SSG500シリーズ セキュア・サービス・ゲートウェイ

製品概要

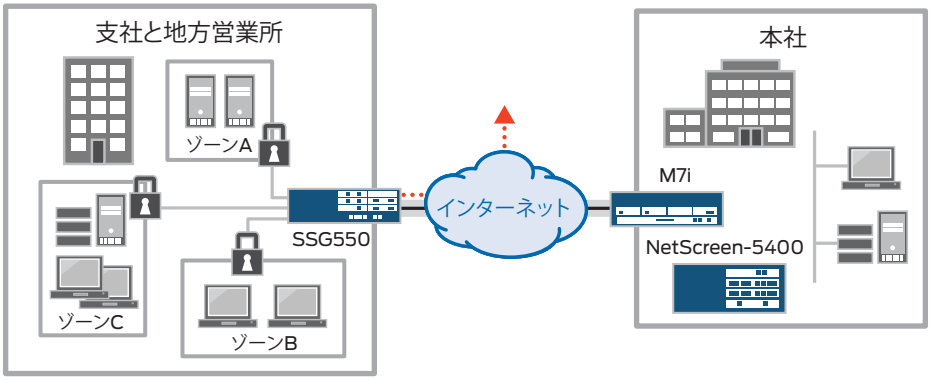
ジュニパーネットワークス セキュア・サービス・ゲートウェイ（SSG）500シリーズは、大企業、地方営業所、中規模拠点、SOHOを対象として、セキュリティ機能、ルーティング機能、LAN/WAN接続を完全に統合した高性能な次世代スマートファイアウォール/VPNです。

ステートフル・ファイアウォール、IPSec VPN、IPS（ディープ・インスペクションFW）、アンチウィルス（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）、アンチスパム、Webフィルタリング機能を備えたUTM（統合脅威管理）セキュリティ機能により、地方営業所や中規模拠点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、マルウェアから保護します。SSG 500シリーズには、SSG 550MとSSG 520Mプラットフォームがあります。

製品説明

SSG 500シリーズは、支店、地方営業所、中規模拠点、SOHO向けの高性能なセキュリティプラットフォームです。ネットワーク内外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 550Mは、ステートフル・ファイアウォール1Gbps以上、IPSec VPNスループット500Mbpsを実現します。SSG 520Mは、ステートフル・ファイアウォール650 MbpsとIPSec VPNスループット300 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（統合脅威管理）でワーム、ウィルス、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。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。



SSG 550M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。
支店のリソースは、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。

接続性とルーティング：SSG 500シリーズは、10/100/1000インターネット4ポートをオンボードに実装し、LANまたはWANインタフェースを収容するI/O拡張スロット6ポートを備えており、非常に柔軟なプラットフォームです。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。

統合型アクセス・コントロール：SSG 500シリーズのプラットフォームは、インフラネット・コントローラ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・エンフォーサとして動作します。中央ポリシー管理エンジンであるインフラネット・コントローラは、SSG 500シリーズと通信し、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。

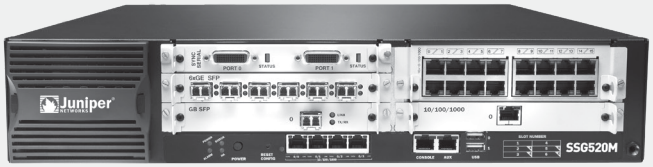
機能と利点

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（アンチウィルス、アンチスパム、Webフィルタリング、IPS）であらゆるウィ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
統合型アンチウィルス	Kaspersky Lab社のアンチ・ウィルス・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）	ウィルス、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）	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）	ジュニパーネットワークスIPS（ディープ・インスペクションFW）シグネチャパックの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 500シリーズの全モデルで10/100/1000×4固定インタフェース 、USBポート×2、コンソールポート×1、補助ポート×1を搭載	高速なLAN接続、拡張性に優れた接続性、柔軟な管理機能を提供
ネットワークのセグメント化	ブリッジグループ、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、外部ネットワーク、ネットワーク上のサブグループに配置した非武装セグメント（DMZ）にセキュリティ機能を迅速に導入し、不正アクセスを防ぐ
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6ポートを装備し、オプションのインタフェースとして、T1、E1、シリアル、10/100/1000、10/100、SFPをサポート	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、フレームリレー、マルチリンク・フレーム・リレー、PPP、マルチリンクPPP、HDLC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
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・エンフォーサ	中央ポリシー管理エンジン（インフラネット・コントローラ）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またはジュニパーネットワークスNetwork and Security Manager（NSM）を使用したセキュリティポリシーの確実な導入、監視、管理	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、レスポンスタイムを短縮して、運用費用を削減できる
自動接続	ハブアンドスポーク型トポロジのスポークサイト間でVPNトンネルを自動的に設定/停止	VoIPビデオ会議など、遅延が許されないアプリケーションのメッシュ型トポロジに拡張性の優れたVPNソリューションを提供
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

