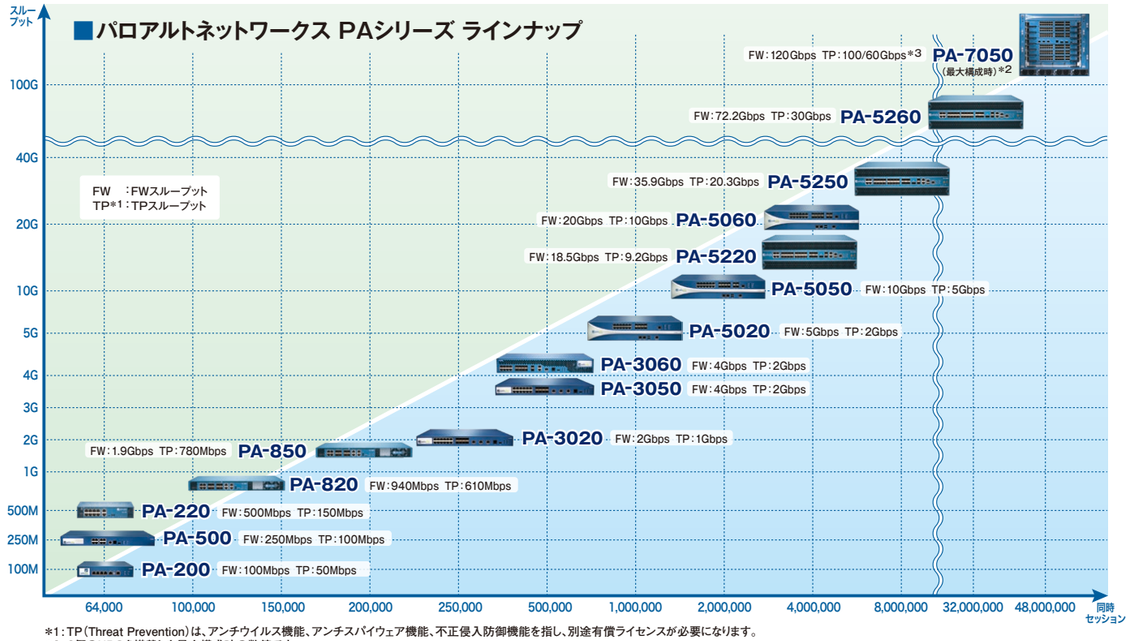
■パロアルトネットワークス PAシリーズ ラインナップ



*1：TP（Threat Prevention）は、アンチウイルス機能、アンチスパイウェア機能、不正侵入防御機能を指し、別途有償ライセンスが必要になります。
*2：6個のNPCを搭載した最大構成時の数値です。
*3：DSRI(Disable Server Response Inspection：片方向検知)の場合は100Gbps、双方向検知を実施する場合は60Gbpsとなります。
※全ての機種はPAN-OS 8.0のハードウェア・スペックになります。　※上記の値は、設計上の理論値、またはテスト環境において認知した値であり、実環境においてこの値を保証するものではありません。

■統合管理製品仕様

製品名	M-100
筐　体	
管理インタフェース	10/100/1000（×4） DB9コンソールシリアルポート（×1）
ストレージ	最小1TB、最大4TBのHDD（RAID 1構成）
ユニットサイズ 外部寸法（H×W×D/cm）	1U 4.45×48.8×61.2
電源	500W AC電源

■仮想アプライアンス製品仕様

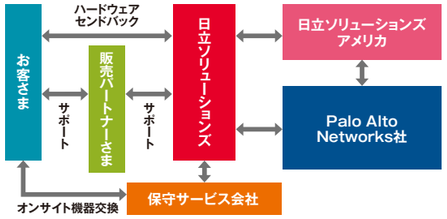
製品名		VM-50	VM-100/200	VM-300	VM-500	VM-700
性　能	ファイアウォールスループット TPスループット IPSec VPNスループット	200Mbps 100Mbps 100Mbps	2Gbps 1Gbps 1Gbps	4Gbps 2Gbps 1.8Gbps	8Gbps 4Gbps 4Gbps	16Gbps 8Gbps 6Gbps
	新規セッション数/秒 最大セッション数	3,000 50,000	15,000 250,000	30,000 800,000	60,000 2,000,000	120,000 10,000,000
	IPSec VPNトンネル数 SSL VPN同時ユーザー数	250 250	1,000 500	2,000 2,000	4,000 6,000	8,000 12,000
機能仕様	VR数（仮想ルータ）	3	3	10	20	125
	セキュリティゾーン 最大ポリシー数	15 250	40 1,500	40 10,000	200 10,000	200 20,000

＊パフォーマンスと容量は、最適なテスト条件のもと PAN-OS 8.0で測定されています。

Palo Alto Networks社の製品・技術を熟知した日立ソリューションズが提供します。

セキュリティ分野の主力製品をこれまで多数取り扱ってきたソリューションプロバイダ、
日立ソリューションズの「経験、実績、技術、ノウハウ」を活かし、
「国内初のPalo Alto Networks社認定の技術者」として、
PAシリーズのシステム設計から構築、運用までサポートします。

- 製品・技術を熟知したPalo Alto Networks社認定技術者が担当
- OSの検証など、十分な安全性確認を実施してからの出荷
- Palo Alto Networks社との密接な連携による包括的なサービスの実現
- 導入後の運用までトータルにカバーしたメニューの用意



株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/paloalto/sp/

S11K-32-03　2018.03

HITACHI
Inspire the Next

次世代ファイアウォール
パロアルトネットワークス PAシリーズ
テクニカルガイド

“従来型”と“次世代”ファイアウォールの違い。
“他社製”と“Palo Alto Networks社製”次世代ファイアウォールの違い。
日立ソリューションズが選ぶ理由。
すべてをご紹介します。

