



PA-5410



PA-5420



PA-5430



PA-5440



PA-5445

PA-5400 Series

パロアルトネットワークスの PA-5400 Series は ML を活用した次世代ファイアウォールであり、PA-5410、PA-5420、PA-5430、PA-5440、PA-5445 から構成されます。高速データセンター、インターネットゲートウェイ、サービスプロバイダ向けの導入に最適な NGFW です。暗号化されたトラフィックを含む、すべてのトラフィックのセキュリティ対策を実施します。

特長

- 世界初の ML を活用した NGFW
- Gartner Magic Quadrant ネットワークファイアウォール部門で 11 回連続リーダー評価
- Forrester Wave: Enterprise Firewalls, Q4 2022 でリーダーに選出
- サービスプロバイダや企業による 5G 変革とマルチアクセスエッジコンピューティング (MEC) の保護を目的に構築された、5G ネイティブなセキュリティを提供
- 追加のセンサーを導入することなく、管理対象外の IoT デバイスを含むすべてのデバイスの可視性とセキュリティを強化
- アクティブ/アクティブとアクティブ/パッシブの両モードで高可用性をサポート
- セキュリティサービスにより予測可能なパフォーマンスを発揮
- Panorama ネットワークセキュリティ管理による集中管理をサポート
- Strata[™] Cloud Manager によってセキュリティ投資を最大限活用し、ビジネスの中断を防ぐ

MLを活用した世界初の次世代ファイアウォールが未知の脅威の阻止、モノのインターネット (IoT) などあらゆる要素の可視化と保護、ポリシーの自動推奨によるエラー削減を可能にします。

PA-5400 Series を制御するのは、PAN-OS® です。このソフトウェアは、パロアルトネットワークスのすべての NGFW で採用されています。PAN-OS は、アプリケーション、脅威、コンテンツ等、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。業務遂行に欠かせない要素である、アプリケーション、コンテンツ、およびユーザーをセキュリティポリシーの基礎に据えることで、セキュリティ体制を強化するとともに、インシデントの応答時間を短縮します。

主要なセキュリティ機能と接続機能

ML を活用した次世代ファイアウォール

- ・ファイアウォールの中核に機械学習 (ML) を組み込むことで、ファイルベース攻撃に対するシグネチャレスの防御をインラインで実施し、未知のフィッシング攻撃を特定して即座に阻止します。
- ・クラウドベースの ML プロセスを活用することで、シグネチャと命令を即座に NGFW へ配信します。
- ・動作分析を使用して、IoT デバイスを検出し、ポリシーを推奨します。これは、NGFW にネイティブで統合されているクラウド型サービスです。
- ・自動的にポリシーを推奨するので、時間が節約され、人的ミスの可能性が低くなります。

完全なレイヤー 7 の検査により、すべてのアプリケーションをすべてのポートで常に識別して分類

- ・使用されているポート、プロトコル、セキュリティの回避技術、暗号化 (TLS/SSL) に関わらず、ネットワークを通過するアプリケーションを識別します。SaaS Security サブスクリプションによって新規アプリケーションを自動的に検出・管理することで、SaaS の急増に対応します。
- ・許可、拒否、スケジュール、検査、帯域制御の適用などのあらゆるセキュリティ ポリシーを、ポートではなくアプリケーションを基に決定します。
- ・自社開発のアプリケーション向けにカスタム App-ID™ タグを作成できます。また、新規アプリケーション向けの App-ID の開発をパロアルトネットワークスに依頼することも可能です。
- ・アプリケーション内のすべてのペイロード データ (ファイルやデータ パターンなど) を識別して悪意のあるファイルをブロックし、データ漏えいを阻止します。
- ・標準およびカスタムのアプリケーション使用状況レポート、たとえば、ネットワーク上の承認済みおよび未承認のすべての Software-as-a-Service (SaaS) トラフィックに対する洞察を提供する SaaS レポートを作成します。
- ・組み込みの Policy Optimizer を使用して、従来のレイヤー 4 ルールセットから App-ID ベースのルールに安全に移行できます。また、移行後はルールセットをより安全かつ簡単に管理できます。

