの製品の中で最大のI/Oポート密度を誇ります。SRX 3000シリーズのサービスゲートウェイには、1枚で16ギガビット相当(16×1のカッパーまたはファイバーギガビットイーサネット)または20ギガビット相当(2×10のギガビットXFPイーサネット)のインタフェースをサポートするIOCを1枚以上実装することができます。IOCを複数提供できる柔軟性があるので、インタフェースと処理能力を理想的なバランスでサポートできるようにSRX 3000シリーズを構成できます。(注:システムを適切に機能させるための最小構成として、1枚のNPCと1枚のSPCが必要です。)

SRX 3000シリーズのネットワーク処理カード*

最大の処理性能と柔軟性を確保するため、SRX 3000シリーズは装置に出入りするトラフィックを、該当のSPCやIOCに分配するためにNPCを利用し、QoSを適用し、DoSや 分散型DoS攻撃に対する防御を強化しています。SRX 3400は1枚から2枚のNPCをサポートする構成が可能ですが、SRX 3600では、1枚から3枚のNPCをサポートする構成が可能です。またSRX 3000シリーズにNPCを追加することで、組織ごとの性能要件に応じたソリューションを用意することが可能となります。(注:システムを適切に機能させるための最小構成として、1枚のNPCと1枚のSPCが必要です。)

また、SRX3000シリーズでは、新しい複合型のNPC/IOCカード(NP-IOC)も用意されています。1つのスロットにこのカードを1枚差し込むだけで、ネットワーク処理と入力/出力の2つの機能が提供され、ゲートウェイの能力が拡張されます。他のカードと同様に、このカードもインサービス・ソフトウェア・アップグレードおよびインサービス・ハードウェア・アップグレードに対応しています。現在のSRX3000シャーシおよびカードとの下位互換性も完全に維持されています。

*ジュニパーネットワークスのSRX3000シリーズは、SRX5000シリーズと同じく先進的で高度なダイナミック・アーキテクチャを採用しながらも、ミッドプレーン設計を実現しています。なお、SRX3000シリーズでは、Common Form-factor Module(CFM)設計を採用したSPC、NPC、IOCを利用できますが、これらのカードは、SRX5000シリーズでは使用できません。同様に、すべてのSRX 5000シリーズのモジュールはSRX 3000シリーズとの互換性はありません。