パロアルトネットワークス PAシリーズは、
世界ではじめてアプリケーションを制御する機能を搭載した次世代ファイアウォール。
そして、ファイアウォール市場ではじめて製品化された次世代ファイアウォールです。
日立ソリューションズは、このPAシリーズを2008年9月から販売。
さらに性能試験、負荷試験、過去に摘出した不具合の確認などの独自の品質評価を実施し、
Palo Alto Networks社と品質向上への取り組みを続けています。
本テクニカルガイドでは、こうした経験とノウハウ、さらには幅広い分野で様々なネットワーク製品、
セキュリティ製品を取り扱ってきた実績を活かし、PAシリーズの技術を解説致します。
“従来型”と“次世代”ファイアウォールの違い、
“他社製”と“Palo Alto Networks社製”次世代の違い、
そして日立ソリューションズが選ぶ理由も、
きっとご理解いただけるはずです。

従来のファイアウォールやUTMとは異なる発想から生まれた、次世代ファイアウォール パロアルトネットワークス PAシリーズ。

企業におけるアプリケーション利用の拡大に伴い、アプリケーションを介したセキュリティ脅威や情報漏えいの危険性が高まっています。
しかし、従来のファイアウォールでは巧妙化・複雑化したインターネットの攻撃には対応ができなくなっています（図1）。
現在、多くの企業はファイアウォールを社内LANとインターネットの境界に設置し、それを補完するためにウイルス対策やIPS、URLフィルタリングなどの専用装置を配置しています（図2）。
このような効率の悪い構成を採る理由は、従来のファイアウォールやセキュリティ製品では、検査対象（スコープ）が狭いからです。これまでのファイアウォールはIPアドレスやポート、ウイルス対策ソフトはウイルス、URLフィルタリングはURLのみ。こうした個々の対策では、複合化する脅威を検知するのはきわめて困難です。
では、ファイアウォールとIPS、アンチウイルス、Webフィルタリングなどセキュリティ機能を単一のハードウェアに統合したUTM（Unified Threat Management）はどうでしょう。確かにUTMには脅威に対してそれぞれ対策が用意されていますが、複数のエンジンが存在するので、どうしてもパフォーマンスの劣化が避けられません。ファイアウォールのスループットは超高速なのに、複数の機能をオンにしたUTMとして使うと、スループットが実に2桁も下がってしまう製品さえあります。また、機能ごとにポリシーを設定する必要もあり、制御に関してはブロックか、通過かといった二者択一でしか選べない製品も多く存在します。
アプリケーションを安全に使うためには、これまでのファイアウォールやUTMと異なった、いわばまったく発想の異なった次世代ファイアウォールが必須になってくるのです。
パロアルトネットワークス　PAシリーズは、アクセス制御とログ採取というファイアウォール本来の目的に立ち戻り、アプリケーション可視化と制御のために構造自体を設計し直した新次元のファイアウォールです。IPアドレスではなくユーザ名でトラフィック制御を行うユーザ識別、リアルタイムに脅威を防御するコンテンツ識別、ハイパフォーマンスを実現するアーキテクチャ、さらには未知のマルウェア検知、振る舞い検知などの機能を備えています。
次ページより、その仕組みと技術について、詳細にご紹介します。

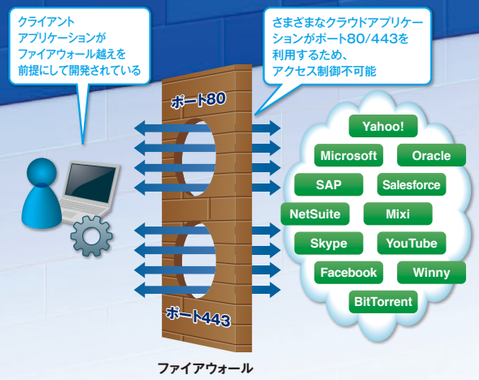


図1：多くのアプリケーションは、ポート80:HTTP/ポート443:HTTPSを利用する

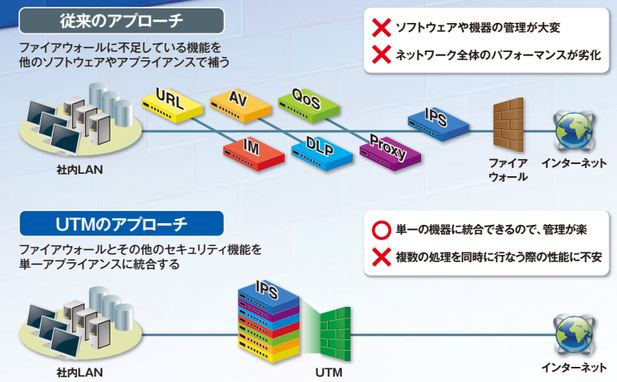


図2：従来のファイアウォールとUTMのアプローチの違い

アプリケーション、ユーザ、コンテンツの識別技術で、危険なアプリケーションの利用を制御します。

App-ID 2,500種類以上のアプリケーションを識別・制御。

パロアルトネットワークス　PAシリーズがアプリケーションを的確に検出できる秘密は、App-IDという技術をベースにしたアプリケーション解析専用のエンジンを採用しているからです。App-IDによる識別は、4つのプロセスで実施されます。①まず、すべてのトラフィックをチェック、HTTP、HTTPSなどアプリケーションプロトコルを判別。SSLが使われていれば復号化の処理を行うことも可能です。②そのプロトコルをデコーディング（解析）し、アプリケーションが偽装してトンネル化された別のプロトコルが含まれていないかを判別します。③この段階を経てからいよいよアプリケーションを定義づけるシグネチャとのマッチングを行い、特定のアプリケーションと識別します。④この定義から外れたトラフィックは、ヒューリスティック（振る舞い）検査が行われます。独自の暗号化を施すアプリケーションやP2Pはこの段階で識別されることになります。
このようにApp-IDではトラフィックの分類処理の段階で、アプリケーションを識別します。たとえば、同じポート80番を使用していても、SkypeとFacebookが違うアプリケーションであることを認識できるのです。対応アプリケーションも2,500種類を越えており、DBの更新により毎週増加しています。独自にカスタムされたアプリケーションの作成が可能です。
同様の処理はIPS（侵入防止システム）でも可能で、他社製“次世代”ファイアウォールの多くはIPSの拡張でアプリケーションの可視化と制御を行っています。しかし、IPSはあくまでファイアウォールと異なるエンジンで動いており、しかもファイアウォールのルールにマッチしたトラフィックしか精査できません。

