



## 製品概要

Advanced Threat Prevention Appliance は、高度な脅威検出と統合セキュリティ分析を組み合わせた仮想オンプレミスデバイスであり、セキュリティ運用チームの生産性を向上させながら、高度な脅威検出と統合セキュリティ分析を組み合わせて、企業を既知および未知のサイバー攻撃から保護します。

ATP アプライアンスはジュニパーネットワークスの [SRX シリーズファイアウォール](#) と連携することで、Web、電子メール、および横方向のトラフィックへの脅威を検出し、ファイアウォールがインラインに導入されている場合にこれらの脅威をブロックします。ATP Appliances はまた、既存のセキュリティデバイスからログを取り込むことや、コンテキスト分析を適用して、脅威の状況の統合的な見通しを提供することもできます。

# ADVANCED THREAT PREVENTION APPLIANCE データシート

## 製品説明

Juniper Networks® Advanced Threat Prevention Appliance は、オンプレミスでの仮想脅威の検知と緩和ソリューションの必要性に対処します。

拡張性の要件に基づいて、2種類の仮想プラットフォームから選べます。VMware vSphere または ESXi で運用されている ATP Appliances の仮想バージョンは、8 または 24 の仮想 CPU コアで 1 日あたり最大 116,000 ファイルを処理することができます。

Juniper ATP Appliance は、ジュニパーネットワークスの SRX シリーズファイアウォールまたはその内蔵コレクターを使用して、Web、電子メール、横方向のトラフィックを収集するため、複数のファイアウォールソリューションを採用している企業に最適です。収集されたデータは、ATP アプライアンスコアでさらに処理するためにオンプレミス ATP アプライアンスに送信されます。ATP アプライアンスコアでは、既知および未知の脅威が特定され、検出したものを攻撃キルチェーンにマッピングすることで、環境内の脅威の進行を詳細に説明する包括的な分析を提供します。いったん脅威が検出されると、ATP Appliance は、ファイアウォールポリシーの更新を SRX シリーズのファイアウォールに送信します。ATP アプライアンスは、Palo Alto Networks、Fortinet、Cisco などのベンダーのサードパーティファイアウォールのポリシーを更新するように設定することができます。JATP アプライアンスは、ジュニパーネットワークス [EX シリーズイーサネットスイッチ](#)、ジュニパーネットワークスの [QFX シリーズスイッチ](#)、または他のサードパーティ製スイッチと連動します。脅威を分離して、ワンタッチの攻撃緩和を活用して侵害されたホストを隔離し、横方向の広がりを制限します。

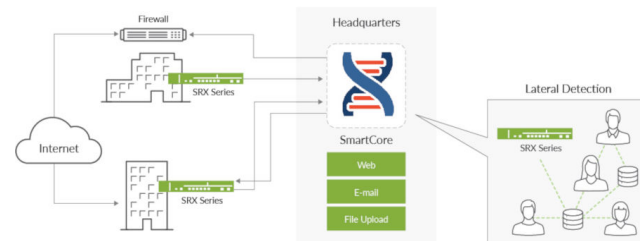


図1 : Juniper Networks ATP Appliance アーキテクチャ

## アーキテクチャと主要コンポーネント

オンプレミス ATP ソリューションでは、インラインの検知とブロックのコレクターとして、SRX シリーズのファイアウォールを使用できます。JATP Appliances は、内蔵コレクターをサードパーティファイアウォールで使用することもできます。MSSP ( Managed Security Service Provider) 環境の場合、マルチテナントをサポートするためにコレクターとコアを分けて ATP Appliance を展開することもできます。お客様の各拠点にコレクターを設置し、コアまたはコアのクラスターが、すべてのトラフィックを分析します。Juniper ATP Appliance は、外部から隔離された環境向けにプライベートモードで実行することができるため、インターネットアクセスが利用できない場合でもマルウェア検出、攻撃の緩和、さらには関連付けを実行できます。

ネットワーク全体から収集されたファイルと関連する実行可能ファイルは、さらなる分析のために、仮想化された ATP アプライアンス上の SmartCore 検出および分析エンジンに配信されます。SRX シリーズファイアウォールは、SmartCore エンジンによって検出された脅威をブロックすることができます。

ATP アプライアンスは、アクティブディレクトリ、エンドポイントアンチウイルス、ファイアウォール、Secure Web Gateways (SWG)、侵入検出システム、エンドポイント検出および応答ツールなどの、他の識別およびセキュリティソリューションからログを取り込むこともできます。ログは、サードパーティデバイスから直接取り込むか、既存のセキュリティ情報およびイベント管理 (SIEM) /syslog サーバーに転送することができます。