特長・メリット

ネットワーキングとセキュリティ

SRX 3000シリーズは、堅牢なネットワーキングおよびセキュリティサービスを提供できるように一から設計されています。

特長	概要	メリット
目的特化型プラットフォーム	専用ハードウェア上で一から構築してネットワーキングサービスとセキュリティサービスを強化します。	他の追随を許さないパフォーマンスと柔軟性を提供して高速ネットワーク環境を保護します。
拡張可能なパフォーマンス	ダイナミック・サービス・アーキテクチャによる拡張可能な処理能力を提供します。	新しいサービスと適切な処理能力を利用したシンプルでコスト効率の良いソリューションを提供します。
システムとネットワークの障害許容力	キャリアクラスのハードウェア設計と実証済みのOSを提供します。	重要な高速ネットワークの展開に必要な信頼性を提供します。
高可用性(HA)	専用の高可用性インタフェースを使用したアクティブ/パッシブHAおよびアクティブ/アクティブHA構成を採用しています。	重要なネットワークに必要な可用性と障害許容力を実現します。
柔軟なインタフェース	オンボードポートやモジュール型CFM I/Oカードなどの柔軟なI/Oオプションを提供します。	さまざまなネットワーク環境で必要とされるポート密度の要件を満たす柔軟なI/O構成と他に依存しないI/O拡張性を提供します。
ネットワークのセグメント化	管理者はセキュリティゾーン、VLAN、バーチャルルーターにより、ゲストユーザー、遠隔拠点のサーバー、データベースを分離してセキュリティポリシーを設定可能です。	内部、外部、およびDMZのサブグループごとにセキュリティおよびネットワーキングに関する専用の独自ポリシーを設定可能です。
堅牢なルーティングエンジン	専用のルーティングエンジンを採用し、物理的/論理的にデータプレーンと制御プレーンに分割します。	専用の管理環境から、ルーティング機能とセキュリティ機能が統合されたデバイスの展開を実現し、ルーティングインフラのセキュリティを確保します。
脅威インテリジェンス	Spotlight Secureの統合により、高度な脅威検出技術とフィードをポリシー適用のために活用します。	最適化された最新の脅威インテリジェンスに基づくポリシー適用が、ファイアウォール内の財産全体にわたって自動的にシンジケート化されることにより、セキュリティ効果と運用効率が向上します。
UTM(Unified Threat Management)	IPS、アンチウィルス、アンチスパム、Webフィルタリング、コンテンツフィルタリングなどの強力なUTM機能。事前に導入済みで、すぐに利用できる状態です。拡張性と適応性に優れた機能により、ゼロデイ攻撃防御を簡単かつ迅速に実現できます。アンチウィルスオプションはSophosとKaspersky、Webフィルタリングオプションはwebsense、アンチスパムオプションはSophosからそれぞれ入手できます。	さまざまなセキュリティ専門企業から提供される情報を活用し、強力かつハイパフォーマンスなコンテンツセキュリティにより、クラス最高のUTM保護を実現します。
AppTrack	バイト、パケット、およびセッション単位にネットワーク内のアプリケーションの容量/使用状況を詳細に分析します。	ネットワークの運用管理の改善を目的として、アプリケーションの使用状況を追跡する機能を提供し、高リスクなアプリケーションの特定や、トラフィックパターンの分析を支援します。
AppFirewall	きめ細やかなアプリケーションコントロールポリシーにより、アプリケーション名やグループ名に基づいてトラフィックを動的に許可または拒否できます。	従来のポートやプロトコルの分析ではなく、アプリケーションとユーザーロールに基づいて、セキュリティポリシーの作成とポリシー適用を可能にします。
AppQoS	ジュニパーネットワークスの多彩なQoS機能を活用します。	アプリケーションとネットワーク全体のパフォーマンス向上を目的として、アプリケーションの情報やコンテキストに基づいて、トラフィック優先度を設定するとともに、帯域幅を制限および確保する機能を提供します。
アプリケーションシグネチャ	オープンなシグネチャライブラリを使用して、アプリケーションやネストされたアプリケーションを特定します。	アプリケーションを正確に特定して、その情報に基づいて可視化、ポリシー適用、制御、保護を実現できます。
SSLプロキシ(フォワードおよびリバース)	クライアントとサーバーの間でSSL暗号化および暗号化解除を実行します。	アプリケーション識別との組み合わせにより、SSL暗号化トラフィックに埋め込まれた脅威に対する可視化と防御を実現します。
IPS(Intrusion Prevention System)	ネットワークトラフィックストリームに含まれる悪用や異常を検知します。	重要な防御層をステートフルファイアウォールの外側に追加することで、ネットワークトラフィックの脆弱性の検知とともに、IPSポリシー適用のきめ細かい制御を可能にします。
ステートフルGPRSおよびSCTPインスペクション	モバイル通信事業者のネットワークでGPRSおよびSCTPファイアウォールをサポートします。	SRX3000シリーズでステートフルファイアウォール機能を使用することで、モバイル通信事業者のネットワークに接続されている重要なGPRSノードを確実に保護できます。

特長	概要	メリット
ユーザーIDベースのアクセスコントロール	ジュニパーネットワークスJunos Pulseアクセスコントロールサービスおよび SRX3000シリーズに搭載されている標準ベースのアクセスコントロール機能と、SRX5000シリーズとの緊密な統合により、データセンターリソースへのセキュアなアクセスを実現します。	Junos Pulseアクセスコントロールサービスに搭載されている標準ベースのアクセスコントロール機能とSRX3000シリーズを統合することで、エージェントおよびエージェントレスによるIDベースのセキュリティサービスを企業のデータセンターで実現できます。このため、企業ユーザーやゲストユーザー、モバイルユーザーなどによる多様なユーザーアクセスを柔軟に管理することが可能です。
NP-IOC	他のカードと同様に、このカードもインサービス・ソフトウェア・アップグレードおよびインサービス・ハードウェア・アップグレードに対応しています。現在のSRX3000シャーシおよびカードとの下位互換性も完全に維持されています。	ビジネス要件を満たすために、ゲートウェイの能力を拡張し、遅延の影響を受けるアプリケーション（高速金融取引など）を支援します。
AutoVPN	新規に追加したスポークを含め、すべてのスポークに対してサイト間VPNのハブ構成を1回で行います。構成オプションは、ルーティング、インタフェース、IKE、およびIPsecです。	IT管理にかかる時間とコストを削減し、IPsec VPNネットワークを簡単かつ自動的に導入できます。

