



# SSG 5 & SSG 20

## 次世代スマート・ファイアウォール — ウルトラUTM —

### 製品概要

ジュニパーネットワークスのセキュア・サービス・ゲートウェイ (SSG) 5とセキュア・サービス・ゲートウェイ (SSG) 20は、小規模拠点、営業所、在宅勤務、SOHOを対象として、パフォーマンス、セキュリティ、ルーティング、LAN/WAN接続機能をバランスよく統合した次世代スマートファイアウォール/VPNです。

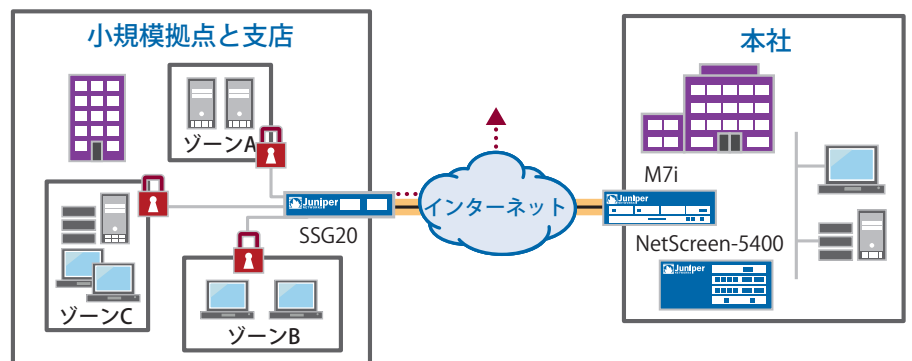
ステートフル・ファイアウォール、IPSec (IP Security Protocol)、IPS (ディープ・インスペクションFW)、アンチウイルス (アンチスパイウェア、アンチアドウェア、アンチフィッシングなど)、アンチスパム、Webフィルタリングを統合したUTM (統合脅威管理) により、支店や営業所を流れるトラフィックをワーム、スパイウェア、トロイの木馬などのマルウェアから保護します。

### 製品説明

SSG 5とSSG 20は、小規模拠点、支店、SOHO向けの高性能なセキュリティプラットフォームであり、ネットワーク内部と外部からの攻撃を防御し、不正アクセスを拒否するほか、法令遵守を徹底します。SSG 5とSSG 20は、ステートフル・ファイアウォール・トラフィック160 Mbps、IPSec VPNスループット40 Mbpsを実現します。

**セキュリティ:** 業界最高クラスのパートナー企業から提供されたセキュリティ機能を結集したUTMでワーム、ウイルス、トロイの木馬、スパムなどの新たに登場するマルウェアからネットワークを保護します。SSG 5とSSG 20は、内部ネットワークのセキュリティ要件を満たし、法令遵守を徹底するために、セキュリティゾーン、バーチャルルーター、VLANなどの高度なネットワーク保護機能をサポートしています。VLANを使用すると、ネットワークをセキュアドメインに分割し、それぞれにセキュリティポリシーを設定できます。セキュリティゾーンを保護するポリシーには、UTMセキュリティ機能に統合されたアクセス・コントロール・ルールを設定できます。

**接続性とルーティング:** SSG 5は、10/100インタフェース 7ポートをオンボードに実装し、オプションとして固定WANポートを備えています。SSG 20は10/100インタフェース5ポートに加え、オプションのWANインタフェースとして、I/O拡張スロット2ポートを備えています。WANプロトコルとカプセル化に対応した多彩なI/Oインタフェースを備えているため、従来の支店用ルーターとして簡単に導入できるだけでなく、セキュリティ機能とルーティング機能を備えた統合デバイスとして活用すると、設備投資と運用コストを大幅に削減できます。SSG 5とSSG 20は、無線LAN規格のIEEE 802.11 a/b/gに対応しており、無線ネットワークのセキュリティ機能を出荷時に選択できます。



SSG 20を支店に導入して、セキュアなインターネット接続と本社とのVPN接続を構築します。社内無線および無線リソースは、セキュリティポリシーを各セキュリティゾーンに設定して保護します。

