

# パロアルトネットワークスについて

パロアルトネットワークス合同会社

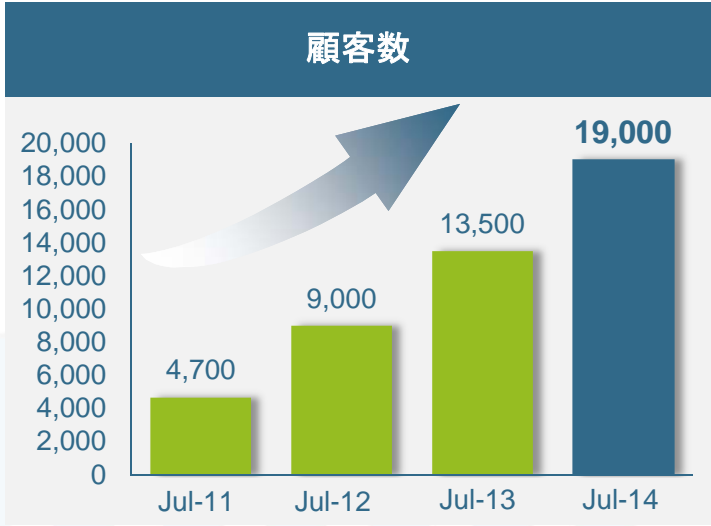
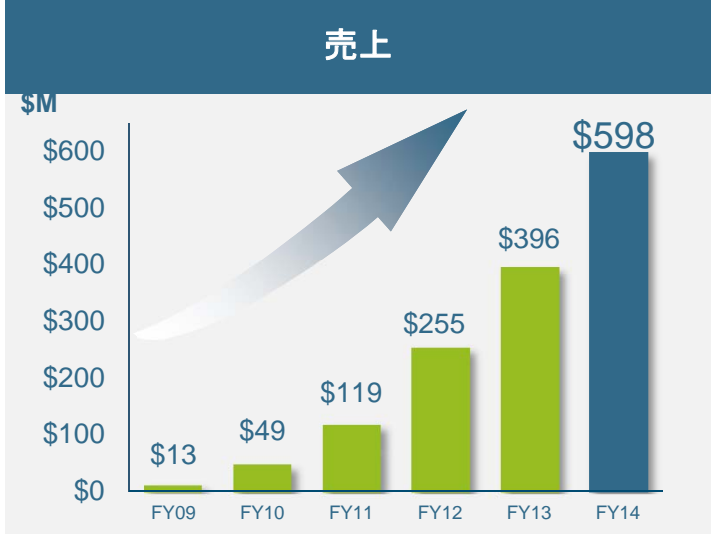
2015年 6月 18日



# パロアルトネットワークスについて

## ハイライト

- 2005年 設立  
(本社: 米国カリフォルニア州サンタクララ)  
2012年 NYSE上場
- “次世代ファイアウォール”の生みの親  
ファイアウォール市場のマーケットリーダー
- アプリケーションの安全な活用を実現  
ネットワークの幅広いセキュリティニーズに対応
- ハイエンドなお客様にも対応できる  
グローバルでの販売体制  
24時間365日のテクニカルサポート体制
- 圧倒的な技術力を持ったエンジニア集団と  
経験豊富な経営陣
- 従業員数: ワールドワイドで 1600 名以上  
世界22カ国、26拠点で事業展開



# ファイアウォール市場のマーケットリーダー

“Palo Alto Networks は引き続き競合メーカーに影響を与え、

## ファイアウォール市場自体を牽引して

おり、リーダーと評価される。

その理由は次世代ファイアウォールというデザインによる部分が多い。

市場全体が次世代ファイアウォールの方向に向かっており、

継続的に競合製品を置き換えながら、急激に売上と

## マーケットシェアを伸ばしており、

市場を席巻しているためすべてのメーカーが反応せざるをえなくなっている”