一方PAシリーズは、以下の2点が異なります。

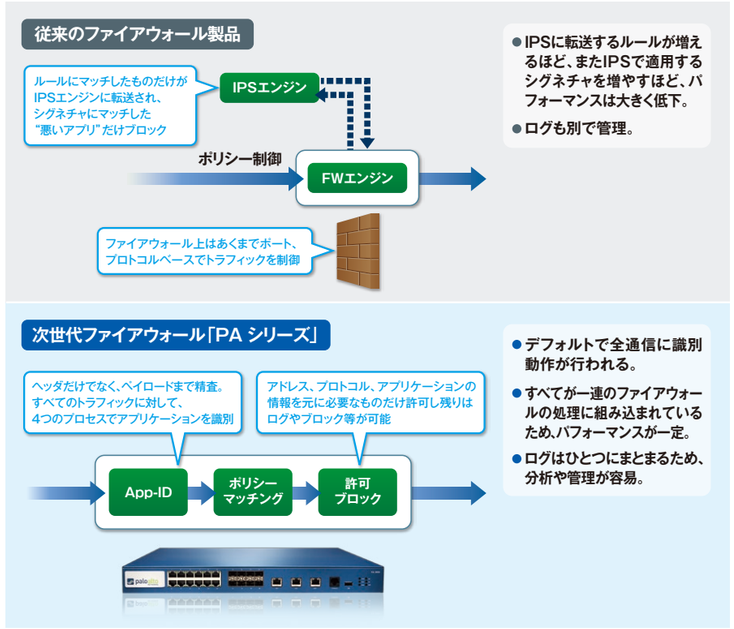
違い①アプリケーション制御するトラフィックの範囲

アプリケーション識別を実施する前提で、新規開発されたファイアウォールエンジンを搭載。ポリシー適用などのトラフィック制御とアプリ識別を同時に実施でき、ファイアウォールエンジンに到達するすべてのトラフィックをアプリケーション識別の対象としています。

違い②制御できるアプリケーション

アプリケーション識別用の全シグネチャをデフォルトで適用。そのため、シグネチャの選定などの管理作業が不要です。また、シグネチャに無いアプリケーションは「未知のアプリケーション」（unknown）として識別可能。攻撃者が新規開発したアプリケーションなど未知の脅威を把握し、必要なセキュリティ対策を実施可能です。
こうした仕組みの違いが“次世代”を名乗る大きな理由です。

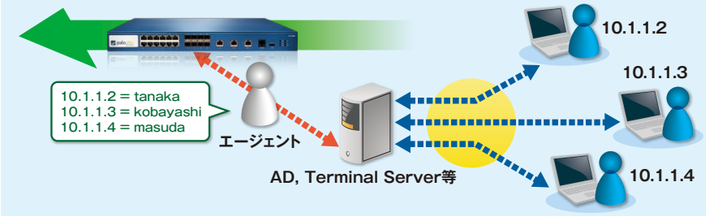
図3：既存のUTMとApp-IDでのアプリケーション可視化・制御の流れ



User-ID 誰が、どのアプリケーションを使っているか識別。

User-IDは、ユーザ名と所属グループ、IPアドレスなどのマッピングテーブルを自動的に作成することで、ユーザ識別を実現します（図4）。
具体的にはPalo Alto Networks社が開発した独自エージェントが外部ディレクトリサーバと連携し、ドメインログオンを監視したり、ユーザ端末へのポーリングを実施し、さらにはWeb認証であるキャプティブポータル機能を用いて、ユーザ情報を収集します。これらの動きによってActive DirectoryやLDAP、RADIUSサーバなどからユーザ情報を引き出すことで、IPアドレスをユーザ名とひも付けることが可能になります。これにより、誰が、どのアプリケーションを使っているか見ることができます。

図4：Active Directoryなどと連携するUser-IDによるユーザ情報の識別

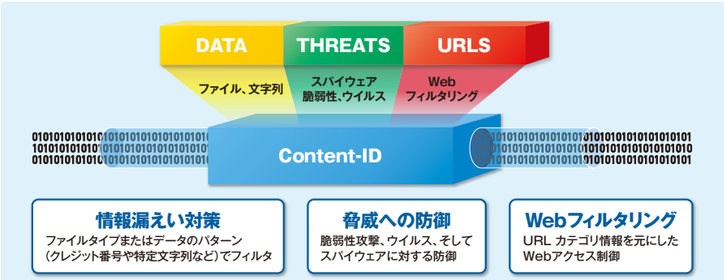


▶外部サーバからユーザ名とIPアドレスそして所属グループ情報を取得しそれを元に自動的にマッピングテーブルを作成
Active Directory、Novell eDirectory、Microsoft Terminal Server、Citrix Metaframe Presentation Server/XenApp、LDAP（Web認証+Directory内のグループ検索）、Radius（Web認証のみ）、Syslogに対応
▶ユーザまたはグループ情報を基にポリシーを適用し、ログ・レポートを生成

Content-ID コンテンツを識別し、リアルタイムに脅威を防御。

Content-IDはコンテンツを識別するもので、1つのエンジンで、情報漏えいにつながるファイルタイプや文字列（クレジットカード番号や社会保障番号等）、脆弱性を突く攻撃やウイルスなどの脅威、そしてURLの3つを同時にスキャニングし、ポリシーを適用します（図5）。
こうしたアプリケーションやユーザ、コンテンツなどの状態は、ACC（Application Control Center）という可視化ツールで一元的に把握することができます。どのようなアプリケーションが使われているか、どのようなサイトが見られているのか、どのような脅威に狙われているのか、などをランキング形式で調べることが可能です。
もちろん、ユーザを識別しているため、ファイアウォール上でユーザの名前を見ることができます。
さらには、国別ごとのトラフィックやフィルタも可能になっており、ユーザの要件にあわせて条件や表示範囲を絞り込むことができます。今までのログと異なり、ユーザとアプリケーションまで見られるのが、最大の特徴です。