**統合型アクセス・コントロール：**SSG 5とSSG 20は、ICシリーズ UACアプライアンスを追加するだけで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）ソリューションのインフラネット・エンフォースとして動作します。中央ポリシー管理エンジンであるICシリーズは、SSG 5/20と通信して、ファイアウォールベースのアクセス・コントロールを補強するか、より詳細な基準に基づいてアクセスを許可または拒否するソリューションに変更します。インフラネット・コントローラは、エンドポイントの状態とユーザーアカウント（個人属性も含むアカウント情報）を評価し、臨機応変なポリシー管理をネットワーク全域にリアルタイムで実行します。

**業界最高レベルのサポート：**ジュニパーネットワークスのプロフェッショナルサービスは、研究所における簡単な試験から大規模なネットワークの実装まで、幅広い技術サポートを提供しています。お客様のITチームと協力して、プロジェクトの目標を設定し、導入プロセスの定義、ネットワーク設計の作成と検証、配置管理を行います。

## 機能と利点

機能	機能解説	利点
高性能	専用のハードウェア、高い処理能力、セキュリティ専用オペレーティングシステムを組み合わせたセキュリティ専用プラットフォーム	現在の環境と将来的な拡張を視野に入れて、ネットワーク内外からの脅威を確実に防御
業界最高クラスの UTM セキュリティ機能	UTMセキュリティ機能（アンチウイルス、アンチスパム、Webフィルタリング、IPS）であらゆるウイルスとマルウェアによるネットワーク攻撃を未然に阻止	あらゆる攻撃からネットワークを保護
統合型アンチウイルス	Kaspersky Lab社のアンチ・ウイルス・エンジンをジュニパーネットワークスが提供（別途年間ライセンスが必要です）	ウイルス、スパイウェア、アドウェアなどのマルウェアの侵入を防御
統合型アンチスパム	Sophos社のアンチスパム製品をジュニパーネットワークスが提供（別途年間ライセンスが必要です）	既知のスパムやフィッシャーが送信した電子メールをブロック
統合型 Web フィルタリング	Websense SurfControl社のWebフィルタリング・ソリューションを（別途年間ライセンスが必要です）	悪意あるWebサイトへのアクセスを制御またはブロック
統合型侵入検知防御（ディープ・インスペクション）	IPSエンジン（別途年間ライセンスが必要です）	アプリケーションレベルに対するフラッド攻撃を防御
固定インタフェース	SSG 5は、10/100インタフェース7ポート（固定）とISDN BRI S/Tを搭載。SSG20は、10/100インタフェース5ポート（固定）とAUXポートを搭載。SSG 5と20共にコンソールポートを装備	高速LAN接続、WAN接続の冗長化、柔軟な管理機能を提供
ネットワークのセグメント化	セキュリティゾーン、仮想LAN、バーチャルルーターにセキュリティポリシーを設定し、ゲスト、無線ネットワーク、拠点サーバー、データベースを分離	内部ネットワークにセキュリティ機能を迅速に実装して、不正アクセス、攻撃防御、法令遵守を徹底
モジュール型インタフェース	インタフェース拡張スロット2個（SSG 20のみ）。オプションとして、ISDN BRI S/T、シリアル、SFP、インタフェースモジュール（Mini-PIM）に対応*	優れたセキュリティ機能とLAN/WAN接続を提供し、運用費用を削減し、既存の投資を保護
堅牢なルーティングエンジン	OSPF、BGP、RIP v1/2に対応した定評あるルーティングエンジン	セキュリティ機能とルーティング機能を統合し、運用費用と設備投資を削減可能
IEEE 802.11 a/b/g 準拠のセキュリティ機能	無線ネットワークのプライバシー保護と認証機能でUTM機能を強化して、無線トラフィックを保護	小規模拠点にWANアクセスポイント、セキュリティ、ルーティング機能を追加して、デバイスを統合
ジュニパーネットワークス統合型アクセス・コントロールのインフラネット・エンフォース	中央ポリシー管理エンジン（ICシリーズ）と通信し、ユーザーアイデンティティ、デバイスのセキュリティ状態、ネットワークロケーションに基づき、セッション固有のアクセス・コントロール・ポリシーを実行	お客様の既存のネットワークインフラと業界最高レベルの技術を活用し、セキュリティをコスト効果的に強化
柔軟なネットワーク管理	コマンドライン・インタフェース（CLI）、WebUI、またはNetwork and Security Manager（NSM）でセキュリティポリシーを確実に配置、監視、管理可能	任意のロケーションから管理機能にアクセス可能。現場に出向かずに、ネットワークを管理できるため、レスポンス時間を短縮して、運用費用を削減できる
業界最高レベルのプロフェッショナルサービス	ジュニパーネットワークスのプロフェッショナルサービスは、研究所における簡単な試験から大規模なネットワーク実装までの広範なサポートサービスを提供。お客様のITチームと協力して、プロジェクトの目標を設定し、導入プロセスの定義、ネットワーク設計の作成と検証、配置管理を実施	ネットワークインフラのセキュリティ、柔軟性、拡張性、信頼性を保証