表 1. ジュニパーネットワークス Advanced Threat Prevention Appliance の特徴とメリット

特長	説明	メリット
トラフィックインスペクション	Web、電子メール、水平方向の拡散を含む、複数方向の脅威から保護します。	幅広いプロトコルサポートを提供し、マルウェアとランサムウェアの流通で最も一般的な方法をカバーします
インライン脅威の緩和	SRX シリーズのファイアウォールが導入される場合、インラインブロックを提供します	既知と未知の脅威をブロックする機能を提供します
攻撃分析	サードパーティ セキュリティ ソリューションを含めたネットワーク全体の脅威の状況について、リアルタイムおよび歴史的な見解を提供します	セキュリティ運用担当者は、ネットワーク内で発生する関連した脅威アクティビティを可視化することで、優先度の高い脅威を迅速に特定したり、対応方法を理解したり、アウトブレイクを修復するために隔離することができます。
サードパーティの相互運用性	包括的な API とカスタムメイドのログ取り込みフレームワークが含まれており、サードパーティセキュリティデバイスと容易に統合して、導入済みのセキュリティ製品からの脅威ログ収集とアグリゲーションが可能になります	API を使ったサードパーティ セキュリティデバイスとの統合が容易になり、既存のセキュリティ製品からの脅威ログの収集とアグリゲーションをサポートします
一元管理	MCM ( Manager of Central Managers ) 機能のマネージャーを含みます	複数のコアを必要とする大規模な導入において、クラスター化されたコアアプライアンスの、包括的で集中型の一括管理を提供します
柔軟な導入	仮想オンプレミス導入をサポート	脅威処理と分析における拡張性とパフォーマンスに対する要件に応じて、柔軟なオプションを提供
分散型アーキテクチャ	任意の数のネットワーク拠点に導入可能なコレクターを活用し、本部やクラウドに存在する分析エンジンにすべてのフィードを取り込むことができます。	パブリッククラウドとプライベートクラウドを含むネットワーク全体の、脅威カバレッジが増加します
クラスターリング	拡張可能なアーキテクチャを介して、複数の二次コアのクラスターリングが可能になります	単一以上のアプライアンスが必要な場合、脅威の処理能力を迅速に増加させることができます
認証	SAML と RADIUS を使用したアクセスと認証をサポートします	既存の認証ソリューションと連携します

## 製品オプション

ATP アプライアンスには 8 コアと 24 コアがあり、ネットワーク要件に最も適するオプションを選べるすることができます。仮想アプライアンスは、別のアプライアンスにインストールされている SmartCore やファブリックコレクターを使用して、分散モードで導入することができます。

MacOS のマルウェア検知もサポートされています。お客様からは、二次コアとして導入する Mac mini ハードウェアを提供していただく必要があります。MacOS サンドボックス作成の画像は、ATP Appliances のソフトウェアダウンロードページで利用できます。

表 2. バーチャルアプライアンス パフォーマンス

製品名	バーチャルメモリ/ディスク	コレクターのパフォーマンス	E-Mail MTA (メッセージ転送エージェント) レシーバー	パフォーマンス (対象物のデトネーション) <sup>1</sup>
バーチャル JATP Appliances ソリューション (8 コア CPU)	32GB/1.5TB	1.5 Gbps	720,000	最大 46,000 オブジェクト/日
バーチャル JATP Appliances ソリューション (24 コア CPU)	96GB/1.5TB	4 Gbps	240 万	最大 116,000 オブジェクト/日

<sup>1</sup> 実際のパフォーマンスに近似するトラフィックミックスに基づいた数。実際の数字は、トラフィックミックス、繰り返しオブジェクト、およびその他のユーザーの環境に固有の要因に基づいて異なる場合があります。

表 3. バーチャルアプライアンスハードウェアの仕様

製品名	ハイパーバイザーサポート	バージョン
バーチャル JATP Appliances	VMware vSphere、ESXi	vSphere ( 5.5、6.0、6.5 )、ESXi ( 5.5.1、5.5、7.0 )