図5：1つのエンジンで3つのコンテンツセキュリティを実現するContent-ID

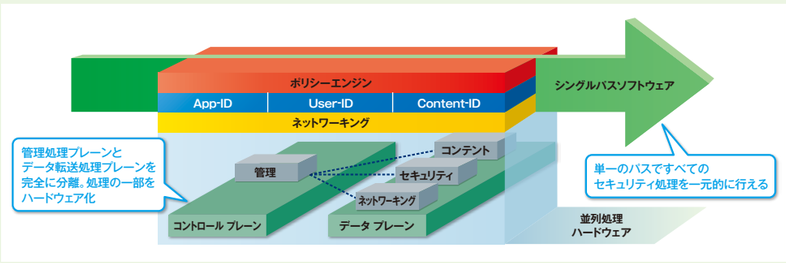


SP3アーキテクチャ

従来のUTMに比べ、高いパフォーマンスを実現。

複数のセキュリティ機能を積載したUTMのアプローチでは、すべての機能をフルに使った場合、パフォーマンスが大幅に劣化します。構造的な限界といえるでしょう。
これに対して、PAシリーズはファイアウォールの処理フローの中に、アンチウイルス、IPS、Webフィルタリングなどのためのスキャニング処理を完全に統合しています。ネットワーク層からのデータを精査し、ユーザを識別し、アプリケーションを捉え、コンテンツをチェックする。SP3（Single-Pass Parallel Processing）というアーキテクチャにより、UTMに比べてはるかに高いパフォーマンスを実現しているのです（図6）。
さらにSP3アーキテクチャをサポートするため、ハードウェア面でもいくつかの工夫を取り入れています。まず内部構造をデータ転送処理プレーン部分と管理処理プレーン部分で完全に分類。これにより、両者の依存関係が減り、いずれかの負荷に左右されない安定した性能が出せるようになりました。また、SSLやIPSecの暗号化処理やシグネチャマッチング、QoS（Quality of Service）、スイッチングなどハードウェア化できる処理は極力専用チップで実装。特定処理のボトルネックを排除するアーキテクチャを採用しています。

図6：シングルパス・並列処理を可能にしたSP3のアーキテクチャ



独自の入口・出口対策で、標的型攻撃に使用される未知のマルウェアを防ぎます。

WildFire

未知のマルウェアを検知し、侵入を防御。

WildFireは、未知のマルウェアの識別機能を提供するクラウドサービスです。Eメール上の未知のURLや、任意のアプリケーションから送られてきた未知のファイル*をPAシリーズで検出すると、仮想環境（サンドボックス）で検査し、マルウェアか否かを判定。マルウェアと判定された場合、5分程度でシグネチャを自動生成し、世界中のWildFire利用者に配信します（図7）。
これらのシグネチャは、急速に拡散するマルウェアを防ぐだけでなく、マルウェア本体内の固有の識別子を追跡することで、マルウェアの亜種を能動的に発見し、ブロックします。これにより、攻撃用に新規開発されたマルウェアも見逃すことなく対策することが可能です。

●200種類以上の振る舞いを分析。

PAシリーズで検出された未知のファイルは、WildFireの仮想環境に転送され、すべての動作と通信が観察されます。200種類を超える悪意のある動作（ホスト変更、ハッキング、セキュリティ回避の動作など）を監視し、ファイルの動作に基づいて、正体を明らかにします。
また、WildFireで検査した振る舞いの詳細情報をWeb上のWildFireポータルから閲覧することも可能です。

●ゼロデイ攻撃への対策が可能。

ゼロデイ攻撃への対策のポイントは、未知のマルウェアをいかに早く捉えて、いかに早く対策できるかです。マルウェアは発生から10時間で急速に感染拡大し24時間後には感染・拡大活動の95%が終了すると言われています。このことから未知のマルウェアが発覚してから5分程度で対策シグネチャが配信される仕組みは、ゼロデイ攻撃対策においても非常に大きなメリットであると言えます。

●WildFireにより シグネチャを最新の状態に更新。

WildFireによって自動配信された対策シグネチャは、その後アンチウイルスやアンチスパイウェア、IPSシグネチャに反映されます。また、サンドボックス内で実行されたマルウェアがアクセスしたURLやサイト等の情報はURLフィルタリングデータベース（PAN-DB）に反映されます。
このような他の機能とのデータベース連携によって未知だった脅威を既知の脅威として認識でき、セキュリティをより強固にすることができます。

●サンドボックスの管理は不要。

WildFireはクラウドサービスのため、リソースが不足する心配はありません。仮想環境のサンドボックスはメーカによって管理されるため、OSのメンテナンスも不要です。
また、WildFire機能は以下のようなApp-IDの強みにより、すべてのトラフィックから対象となる未知のファイルを発見することができます。これにより未知のファイルを抜け漏れなく検査することができます。

●すべてのトラフィックを可視化。

すべてのポートにおけるすべてのトラフィックに対して多層の識別とデコードを実施。この内容は、アプリケーションやプロトコルに変更があった場合に反映できるよう、常に管理されアップデートされます。攻撃者が特殊な方法でトラフィックをルーティングしたり、他の承認されたトラフィック内でトンネリングしたりすることによって隠れることを見抜きます。