< Gartner, April 2013 >

“パロアルトネットワークスは、ガートナーの調査企業の

## 最も競争力のあるNGFWショートリストに上げ

られ、ベンダー調査では、ほとんどのベンダーが競合するベンダーと言及している。

ガートナーのクライアントは、一貫してパロアルトネットワークス

のApp-IDとIPSを高く評価し、利便性と品質も

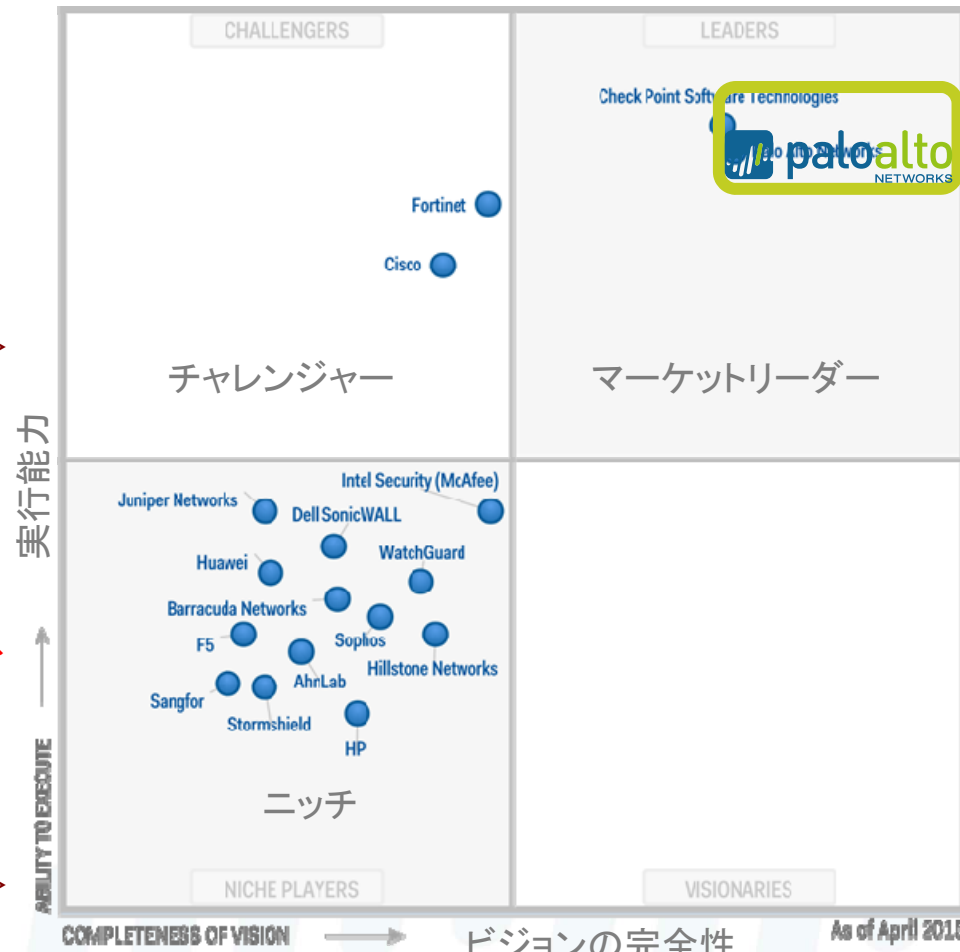
競合他社の製品よりも高いと評価している。

シンプルな料金体系は、競合他社製品と比較し調達際に有効

< Gartner, April 2014 >

エンタープライズネットワークファイアウォールの  
マジック・クアドラント

Gartner



# 脅威への対策 -CYBER THREAT ALLIANCEの設立-



<http://cyberthreatalliance.org/>

## FORTINET AND PALO ALTO NETWORKS CO-FOUND THE INDUSTRY'S FIRST CYBER DEFENSE CONSORTIUM

Palo Alto Networks Santa Clara, May 30, 2014 at 10:00 AM (NYSE: PANW), leading innovators in network security, today announced a new industry effort against cybercrime and cyber criminals.

- Better cross-industry, cross-vendor threat intelligence
- Better coordination of incident response
- Better prevention of cyber attacks using advanced threat intelligence

"At Fortinet we look forward to collaborating with Palo Alto Networks, combining our threat resources to offer customers a more comprehensive and coordinated response from their technology vendors."

"We are pleased to work with another respected industry leader, Palo Alto Networks, to coordinate a response from their technology vendors to malware and APTs," said Mark McLaughlin, Chairman of Palo Alto Networks.



