第1章

Vyattaの全体像

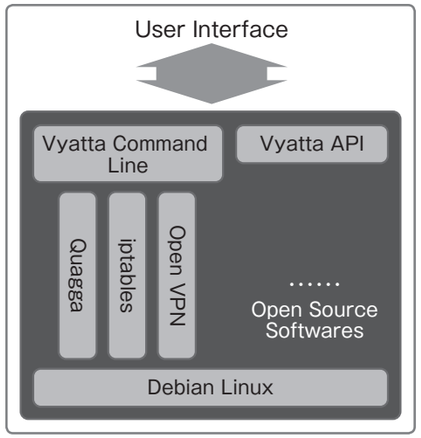
1.1 Vyattaの特徴

Vyattaはソフトウェアルータです。各種オープンソースをベースに構成されており，米国Vyatta Inc.が開発しました。本章では，このVyattaが持つ特徴と有効に活用する方法について解説していきます。

Vyattaは，Debian LinuxをベースのOS（Operating System）として，各種オープンソースソフトウェアを中心に構成した「統合化ソフトウェアルータ」です。その構成内容を**図1.1**に示します。

この図のとおり，OSにはDebian Linuxを採用し，このOS上でさまざまなオープンソースソフトウェアを稼働させています。これらのソフトウェアは，Vyatta Inc.が開発したインターフェースによって統合化されています。

Vyattaが，ユーザーに提供するインターフェースは2つあります。1つはルータの操作体系としてコマンドラインインターフェースです。もう1つはVyatta APIという独自のインターフェースです。コマンドラインインターフェースは，Juniper社[※1]のJUNOSに似ています。つまりJUNOSのルータで採用されているような階層的なコマンド体系が踏襲されています。したがってJUNOSユーザーにとって，親和性の高いユーザーインターフェースであると言えます。



▲**図1.1** Vyattaの構成

※1 Juniper社（http://www.juniper.net/）

1.1.1 Vyattaの構造

Vyattaにはルータとして動作するためにたくさんの機能がありますが，これらは多くのオープンソースソフトウェアによって支えられています。Vyattaがルータとして動作する経路制御機能を提供するために，Quagga[※2]が採用されており，インターネット経路制御で広く使われているBGP（Border Gateway Protocol）をはじめとして，OSPF（Open Shortest Path First）やRIP（Routing Information Protocol）などもサポートされています。また，ファイアウォール機能には，Linuxが標準でサポートしているiptables，VPNの機能にはOpen VPNが採用されているなど，Linuxユーザーなら誰もがご存じのオープンソースソフトウェアが取り込まれています。

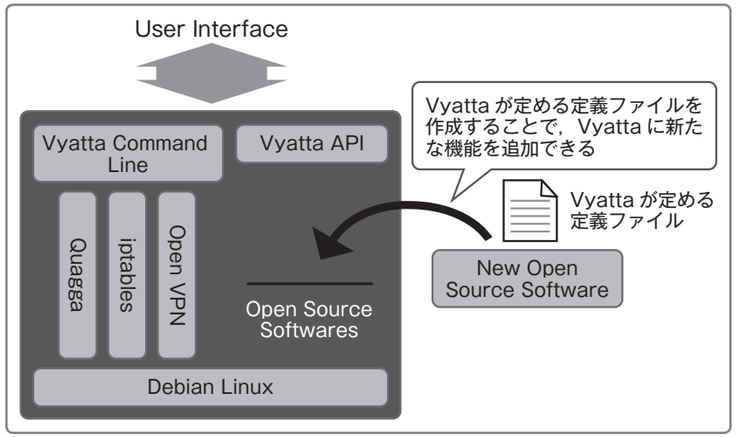
これらのオープンソースソフトウェアを使用するメリットは，単純にアプライアンス（appliance）としてのVyattaを開発することを単純化したり，開発期間を短縮したりするというだけではありません。標準的なソフトウェアによってそれぞれの機能が提供されることで，それらのソフトウェアの機能的・動作的な特徴も引き継いでいることに意味があります。

インターネットの世界では，多種多様なソフトウェアが通信プロトコルを実装し，それらの相互接続で成立しています。ここには常にインターオペラビリティ（相互接続性）の問題がつきまといます。相互接続性の確保は非常に重要です。オープンソースで流通するソフトウェアによって多くの利用者がバグ情報の共有を行いながら修正／開発していくことで行われていますので，たくさんの利用者によって培われているオープンソースソフトウェアを各機能のベースとして利用することは，利用者に対してそれぞれの安定性や機能的特徴を担保することにほかなりません。これは，多機能を成り立たせているソフトウェアルータにとって非常に価値の高いことです。