●SSLで暗号化されたトラフィックを可視化。

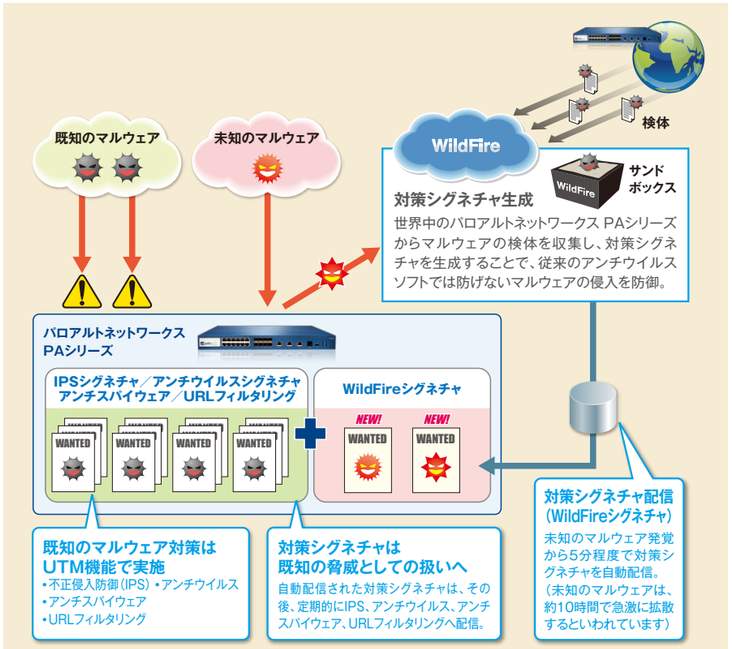
ポリシーに基づいて選択的に適用することができる、オンボックスSSL復号化機能を提供。希望するトラフィックのみを復号化し、機密を扱うトラフィックは復号化されないようにポリシーを設定します。

●未知のトラフィックを可視化。

すべてのトラフィックを確実に分類することで、未知のトラフィックまたはカスタムトラフィックの存在を明らかにできます。カスタムトラフィックは、マルウェアなどの脅威と強く相関しているため、これらを早期に発見し、自動的にポリシーを適用します。

*:EXE、DLL、PDF、apk、Microsoft Officeファイル、Javaアプレット、MacOSX実行ファイル、flash。

図7：WildFireによるマルウェア侵入防御



ボットネット検知

振る舞いを検知し、マルウェアの拡大・拡散を効果的に防止。

ボットネットとは、不正なプログラム（ボット）が組み込まれたことで、攻撃者が思いのままに操れるようになった多数のゾンビマシンで構成されたネットワークです。
PAシリーズは、このボットネットを3つのアプローチで効果的に検知・ブロックし、拡大・拡散を防ぎます。

①ボットネットの拡大を検知、ブロック。（図8）

悪意のあるWebサイトに誘導されマルウェアをダウンロードしてしまい、ボットに感染するケースがあります。この場合、アンチウイルスのシグネチャでダウンロードを検知してブロックします。
もしも社内にボットネットができて、ゾンビマシンからマルウェアサイトやC&Cサーバ*へダウンロード要求が行われた場合、URLフィルタリングで検知してブロック。ボットネットの拡大を防ぎます。

②情報漏えい等の被害発生を防止。（図9）

ボットに感染したゾンビマシンは、C&Cサーバに対して、定期的にHTTPやUnknownアプリケーションを通して、命令がないか確認を入れます。PAシリーズは、この通信をアンチスパイウェアで検知。攻撃者との通信を遮断し、被害の発生を防ぎます。

③感染が疑われる端末をリストアップして通知。（図10）

ボットに感染したゾンビマシンには特有の振る舞いがあります。PAシリーズでは、振る舞いベースのメカニズムを用いて、各種ログ（Traffic log / Threat log / URL Filtering log /Data Filtering log）を元に、トラフィックのタイプに応じた複数の判断基準によるしきい値チェックを実施。しきい値を超えた通信を行ったマシンを、ボットネットに感染した可能性があると判断します。

*:C&Cサーバ：ボットネットに指令を送り、制御の中心となるサーバ。

図8：ボットネットの拡大を検知、ブロック

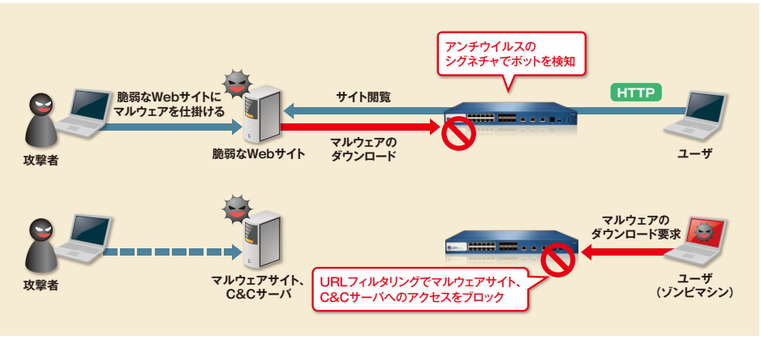


図9：情報漏えい等の被害発生を防止

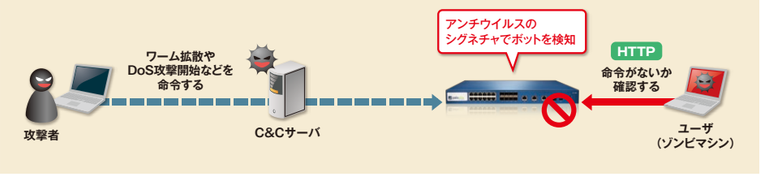
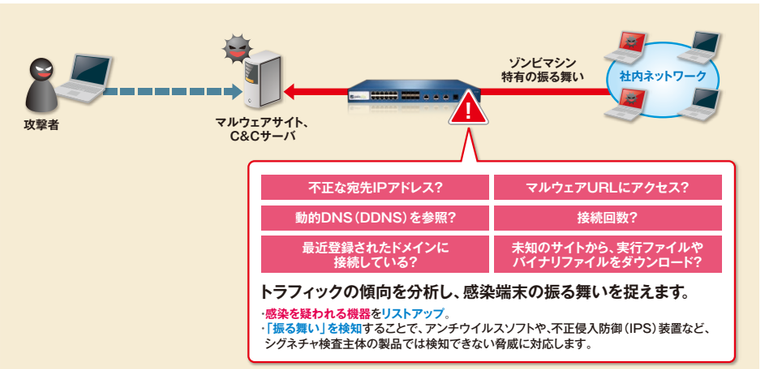


