Arbor Networks SP ソリューション

ネットワーク全体の視認性、脅威管理、サービス・イネーブルメント

主な特長と利点

ネットワーク・インフラの保護
DDoS 攻撃をわずか 4 秒で検知し、固定またはモバイル・ネットワーク・インフラの可用性と性能に影響が生じる前にこれを阻止します。

サービスの保護
DNS、音声、ビデオ、Web、E コマース、電子メールといったクリティカルなサービスの可用性を、標的型攻撃から防御します。

モバイル・パケット・コアの視認性および脅威検知
GTP トラフィックの視認性を確保し、モバイル・ネットワークの性能に影響が生じる前に脅威を検知します。

ネットワーク・リソースの最適化
トラフィックの視認性と包括的なレポートを使用して、より優れたトラフィック・エンジニアリングと、より効率的で迅速なトラブルシューティングを実現できます。トランジット・コストを削減して利用効率を向上させ、インテリジェントな事業拡大計画を策定することができます。

マネージド・セキュリティ・サービスの提供
ネットワークの視認性とセキュリティのために使用するのと同じ SP プラットフォームを活用して、差別化要因となる高収益のクラウド内 DDoS 防御サービスを容易に準備、提供、および維持することができます。

Flexible Licensing
SP の Flex Licensing は、新しいパフォーマンスと拡張性の向上を実現し、より最適かつ低価格の展開を可能にします。

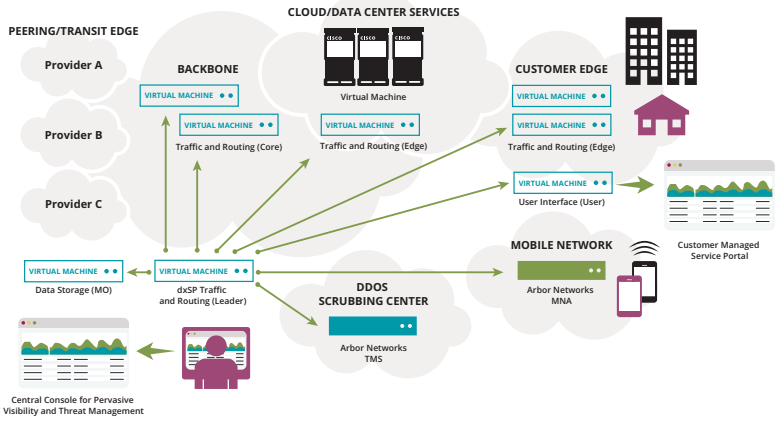
ARBOR NETWORKS
The Security Division of NETSCOUT

インターネット・サービス・プロバイダ、モバイル・ネットワーク・オペレータ、クラウド／マス・ホスティング・プロバイダ、および大企業は、より豊富なサービスとより高い可用性に対するユーザーの需要の高まりに応えるという、共通の課題に直面しています。運用スタッフ、エンジニアリング、および経営陣は、可用性に影響を与えるイベントにリアルタイムに対応するためのネットワーク・インテリジェンスおよびツールを必要としています。また、ネットワーク・エンジニアリングおよびキャパシティ・プランニングにおける適切な決定を行って、将来的なサービスへの需要の高まりに応えつつスムーズで効率的な運用を実現することも必要になります。Arbor Networks® SP ソリューションは、ネットワーク・インテリジェンスとインフラストラクチャの可用性におけるデファクトスタンダードとなっています。SP は、他のすべてのソリューションを合わせたよりもさらに多くのインターネット・サービス・プロバイダ、クラウド・プロバイダ、および企業を対象に、サービスの可用性を保護しています。

ネットワーク・インテリジェンスの力

SP はネットワーク全体のパケット、NetFlow、SNMP、および BGP ルートを収集、集約、および解析します。大量のデータを実効性の高いインテリジェンスに変換し、日々のオペレーショナル・エクセレンスと将来に向けた健全な計画をサポートします。SP ソリューションは以下のような原理を基盤としています。