\*シリアルおよびSFP Mini-PIMは ScreenOS6.0以降でサポートされます。

## 製品オプション

オプション	オプション解説	対象製品
DRAM	128 MB 256 MB	SSG 5 SSG 20
UTM/コンテンツセキュリティ (ハイメモリオプション)	ジュニパーネットワークス SSG 5/20では、アンチウイルス (アンチスパイウェア、アンチフィッシング)、IPS (ディープインスペクション)、Webフィルタリング、アンチスパムなど、業界最高レベルのUTMとコンテンツ機能を自由に組み合わせることで構成することが可能	ハイメモリ版のSSG 5またはSSG 20のみ
I/O オプション	インターフェース拡張スロット2個。オプションとして、ISDN BRI S/T、シリアル、SFP、インターフェースモジュール (Mini-PIMs) に対応	SSG 20のみ
802.11 a/b/g の接続性	SSG 5/20は、IEEE 802.11 a/b/g準拠の無線接続を選択可能	SSG 5 SSG 20
ライセンス延長	主要機能キャパシティ (セッション、VPNトンネル、VLAN) のライセンス延長及び、ファイアウォールとVPNにステータフルな高可用性 (HA) を追加可能	SSG 5 SSG 20



仕様 <sup>(1)</sup>

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>最大パフォーマンス・設定数 <sup>(2)</sup></b>		
ScreenOSバージョンチェック	ScreenOS 6.2	ScreenOS 6.2
ファイアウォール・パフォーマンス(ラージパケット)	160Mbps	160Mbps
ファイアウォール・パフォーマンス (IMIX) <sup>(3)</sup>	90Mbps	90Mbps
ファイアウォールパケット/秒 (64バイト)	30,000PPS	30,000PPS
AES256+SHA-1 VPNパフォーマンス	40Mbps	40Mbps
3DES+SHA-1 VPNパフォーマンス	40Mbps	40Mbps
最大同時セッション数	8,000/16,000	8,000/16,000
新規セッション数/秒	2,800	2,800
最大セキュリティポリシー数	200	200
最大サポートユーザー数	無制限	無制限
<b>ネットワーク接続</b>		
固定I/O	7×10/100	5×10/100
物理インタフェースモジュール (PIM) スロット数	0	2
WANインタフェースオプション	工場出荷時構成：RS232 Serial AUXまたはISDN BRI S/TまたはV.92	Mini-PIM：1×ADSL 2+、1×T1、1×E1、V.92、ISDN BRI S/T、1×SFP、1×Serial
<b>ファイアウォール</b>		
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	○	○
<b>UTM <sup>(4)</sup></b>		
IPS (ディープ・インスペクション・ファイアウォール)	○	○
プロトコル異常検知	○	○
ステートフル・プロトコル・シグネチャ	○	○
アンチウィルス	○	○
インスタントメッセージAV	○	○
シグネチャデータベース	200,000以上	200,000以上
対応プロトコル	POP3、HTTP、SMTP、IMAP、FTP、IM	POP3、HTTP、SMTP、IMAP、FTP、IM
アンチスパイウェア	○	○
アンチアドウェア	○	○
アンチキーロガー	○	○
アンチスパム	○	○
統合型URLフィルタリング	○	○
外部URLフィルタリング <sup>(5)</sup>	○	○
<b>VoIPセキュリティ</b>		
H.323対応アプリケーション・レベル・ゲートウェイ (ALG)	○	○
SIP ALG	○	○
MGCP ALG	○	○
SCCP ALG	○	○
VoIPプロトコル対応NAT	○	○