IPSの機能

ジュニパーネットワークスのIPS機能は、最高レベルのネットワークセキュリティを保証する独自の機能をいくつも備えています。

特長	概要	メリット
ステートフルシグネチャインスペクション	シグネチャは、ネットワークトラフィックのうち、適切なプロトコルコンテキストによって判断された該当部分のみに適用されます。	誤検知を防ぎ、柔軟なシグネチャ開発機能を提供します。
プロトコルデコード	最も正確な検知方式を実現するとともに、誤検知を減らす効果があります。	プロトコルコンテキストの正確な対応により、シグネチャの精度が改善されます。
シグネチャ	8,500以上のシグネチャで異常、攻撃、スパイウェア、およびアプリケーションを特定します。	攻撃を正確に識別して、既知の脆弱性を悪用しようとする攻撃を検出します。
トラフィックの正規化	リアセンブリ、正規化、およびプロトコルデコードが利用できます。	難読化技術を用いて、他のIPS検知を回避する攻撃に対応します。
ゼロデイ攻撃防御	プロトコル異常検知が提供され、新しい脆弱性が発見された場合には即日で対応パッチが提供されます。	ネットワークは新しい攻撃に対してもすでに保護されています。
推奨ポリシー	ジュニパーネットワークスのセキュリティチームが、一般企業が防御すべき危険度の高い脅威を攻撃シグネチャのグループとして特定します。	単純化されたインストールとメンテナンスで最高レベルのネットワークセキュリティを確保できます。
アクティブ/アクティブ構成のトラフィックモニタリング	アクティブ/アクティブ構成のシャーシクラスタでIPSをモニタリングします。	アクティブ/アクティブ構成のIPSモニタリングのほか、インサービス・ソフトウェア・アップグレード（ISSU）などの高度な機能が利用できます。
パケットキャプチャ	IPSポリシーが、ルールごとにパケットキャプチャのログを記録します。	周辺のトラフィックを分析し、保護を実行する手順を決定します。

その他のUTM機能

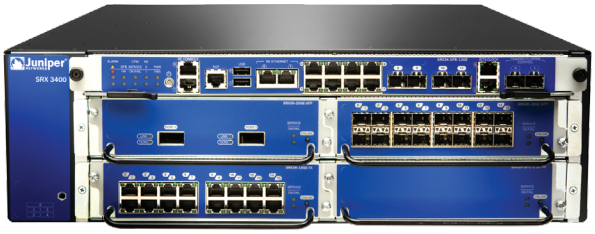
ジュニパーネットワークスSRX3000で提供されるUTMサービスには、業界屈指のアンチウィルス、アンチスパム、コンテンツフィルタリング、その他のコンテンツセキュリティサービスが含まれます。

特長	概要	メリット
アンチウィルス	アンチウィルスには、レピュテーション対応を強化したクラウドベースのアンチウィルス機能が含まれており、POP3、HTTP、SMTP、IMAP、およびFTPプロトコル上でスパイウェア、アドウェア、ウィルス、キーロガー、その他のマルウェアを検知してブロックします。このサービスは、セキュリティ専門企業のSophos Labsとの連携により提供されます。	一流のアンチウィルス専門家によって提供される高度な防御策により、データブリーチ（漏えい）や生産性の損失をもたらす可能性があるマルウェア攻撃に対抗します。
アンチスパム	マルチレイヤー型のスパム防御、最新のフィッシングURL検知、標準ベースのS/MIME、Open PGPおよびTLS暗号化、MIMEタイプと拡張子に基づくブロッカーといった機能は、セキュリティ専門企業のSophos Labsとの連携により提供されます。	電子メールフィルタリングやコンテンツブロッカーを駆使することにより、ソーシャルネットワーキング攻撃や最新のフィッシング詐欺による高度で永続的な脅威に対抗する防御を実現します。
拡張型Webフィルタリング	広範なカテゴリの細分化（95種類以上のカテゴリ）や、Webセキュリティ専門プロバイダのWebsenseが提供するリアルタイムの脅威スコアなどを特長とする拡張Webフィルタリング。	生産性の損失や、悪意のあるURLによる影響を防止すると同時に、ビジネスに不可欠なトラフィック用のネットワーク帯域幅の確保を支援します。
コンテンツフィルタリング	MIMEタイプ、ファイル拡張子、プロトコルコマンドなどに基づく効果的なコンテンツフィルタリング。	生産性の損失や、ネットワーク上に存在する外部コンテンツや悪意のあるコンテンツによる影響を防止すると同時に、ビジネスに不可欠なトラフィック用の帯域幅の確保を支援します。