Vyattaは，このようなオープンソースソフトウェアを一定の方法によって取り込むことを標準的にサポートしていることも特徴の1つと言えます。つまり，Vyattaが提供する標準的インターフェースによって，機能追加が容易に可能であることです（**図1.2**）。

このような新たな機能のサポートを容易に行えることは，Vyattaは利用者に対してもルータという基盤を使い，新たな機能を持ったルータを作り出して進化していく可能性を提供していると言えるでしょう。

※2 Quagga（http://www.quagga.net/）



▲図1.2　Vyattaは新しい機能も容易に取り込める

1.2 ソフトウェアルータの性能と実用性

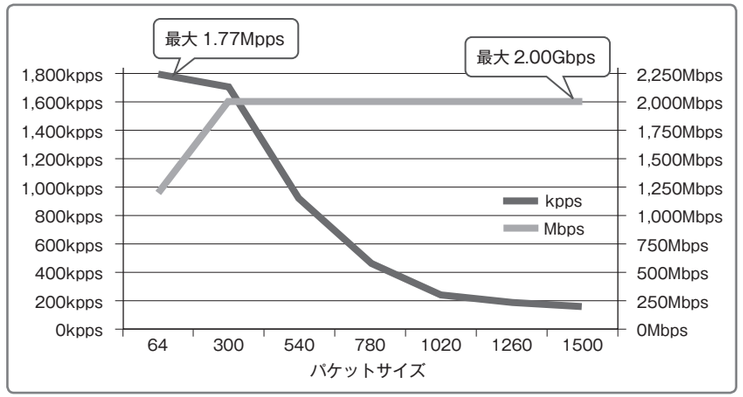
Vyattaは，ソフトウェアルータである特長を活かし，標準的なオープンソースソフトウェアによってインターオペラビリティ（相互運用性）や安定性を確保するとともに，高い機能拡張性も提供します。しかし，一方で弱点もあります。

標準的なOS上にソフトウェアだけで構成されたルータは「ソフトウェアルータ」と呼ばれています。これは，Vyattaが提供される以前からあります。古くはgatedのようなルーティングソフトウェアがあり，これは単体で提供されていました。

ソフトウェアルータは，LinuxやFreeBSDなどのOSが稼働するハードウェア上で動作するように作られているため，OSの性能に大きく依存します。そもそも，それらのOSはルータとしての性能を発揮するために設計されていません。むしろ汎用的な用途で使うことを目的としています。また，ソフトウェアウェアが動く基盤であるハードウェアも，汎用目的で作られたインテルアーキテクチャのPCです。つまり，このような汎用の環境を前提としてソフトウェアルータを稼働させなければなりません。このため，ソフト／ハードウェアの両面から見ても，ハードウェアルータ（市販されているいわゆる製品）のようにパケット転送に特化した構成になっておらず，ソフトウェアルータは，ハードウェアルータに比較して非常に性能が悪いものとみなされ，事実そのように扱われてきました。このような状況もあり，ソフトウェアルータは実験目的（経路制御や試験）で使用されることが多かったのです。

1.2.1 クラウドコンピューティング時代で躍進

しかし，2009年ごろからのクラウドコンピューティングの発展に伴い，インテルアーキテクチャで構成されるPCサーバの性能にも大きな変化が訪れました。PCサーバは，仮想コンピュータを大量に稼働させるために，マルチCPU化やマルチコア化が進みました。それとともに，CPUそのものの性能も向上し，さらにはI/Oなどの周辺デバイスの性能が飛躍的に向上しました。これにより，PCサーバ上で動く汎用的なOSでも大量のパケットを処理できるレベルに達したのです（**図1.3**）。



▲図1.3　パケットサイズと転送性能（IPv6）

図1.3には，2010年のInternet Weekで日本Vyattaユーザー会が主催した「Vyatta紹介プログラム」で発表されたIPv6パケットの処理性能について示したグラフです。性能測定には，CPUにXeon E5620 2.40GHzを搭載した標準的なインテルアーキテクチャのPCを用いており，インターフェースには1000BASE-T（送受信で2Gbpsの性能）が使用されています。これによれば，64バイトのショートパケットによる測定では1.26Mppsの性能が出ており，パケット長が540バイトを超えたあたりからは，インターフェースの最大性能である2Gbpsを記録しています。