詳細は『[App-ID 技術概要](#)』をご覧ください。

使用中のデバイスや所在地に関わらず、ユーザーにセキュリティを適用すると同時に、ユーザー アクティビティに基づくポリシーを導入

- ・IP アドレスだけでなく、ユーザーやグループに基づいて可視化、セキュリティ ポリシー、レポート、フォレンジックを利用できます。
- ・ワイヤレス LAN コントローラ、VPN、ディレクトリ サーバ、SIEM、プロキシなどのリポジトリを簡単に統合して、ユーザー情報を活用できます。
- ・ファイアウォールにダイナミック ユーザー グループ (DUG) を定義して、ユーザー ディレクトリに変更が適用されるのを待たずに、時間制限付きセキュリティ アクションを実行できます。
- ・ユーザーの所在地 (オフィス、自宅、移動先など) や使用中のデバイス (iOS/Android モバイル デバイス、macOS/Windows/Linux PC、Citrix/Microsoft VDI、ターミナルサーバ) に関わらず、一貫したポリシーが適用されます。

- ・アプリケーションを変更することなくアプリケーションのネットワーク レイヤーに多要素認証 (MFA) を導入。外部 Web サイトへの企業認証情報の漏洩や、盗まれた認証情報の再利用を防ぎます。
- ・ユーザーの行動に基づいて動的なセキュリティ アクションを提供し、疑わしいユーザーや悪意のあるユーザーを制限します。
- ・ID ベースのセキュリティを実施する全く新しいクラウドベース アーキテクチャ「Cloud Identity Engine」を採用。ユーザーやユーザーの ID ストアの所在に関わらず、ユーザーの認証と認可を一貫して提供することで、ゼロトラスト セキュリティ体制への移行を加速させます。

詳細は『[Cloud Identity Engine ソリューション概要](#)』をご覧ください。

暗号化トラフィックに隠蔽された悪意のあるアクティビティを阻止

- ・ TLS 1.3 や HTTP/2 を使用するトラフィックなど、インバウンドとアウトバウンド両方の TLS/SSL 暗号化トラフィックを検査し、ポリシーを適用します。
- ・ 暗号化されたトラフィックの量や TLS/SSL バージョン、暗号スイートなど、TLS トラフィックに対する優れた可視性を復号なしで提供します。
- ・ 従来の TLS プロトコル、安全でない暗号、誤って設定されている証明書の使用を制御して、リスクを軽減します。
- ・ 復号機能を簡単に導入できます。また、証明書がピン留めされているアプリケーションなどの問題を、組み込みのログを使用してトラブルシューティングできます。
- ・ プライバシーとコンプライアンスの確保を目的として、URL カテゴリ、送信元ゾーンと宛先ゾーン、アドレス、ユーザー、ユーザー グループ、デバイス、ポートを基に復号機能を柔軟に有効化/無効化できます。
- ・ ファイアウォールから送られた復号トラフィックのコピーを作成して (復号ミラーリング)、トラフィック収集ツールに送信し、フォレンジック、履歴調査、データ損失防止 (DLP) に利用できます。
- ・ Network Packet Broker を使用してサードパーティ セキュリティ ツールにすべてのトラフィック (復号済み TLS、未復号 TLS、非 TLS) をインテリジェントに転送することで、ネットワーク パフォーマンスを最適化し運用経費を削減できます。

いつ、どこで、どのように復号を行って脅威を阻止し、企業を保護できるかは、[復号に関するホワイト ペーパー](#)をご覧ください。

Strata Cloud Manager による AI を活用した統一的な管理と運用

ネットワーク障害を防止: 導入の正常性を予測し、予測分析によって最長 7 日先までの容量ボトルネックを予防的に特定して、業務の中断を予防します。

セキュリティをリアルタイムに強化: 弊社および業界のベストプラクティスに基づく、AI を活用したポリシー分析とリアルタイム コンプライアンス チェック。

シンプルで一貫したネットワークセキュリティ管理と運用を実施: あらゆるフォーム ファクタ (SASE、ハードウェア/ソフトウェア ファイアウォール、セキュリティ サービスなど) の設定とセキュリティ ポリシーを管理して一貫性を確保し、運用経費を削減することができます。

クラウド提供型セキュリティ サービスによる高度な脅威の検出と防御

サイロ化したセキュリティ ツールを使用する従来のアプローチは、セキュリティ ギャップの発生、セキュリティ チームの負担増大、業務生産性の低下などの問題の原因となります。業界最先端の次世代ファイアウォールとシームレスに統合されたパロアルトネットワークスのクラウド提供型セキュリティ サービスは、6 万 5,000 社の顧客の間で脅威インテリジェンスを共有して、あらゆる攻撃経路からの既知および未知の脅威をリアルタイムに阻止します。ネットワーク全体のセキュリティ ギャップを解消し、インライン AI を活用したセキュリティ サービスを利用して、あらゆる場所でリアルタイム防御を提供します。

