

PA-7000 SERIES

パロアルトネットワークスの次世代ファイアウォール PA-7000 Series は、エンタープライズ規模の組織やサービス プロバイダが、データセンターや広帯域幅ネットワーク境界などの高い性能が求められる環境にセキュリティを導入できるようにします。アプリケーション、ユーザー、デバイスが生成するデータを処理するためのスループットに対する要求は高まり続けています。そうした要求に応えるために、PA-7000 Series のシステムは驚異的な性能を発揮します。また、非常に高度なサイバー攻撃をくい止めるための防御機能や、暗号化の下に潜む脅威をくい止めるための高スループットの復号機能も備えています。PA-7000 Series は、セキュリティ処理のためのリソース利用率を最大化し、新しいコンピューティング能力が追加されるとそれに合わせて自動的にスケールするように設計されています。また、管理とライセンスに対するシングルシステム アプローチによってシンプルさが確保されています。

主なセキュリティ機能

すべてのアプリケーションをすべてのポートで常時識別

- 使用されているポート、SSL/SSH 暗号化、セキュリティの回避技術に関わらず、アプリケーションを識別します。
- セキュリティ ポリシー決定の要素として、ポートではなくアプリケーションを使用します。
- 不明なアプリケーションを、ポリシー コントロール、脅威のフォレンジック、または App-ID™ テクノロジーの開発が行えるよう分類します。

あらゆる場所のあらゆるユーザーにセキュリティ ポリシーを適用

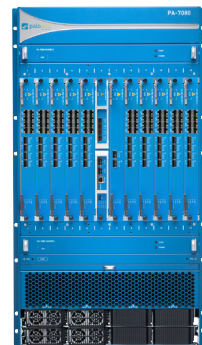
- Windows®, macOS®, Linux, Android®, Apple iOS の各プラットフォームに一貫したポリシーを導入します。
- Microsoft Active Directory® と Remote Desktop Services, LDAP, Novell eDirectory™, Citrix とエージェントレスに統合します。
- ファイアウォール ポリシーを、802.1X ワイヤレス、プロキシ、ネットワーク アクセス コントロール、および他の任意のユーザー ID 情報ソースと簡単に統合します。

既知および未知の脅威を阻止

- すべてのポートを通じて、エクスプロイト、マルウェア、スパイウェア、コマンドアンドコントロールを含む様々な既知の脅威をブロックします。
- ファイルや機密データの無許可の転送を制限し、仕事とは関係ない Web の利用を安全化します。
- 数百件の悪意の振る舞いに基づく分析により、未知のマルウェアを識別して自動的に防御シグネチャを作成して配信します。



PA-7050



PA-7080

表 1: PA-7000 Series のパフォーマンスと容量

	PA-7080	PA-7050	PA-7000 NPC-100G	PA-7000 NPC-XM
ファイアウォール スループット (HTTP/appmix) ¹	600/700 Gbps	360/420 Gbps	60/70 Gbps	17.1/20.0 Gbps
Threat Prevention スループット (DSRI が有効) ²	610 Gbps	366 Gbps	61 Gbps	18 Gbps
Threat Prevention スループット (HTTP/appmix) ³	270/330 Gbps	162/198 Gbps	27/33 Gbps	8.1/11.1 Gbps
IPsec VPN スループット ⁴	280 Gbps	168 Gbps	28 Gbps	8.7 Gbps
最大セッション数	320M	192M	32M	8M
新規セッション / 秒 ⁵	4.56M	2.73M	456,000	225,000
仮想システム (基本 / 最大) ⁶	25/225*	25/225*	-	-

1. スループットは、App-IDとログギングが有効な状態で64KB HTTP/appmixトランザクションを利用した場合の測定値です。
2. サーバレスポンス検査の無効化(DSRI)のスループットは、App-ID、IPS、アンチウイルス、アンチスパイウェア、WildFire、ファイル ブロッキング、およびログギングが有効な状態で、64KB HTTPトランザクションを利用した場合の測定値です。
3. Threat Preventionスループットは、App-ID、IPS、アンチウイルス、アンチスパイウェア、WildFire、およびログギングが有効な状態で、64KB HTTP/appmixトランザクションを利用した場合の測定値です。
4. IPsec VPNスループットは、ログギングが有効な状態で64KB HTTPトランザクションを利用した場合の測定値です。
5. 新規セッション/秒は、アプリケーション オーバーライドを有効にして、1バイトのHTTPトランザクションを利用した場合の測定値です。
6. 基本数量に仮想システムを追加するには別途ライセンスの購入が必要です。

PA-7000 Series のアーキテクチャ

PA-7000 Series では、ネットワーキング、セキュリティ、管理の各主要機能に適した処理能力の種類や量を適用するため、拡張性に優れたアーキテクチャが採用されています。PA-7000 Series のシャーシは処理要求を 3 つのサブシステムにインテリジェントに分配します。それぞれのサブシステムには、優れたコンピューティング能力と専用メモリが搭載されています。