集中管理

ジュニパーネットワークスJunos® Space Security Directorは、拡張性と即応性に優れたセキュリティ管理を実現することにより、セキュリティポリシー管理の利便性や簡便性、正確性を高めます。標準的なブラウザを使用して、単一のウェブベースのインタフェースからアクセスすることにより、セキュリティポリシーのライフサイクルにおけるすべての階層を管理することができます。さらに、アプリケーション識別やファイアウォール、IPS、NAT、VPNセキュリティ管理を一元化して、直感的かつ迅速なポリシー管理を実現します。

Junos Space Security Directorは、優れた拡張性を持つネットワーク管理機能に対応したJunos Spaceネットワーク管理プラットフォームで動作し、ジュニパーネットワークスおよびサードパーティ製の革新的なJunos Spaceエコシステムの継続利用などを可能にします。



SRX3400
サービスゲートウェイ

SRX3600
サービスゲートウェイ

Specifications

	SRX3400	SRX3600
最大パフォーマンス・設定数[1]		
テストしたJunos OSのバージョン	Junos OS 12.1X47	Junos OS 12.1X47
ファイアウォールパフォーマンス（最大）	30Gbps	55Gbps
ファイアウォールパフォーマンス（IMIX）	10Gbps	20Gbps
最大AES256+SHA-1 VPNパフォーマンス	8Gbps	15Gbps
最大3DES+SHA-1 VPNパフォーマンス	8Gbps	15Gbps
最大IPSパフォーマンス（NSS 4.2.1）	8Gbps	15Gbps
最大同時セッション数	2.25/3million[2]	2.25/6million[2]
新規セッション数/秒（持続、tcp、3ウェイ）	150,000	150,000/270,000[2]
最大サポートユーザー数	無制限	無制限
遅延	Sub-10µs	Sub-10µs
SRX3600サービスゲートウェイ		
固定I/O	8 10/100/1000 + 4 SFP	8 10/100/1000 + 4 SFP
LANインタフェースオプション	16×1 10/100/1000 カッパー 16×1 ギガビットイーサネットSFP 2×10 ギガビットイーサネットXFP	16×1 10/100/1000 カッパー 16×1 ギガビットイーサネットSFP 2×10 ギガビットイーサネットXFP
IOC用最大スロット数	4（前面スロット）	6（前面スロット）
処理の拡張性		
SPC用最大スロット数[3]	シャーシ当たり最大4[4]（任意のスロット）	シャーシ当たり最大7（任意のスロット）
NPC用最大スロット数[3]	シャーシ当たり最大2[4]（背面スロットに3つ）	シャーシ当たり最大3（背面右スロットに3つ）

[1] 記載の性能、処理能力、機能はJunos OS 12.1X44が動作するシステムに基づいており、理想的なテスト条件下で測定した値です。他のリリースのJunos OSを使用する場合や導入環境が異なる場合は、実際の結果が異なる可能性があります。SRXシリーズのサービスゲートウェイがサポートするJunos OSのバージョンの詳細なリストについては、Juniper Customer Support Center（http://www.juniper.net/customers/support/）をご覧ください。