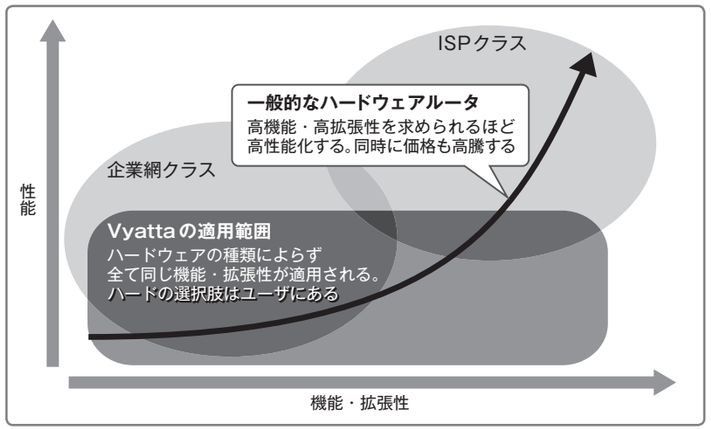
大規模なISPやデータセンターのネットワークでは，100Gbpsを超えるトラフィックの処理性能が必要となるため，このグラフで示されている2Gbps程度の処理性能では到底十分ではありません。しかし，企業網や中・小規模のISPやデータセンターのネットワークでは，1Gbps〜10Gbpsの性能が要求されていることを考えれば，ソフトウェアルータは十分な処理性能を提供すると言えます。

Vyattaは，ベースとなっているOS（Debian Linux）のカーネルパラメータをチューニングしパケット転送性能を向上させています。近年ではVyattaが稼働できるハードウェアの性能が非常に高速化したことで，実用に耐えられるルータとなったと言えます。また，最近のPCサーバでは，10Gbpsインターフェースの採用も徐々に行われてきており，Vyattaも標準的な10Gbpsインターフェースカードはすでにサポートしました。したがって，より適用範囲が広くなってきています。

1.2.2 クラウドコンピューティングでのVyattaの活用

図1.4にVyattaの活用シーンについて簡単に図示しました。ISPやデータセンターなどのISPクラスのネットワークや大規模なネットワークにおいては，100Gbpsクラスの高性能が求められます。一般的なハードウェアルータは，パケット処理性能や機能や拡張性の高さに応じて価格が高くなります。また，ISPクラスに特化したBGP等の経路制御プロトコルもサポートされています。一方，企業網クラスでは，莫大なトラフィック処理性能は要求されず，むしろファイアウォールやサポートするプロトコルの多様性，そして機能の拡張性が要求されます。

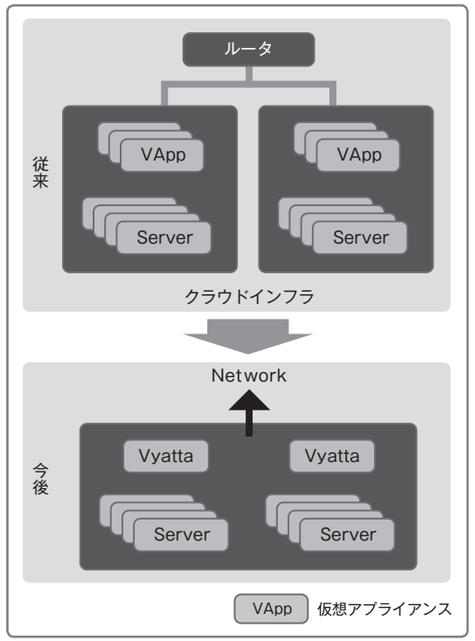
Vyattaは，プロトコルの多様性や機能の拡張性はオープンソースソフトウェアによって支えられており，十分な機能が提供されています。性能面では数Gbpsを処理範囲としていますので企業網クラスでも相応のものです。加えてISPクラスでも必要とされるBGPなどの経路制御プロトコルもサポートします。トラフィック処理性能がそれほど要求されないネットワークでは十分活用の価値があります。むしろ，Vyattaは，求める性能に応じてハードウェアを選択して，必要に応じた処理性能を利用者が構成できるというメリットもあります。