- **ネットワーク全体の視認性：**安全なネットワークおよび脅威管理には、適切な視認性が不可欠です。SP はピアリング・エッジからバックボーン、顧客側エッジ、データ・センター、モバイル・ネットワークに至るまで、ネットワーク全体にわたる視認性を提供します。
- **高度な脅威管理：**組織の成功にとって、サービスに被害が及ぶ前に脅威を阻止することは不可欠となります。SP は高度な脅威をわずか 1 秒で検知し、わずか 4 秒でミティゲーションを行うため、ネットワークやデータ・センター、サービス、顧客に対し悪影響が及ぶのを防ぐことができます。
- **サービス・イネーブルメント：**今日のビジネス環境には、競争の激化、サービスのコモディティ化、収益性向上に対するプレッシャーの高まりといった厳しい現実があります。ネットワークの可視化とセキュリティに使用するのと同じ SP プラットフォームを活用して、差別化要因となる高収益のクラウド内分散型サービス拒否（DDoS）防御サービスを提供することができます。



SP アーキテクチャ

1) ピアリング／トランジット・エッジおよび／またはバックボーンでのコア・トラフィックおよびルーティング解析、2) 顧客側エッジおよびデータ・センターでのエッジ・トラフィックおよびルーティング解析、3) モバイル・パケット・コアでのモバイル・ネットワーク解析、4) 拡張性を向上し冗長性を追加するためのデータ・ストレージ、5) 顧客ポータルのユーザー・インターフェイス、6) DDoS スクラビング・センターにおけるネットワーク脅威のサージカル・ミティゲーション。

リアルタイムのグローバル脅威解析を 1 台のコンソールで

Arbor Security Engineering and Response Team (ASERT) は、全世界の大半のインターネット・サービス・プロバイダと Arbor との信頼関係を活用して、グローバルな脅威活動に関する独自の解析を行います。ASERT は Active Threat Level Analysis System (ATLAS®) と呼ぶしくみの下で、業界および Arbor の顧客にさまざまな利点をもたらしています。この利点には次のようなものがあります。

ATLAS セキュリティ・ポータル

ATLAS セキュリティ・ポータル (atlas.arbor.net) は、グローバルな脅威活動をリアルタイムで表示する機能を提供します。この情報には SP コンソールから簡単にアクセスでき、サービス・プロバイダは世界的な脅威活動が自社のネットワークにどのような影響を与えるかを把握することができます。

ATLAS スレット・フィードおよび ATLAS インテリジェンス・フィード

Arbor の研究者は ATLAS のグローバル監視機能を利用して、ネットワーク層およびアプリケーション層への新たな攻撃を発見し、適切な防御策を開発しています。こうした防御策は、ATLAS スレット・フィードおよび ATLAS インテリジェンス・フィードを経由して自動的に SP システムにアップロードされます。

Cloud Signaling™ テクノロジー

Arbor の高度な DDoS 防御機能は、ネットワークの帯域とデータ・センターのサービスの両方を脅かす攻撃に対し、冗長で自動的かつ連動的な対処を行います。

「弊社は、小規模な ISP としてスタートした創業時からグローバル・サービス・プロバイダとなった現在に至るまで、SP 製品セットとともに成長してきました。この 5 年間に渡り、Arbor 社と協力し合ってこられたことは、大きな喜びです。ローカルかグローバルかを問わず、IP ネットワークの運営に携わるあらゆる人に、Arbor 製品を自信を持って推奨します。」

Easynet Global Services 社、ネットワーク・サービス・ディレクター

インテリジェント・ネットワークの設計および管理においてはネットワーク全体の視認性が不可欠となる

SP はネットワーク上において非侵入型であり、ルーターやスイッチによるネットワーク・テレメトリ (NetFlow、sFlow など) を活用して、インラインのプローブやタップに依存することなくネットワーク全体の視認性を提供します。SP の強力なレポート機能を通じ、ネットワーク・オペレータは以下を確認できます。

- ネットワーク上のトラフィックがどこから来てどこへ行くのか。
- トラフィックがどのルートを通っているか。
- どのインターフェイスおよびデバイスが最も頻繁に使用されているか。
- ネットワーク上のトップ・トーカーまたはアプリケーションは誰／何か。
- 短期的および長期的な傾向はどういったものか。