[2] 300万および600万のセッションには、追加の高度なライセンスが必要です。

[3] SRX3000シリーズのサービスゲートウェイは、シャーシの前後にCFM（コモンフォームファクターモジュール）拡張スロットを複数搭載し、お客様のご希望に合わせたI/Oおよび処理機能構成のカスタマイズを可能にしています。SPCおよびNPCは搭載されているすべてのCFMスロットを利用可能ですが、適切なシステム機能性やI/Oの拡張性を考慮して、SRX3400ではシャシー当たり最大SPC×4／NPC×3まで、SRX3600では最大SPC×7／NPC×3までの対応としています。SPCおよびNPCについての詳細情報は、設置ガイドラインの他、関連のハードウェア説明書も合わせてご覧ください。

[4] DC電源使用時の指針についてはユーザーガイドを参照してください。

	SRX3400	SRX3600
ファイアウォール		
ネットワーク攻撃検知	○	○
DoS/DDoS攻撃防御	○	○
TCPパケット再構成によるフラグメントパケット攻撃防御	○	○
総当たり攻撃緩和	○	○
SYN Cookie防御	○	○
ゾーンベースIPスプーフィング	○	○
異常パケット攻撃防御	○	○
IPsec VPN		
サイト間のトンネル数	7,500	7,500
トンネル用インタフェース	7,500	7,500
DES (56-bit)、3DES (168-bit)、およびAES暗号化	○	○
MD5およびSHA-1認証	○	○
Manual key、IKE、PKI (X.509)	○	○
PFS (DHグループ)	1,2,6	1,2,6
リプレイ攻撃防御	○	○
リモートアクセスVPN	○	○
IPv4およびIPv6 VPN	○	○
VPNゲートウェイ冗長化	○	○
侵入防御システム		
シグネチャベースおよびカスタマイズ可能（テンプレート使用）	○	○
アクティブ/アクティブ構成のトラフィックモニタリング	○	○
ステートフルプロトコルシグネチャ	○	○
攻撃検知方式	ステートフルシグネチャ、プロトコル異常検知（ゼロデイ対応）、アプリケーション識別	ステートフルシグネチャ、プロトコル異常検知（ゼロデイ対応）、アプリケーション識別
攻撃対応方式	接続切断、接続遮断、セッションパケットログ、セッションサマリ、電子メール、カスタムセッション	接続切断、接続遮断、セッションパケットログ、セッションサマリ、電子メール、カスタムセッション
攻撃通知方式	構造化されたシステムロギング	構造化されたシステムロギング
ワーム防御	○	○
推奨ポリシーによるインストールの簡素化	○	○
トロイの木馬防御	○	○
スパイウェア/アドウェア/キーロガー防御	○	○
その他のマルウェア防御	○	○
アプリケーションサービス拒否（DoS）の防御	○	○
感染したシステムからの拡散防御	○	○
ポートスキャンの防御	○	○
リクエスト＆レスポンスサイド攻撃防御	○	○
複合攻撃防御 - ステートフルシグネチャ検知とプロトコル異常検知の組み合わせ	○	○
カスタムシグネチャの作成	○	○
コンテキスト(プロトコル要約)	600以上	600以上
攻撃の編集(ポート範囲など)	○	○
ストリームシグネチャ	○	○
プロトコルしきい値	○	○
ステートフルプロトコルシグネチャ	○	○
防御可能な攻撃数	15,000以上	15,000以上
攻撃の詳細説明と対応策・パッチ情報	○	○