サービス内容:

- **Advanced Threat Prevention:** インライン AI を利用した検出によって既知および未知の 익스プロイト、コマンドアンドコントロール (C2) 攻撃を阻止。従来型 IPS ソリューションと比べてゼロデイ インジェクション攻撃を 60% 多く、高度な回避技術を用いたコマンドアンドコントロールトラフィックを 48% 多く阻止します。
- **Advanced WildFire®:** 業界最大の脅威インテリジェンスとマルウェア防御エンジンを利用して、既知/未知のマルウェアや高度な回避型マルウェアを競合他社の 180 分の 1 の時間で自動的に阻止し、ファイルの安全を確保します。
- **Advanced URL Filtering:** 既知と未知の脅威をリアルタイムに防御する業界初の機能で、悪意のあるサイトの 88% を他社の 48 時間以上前に阻止。安全なインターネット アクセスを確保し、Web ベース攻撃を 40% 多く防ぎます。
- **DNS Security:** インフラを変更することなく DNS 攻撃に対するカバー範囲を 68% 改善し、コマンドアンドコントロールやデータ窃盗に DNS を悪用した攻撃の 85% を阻止します。
- **Enterprise DLP:** あらゆるクラウド提供型エンタープライズ DLP の 2 倍のカバー範囲で、データ侵害リスクを最小化し、ポリシー違反のデータ転送を阻止し、エンタープライズ環境全体で一貫したコンプライアンスを可能にします。
- **SaaS Security:** 業界唯一の次世代 CASB によって SaaS の急増に先手を打ち、すべてのプロトコルですべてのアプリケーションを自動的に可視化して保護します。
- **IoT Security:** 業界で最もスマートなセキュリティをスマート デバイスに導入してあらゆる「モノ」を保護することで、20 倍高速なゼロトラスト デバイスセキュリティを実施します。

シングルパス アーキテクチャを使用した独自のパケット処理アプローチ

- ネットワーキング、ポリシー検索、アプリケーションの識別とデコード、シグネチャ マッチングを、すべての脅威とコンテンツに対してシングルパスで実行します。これにより、1 つのセキュリティ デバイスで複数の機能の実行に必要なオーバーヘッドが大幅に減少します。
- ストリームベースの統一されたシグネチャ マッチングを使用したトラフィックのスキャンでは、シングルパスですべてのシグネチャを確認するため、遅延の発生を回避できます。
- セキュリティ サブスクリプションを有効にした場合でも、安定した予測可能なパフォーマンスを発揮できます (表 1 の「Threat Prevention のスループット」は、複数のサブスクリプションを有効にした場合の測定値です)。

SD-WAN 機能の有効化

- SD-WAN を、既存のファイアウォールで有効にするだけで簡単に導入できます。
- SD-WAN を安全に実装できます。この機能は、業界をリードするパロアルトネットワークスのセキュリティ機能にネイティブに統合されています。
- 遅延、ジッター、パケット損失を最小限に抑えることで、卓越したエンドユーザー エクスペリエンスを提供します。

表 1: PA-5400 Series のパフォーマンスと容量

	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
ファイアウォールのスループット (appmix)*	52 Gbps	70 Gbps	82 Gbps	90 Gbps	90 Gbps
Threat Prevention のスループット (appmix) †	35 Gbps	50 Gbps	60 Gbps	70 Gbps	76 Gbps
IPsec VPN のスループット ‡	20 Gbps	28 Gbps	42 Gbps	58 Gbps	64 Gbps
最大セッション数 §	5M	7M	9M	20M	48M
新規セッション/秒	270,000	370,000	380,000	390,000	449,000
仮想システム (基本/最大) ¶	10/20	15/65	25/125	25/225	25/225

注: PAN-OS 11.1 で測定した値です。

* ファイアウォールのスループットは、App-ID とロギングが有効な状態で、appmix トランザクションを利用した場合の測定値です。

† Threat Prevention 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、DNS Security、ファイル ブロック、ロギングが有効な状態で、appmix トランザクションを利用した場合の測定値です。