▲**図1.4** Vyattaの活用シーン

さらに，このハードウェアに依存しないルータというVyattaの特徴は，クラウドコンピューティング環境でネットワークに大きな変革をもたらします。**図1.5**を見てください。これまで，ルータはハードウェアで提供されるのが一般的でした。クラウドコンピューティング環境では，仮想サーバを仮想インフラストラクチャ上に配置し，それらの経路制御は仮想インフラストラクチャとは別に用意したハードウェアルータに依存しなくてはなりませんでした（図上部）。一方，ルータがハードウェアに依存せず標準的なインテルアーキテクチャのコンピュータ上に配置可能になると，仮想インフラストラクチャに「仮想アプライアンス」という形でルータを配置できるようになります。こうすると，仮想サーバ群とルータは物理的接続に依存せず，論理的な結合だけで構成していくことが可能です。

具体的な例を示せば，クラウドコンピューティング環境上で，クラウドユーザーは，サーバコンポーネントやロードバランサコンポーネントなどの仮想アプライアンスをネットワーク上の機能ブロックとして論理的に配置しネットワークを構成します。このコンポーネントのラインナップに「ルータ」が登場します。つまり，クラウドコンピューティング環境で複雑なネットワークが構成できるようになることで，ユーザーはより柔軟なネットワークを構成できるようになるのです。



▲**図1.5** ルータの仮想化によるネットワークの変化

1.3 Vyattaの種類と機能

このように高い拡張性と十分な性能を提供してくれるVyattaですが，サポートする機能によって主に3つの製品に分類されます。Vyattaの製品群について**表1.1**に示します。

製品は，「Vyatta Core」，「Vyatta Subscription Edition」そして「Vyatta PLUS」の3つに分かれます。これらは表にあるようにサポートする機能やVyatta社がサポートするサポートプログラムの種類によって分かれています。

Vyatta Coreは，主にSOHOや試験環境で用いる場合での使用を目的としており，無償で提供されています。このため，Vyatta社の正式なサポートは受けられません。

Vyatta Subscription Edition（Vyatta SE）は有償で提供されますが，Vyatta Coreがサポートする範囲を包含し，さらに複数ルータで設定を同期する「Configuration Sync」機能等の便利な機能や多くのセキュリティ機能を提供するとともに，Vyatta社の正式なサポートを受けることが可能になります。

Vyatta PLUSでは，さらに高度なIPS/IDSなどの機能がサポートされるなど，より高度な利用シーンに対応しています。

▼**表1.1** Vyatta製品群（出展：http://www.vyatta.com/downloads/index.php）

Edition	Primary Features	Support Model	Customer Usage
CORE	Basic Routing Stateful Firewall IPSec and SSL-Based OpenVPN WAN Load Balancing	Unsupported Community Only Vyatta University	Test/Development/SOHO Router Firewall
SE	Vyatta Remote Access API Configuration Synch IPv6 Ready Certified WAN Device Drivers DSL/T1/T3 VPN Client Auto-Configuration TACACS+ Integrated Hardware Appliances Optimized Virtual Machines Riverbed RSP Ready	Vyatta Supported (up to 24x7) Pro Services Quick Start Config Upgrade Service Vyatta University	Enterprise/xSP/Cloud Router Firewall VPN IPS Web Filter and more
PLUS	VyattaGuard Web Filtering Vyatta Snort VRT IDS/IPS Rules	Vyatta Supported (up to 24x7) Pro Services Quick Start Config	Enterprise/xSP/Cloud Threat Mitigation HR Compliance Productivity Managing Bandwidth Threat Mitigation

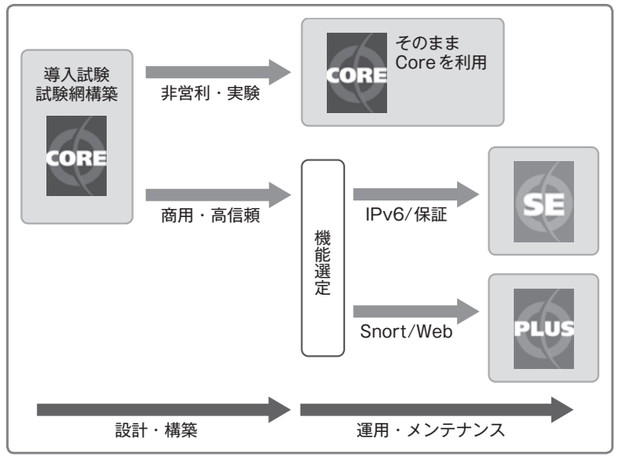
1.3.1 Vyatta導入までの流れの例

Vyatta Coreは，ルーティング機能とVyattaの基本的な機能を無償で提供してくれますが，これにより利用者は多くの利便性を享受できます。ネットワーク構築のための流れの例を**図1.6**に示しました。