仕様<sup>(1)</sup> (続き)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>IPSec VPN</b>		
Auto-Connect-VPN	○	○
同時VPNトンネル数	25/40	25/40
トンネル用インタフェース数	10	10
DES暗号化 (56ビット)、3DES暗号化 (168ビット)、AES (米次世代暗号標準、256ビット)	○	○
MD-5/SHA-1認証	○	○
手動鍵、IKE、PKI (X.509)	○	○
PFS (DHグループ)	1、2、5	1、2、5
リプレイ攻撃防御	○	○
リモートアクセスVPN	○	○
IPSecのL2TP (Layer2 Tunneling Protocol)	○	○
IPSecネットワークアドレス変換 (NAT) トラバーサル	○	○
VPNゲートウェイ冗長化	○	○
<b>ユーザー認証とアクセス・コントロール</b>		
組み込み (内部) データベース (ユーザー制限用)	100	100
外部認証	RADIUS、RSA SecureID、LDAP	RADIUS、RSA SecureID、LDAP
RADIUSアカウントティング	○	○
XAUTH VPN認証	○	○
ウェブベースの認証	○	○
802.1X認証	○	○
統合型アクセス・コントロール (UAC) 対応 インフラネット・エンフォース	○	○
<b>PKIサポート</b>		
PKI証明書要求 (PKCS 7、PKCS 10)	○	○
自動証明書登録 (SCEP)	○	○
OCSP (Online Certificate Status Protocol)	○	○
対応認証局	VeriSign、Entrust、Microsoft、RSA Keon、iPlanet (Netscape)、Baltimore、DoD PKI	VeriSign、Entrust、Microsoft、RSA Keon、iPlanet (Netscape)、Baltimore、DoD PKI
自己署名証明書	○	○
<b>バーチャリゼーション</b>		
セキュリティゾーン最大数	8 (Base) /10 (Extended)	8 (Base) /10 (Extended)
バーチャルルーター最大数	3/4	3/4
最大VLAN数	10/50V	10/50V
<b>ルーティング</b>		
BGPインスタンス	3/4	3/4
BGPピア	10/16	10/16
最大BGPルート数	1,024	1,024
OSPFインスタンス	3	3
最大OSPFルート数	1,024	1,024
RIP v1/v2インスタンス	16	16
最大RIP v2ルート数	1,024	1,024
最大ルーティングエントリ数	1,024	1,024
ソースベース・ルーティング	○	○
ポリシーベース・ルーティング	○	○
ECMP (等価コストマルチパス)	○	○
マルチキャスト	○	○
リバース・フォワーディング・パス (RFP)	○	○
IGMP (v1、v2)	○	○
IGMPプロキシ	○	○
PIMシングルモード	○	○
PIMソース・スペシフィック・マルチキャスト	○	○
マルチキャスト内IPSecトンネル	○	○
IRDP (ICMP Router Discovery Protocol)	○	○

仕様<sup>(1)</sup> (続き)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>カプセル化</b>		
PPP (Point-to-Point Protocol)	○	○
MLPPP (Multilink Point-to-Point Protocol)	—	○
フレームリレー	○	○
MLFR (Multilink Frame Relay) (FRF 15、FRF 16)	○	○
HDLC	○	○
<b>IPv6</b>		
IPv4/IPv6ファイアウォールとVPNのデュアルスタック	○	○
IPv4とIPv6の変換とカプセル化	○	○
Syn-CookieとSyn-ProxylによるDoS攻撃検出	○	○
SIP、RTSP、Sun-RPC、MS-RPC ALG	○	○
RIPng	○	○
BGP	○	○
透過モード	○	○
NSRP	○	○
DHCPv6リレー	○	○
<b>動作モード</b>		
レイヤ2 (透過) モード <sup>(6)</sup>	○	○
レイヤ3 (ルート/NAT) モード	○	○
<b>アドレス変換</b>		
NAT (ネットワークアドレス変換)	○	○
PAT (ポートアドレス変換)	○	○
ポリシーベースNAT/PAT (レイヤー2、レイヤー3モード)	○	○
MIP (IPマッピング、レイヤー3モード)	300	300
VIP (バーチャルIP、レイヤー3モード)	4/5	4/5
MIP/VIPグループ (レイヤー3モード)	○	○
Dual untrust	○	○
ブリッジグループ*	○	○
<b>IPアドレス割り当て</b>		
静的割り当て	○	○
DHCP、PPPoEクライアント	○	○
内部DHCPサーバー	○	○
DHCPリレー	○	○
<b>トラフィック管理とサービス品質 (QoS)</b>		
帯域保証	○ (ポリシー単位)	○ (ポリシー単位)
最大帯域	○ (ポリシー単位)	○ (ポリシー単位)
受信トラフィックのポリシング	○	○
優先帯域利用	○	○
DiffServeマーキング	○ (ポリシー単位)	○ (ポリシー単位)