このレポート機能はネットワーク・オペレータにとって極めて有益です。効率的かつ費用効率の高いネットワーク・エンジニアリングが可能になるため、オペレータはピアリングやトランジット契約について適切な判断を下し、使用率の高い、または、低いデバイスや回路を特定し、顧客の利用傾向や要件についての理解を得ることができます。

攻撃を受けた場合、1 秒の違いが大きな差を生む

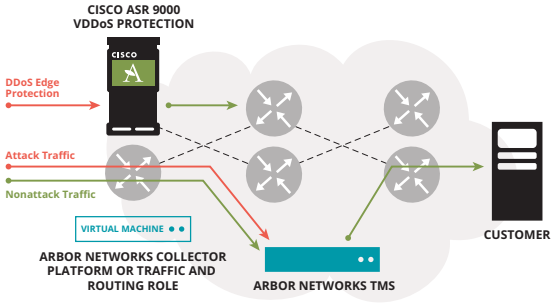
SP は、「高速フラッド型」の攻撃をわずか 1 秒で検知し、4 秒以内に自動でミティゲーションを開始します。複数のインタラクティブなダッシュボードを介し、簡単な操作で攻撃に関する最も重要な情報を提供します。SP ダッシュボードを通じ、オペレータは以下を確認できます。

- 攻撃トラフィックがどこから来てどこへ行くのか。
- トップの攻撃トラフィックのパターンはどのようなものか。
- 攻撃により最も深刻な影響を受けているのはどのルーター・インターフェイスおよびデバイスか。
- 攻撃のソースと標的は何か。
- 攻撃により使用されるプロトコルは何か。

SP の DoS アラート・ダッシュボードはインタラクティブな表示機能を備えているため、オペレータは主要な攻撃の詳細に迅速にアクセスしてミティゲーションまでの時間を短縮し、最終的に攻撃による被害を最小化できます。

サービス拒否攻撃からの防御

Arbor Networks TMS は、「ダイバージョン／リインジェクション」というミティゲーション・アーキテクチャをサポートしています。このモードでは、SP コンソールからのルーティングアップデイトによりトラフィックが TMS にリダイレクトされます。次に TMS により攻撃トラフィックのみがパケット・ストリームから排除され、正規のトラフィックが目的の宛先へと送信されます。



TMS サージカル・ミティゲーション

これはサービス・プロバイダ、大企業、および大規模なホスティング / クラウド・プロバイダにとって大きな利点となります。単一の TMS により複数のデータ・センターを一元的に保護できるため、ミティゲーション能力をはるかに効率的に利用できます。インライン装置は、監視しているすべてのリンクで常にすべてのトラフィックを検査する必要があります。TMS は、TMS にリダイレクトされたトラフィック（大規模なネットワーク全体を流れるすべてのトラフィックのごく一部）を検査するだけですみます。

有益なマネージド DDoS サービスソリューション

SP は運用を簡易化し、マネージド DDoS サービスの展開コストを削減します。主な機能には、カスタマイズ可能なポータル向けのテンプレート／ API、冗長性、自動フェールオーバー、データ同期化、「ワン・クリック」または自動ミティゲーション、カスタマイズ可能なミティゲーション・テンプレート、リアルタイムのミティゲーション・ダッシュボード、詳細なミティゲーション・レポートが含まれます。これらの機能によって、マネージド DDoS サービスのプロビジョニングと運用サポートを単純化し、収益と顧客の満足度を向上させることができます。SP は、他のすべてのソリューションを合わせたよりもさらに多くのマネージド・サービス・プロバイダで、DDoS 防御サービスを提供するために利用されています。

モバイル・パケット・コアの視認性および異常検知

Arbor Networks MNA は SP に完全に一体化された拡張機能で、単一のコンソールを通じて固定およびモバイル・ネットワーク全体にわたる統合的な視認性と脅威管理を提供します。

MNA は主要な 3G (HSPA) および 4G (LTE) GTP-C メッセージ・フローに対するリアルタイム解析と過去データの解析を行うことで、防御の基礎となるモバイル・コア内での信号パターンと不要なトラフィック活動に対する理解を促します。

MNA はまた、悪意の有無にかかわらず GTP-C トラフィック異常を検知してアラートを発し、ネットワークとサービスの性能と可用性に対する脅威に関し早期段階での警告を提供します。