	SRX3400	SRX3600
適切なアプリケーションポリシー設定	○	○
攻撃者・標的の監査証跡とレポート作成	○	○
アップデート頻度	毎日・緊急時	毎日・緊急時
UTM（Unified Threat Management）		
アンチウィルス（Sophos AV）スループット	2.5Gbps	4.5Gbps
拡張Webフィルタスループット	8Gbps	14Gbps
GPRSセキュリティ		
ステートフルなGPRSファイアウォール	○	○
宛先アドレス変換（NAT-Dst）		
NAT-Dst、PATあり	○	○
NAT-Dst、受信インタフェースと同一サブネット内IPアドレスに変換	○	○
NAT-Dst、多対多、PATあり（M:1P）	○	○
NAT-Dst、多対1（M:1）	○	○
NAT-Dst、多対多（M:M）	○	○
ソースアドレス変換（NAT-Src）		
静的NAT-Src、DIPプールからアドレスシフティングによりアドレス取得	○	○
NAT-Src、PATあり、ポート変換	○	○
NAT-Src、PATなし、固定ポート	○	○
NAT-Src、IPアドレス永続的	○	○
ソースプールのグルーピング	○	○
ソースプールの利用率アラーム	○	○
インタフェースサブネット外のソースIP	○	○
インタフェースNAT-Src、インタフェースDIP	○	○
要求がNATプールを上回りアドレスプールが枯渇したときはPATにフォールバック	○	○
対称NAT	○	○
NATプールへの複数範囲割り当て	○	○
物理ポートのプロキシARP	○	○
NAT-Dst （ループバックグルーピング）– DIP （ループバックグルーピング）	○	○
ユーザー認証とアクセスコントロール		
組み込み（内部）データベース	○	○
RADIUSアカウンティング	○	○
ウェブベースの認証	○	○
UACエンフォースメントポイント	○	○
PKIサポート		
PKI証明書要求（PKCS 7、PKCS 10）	○	○
自動証明書登録（SCEP）	○	○
対応認証局	○	○
自己署名証明書	○	○
仮想化		
データプレーンのトラフィックセグリゲーション（仮想ルーター（1,000）と	512	512
ゾーン（512））による仮想ファイアウォール最大数	32	32
データプレーンと管理用の分離（論理システム）による仮想ファイアウォール最大数	無制限	無制限
Firefly（VMベース）による追加のオフプラットフォーム仮想ファイアウォールオプション	16,384[5]	16,384[5]

L3サブインタフェース最大数	4,096	4,096

サポートVLAN最大数

	SRX3400	SRX3600
ルーティング		
BGPインスタンス	1,000	1,000
BGPピア	2,000	2,000
BGPルート	1,000,000[6]	1,000,000[6]
OSPFインスタンス	256	256
OSPFルート	1,000,000[6]	1,000,000[6]
RIP v1/v2インスタンス	50	50
RIP v2テーブルサイズ	30,000	30,000
ダイナミックルーティング	○	○
スタティックルート	○	○
フィルターベースフォワーディング(FBF)	○	○
イコールコストマルチパス(ECMP)	○	○
リバースパスフォワーディング(RPF)	○	○
マルチキャスト	○	○
IPv6		
ファイアウォール/ステートレスフィルタ	○	○
VPN	○	○
デュアルスタックIPv4/IPv6ファイアウォール	○	○
RIPng	○	○
BFD、BGP	○	○
ICMPv6	○	○
OSPFv3	○	○
Class of Service	○	○
動作モード		
レイヤー2(透過)モード	○	○
レイヤー3(ルートおよび/またはNAT)モード	○	○
IPアドレス割り当て		
静的割り当て	○	○
動的ホスト構成プロトコル(DHCP)	○	○
内部DHCPサーバー	○	○
DHCPリレー	○	○
トラフィック管理QoS		
最大帯域	○	○
RFC2474 IPv4のIP DiffServ	○	○
CoSのフィルタ	○	○
クラス分け機能	○	○
スケジューリング	○	○
シェーピング	○	○
インテリジェントドロップメカニズム(WRED)	○	○
3段階のスケジューリング	○	○
スケジューリングの各レベルでのWRR (Weighted Round Robin)	○	○