\*ブリッジグループは ScreenOS 6.0以降でサポートされます。

## 仕様<sup>(1)</sup> (続き)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>高可用性 (HA)<sup>(7)</sup></b>		
アクティブ/アクティブ構成 – L3モード	○	○
アクティブ/パッシブ構成 – 透過モードとL3モード	○	○
コンフィグレーション同期	○	○
ファイアウォール/VPNセッション同期	○	○
ルーティング変更の為のセッション・フェイルオーバー	○	○
VRRP	○	○
デバイス障害検知	○	○
リンク障害検知	○	○
新規HAメンバーの認証	○	○
HAトラフィックの暗号化	○	○
<b>システム管理</b>		
ウェブ・ユーザーインターフェース (HTTP/HTTPS)	○	○
コマンドライン・インターフェース (コンソール)	○	○
コマンドライン・インターフェース (telnet)	○	○
コマンドライン・インターフェース (SSH)	○ (v1.5およびv2.0互換)	○ (v1.5およびv2.0互換)
Network and Security Manager (NSM)	○	○
インターフェース上でVPNトンネル経由の管理	○	○
ラピッド・ディプロイメント機能	○	○
<b>運用管理</b>		
ローカル管理者データベースサイズ	20	20
管理者用外部データベースサポート	RADIUS、RSA SecurID、LDAP	RADIUS、RSA SecurID、LDAP
管理者専用ネットワーク	6	6
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	TFTP、WebUI、NSM、SCP、USB	TFTP、WebUI、NSM、SCP、USB
コンフィグレーション・ロールバック	○	○
<b>ログ収集・モニタリング</b>		
Syslog (複数サーバー)	○、最大4サーバー	○、最大4サーバー
Eメール (2アドレス)	○	○
NetIQ WebTrends	○	○
SNMP (v2)	○	○
SNMP用のフルカスタムMIB	○	○
Traceroute	○	○
VPNトンネルモニター	○	○
<b>外部フラッシュメモリ</b>		
ログストレージ増設	USB 1.1	USB 1.1
イベントログ/アラーム	○	○
システムコンフィグ・スクリプト	○	○
ScreenOSソフトウェア	○	○

## 仕様<sup>(1)</sup> (続き)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>寸法・電源仕様</b>		
寸法 (幅×高さ×奥行き)	22.2×4.1×14.3 cm	29.5×4.5×18.7 cm
重量	0.95 Kg	1.5 Kg
ラックマウント対応	○	○
電源 (AC) <sup>(8)</sup>	AC100~240 V	AC100~240 V
最大熱出力	122.8BTU/時 (W)	122.8BTU/時 (W)
<b>準拠規格</b>		
安全規格	CSA、CB	CSA、CB
EMC規格	FCC class B、CE class B、A-Tick、VCCI class B	FCC class B、CE class B、A-Tick、VCCI class B
<b>平均故障間隔 (MTBF)</b>		
有線	40.5年	35.8年
無線	22.8年	28.9年
<b>セキュリティ準拠規格</b>		
共通基準 (CC) : EAL4	○	○
FIPS 140-2 : レベル2	○	○
ICSA (Firewall/VPN)	○	○
<b>動作環境</b>		
動作時温度範囲	0°C~40°C	0°C~40°C
非動作時温度範囲	-20°C~65°C	-20°C~65°C
湿度範囲	10~90% (結露しないこと)	10~90% (結露しないこと)
<b>無線仕様 (無線モデルのみ)</b>		
送信電力	最大200mW	最大200mW
対応無線規格	802.11a + 802.11b/gデュアル対応	802.11a + 802.11b/gデュアル対応
サイトサーベイ	○	○
設定可能SSID最大数	16	16
アクティブSSID最大数	4	4
Atheros SuperG	○	○
Atheros eXtended Range (XR)	○	○
Wi-Fi CERTIFIED®	○	○
<b>無線LANセキュリティ (無線モデルのみ)</b>		
無線LAN プライバシー保護	WPA、WPA2 (AES/TKIP)、IPSEC VPN、WEP	WPA、WPA2 (AES/TKIP)、IPSEC VPN、WEP
無線LAN認証	PSK、EAP-PEAP、EAP-TLS、EAP-TTLS over 802.1x	PSK、EAP-PEAP、EAP-TLS、EAP-TTLS over 802.1x
MAC (メディアアクセス制御)	許可または拒否	許可または拒否
クライアント隔離	○	○
<b>アンテナオプション (無線モデルのみ)</b>		
ダイバーシティアンテナ	内蔵	内蔵
指向性アンテナ	オプション	オプション
無指向性アンテナ	オプション	オプション