図10：感染が疑われる端末をリストアップして通知



リモート環境や仮想ネットワークにも、PAシリーズのセキュリティと可視性を適用します。

GlobalProtect

ネットワーク境界外のユーザに対しても一貫したセキュリティを確保。

スマートデバイスの普及、通信インフラの整備が進んでいます。今やビジネスは、タブレットやノートPCなどのモバイルデバイスを活用したワークスタイルが、日常的なものになってきました。そこで重要となってくるのが、ネットワーク境界外のセキュリティです。社内ネットワークと同様のセキュリティを維持し、ユーザを保護する必要があります。

GlobalProtectは、PAシリーズを適用した社内ネットワークのセキュリティを、リモートのユーザ端末にまで拡大し、かつ高速なパフォーマンスによる容易な管理を実現するものです。Palo Alto Networks社が培ってきたアプリケーションやユーザ、そしてコンテンツを可視化・制御する技術アプローチを活用しています。

●ユーザの場所に関わらず、あらゆるユーザにセキュリティポリシーを適用。（図11）

GlobalProtectは、セキュリティポリシーを適用させるため、ユーザのロケーションに関係なくエージェントを提供します。これによりPAシリーズの可視化、制御、脅威防御などの機能が、一貫してすべてのトラフィックに適用されます。

次に、OSのパッチレベルや、アンチウイルス機能が最新であるか、またはディスク暗号化が有効にされているかなどの検証を行い、エンドポイントの構成に基づいたポリシー制御を可能にします。

●GlobalProtectクライアントは最もレスポンスの早いゲートウェイに対して、セキュアなトンネルを接続。

GlobalProtectの制御機能はPAシリーズに統合されています。たとえば、ユーザのシステムが適切に構成されていなかったり、最新の状態になっていない場合は、リスクの高い、または重要なアプリケーションへのアクセスを制限するなど、適切なポリシーを適用します。アプリケーション、ユーザ、およびコンテンツに基づく制御機能が追加されると、セキュリティ部門は企業に最適なセキュリティポリシーをこれまでより柔軟に設計できるようになります。

●ロケーションや設定に応じて、最適なゲートウェイを自動的に発見。（図12）

GlobalProtectを利用すると、ユーザのロケーションや設定に応じて、最適なゲートウェイを自動的に発見。セキュアなVPN接続を確立してネットワークにアクセスできます。リモートアクセスはいずれかの認証方式（ローカルDB,RADIUS, LDAP,ActiveDirectory,Kerberos,SAML, スマートカード）を利用可能です。

●現在普及しているプラットフォームを幅広くサポート。

- Microsoft Windows XP、Vista、7、8、8.1、10
- Apple Mac OS X 10.6以降
- Apple iOS 8.0以降
- Android 4.4以降
- ChromeOS 45 以降
- Linux（VPNCまたはstrongSwanを利用）Ubuntu、CentOS

※GlobalProtect4.0.3時点

図11：ユーザの場所に関わらず、あらゆるユーザにセキュリティポリシーを適用

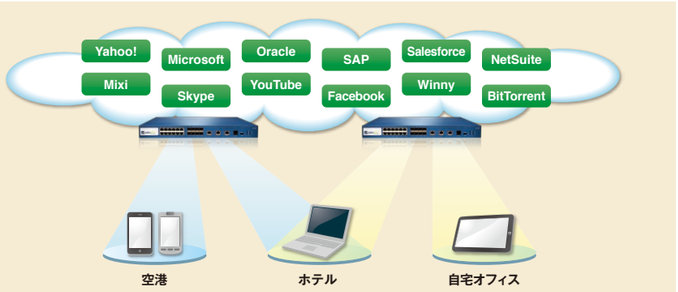
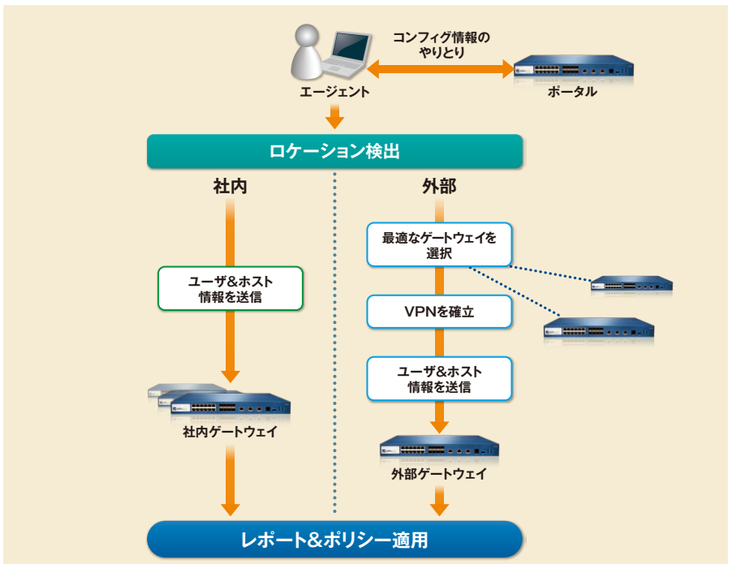


図12：ロケーションや設定に応じて、最適なゲートウェイを自動的に発見



Panorama

管理対象の幅広さと充実したログ管理/レポーティングで、分析と可視化を実現。

Panoramaは、複数台のPAシリーズで構成されたネットワーク全体を制御する統合管理製品です。ハードウェアアプライアンス（M-100）、仮想アプライアンスの2タイプが用意されています。

ネットワーク内のすべてのPAシリーズを通過するアプリケーション、ユーザ、コンテンツの情報を、デバイス単体レベル・デバイスグループレベルで収集・集約し、分析と可視化を実現。さらに、通信を制御するポリシーを統合的に管理し、適用することができます。（図13）

また、PanoramaはPAシリーズの管理画面とほとんど同じインターフェイスで利用できるため、新たに操作を覚える手間が省けます。

●仮想アプライアンス VMシリーズも管理。

VMシリーズは、App-ID、User-ID、Content-ID、WildFire、ボットネット検知、GlobalProtectといったPAシリーズが備えるファイアウォール機能を仮想マシン間の通信に対して適用します。これにより、Trust（LAN側）-Untrust（WAN側）間の通信に加えEast-West間（仮想マシン間）の通信も可視化できます。Panoramaは、PAシリーズだけでなくVMシリーズも含め最大1000台を統合管理できるため、仮想ネットワークやクラウドコンピューティング環境も安全かつ容易に運用することができます。