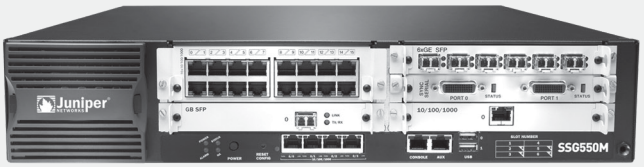
* ブリッジグループはScreenOS 6.0以降、uPIMのみサポートされます。

製品オプション

オプション	オプション説明
AC/DC電源（単一または冗長構成）	SSG500シリーズでは、全モデルでAC電源とDC電源の選択が可能。SSG520Mは単一電源のみ。SSG550Mは冗長電源をオプションとして選択可能。
NEBS（Network equipment Building Systems）準拠	SSG520MとSSG550MはNEBSに準拠。
DRAM	SSG500シリーズでは、全モデルに1GBのDRAMを搭載。
UTM/コンテンツセキュリティ（ハイメモリオプション）	SSG500シリーズでは、アンチウィルス（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とコンテンツセキュリティ機能を自由に組み合わせて構成することが可能。
I/Oオプション	6個のインタフェース拡張スロットは、オプションとして、T1、E1、シリアル、DS3、10/100/1000、10/100、SFP接続に対応。



SSG520M



SSG550M

仕様

	SSG520M	SSG550M
最大パフォーマンス・設定数[1]		
ScreenOSバージョンチェック	ScreenOS 6.3	Screen OS 6.3
ファイアウォール・パフォーマンス（ラージパケット）	650Mbps以上	1Gbps以上
ファイアウォール・パフォーマンス（IMIX）[2]	600Mbps	1Gbps
ファイアウォールパケット/秒（64バイト）	300,000PPS	600,000PPS
AES256+SHA-1 VPNパフォーマンス	300Mbps	500Mbps
3DES+SHA-1 VPNパフォーマンス	300Mbps	500Mbps
最大同時セッション数	128,000	256,000
新規セッション数/秒	10,000	15,000
最大セキュリティポリシー数	4,000	4,000
最大サポートユーザー数	無制限	無制限
Junos® OS 8.0以降に移行可能[3]	○	○
ネットワーク接続		
固定I/O	4×10/100/1000	4×10/100/1000
物理インタフェースモジュール（PIM）スロット数	6（2 ePIM/uPIM/PIM + 4 uPIM/PIM）	6（4 ePIM/uPIM/PIM + 2 uPIM/PIM）
WANインタフェースオプション（PIMS）	シリアル、T1、E1、DS3、E3	シリアル、T1、E1、DS3、E3
LANインタフェースオプション（ePIMS/uPIMS）	10/100、10/100/1000、SFP	10/100、10/100/1000、SFP
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	○	○
UTM[4]		
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	○	○
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	○	○
インスタントメッセージAV	○	○
アンチスパム	○	○
統合型Webフィルタリング	○	○
外部Webフィルタリング[5]	○	○
VoIPセキュリティ		
H.323 ALG	○	○
SIP ALG	○	○
MGCP ALG	○	○
SCCP ALG	○	○
VoIPプロトコル対応NAT	○	○

仕様（続き）

	SSG520M	SSG550M
IPSec VPN		
同時VPNトンネル数	500	1,000
トンネル用インタフェース数	100	300
DES（56ビット）、3DES（168ビット）、AESによる暗号化	○	○
MD-5/SHA-1認証	○	○
手動鍵、IKE、IKEv2 with EAP、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内のL2TP利用	○	○
IPSec NATトラバーサル	○	○
VPN自動接続	○	○
VPNゲートウェイ冗長化	○	○
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（ユーザー制限用）	500	1,500
外部認証	RADIUS、RSA SecureID、LDAP	RADIUS、RSA SecureID、LDAP
RADIUSアカウンティング	○、起動/停止	○、起動/停止
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・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）	○	○
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	○	○
バーチャリゼーション		
セキュリティゾーン最大数	60	60
バーチャルルーター最大数	11	16
ブリッジグループ*	○	○
最大VLAN数	125	150
ルーティング		
BGPインスタンス	10	15
BGPピア	64	128
最大BGPルート数	250,000	250,000
OSPFインスタンス	3	8
最大OSPFルート数	250,000	250,000
RIP v1/v2インスタンス	128	256
最大RIP v 2ルート数	250,000	250,000
最大ルーティングエントリ数	250,000	250,000
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	○	○