English (English) | Sales: 866.320.4788 | Support | Resource Center

PRODUCTS SOLUTIONS SERVICES PARTNERS

[Home](#) > [Company](#) > [Press Releases](#) > [Palo Alto Networks Press Releases - 2014](#) >

McAfee and Symantec Join Fortinet and Palo Alto Networks as Co-founders of the Industry's First Cyber Threat Alliance

### MCAFFEE AND SYMANTEC JOIN FORTINET AND PALO ALTO NETWORKS AS CO-FOUNDERS OF THE INDUSTRY'S FIRST CYBER THREAT ALLIANCE

FOUNDATIONS OF INDUSTRY COLLABORATION UNDERSCORES

2014年5月に Fortinet 社と Cyber Defense Consortium を共同設立。9月には McAfee社,Symantec 社も加わり、クロスベンダでマルウェア情報を交換する取り組みも実施しております。

<https://www.paloaltonetworks.com/company/press/2014/mcAfee-symantec-join-fortinet-palo-alto-networks-as-cofounders-of-the-industry-first-cyber-threat-alliance.html>

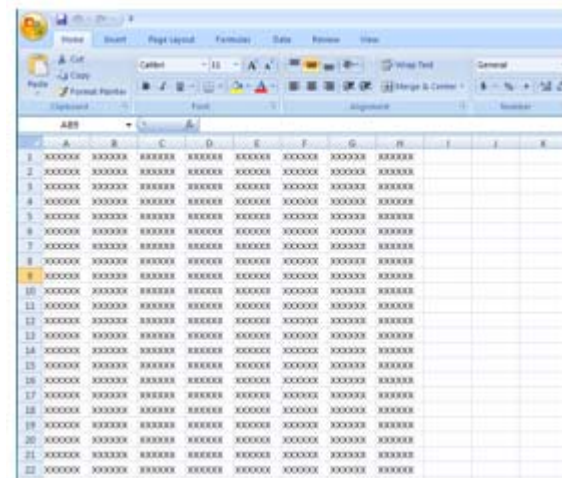
While past industry efforts have often been limited to the exchange of malware samples, this new alliance will provide more actionable threat intelligence from contributing members, including information on zero-day vulnerabilities, botnet command and control (C&C) server information, malware samples, and indicators of compromise (IOCs).

SALES: 866.320.4788 [ignite2015](#) [LEARN MORE >](#) [Privacy Policy](#) | [Legal Notices](#) | [Site Index](#) | [Subscriptions](#)