●ログ容量が大幅に増加。

分析と可視化を実現するために重要な情報源となるのが、収集するログであり、量も膨大になります。M-100では、この点に留意し、最大4TBのHDDを搭載。これは一例ですが、1件のログを1500Byte（1件あたりの最大容量）とすると、約26億7000万件の保存を可能にしています。これは、PA-3000シリーズ単体に比べ、約33.5倍ものボリューム。さらに仮想アプライアンス版のPanoramaなら、仮想ディスクを柔軟に追加することができ、標準の2TBから、最大24TBまでのログ容量を実現します。

●複数のログを一元的に管理。

例えば、ネットワーク構成に冗長化を施している場合、主系統がダウンして副系統に切り替わると、それぞれのログが機器ごとに保存されます。そして、分析する際は2つのログをまとめる作業が必要となります。しかし、Panoramaは、複数のログを結合して一元管理するため、管理負担を大きく軽減できます。

●メール出力を実装したレポーティング機能。（図14）

保存されたログは解析され、図表を用いたわかりやすいレポートにまとめられます。またレポーティング機能には、スケジュール機能、メール出力機能が実装され、カスタマイズしたレポートを、毎日または特定の曜日に、管理者宛にメールで送信することが可能です。管理画面にアクセスすることなく、ネットワークの状況を把握できるため、リスクの見逃しを防止できます。

図13：ログ収集とポリシー一括適用の流れ

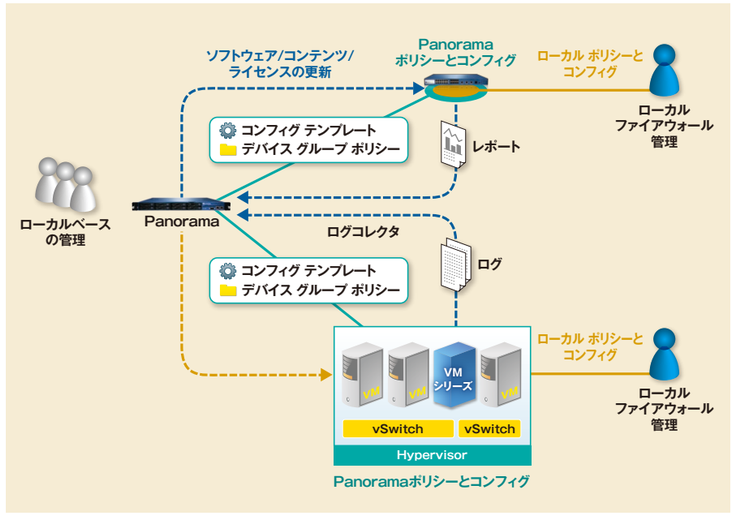
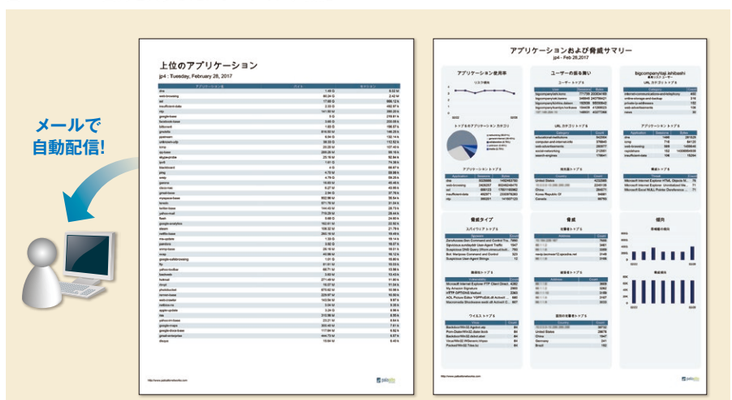


図14：メール出力を実装したレポーティング機能



導入事例

北九州市様

Green Frontier 環境モデル都市 北九州市

市民行政サービスの向上、コスト削減を目指してシステム再編を推進

名　称　北九州市役所
所在地　福岡県北九州市小倉北区城内1-1
ＵＲＬ　http://www.city.kitakyushu.lg.jp/

課題

基幹系業務システムとのセキュアかつシームレスな連携

電子自治体への取り組みを強化している北九州市。住民情報などクリティカルな情報を扱う現行の基幹系業務システムは、その他のネットワークとは物理的に独立しており、その間のデータのやり取りは職員が介在する人的作業に頼っていました。

「ここでの最大の課題は、住民記録システムや税務システム、国民年金システムといったクリティカルな情報を扱う基幹系業務システム基盤への接続において、いかに強固なセキュリティを担保するかでした。そこで、住民情報や税務、年金など基幹系業務システムの統合基盤をハイセキュアエリア、情報系システムネットワークをミドルセキュアエリアと明確に位置付け、両エリアのサーバ間通信を担う中継エリアを設けて、通信をきめ細かく制御し、二重三重のセキュリティチェックを実施することにより、セキュアな通信を実現することにしました」と語る北九州市役所　ご担当様　総務市民局情報政策室 情報ネットワーク班 藤田年男氏。

選定のポイント

抜群のコストパフォーマンスと、日立ソリューションズ(旧日立システム)がサポートを行う安心感

「当初、アプリケーション制御ということで、プロキシ型のファイアウォールである他社の製品を調べていましたが、日本国内で販売・サポートされている製品では、冗長化を考慮すると、費用対効果を期待できるものが少なかった。紹介されたPA-2020は、機能要件を十分に満たしつつ、コストパフォーマンスが抜群であったことが決め手。1カ月の検討で導入を決断しました。特にPAシリーズの機能の1つであるアプリケーションプロトコルを識別し、その解析によってアプリケーションを絞り込み、通信の許可/遮断ができることを高く評価しました。