管理とスケール

SP は、ネットワーク視認性とセキュリティに関する、業界で最も包括的で柔軟なレポートおよび管理システムを提供します。また、企業、ホスティング / クラウド・プロバイダ、サービス・プロバイダの環境など、さまざまな状況で使用できるように設計されています。最大 20,000 のマネージド・オブジェクト（顧客、IP アドレス範囲、インターフェイス、ルート、サービスなど）の監視、レポート、保護機能に加え、550,000 のネットワーク・インターフェイスのサポート、総合的なレポートおよびドリルダウン機能、レポートのカスタマイズ、また柔軟かつカスタマイズ可能な管理ロールの定義など、さまざまな機能があります。

SP を利用している企業

ビジネス	サービスの利点
インターネット・サービス・プロバイダ（ISP、MSO）	有線 ISP では、SP を使用してネットワークの視認性と対 DDoS 機能を確保することで、ネットワーク・エンジニアリングを改善する、ピアリングやトランジットの関係をより有効に管理する、不正または不要なトラフィックによるネットワーク容量の消費を防止する、顧客に MPLS の視認性を提供する、DDoS 攻撃の影響がエンドユーザーに及ぶのを防ぐことができます。
モバイル・ネットワーク・オペレータ（MNO）	モバイル・プロバイダは SP を利用することで、コア・インフラストラクチャ（GGSN）およびコア・サービス（AAA、DNS）を、インターネットやサブスクライバからの DDoS 攻撃およびリソースを消耗させる攻撃から保護できます。
ホスティング／クラウド・プロバイダ（IaaS、PaaS、SaaS）	ホスティングおよびクラウド・プロバイダは、SP の利用を通じてトラフィック・エンジニアリングを改善する、 不要なトラフィックが全体的なサービス・レベルに影響を及ぼすのを防ぐ、コアおよび顧客の操作を DDoS 攻撃から保護することができます。
企業	企業は SP の利用を通じ、オンライン小売業や SaaS、ゲーム、メディア、エンターテインメント、金融サービスといったオンライン操作を DDoS 攻撃から保護できます。
マネージド・セキュリティ・サービス・プロバイダ（MSSP）	専業 MSSP およびホスティング・プロバイダ、ISP はすべて、DDoS 防御をマネージド・サービスとして提供する目的で SP を使用します。

実績のある包括的な脅威検知とミティゲーション

SP ソリューションは、他のすべてのソリューションを合わせたよりもさらに幅広く展開されています。その理由は明らかであり、貴重なビジネス・インテリジェンス、ネットワークの視認性、およびサービス可用性を脅かすイベントからの保護機能を提供できるからです。

既知の悪意あるホストをブロック。ホワイトリストとブラックリストを利用します。ホワイトリストには承認を得たホストが、一方ブラックリストにはゾンビ（感染ホスト）がリストされ、ブラックリストのホストのトラフィックをブロックします。

IP ロケーションを使用して視認性を確保。望ましくないソースからのトラフィックをブロックします。HTTP 固有の攻撃に対する検知とミティゲーション用のメカニズムを使用して、Web ベースの脅威および異常から防御します。

DNS サービスの保護と管理。SP プラットフォームの高度な DNS 保護とレポートの機能により、こうした重要なサービスの可用性が確保されます。

クリティカルな VoIP サービスの防御。pps を悪用して大量の異常なリクエストを実行する自動スクリプトやボットネットの攻撃から保護します。

大規模なリフレクション／増幅攻撃を阻止。単一のスレット・マネジメント・システム・シャーシ内で最大 80 Gbps の攻撃ミティゲーションを利用することで、NTP、DNS、SNMP、SSDP、SQL RS、Chargen といった攻撃を阻止します。

SSL パケットに隠れた攻撃を検知阻止。オプションの Arbor Networks TMS 2300 ハードウェア・セキュリティ・モジュール（HSM）が SSL パケットを復号化して攻撃トラフィックを検知、ドロップし、さらに正規トラフィックを再度暗号化してネットワークに戻します。

SP トラフィックとルーティング、ユーザー・インターフェイス、およびデータ・ストレージの各ロールは、それぞれ SP 6000 アプライアンスの記載のエンクロージャまたは VMware、KVM、Xen 仮想マシン上に展開できます（オプション）。