[5] HA構成でサポートしているL3サブインタフェースの最大数は1,000です。
[6] BGPおよびOSPFルートの推奨最大数は100,000です。1

ルーティングプロトコルのプライオリティ	○	○

	SRX3400	SRX3600
高可用性		
アクティブ/パッシブ、アクティブ/アクティブ	○	○
衝撃の少ないシャーシクラスタのアップグレード	○	○
コンフィグレーション同期	○	○
ファイアウォール/IPSec VPNセッション同期	○	○
ルーティング変更のためのセッションフェイルオーバー	○	○
デバイス障害検知	○	○
リンク/アップストリームの障害検知	○	○
インタフェースのリンクアグリゲーション/LACP	○	○
冗長データおよびコントロールリンク[7]	○	○
インサービス・ソフトウェア・アップグレード（ISSU）[8]	○	○
管理		
ウェブユーザーインタフェース(HTTP/HTTPS)	○	○
コマンドラインインタフェース(コンソール)	○	○
Network and Security Managerバージョン2008.2以降	○	○
運用管理		
ローカル管理者データベースサポート	○	○
管理者用外部データベースサポート	○	○
管理者ネットワーク	○	○
Root Admin、Admin、Read Onlyの各ユーザーレベル	○	○
ソフトウェアアップグレード	○	○
コンフィグレーションロールバック	○	○
ログ収集・モニタリング		
構造化されたシステムロギング	○	○
SNMP (v2/v3)	○	○
Traceroute	○	○
寸法・電源仕様		
寸法(幅×高さ×奥行)	44.5×13.3×64.8cm (17.5×5.25×25.5インチ)	44.5×22.2×64.8cm (17.5×8.75×25.5インチ)
重量	シャーシ：14.7kg (32.3lb) フル構成時：34.1kg (75lb)	シャーシ：19.8kg (43.6lb) フル構成時：52.6kg (115.7lb)
電源(AC)[9]	AC 100～240V	AC 100～240V
電源(DC)	DC -40～-72V	DC -40～-72V
最大消費電力	1,100W (AC電源) 1,050W (DC電源)	1,750W (AC電源) 1,850W (DC電源)
電源冗長方式	1 + 1	2 + 1 / 2 + 2
準拠規格		
安全規格	○	○
EMC規格	○	○
NEBSレベル3対応の設計	○	○
NIST FIPS-140-2レベル2	○（Junos OS 10.4R4使用時）	○（Junos OS 10.4R4使用時）
ISOコモンクライテリアNDPP+TFFW EP	○（Junos OS 12.1x44使用時）	○（Junos OS 12.1x44使用時）
ICSAネットワークファイアウォール	○	○
IPsec	○	○
USGv6	○（Junos OS 11.4R1使用時）	○（Junos OS 11.4R1使用時）

[7] SRX3000ラインでデュアルコントロールリンクを有効にするには、各クラスタメンバーにSRX3K CRMモジュールをインストールする必要があります。
[8] ISSUの互換性機能の詳細については、技術資料およびリリースノートを参照してください。
[9] ご購入の際にご利用環境にあわせた電源ケーブルを選択してください。

	SRX3400	SRX3600
3GPP TS 20.060規格への準拠[10]		
R6：3GPP TS 29.060バージョン6.21.0	○	○
R7：3GPP TS 29.060バージョン7.3.0	○	○
R8：3GPP TS 29.060バージョン8.3.0	○	○
環境		
動作時温度範囲（長期間）	5～40°C（41～104°F）	5～40°C（41～104°F）
動作時温度範囲（短期間[11]）	-5～55°C（23～131°F）	-5～55°C（23～131°F）
湿度範囲（長期間）	5～85%（結露しないこと）	5～85%（結露しないこと）
湿度範囲（短期間[11]）	5～93%（結露しないこと） ただし、水蒸気0.026kg/乾燥空気1kgを超えないこと	5～93%（結露しないこと） ただし、水蒸気0.026kg/乾燥空気1kgを超えないこと

[10] Junos OSリリース10.0およびそれ以降を使用しているSRX3000ラインゲートウェイは、以下（SRX3000ラインではサポートされない）を除き、3GPP TS 20.060のR6、R7、およびR8リリースに準拠しています。
- セクション7.5A マルチメディアブロードキャストおよびマルチキャストサービス（MBMS）メッセージ
- セクション7.5B モバイルステーション（MS）情報変更メッセージ
- セクション7.3.12 GGSNからのセカンダリPDPコンテキスト要求の開始

[11] 短期間とは、連続して96時間未満、かつ年間に15日未満を意味します。

ジュニパーネットワークスの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を可能にします。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、ネットワークイノベーション企業です。デバイスからデータセンター、消費者からクラウド事業者にいたるまで、ジュニパーネットワークスは、ネットワーキング体験とビジネスを変革するソフトウェア、シリコン、システムを提供しています。ジュニパーネットワークスに関する詳細な情報は、以下をご覧ください。

http://www.juniper.net/jp/ 、**Twitter** 、**Facebook**

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 45F
電話　03-5333-7400
FAX　03-5333-7401

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

米国本社
Juniper Networks, Inc.
1194 North Mathilda Avenue
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、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　31-0-207-125-700
FAX　31-0-207-125-701

URL http://www.juniper.net/jp/