‡ IPsec VPN のスループットは、ロギングが有効な状態で 64KB の HTTP トランザクションを利用した場合の測定値です。

§ 最大セッション数は、HTTP トランザクションを利用した場合の測定値です。

|| 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。

¶ 仮想システムを基本数量から増やすには、別途ライセンスの購入が必要です。

表 2: PA-5400 Series のネットワーキング機能

インターフェイス モード
L2、L3、タップ、バーチャル ワイヤ (透過的モード)
ルーティング
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
ポリシーベース フォワーディング
動的アドレス割り当てのため、PPPoE (Point-to-Point Protocol over Ethernet) と DHCP に対応
マルチキャスト: PIM-SM、PIM-SSM、IGMP v1、v2、v3
双方向転送検出 (BFD)
SD-WAN
バスの品質測定 (ジッター、パケット損失、遅延)
初期のバス選択 (PBF)
鍵交換: 手動鍵、IKEv1、および IKEv2 (事前共有鍵、証明書に基づく認証)
IPv6
L2、L3、タップ、バーチャル ワイヤ (透過的モード)
機能: App-ID、User-ID、Content-ID、WildFire、SSL 復号
SLAAC
IPsec と SSL VPN
鍵交換: 手動鍵、IKEv1、および IKEv2 (事前共有鍵、証明書に基づく認証)
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 による構成と管理の簡素化 *
GlobalProtect のゲートウェイとポータルを用いた IPsec と SSL VPN トンネル経由のセキュア アクセス *

表 2: PA-5400 Series のネットワーキング機能 (続き)

VLAN
デバイス/インターフェイスごとの 802.1Q VLAN タグ: 4,094/4,094
集約インターフェイス (802.3ad)、LACP
ネットワーク アドレス変換
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)
NAT64、NPTv6
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 およびポートのオーバーサブスクリプション
高可用性 (HA)
モード: アクティブ/アクティブ、アクティブ/パッシブ、HA クラスタリング
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
モバイル ネットワーク インフラストラクチャ [†]
5G セキュリティ
GTP Security
SCTP Security

* GlobalProtect ライセンスが必要。

† 詳細は、機械学習 (ML) を活用した 5G 向け次世代ファイアウォール (NGFW) データシートを参照してください。

表 3: PA-5400 Series のハードウェア仕様

I/O
1G/2.5G/5G/10G (x8)、1G/10G SFP/SFP+ (x12)、1G/10G/25G SFP/SFP+/SFP28 (x4)、40G/100G QSFP+/QSFP28 (x4)
管理 I/O
1G/10G SFP/SFP+ アウトオブバンド管理ポート (x1)、1G/10G SFP/SFP+ 高可用性ポート (x2)、40G QSFP+ 高可用性ポート (x1)、RJ-45 コンソール ポート (x1)、Micro USB
ストレージ容量
480GB SSD ペア、システム ストレージ
電源 (平均 / 最大消費電力)
630/760 W
最大 BTU/ 時
1638
電源 (基本 / 最大)
1:1 のフル冗長性 (2/2)
AC 入力電圧 (入力 Hz)
100 ~ 240 VAC (50 ~ 60Hz)
AC 電源出力
1,200 ワット/電源
最大消費電流
AC: 7 A @ 100 VAC、3 A @ 240 VAC
DC: 15 A @ -48 VDC、12 A @ -60 VDC

表 3: PA-5400 Series のハードウェア仕様 (続き)

最大流入電流
AC: 50 A @ 230 VAC、50 A @ 120 VAC
DC: 200 A @ 72 VDC
平均故障間隔 (MTBF)
22 年
ラックマウント (寸法)
2U、19 インチ標準ラック (高さ 8.76cm x 奥行き 57.15cm x 幅 44.04cm)
重量 (デバイス単体 / 出荷時)
15.97kg/22.14kg
安全規格
cTUVus、CB
EMI
FCC Class A、CE Class A、VCCI Class A
認定
paloaltonetworks.jp/legal-notice/trust-center/technical-certifications をご覧ください
環境
動作温度: 0 ~ 50°C (32 ~ 122°F)
非動作温度: -20 ~ 70°C (-4 ~ 158°F)
許容湿度: 10% ~ 90%
最大高度: 10,000 ft/3,048 m
エアフロー: 前面から背面