(1) 一部の機能はScreenOS 5.4以降に対応しています。

(2) 実際の数値はScreenOSのバージョンや導入環境によって異なることがあります。

(3) IMIXは、インターネット・ミックス (Internet Mix) の略語です。実運用環境では、単一サイズのパケットだけという状況は少なく、さまざまなサイズのパケットが混在しているのが一般的です。このような条件では、単一サイズのパケットだけの環境よりもはるかに高い処理能力が求められます。そのような実運用環境を想定したトラフィックをIMIXトラフィックと呼びます。弊社が採用するIMIXトラフィックは、64バイト長が58.33%、570バイト長が33.33%、1518バイト長が8.33%の割合のUDPトラフィックです。

(4) 各UTM機能 (IPS (ディープ・インスペクションFW)、アンチウイルス、アンチスパム、統合型URLフィルタリング) は、別途ジュニアネットワークスとの年間ライセンス契約が必要です。このライセンス契約により、各シグネチャのアップデートやサポートが提供されます。

(5) Webフィルタリングのリダイレクト機能は、ファイアウォールから受信したトラフィックをセカンダリサーバーに送ります。リダイレクト機能は無料ですが、Websense社またはSurfControl社のWebフィルタリング・ライセンスを別途購入する必要があります。

(6) NAT、PAT、ポリシーベースNAT、バーチャルIP、IPマッピング、バーチャルシステム、バーチャルルーター、VLAN、OSPF、BGP、RIPv2、アクティブ/アクティブHA、IPアドレス割り当ての各機能は、レイヤ2 (透過モード) ではサポートされていません。

(7) アクティブ/パッシブとアクティブ/アクティブHAを使用するには、Extendedライセンスを購入する必要があります。Extendedライセンスキーを取得すると、HA機能に加えて、次の説明する機能のサブセットが追加されます。

(8) 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。

## IPS (ディープ・インスペクションFW) シグネチャパック

シグネチャパックでは、配置方法と攻撃タイプに応じて、防御方法を調整できます。SSG 5/20で利用できるシグネチャパックは、次のとおりです。

シグネチャパック	導入対象	防御タイプ	標的タイプ
ベース	支社、中小企業	クライアント/サーバー、ワーム保護	各種シグネチャ、プロトコル異常
クライアント	リモートオフィス、支店	境界防御、ホストのコンプライアンス (デスクトップなど)	サーバーからクライアントへの攻撃
サーバー	中小企業	境界防御、サーバーインフラのコンプライアンス	クライアントからサーバーへの攻撃
ワーム攻撃緩和	大企業の支店、リモートオフィス	ワーム攻撃に対する総合的な防御	ワーム、トロイの木馬、バックドア攻撃

## ファイアウォール拡張ライセンス

Extendedライセンス機能	SSG 20/SSG 5
セッション数	最大数が8000から16000に増加
VPNトンネル数	最大数が25から40に増加
VLAN数	最大数が10から50に増加
VoIP通話数	最大数が64から96に増加
高可用性	ステートフルなアクティブ/アクティブまたはアクティブ/パッシブ

## 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・ネットワーク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。

1000176-004 JP Oct 2009