ネットワーク処理カード

ネットワーク処理カード (NPC) は、ネットワーキング、トラフィックの分類、脅威防御を含む、すべてのパケット処理タスクを実行するためのものです。各 NPC には、64 個 (第 1 世代) ~ 144 個 (第 2 世代) の処理コアが搭載されています。すべての処理コアがネットワーク保護のために動作し、NPC あたりの処理能力は最大 72 Gbps に達します。スロットの拡張は、PA-7080 では 720 Gbps まで、PA-7050 では 430 Gbps まで、NPC を追加することで簡単に行えます。また、新しい NPC の利用はシステムによって決定されます。40 Gbps や 100 Gbps といった大容量の接続性に対する需要が高まっている一方で、より一般的な 10 Gbps インターフェイスも引き続き利用されています。こうした需要に対応するために、第 1 世代の NPC-20GXM と NPC-20GQXM、第 2 世代の NPC-100G という 3 つの NPC のオプションが用意されています。これらは交換可能であり、第 1 世代のスイッチ管理カードと組み合わせて使用できます。

スイッチ管理カード

PA-7000 Series の制御センターとして機能するスイッチ管理カード (SMC) は、あらゆるトラフィックをインテリジェントに監視し、First Packet Processor (FPP)、高速バックプレーン、管理サブシステムという 3 つの要素の組み合わせを使用して、すべての管理機能を実行します。第 1 世代と第 2 世代の SMC が提供されており、第 2 世代の製品は次の 3 つの機能分野で大幅な性能向上が図られています。

- First Packet Processor (FPP) は、PA-7000 Series のパフォーマンス最大化とリニアな拡張性に大きな役割を果たしています。FPP は、共有可能な処理と I/O リソースを、すべての NPC で常時監視しており、インバウンドトラフィックを余力のあるプロセッサにインテリジェントに転送します。つまり、NPC の追加によってパフォーマンスの向上と容量の増加が実現されても、トラフィック管理の変更は必要ありません。また、PA-7000 Series の再ケーブルリングや、再設定も必要ありません。
- 高速なバックプレーンによって、各 NPC は 100 Gbps を超えるノンブロッキングトラフィック容量にアクセスできます。それぞれの NPC スロットに専用の容量が設定されており、パフォーマンスは線形的に拡張されます。要求の高まりに応じて NPC を追加でき、バックプレーンの競合が発生することなく合計のシステム容量を高めることができます。
- 管理サブシステムは、PA-7000 Series のすべてを制御する専用の接続先として機能します。

専用のロギングカード

ロギングカードはすべてのシステムにとって重要な要素です。デュアル CPU 設計を採用しており、PA-7000 Series が生成する大量のログを管理するための専用のサブシステムとなっています。第 1 世代のログ処理カード (LPC) と第 2 世代のログ転送カード (LFC) の 2 つのログカードが用意されています。LPC は最大 4 TB の RAID 1 ストレージを使用して、ログ関連の処理をオフロードします。これにより、収集された最新のログに対してクエリを実行したり、レポートを作成したりすることができます。LFC は、ログメッセージをエクスポートするための高性能な専用カードです。いずれも、Panorama™ ネットワークセキュリティ管理、Cortex™ Data Lake、Syslog にログを転送してオフラインで分析できます。LPC は NPC-20G と NPC-100G の混合構成をサポートしています。一方、LFC は第 2 世代の SMC や NPC-100G と組み合わせて使用するよう最適化されています。

PA-7000 Series は、1 つの統合システムとして管理されるため、使用可能なリソースすべてを簡単に割り当てて、データ保護に専念させることができます。PA-7000 Series を制御する PAN-OS® は、アプリケーション、脅威、コンテンツを含め、すべてのトラフィックをネイティブに分類し、場所やデバイスの種類に関わらず、トラフィックをユーザーと関連付けます。ビジネスを遂行する要素であるアプリケーション、コンテンツ、ユーザーはセキュリティポリシーの基礎としての役割を果たし、セキュリティ体制の向上とインシデント対応時間の短縮が実現します。また、高度に動的な環境でセキュリティポリシーを最新状態に保つための管理作業の負担が軽減されます。

管理作業をさらに簡素化するため、PA-7000 Series の年間サポート料とサブスクリプション料は、システム全体に対して設定されています。インストールされている NPC の数に関係なく年間料金は一定であり、コストが予測しやすくなっています。