JATP700



JATP400

## 仕様

仕様	JATP400	JATP700
重量	13.79 kg ( 30.4 ポンド )	19 kg ( 42 ポンド )
外形寸法 ( 幅 x 高さ x 奥行き )	43.7 x 4.3 x 65 cm ( 17.2 x 1.7 x 25.6 インチ )	43.7 x 8.9 x 63 cm ( 17.2 x 3.5 x 24.8 インチ )
フォーム ファクター	1 U ( ラックマウント可能 )	2 U ( ラックマウント可能 )
A/C 電源	500W 高効率 ( 94%+ ) AC-DC 冗長電源 ; AC 入力 : -100 ~ -240V、50 ~ 60 Hz、11-4.4 アンペア	920W 高効率 ( 94%+ ) AC-DC 冗長電源 ; AC 入力 : -100 ~ -240V、50 ~ 60 Hz、11-4.4 アンペア
DC 電源	650W 高効率の冗長電源 DC-to DC 電源供給 ; DC 入力 : 650W ; -44 ~ -74VDC、20 アンペア	850W/1010W 高効率の冗長電源 DC-to DC 電源供給 ; DC 入力 : 850W ; -35 ~ -42VDC、30-25 アンペア
ファン	4 x 4 x 5.6 cm ( 1.6 x 1.6 x 2.2 インチ ) 13K-11K RPM カウンター回転ファン、RoHS/REACH	4 x 4 x 5.6cm ( 1.6 x 1.6 x 2.2 インチ ) 13K-11K RPM カウンター回転ファン、RoHS/REACH
動作時温度	10° ~ 40°C ( 50° ~ 104°F )	10° ~ 40°C ( 50° ~ 104°F )
保管時温度	-40 ~ 70°C ( -40 ~ 158°F )	-40 ~ 70°C ( -40 ~ 158°F )
相対湿度 ( 動作時 )	8 ~ 90% ( 結露しないこと )	8 ~ 90% ( 結露しないこと )
相対湿度 ( 保管時 )	5 ~ 95% ( 結露しないこと )	5 ~ 95% ( 結露しないこと )
高度 ( 動作時 )	最大 1,981 m ( 6,500 フィート )	最大 1,981 m ( 6,500 フィート )
高度 ( 保管時 )	最大 10,668 m ( 35,000 フィート )	最大 10,668 m ( 35,000 フィート )
安全規格	CAN/CSA-C22.2 No.60950-1 情報技術機器の安全性 EN60950-1 UL60950-1 ( 2nd Edition ) IEC60950-1 : 2005/A2:2013	CAN/CSA-C22.2 No.60950-1 情報技術機器の安全性 EN60950-1 UL60950-1 ( 2nd Edition ) IEC60950-1 : 2005/A2:2013
電磁波放射基準認定	47CFR パート 15, (FCC) クラス A ICES-003 クラス A EN 55022 クラス A CISPR 22 クラス A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 クラス A CNS13438 クラス A EN 61000-3-3 VCCI クラス A KN22 クラス A EN 61000-3-2 BSMI CNS 13438	47CFR パート 15, (FCC) クラス A ICES-003 クラス A EN 55022 クラス A CISPR 22 クラス A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 クラス A CNS13438 クラス A EN 61000-3-3 VCCI クラス A KN22 クラス A EN 61000-3-2 BSMI CNS 13438
NEBS	x	x
RoHS	o	o
CPU	10 コア	10 コア x 2
メモリ	32 GB	128GB
ストレージ	8TB ( 4 x 2TB )、RAID6	10K SAS の 900GB 2.5 x 8、RAID6
トラフィック ポート	SFP+ 10 GbE x 2、RJ-45 GbE x 4	SFP+ 10 GbE x 2、RJ-45 GbE x 4

## 注文情報

ジュニパーネットワークスの Advanced Threat Prevention Appliances は、柔軟な導入オプションをサポートします。必要なコンポーネントは、導入モデルによって異なります。

- 物理的な導入には、物理的な ATP Appliance ソリューションと、関連ソフトウェアのサブスクリプションが必要です。
- 仮想導入には、ソフトウェアサブスクリプションのみが必要です。

バーチャル ATP Appliance およびソフトウェアライセンスに関する情報や、ご注文に関する一般的なご質問については、購入方法ページ ([>www.juniper.net/jp/ja/how-to-buy/form.html](https://www.juniper.net/jp/ja/how-to-buy/form.html)) をご覧ください。

## 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、ネットワーク運用を劇的に簡素化し、エンドユーザーに最上のエクスペリエンスを提供することに注力しています。業界をリードするインサイト、[自動化](#)、[セキュリティ](#)、[AI](#) を提供する当社のソリューションは、ビジネスで真の成果をもたらします。つながりを強めることにより、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは確信しています。

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, CA 94089 USA

電話番号：888.JUNIPER (888.586.4737)

または +1.408.745.2000

[www.juniper.net](http://www.juniper.net)

### APAC and EMEA Headquarters

日本, 東京本社  
ジュニパーネットワークス株式会社  
〒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 45 階

電話番号：03-5333-7400

FAX：03-5333-7401

[www.juniper.net/jp/ja/](http://www.juniper.net/jp/ja/)