SP の展開スケール

ミティゲーション能力	TMS で 8 Tbps
BGP ルート（一意）	3,750,000,000
フロー／秒（非サンプル化）	30,000,000
ルーター	5,000
監視対象インターフェイス	200,000
インターフェイス合計	550,000
マネージド・オブジェクト	20,000
収集アプライアンス	150
SP スレット・マネジメント・システムアプライアンス	100
APS アプライアンス	200
ユーザー数	700

ARBOR NETWORKS

The Security Division of NETSCOUT

本社

76 Blanchard Road
Burlington, MA 01803 USA

米国内フリーダイヤル：+1 866 212 7267
TEL：+1 781 362 4300

北米販売担当者

フリーダイヤル：+1 855 773 9200

欧州

TEL：+44 207 127 8147

アジア太平洋

TEL：+65 6664 3140

日本

〒 101-0063
東京都千代田区神田淡路町 2-105
ワテラス アネックス 13 階
TEL：03 3525 8040
お問い合わせ japan@arbor.net

www.arbornetworks.com

DS/SPSOLUTION/EN/1115-LETTER

Arbor Networks SP プラットフォーム

ロール／説明	アプライアンス・ライセンス	Flex ライセンス
トラフィックとルーティング	**SP Collector Platform (CP) アプライアンス： CP 6000-5、CP 6000-2 または SP フロー・センサ（FS）：FS 6000-15**	**SP-6000 アプライアンス**
SP Collector Platform (CP)： ・SP 展開の中のフロー・データを収集します **SP フロー・センサ（FS）：** ・BGP ピアリングの解析を除く、CP アプライアンスの収集／解析機能を実行します	**コア・バックボーンおよびピアリング・ルーターの場合：** ・CP 6000-5 は 5 台のルーターから 200k フロー／秒で収集を行います。 ・CP 6000-2 は 2 台のルーターから 200k フロー／秒で収集を行います。 **小型の顧客側エッジ・ルーターの場合：** ・FS 6000 は 15 台のルーターから 200k フロー／秒で収集を行います。	・32 台のコア・ルーターまたは 100 台のエッジ・ルーターから、200k フロー／秒で収集を行います。
ユーザー・インターフェイス	**SP ポータル・インターフェイス（PI）アプライアンス： PI 6000-25**	**SP-6000 アプライアンス**
・SP 展開専用の管理プラットフォーム ・CP アプライアンスからのオフロード管理とレポート生成 ・顧客ポータル、ポータル API、およびより多くの同時ユーザーをサポートする、マネージド・サービス向けの設計	・5 つ以上の CP アプライアンスを備えた SP 展開に必要 ・PI リーダー・デバイスが最大 25 名の同時ユーザー、または一つの展開につき最大 125 名のユーザーをサポート ・PI は Cloud Signaling™ 向けの SA® アプライアンスを最大 200 サポート	・SP Flex Licensing 展開のユーザー・インターフェイス ・最大 100 の同時ユーザー、または一つの展開につき 700 のユーザーをサポート ・Cloud Signaling™ 向けの SA® アプライアンスを最大 200 サポート
データ・ストレージ	**SP Business Intelligence (BI) アプライアンス： BI 6000-500**	**SP-6000 アプライアンス**
・監視・保護対象となるマネージド・オブジェクト（顧客、ネットワーク、リソース）の作成専用の管理プラットフォーム ・CP アプライアンスを追加することなく SP 展開のスケールを拡大	・最大 500 のマネージド・オブジェクト（MO）をサポート ・SP 展開における 20 の BI アプライアンスで最大 10,000 のマネージド・オブジェクトを有効化できる	・最大 1000 のマネージド・オブジェクト（MO）をサポート ・SP 展開における 20 の BI アプライアンスまたはデータ・ストレージ・アプライアンスで、最大 20,000 のマネージド・オブジェクトを有効化できる（Flex Licensing 使用）
モバイル・コア解析	**SP モバイル・ネットワーク解析**	
・主要な 3G (HSPA) および 4G (LTE) GTP-C メッセージ・フローに対するリアルタイム解析と過去データの解析。 ・悪意の有無にかかわらず GTP-C トラフィック異常を検知してアラートを発信	・SP UI 内に完全に統合 ・25K または 50K、100K GTP-C メッセージ／秒を含むライセンス・レベル ・最大 1M GTP-C メッセージ／秒に対応するシステム	
ミティゲーション	**SP スレット・マネジメント・システム**	
・ディープ・パケット・インスペクション（DPI）、アプリケーション・インテリジェンス、および攻撃のサージカル・ミティゲーション機能を提供	・最大 2 桁の Tbps および 3 桁の Mpps に対する Cisco ASR 9000 vDDoS 防御 ・TMS 4000 で最大 80 Gbps および 80 Mpps のミティゲーション ・TMS 2300 で最大 10 Gbps および 10 Mpps のミティゲーション ・TMS 2300 のオプションのハードウェア・セキュリティ・モジュール（HSM）は、SSL パケットを復号化して最大 5 Gbps の攻撃に対するミティゲーションを実施 ・1 つの展開における 100 の TMS で最大 8 Tbps をミティゲーションできる	