*ブリッジグループはScreenOS 6.0以降、uPIMのみサポートされます。

仕様（続き）

	SSG520M	SSG550M
ルーティング（続き）		
マルチキャスト	○	○
リバース・パス・フォワーディング（RPF）	○	○
IGMP（v1, v2）	○	○
IGMP Proxy	○	○
PIM SM	○	○
PIM SSM	○	○
マルチキャスト内IPSecトンネル	○	○
カプセル化		
PPP	○	○
MLPPP	○	○
MLPPP最大物理インタフェース数	12	12
フレームリレー	○	○
MLFR（FRF .15、FRF .16）	○	○
MLFR最大物理インタフェース数	12	12
HDLC	○	○
IPv6		
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-Proxy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	○	○
動作モード		
レイヤ2（透過）モード[6]	○	○
レイヤ3（ルート/NAT）モード	○	○
アドレス変換		
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）	6,000	6,000
VIP（バーチャルIP、レイヤー3モード）	32	64
MIP/VIPグルーピング（レイヤー3モード）	○	○
IPアドレス割り当て		
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	○	○
トラフィック管理とサービス品質（QoS）		
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	○	○
DiffServマーキング	○（ポリシー単位）	○（ポリシー単位）

仕様（続き）

	SSG520M	SSG550M
高可用性（HA）		
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	○	○
VRRP	○	○
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	○	○
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	○	○
システム管理		
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）	○	○
コマンドライン・インタフェース（telnet）	○	○
コマンドライン・インタフェース（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	×	×
運用管理		
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	○	○
ログ収集・モニタリング		
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（v3）	○	○
SNMP用のフルカスタムMIB	○	○
Traceroute	○	○
VPNトンネルモニター	○	○
外部フラッシュメモリ		
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	○	○
寸法・電源仕様		
寸法（幅×高さ×奥行き）	44.5×8.9×54.6 cm	44.5×8.9×54.6 cm
重量	10.43 Kg（インタフェースモジュール含まず）	11.34 Kg（インタフェースモジュール含まず、電源1基搭載時）
ラックマウント対応	○（2RU）	○（2RU）
電源（AC）[7]	AC100V～240 V、350W	AC100V～240 V、420W
電源（DC）	DC－48～－72 V、420W	DC－48～－72 V、420W
冗長電源（ホットスワップ対応）	×	○
最大熱出力	1,070 BTU/時（W）	1,145 BTU/時（W）

仕様（続き）

	SSG520M	SSG550M
準拠規格		
安全規格	UL、CUL、CSA、CB	UL、CUL、CSA、CB
EMC規格	FCC class A、CE class A、C-Tick、VCCI class B	FCC class A、CE class A、C-Tick、VCCI class B
NEBS	レベル3適合	レベル3適合
MTBF（Bellcoreモデル）	12年	12年
セキュリティ準拠規格		
共通基準（CC）: EAL4	○	○
FIPS 140-2: レベル2	○	○
ICSA（Firewall/VPN）	○	○
動作環境		
動作時温度範囲	0℃～50℃	0℃～50℃
非動作時温度範囲	−20℃～70℃	−20℃～70℃
湿度範囲	10～90%（結露しないこと）	10～90%（結露しないこと）

(1) 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。
(2) 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。
(3) 別途ライセンスの購入が必要です。
(4) 各UTM機能〔IPS（ディープ・インスペクションFW）、アンチウィルス、アンチスパム、統合型URLフィルタリング〕は、別途ジュニパー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) 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 500シリーズ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

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ネットワーク革新に邁進し続けています。デバイスからデータセンター、コンシューマからクラウドにわたり、ネットワークのエクスペリエンスと経済性を一変させる、画期的なソフトウェア、シリコン、およびシステムを提供しています。ジュニパーネットワークスは、世界中で顧客およびパートナーにサービスを提供しています。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
〒163-1445
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 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

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

Copyright© 2012,　Juniper Networks, Inc. All rights reserved.
Juniper Networks、Junos、NetScreen、ScreenOS、Juniper Networksロゴは、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。

1000143-007　JP Mar. 2012