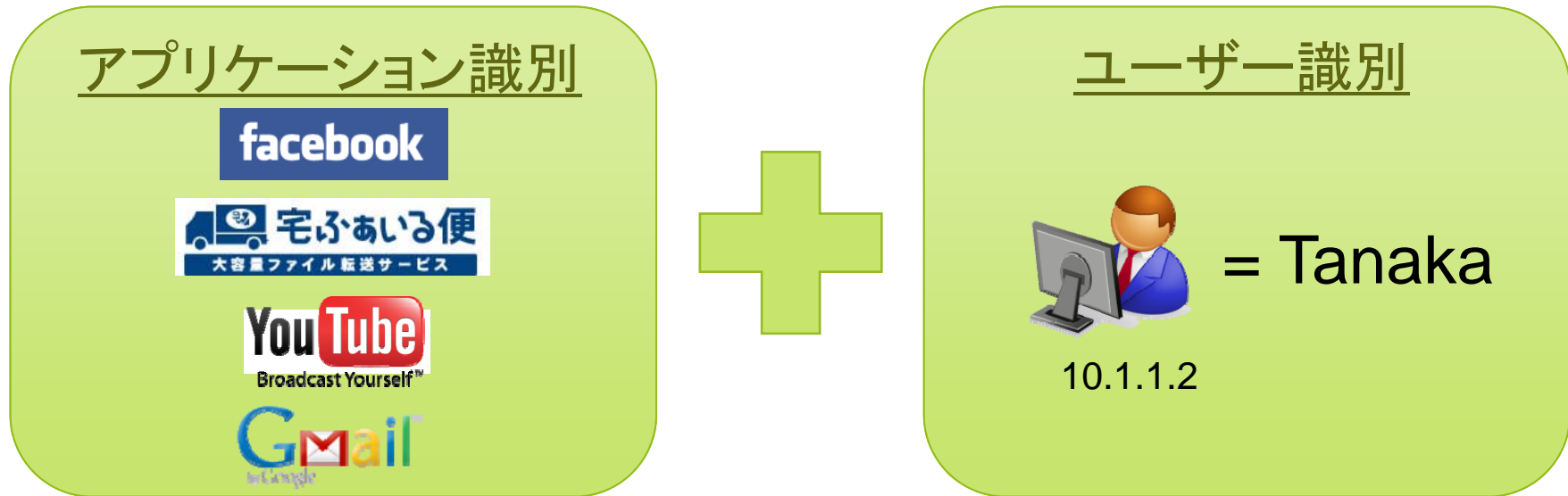


# Unit 42

- Unit 42はPalo Alto Networks内のサイバーセキュリティ研究者やの業界の専門家で構成された集団で、最新の脅威についての情報を収集・調査・分析し、詳細や対策を広く提供しています。
- 実績例 : DragonOK
  - 2015年4月、日本の企業・組織をターゲットとした中国の犯罪集団からの標的型攻撃を確認。
  - 一見無害に見えるMS Word, Excelを模したexeファイルを使用するケースが多く、今回は訃報を知らせるメールに、マルウェアを仕込んだexeファイルが添付されていた。
  - Unit 42はクラウド型サンドボックスWildFireと、WildFireにより収集される情報を元に相関分析を行うAutoFocusというサービスを利用し、「FormerFirstRAT」という新種のバックドアツールを発見。



# これからのファイアウォールに求められること①



## ■ アプリケーション識別

- パスしても良いアプリケーションとブロックしたいアプリケーションが同じポート番号を利用している場合でも、アプリケーションを識別することで、適切な制御を適用する

## ■ ユーザー識別

- 組織の中では、アプリケーションの種類によって、ある人にはブロックしたいが別の人には使わせたいという場合があり、ユーザーを識別することで利便性を確保する

## これからのファイアウォールに求められること②

- UTM(Unified Threat Management) 機能を付加したファイアウォールもありますが・・・
  - URLフィルタリング、アンチスパム、アンチウィルスなどが利用できる
- UTMのよくある問題点
  - ゼロデイアタックには対応できていない
  - ファイアウォールに機能を付加した経緯の製品では
    - UTM機能をenableにするとパフォーマンスが急激に劣化
    - ファイアウォールのログとUTMのログが別々に上がり、管理が煩雑



リアルタイム  
防御

パフォーマンス  
維持

容易な  
ログ管理


# 次世代ファイアウォール PAシリーズ

- ポート番号、プロトコル、暗号に関わらず**アプリケーションを識別し制御**
- IPアドレスに関わらず**ユーザを識別**
- 脆弱性攻撃、情報漏えい、マルウェア等の脅威に対して**リアルタイムに防御**
- 独自のシングルパスアーキテクチャで**パフォーマンスの劣化を抑え高速処理を実現**
- 全ての機能を**一つの管理画面**に集約、ユーザごと、アプリケーションごとにワンクリックで集計可能





# パロアルトネットワークス製品ラインナップ

ネットワーク ロケーション	データセンター/ クラウド	エンタープライズ境界	分散型エンタープライズ /BYOD
<p>次世代 ファイアウォール 製品群</p>	 <p>アプライアンス: PA-200, PA-500, PA-30x0, PA-50x0, PA-70x0</p> <p>仮想ソフトウェア: VM-Series VM-100,200,300,1000-HV</p>		
<p>サブスクリプション サービス</p>	<p>脅威防御</p> <p>URLフィルタリング</p> <p>Global Protect™</p> <p>WildFire™</p>		
<p>管理システム</p>	<p>Panorama および M-100 アプライアンス</p>		
<p>OS</p>	<p>PAN-OS™</p>		

# パロアルトネットワークス製品でできること

- ネットワークセキュリティを全方位でカバー
- ユニークな機能を多数搭載
- 複数のセキュリティ機能を使用しても、パフォーマンス劣化が少ない
- 潜在化しているセキュリティリスクを顕在化できる