SP 6000 アプライアンスおよび仮想マシンの仕様

特長	説明		
電力要件	冗長対応二重化電源、**AC：** 100〜127V/200〜240V、50〜60Hz、6/3A、DC： -48〜-72V、最大 13A		
サイズ	**筐体：**2U ラックサイズ、**重量：**39 lbs (17.7 kg)、**高さ：**3.45 インチ（8.76 cm）、**幅：**17.14 インチ（43.54 cm）、**奥行き：**20 インチ（50.8 cm）、標準 19 インチおよび 23 インチのラックを取り付け可能		
ハード・ドライブ	RAID 5 を実行する 4 つの 480 GB ソリッド・ステート・ドライブ		
ネットワーク・インターフェイス	アドインのネットワーク・インターフェイスなし、または 1 GigE (銅線、GigE SX、GigE LX 用の SFP) × 4、または 1 GigE (銅線、GigE SX、GigE LX 用の SFP) × 8、または 10 GigE (SR または LR 用の SFP+) × 2、または 10 GigE (SR または LR 用の SFP+) × 2、および 1 GigE (銅線、GigE SX、GigE LX 用の SFP) × 4		
環境	**動作温度：** 41°〜104°F (5°〜40°C)、**相対湿度：** 73°〜 104°F (23°〜 40°C) で動作時 5〜85%、非動作時 95%		
オペレーティング・システム	ArbOS は Arbor の特許取得済みの組み込みオペレーティング・システムであり、Linux を基盤としています。		
準拠規格	RoHS 2002/95/EC、IEC/EN/UL 60950-1 第 2 版、E2006/95/EC、2001/95/EC、FCC パート 15 サブパート B クラス A、EN 55022、EN 55024、EN 61000-3-2、EN 61000-3-3、EN 61000-4-2、EN 61000-4-3、EN 61000-4-4、EN 61000-4-5、EN 61000-4-6、EN 61000-4-8、EN 61000-4-11、IC ICES-003 クラス A、ETSI EN 300 386、ETS 300-019-2-1、ETS 300-019-2-2、ETS 300-019-2-3、ETS 753、CISPR 22 クラス A、CISPR 24、Gost、BSMI、VCCI クラス A、KCC クラス A、UL マーク、CE マーク、ETSI、NEBS-3 (DC)、NEBS-1 (AC)		
仮想マシンの要件	**ハイパーバイザ：**VMware vSphere v5.0 および 5.1、5.5、vCPUs ：4 〜 32、**ネットワーク・インターフェイス：**1 〜 10、**メモリ：**8 または 16、24、32 GB、**ストレージ：**最小 100 GB。	**ハイパーバイザ：**Xen クラウド・プラットフォーム v1.6.10-61809c、vCPUs ：4 〜 15、**ネットワーク・インターフェイス：**1 〜 10、**メモリ：**8 または 16、24、32 GB、**ストレージ：**最小 100 GB。	**ハイパーバイザ：**KVM QEMU v1.4.2、vCPUs ：4 〜 32、**ネットワーク・インターフェイス：**1 〜 10、**メモリ：**8 または 16、24、32 GB、**ストレージ：**最小 100 GB。