表 2: PA-7000 Series のハードウェア仕様

	PA-7000 NPC	PA-7080 システム全体	PA-7050 システム全体
NPC-100G (PA-7000-100G-NPC-A)	(8) SFP/SFP+ (4) QSFP+ /QSFP28	(80) SFP/SFP+ (40) QSFP+/QSFP28	(48) SFP/SFP+, (24) QSFP+/QSFP28
NPC-20G XM オプション 1: (PA-7000-20GQXM-NPC)	(2) QSFP+、 (12) SFP+	(20) QSFP+、 (120) SFP+	(12) QSFP+、 (72) SFP+
NPC-20G XM オプション 2: (PA-7000-20GXM-NPC)	12x10/100/ 1000、(8) SFP、 (4) SFP+	(120) 10/100/1000、(80) SFP、(40) SFP+	(72) 10/100/1000、(48) SFP、 (24) SFP+
管理 I/O (第 2 世代)	-	(2) SFP MGT、(2) SFP HA1、(2) HSCI HA2/HA3 QSFP+/QSFP28 (1) RJ45 シリアル コンソール、(1) micro-USB シリアル コンソール	
管理 I/O (第 1 世代)	-	(2) 10/100/1000、(2) QSFP+ 高可用性、 (1) 10/100/1000 アウトオブバンド管理、(1) RJ45 コンソール ポート	
ストレージ容量 (第 2 世代)	-	(2) 240 GB SSD システムドライブ、RAID1	
ストレージオプション (第 1 世代)	-	(1) 80 GB SSD システムドライブ、(4) 1 TB デフォルト、 または (4) ログ処理カード上に 2 TB のオプション HDD、RAID	
AC 入力電圧 (入力 Hz)	-	90–305VAC (47–66 Hz)	90–264VAC (47–63 Hz)
AC 電源出力	-	2500 W @ 240VAC 1200 W @ 120VAC	2500 W @ 240VAC 1200 W @ 120VAC
DC 入力電圧	-	-36 ~ -75VDC	-40 ~ -72VDC
DC 電力出力	-	電源あたり 2500 W	電源あたり 2500 W
電源あたり最大電流	-	12ADC @ 240VAC In 75ADC @ >40VDC In	16A @ 180VAC In 75A @ 37.5VDC In
電源数 (基本 / 最大)	-	4/8	4/4
電源あたりの最大突入電流	-	30AAC / 100ADC (ピーク時)	50AAC / 75ADC (ピーク時)
平均故障間隔 (MTBF)	構成に依存する ; MTBF の詳細については、パロアルトネットワークスの代理店にご確認ください。		
最大 BTU/ 時	-	20,132	10,236
ラック マウント可能 (寸法)	-	19U、19 インチ標準ラック (高さ 81.84 x 幅 48.26 x 奥行き 62.64 cm)	9U、19 インチ標準ラック (高さ 40.01 x 幅 48.26 x 奥行き 60.96 cm)
重量 (スタンドアロン デバイス / 出荷時)	-	135.8 kg (AC) / 135.3 kg (DC)	85 kg (AC) / 83.9 kg (DC)
安全性	-	cTUVus、cCSAus、CB	
EMI	-	FCC Class A、CE Class A、VCCI Class A	
認定	-	NEBS レベル 3	
環境			
動作温度	-	0 ~ 50°C	
動作時以外の温度	-	-20 ~ 70°C	

PA-7000 Series では幅広いネットワーキング機能がサポートされており、既存のネットワークに弊社のセキュリティ機能をより簡単に統合できます。

ネットワーキング機能

表 3: PA-7000 Series のネットワーキング機能	
インターフェイス モード	VLAN
L2、L3、タップ、バーチャルワイヤ (トランスペアレント モード)	デバイス / インターフェイスあたりの 802.1Q VLAN タグ : 4,094/4,094
ルーティング	アグリゲート インターフェイス (802.3ad)、LACP
OSPFv2/v3(グレースフルリスタート有効)、BGP(グレースフルリスタート有効)、RIP、スタティックルーティング	ネットワークアドレス変換
ポリシーベース転送	NAT モード (IPv4): スタティック IP、ダイナミック IP、ダイナミック IP およびポート (ポート アドレス変換)
マルチキャスト : PIM-SM、PIM-SSM、IGMP v1、v2、v3	NAT64、NPTv6
双方向転送検出 (BFD)	追加の NAT 機能 : ダイナミック IP の予約、調整可能なダイナミック IP、ポート オーバーサブスクリプション
SD-WAN	高可用性
パスの品質測定 (ジッター、パケット損失、遅延)	モード : アクティブ / アクティブ、アクティブ / パッシブ
初期のパス選択 (PBF)	障害検出 : パス モニタリング、インターフェイス モニタリング
動的なパス変更	
IPv6	
L2、L3、タップ、バーチャルワイヤ (トランスペアレント モード)	
機能 : App-ID、User-ID、Content-ID、WildFire、SSL 復号	
IPsec VPN	
鍵交換 : 手動鍵、IKEv1、IKEv2 (事前共有鍵、証明書に基づいた認証)	
暗号化 : 3DES、AES (128 ビット、192 ビット、256 ビット)	
認証 : MD5、SHA-1、SHA-256、SHA-384、SHA-512	
GlobalProtect 大規模 VPN (LSVPN) による構成と管理の簡素化	

PA-7000 Series のセキュリティ機能および関連した容量について詳しくは、www.paloaltonetworks.com/products をご覧ください。



〒 100-0011
東京都千代田区内幸町
2丁目1番6号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

© 2019 Palo Alto Networks, Inc. パロアルトネットワークスは、パロアルトネットワークスの登録商標です。商標のリストについては、<https://www.paloaltonetworks.com/company/trademarks.html> をご覧ください。本書に記述されているその他の商標はすべて、各社の商標である場合があります。
pa-7000-series-ds-112619