また、『製品が登場して数年であること』『国内の導入実績が少ないこと』に対する不安は、“日立ソリューションズ(旧日立システム)”という国内の大手SIer(システムインテグレータ)が販売代理店としてサポートを行っているということで、十分に信頼できる製品だと考えました」と藤田氏。

導入効果と今後の展望

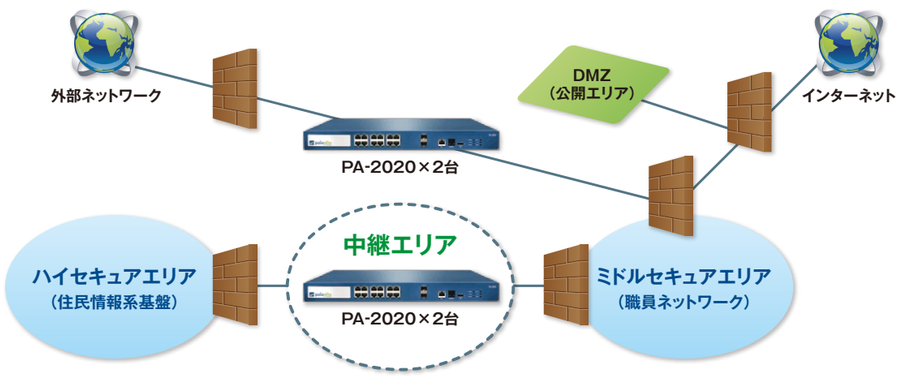
多重のセキュリティ対策を実現しつつ、市民サービスを向上

導入効果は、ハイセキュアエリアへの許可されない通信を完全に排除できることです。

「従来型のファイアウォールによるネットワーク層のチェックに加え、PAシリーズによるアプリケーション層のチェックを行うことにより、セキュアなネットワーク環境を構築できたことは、行政内部の事務の効率化を実現できると共に、市民の皆様に利便性の向上をもたらすことになるでしょう」と藤田氏は強調されます。

また、北九州市は、電子申告サービス、コンビニ納付、マルチペイメントなどのサービスを実現する際に、外部ネットワークとの境界にもPA-2020を設置する予定で、内部のサーバ間通信より多様なプロトコルがやり取りされる境界でこそ、PAシリーズのアプリケーション制御機能の真価が発揮できると期待しています。

■システム構成図



導入事例

大学共同利用機関法人 自然科学研究機構国立天文台様

NAOJ 国立天文台

アプリケーション可視化により不審な通信をブロック 組織の責任として安全なネットワーク運用を実現

名　称　大学共同利用機関法人自然科学研究機構国立天文台
所在地　東京都三鷹市大沢2-21-1
ＵＲＬ　http://www.nao.ac.jp/

課題

セキュリティ製品の統合化によるコスト削減とより安全なネットワークインフラの構築

世界最先端の観測施設を擁する日本の天文学のナショナルセンターである国立天文台は、理論・観測の両面から天文学を研究する研究所であり、大学共同利用機関として全国の研究者の共同利用を進めるとともに、国際協力の窓口として天文学および関連分野の発展のために活動しています。

国立天文台のネットワークは、主要拠点間通信はデジタル高速専用線によるネットワークが、対外ネットワークとしては学術情報ネットワーク「SINET4」に接続されており、研究の重要なインフラになっています。「研究者間の研究資源や研究成果の共有、あるいは社会に対する研究成果の発信・啓発などでネットワークは不可欠な存在。研究者の要求を満たす性能を確保しつつ、セキュリティレベルを高く保たなければなりません」。天文データセンターに所属し、情報ネットワークやネットワークセキュリティを研究する大江将史氏は、ネットワークインフラの重要性をこう述べられます。

選定のポイント

アプリケーションレベルで制御するコンセプトの価値は大きい

国立天文台のネットワークでは、ステートフルインスペクション型ファイアウォール、ステートレスファイアウォールとして利用するマルチサービスルータ、IPSなど、複数の装置を運用してきました。こうした装置を統合化し、運用・保守コストを削減するとともに、インバウンド/アウトバウンドのトラフィックを可視化してセキュリティリスクを低減することを目的にシステムを更改、そこで採用されたのが“次世代ファイアウォール”を標榜する日立ソリューションズ(旧日立システム)のPAシリーズでした。

その理由を大江氏は次のように述べます。

「ポートでなくアプリケーションで止めると言い切って製品化していることを高く評価していました。Webを許可するのであって80番ポートを許可するのではないというコンセプトの価値は大きく、脅威のシグネチャーフォーマットとストリームベースのスキャンニング、URLフィルタリングを融合することでアプリケーションの可視化・制御を実現し、インバウンド/アウトバウンドの両方の脅威を極めて高い確率で止める能力を有していると考えています。トラフィックを解析し、制御することは、さまざまなアプローチやツールを組み合わせれば可能ですが、PAシリーズは単体で実現できる高いコストパフォーマンスを持っています」

導入効果と今後の展望

アプリケーション通信に内在する脅威リスクを排除、安全なネットワーク運用を実現

検証機による1カ月のテストを経て採用されたPA-4020は、テスト環境および運用系ネットワークで約1年をかけて段階的に移行作業を行い、本格運用に入りました。

「従来のファイアウォールやIPSの判定だけでは不審なトラフィックを阻止できず、ログ解析やTCP Dumpツールを使った調査は多大な労力を必要とします。PAシリーズのアプリケーション可視化・制御機能によるリアルタイムのトラフィック検出は通信に潜在する脅威リスクを排除でき、われわれのネットワークが加害者にならないよう組織の責任として安全なネットワーク運用が可能になりました」(大江氏)。

また、従来のファイアウォールやルータ、IPSなどの機能をPA-4020に統合化したことにより、ライセンス費や保守コストの約30%削減を実現、各機器のオペレーション技術の習得にかかわるコストも削減できたという。現在、国立天文台では、他拠点とのIP-SecVPN機能をPA-4020に移管する作業を進めているが、今後は平行運用しているIPSも統合化して、さらに運用効率を高めていくそうです。

■システム構成図