分野	機能			
防御	ファイアウォール	ウイルス対策	スパイウェア対策	URLフィルタ
	IPS/IDS	標的型攻撃/ 未知の攻撃	ボットネット レポート	DOS攻撃
コントロール	アプリケーション 可視化/制御	ファイル/データ ブロック	SSL暗号化/復号化	QoS
運用／管理	ユーザー 識別/制御	SSL-VPN	ログの 一元管理	仮想化FW

# トラフィックの可視化・制御

- Web管理画面により、迅速かつ的確な情報可視化が可能
- 通信の種別や脅威の種類を的確に分析することが可能

The screenshot displays the Palo Alto Networks management console. The main window shows the 'Application Information' for 'facebook-base'. The interface includes a navigation menu on the left with sections like 'Application', 'URL Filtering', 'Threat Prevention', and 'Data Filtering'. The central pane provides detailed information about the application, including its name, related services, and a description. Below this, there are summary tables for 'Top Applications' and 'Top Sources'.

アプリケーション、ユーザ単位、URLフィルタ、攻撃やマルウェア検出、データフィルタリング機能などの統計情報の概要を表示する管理画面

Top Applications				
	Risk	Application	Sessions	Bytes
1	4	web-browsing	300	2,276,586
2	4	facebook-base	123	698,546
3	3	facebook-chat	46	209,009
4	4	dns	26	10,454
5	4	myspace-base	24	605,456
6	2	ntp	21	3,870
7	3	myspace-mail	12	208,662
8	4	flash	10	368,366
9	3	myspace-im	8	34,896
10	3	photobucket	4	38,730
11	1	myspace-video	4	6,214
12	4	rtmpe	2	10,786
13	4	ssl	2	16,702
14	5	http-audio	2	12,402
15	2	google-analytics	2	2,334

Top Sources			
	Source address	Source Host Name	Source User
1	10.154.2.33	engr33.net2.bigedu.local	pancademo\philip.blumste
2	10.154.12.89	engr89.net12.bigedu.local	pancademo\ginger.poppe
3	10.154.1.27	engr27.net1.bigedu.local	pancademo\ellen.cook

# 容易な運用監視 – 豊富なレポート・テイング機能

- 40種類を超える標準レポートを用意
- 必要に応じてカスタマイズレポートの生成が可能
- 確認したいレポートをPDF化してeMailで管理者へ送付可能



Category	Subcategory	Technology	Risk	Characteristic
116 business-systems	8 auth-service	41 browser-based	179 [1]	107 Vulnerabilities
129 collaboration	13 database	129 client-server	63 [2]	55 Prone to Misuse
73 general-internet	11 encrypted-tunnel	160 network-protocol	49 [3]	159 Widely used
49 media	7 erp-crm	4 peer-to-peer	17 [4]	20 Excessive Bandwidth
218 networking	18 general-business		26 [5]	103 Transfers Files
2 unknown	23 infrastructure			53 Evasive
	116 ip-protocol			46 Used by Malware
	37 management			61 Tunnels Other Apps

Name	Shared	Category	Subcategory	Risk	Technology
3pc	✓	networking	ip-protocol	[1]	network-protocol
active-directory	✓	business-systems	auth-service	[2]	client-server
activenet	✓	networking	ip-protocol	[1]	network-protocol
afp	✓	business-systems	storage-backup	[3]	client-server
altiris	✓	business-systems	management	[1]	client-server
apc-powerchute	✓	business-systems	general-business	[2]	client-server
apple-airport	✓	networking	infrastructure	[2]	network-protocol
apple-update	✓	business-systems	software-update	[3]	client-server
argus	✓	networking	ip-protocol	[1]	network-protocol
aris	✓	networking	ip-protocol	[1]	network-protocol
asproxy	✓	networking	proxy	[6]	browser-based
avamar	✓	business-systems	storage-backup	[2]	client-server
avaya-phone-ping	✓	business-systems	management	[2]	client-server
avocent	✓	networking	remote-access	[3]	client-server
avoidr	✓	networking	proxy	[6]	browser-based
backup-exec	✓	business-systems	storage-backup	[3]	client-server
backweb	✓	business-systems	erp-crm	[1]	browser-based
bbn-rcv-mon	✓	networking	ip-protocol	[1]	network-protocol
beinsync	✓	networking	remote-access	[2]	client-server