このように，設計・試験網構築の段階では，サービスの実現性の検証などが主な作業となるため一般に多くのコストはかけられませんが，Vyattaの使用でコストをかけずに実施・実現できます。その後，サービスが非営利や実験で継続的に利用される場合は，コスト削減のためそのままVyatta Coreを使い続けることもできます。一方，商用サービスへ展開したりする場合は，万が一の場合に備えVyattaからのサポートを受けられるようにしておく必要があります。また，さらに多くの機能を使いたい場合も出てきます。このような場合には，Vyatta SEやVyatta PLUS等を利用シーンに合わせてライセンス購入すればよいわけです。

有償版への切り替えは，設定等はそのまま使用可能です。したがってマイグレーション（システムの移行）も非常に簡単なこともメリットです。

表1.2にVyatta Subscription Edition Version 6.1の機能リストを示します。これらの中のほとんどはVyatta Coreでもサポートされている機能ですが，「Vyatta Remote Access API」など一部の機能がSubscription Editionの特有機能として提供されています。



▲**図1.6** Vyatta導入までの流れの例

▼表 1.2　Vyatta Subscription Edition Version6.1 の機能リスト（出展：http://www.vyatta.com/downloads/datasheets/vyatta_software_datasheet.pdf）

Subscription Edition Software Version 6.1			
IPv4 / IPv6 Routing	≫ BGPv4, BGPv6 ≫ OSPFv2, OSPFv3*	≫ RIPv2 ≫ Static Routes	≫ IPv6 Policy ≫ IPv6 SLAAC
IP Address Management	≫ Static ≫ DHCP Server ≫ DHCP Client	≫ DHCP Relay ≫ Dynamic DNS ≫ DNS Forwarding	≫ DHCPv6 Server ≫ DHCPv6 Client ≫ DHCPv6 Relay
Encapsulations	≫ Ethernet ≫ 802.1Q VLANs ≫ PPP	≫ PPPoE ≫ IP in IP ≫ Frame Relay	≫ MLPPP ≫ HDLC ≫ GRE
Firewall	≫ Stateful Inspection Firewall ≫ Zone-based Firewall ≫ P2P Filtering	≫ IPv6 Firewalling ≫ Time-based Firewall Rules ≫ Rate Limiting	≫ ICMP Type Filtering ≫ Stateful Failover
Tunneling / VPN	≫ SSL-based OpenVPN ≫ Site to Site VPN (IPSec) ≫ Remote VPN (PPTP, L2TP, IPSec)	≫ OpenVPN Client Auto-Configuration ≫ Layer 2 Bridging over GRE ≫ Layer 2 Bridging over OpenVPN	
Additional Security	≫ Network Address Translation ≫ Sourcefire VRT Intrusion Prevention ≫ VyattaGuard Web Filtering	≫ DES, 3DES, AES Encryption ≫ MD5 and SHA-1 Authentication ≫ RSA, Diffie Helman Key Mgmt	≫ NAT Traversal ≫ Role based access control
WAN / LAN Device Drivers	≫ WAN Device Drivers - ADSL, T1, T3 ≫ Intel 10/100Mbps - 10Gbps	≫ IEEE 802.11 wireless ≫ Drivers in 2.6.31 Linux Kernel	≫ Synchronous Serial - V.35, X.21, RS-422, EIA530
Performance Optimization	≫ WAN Link Load Balancing ≫ Ethernet Link Bonding ≫ Web Caching	≫ MLPPP ≫ ECMP ≫ Bandwidth Management	
QoS Policies	≫ Priority Queuing ≫ Network Emulator ≫ Round Robin	≫ Random / Weighted Random ≫ Classful Queuing ≫ Ethernet Header Matching	≫ VLAN Tag ≫ IPv6 Address ≫ Port Mirroring
High Availability	≫ Stateful Firewall / NAT Failover ≫ VRRP ≫ HA Clustering	≫ Configuration Replication ≫ RAID 1	≫ IPSec VPN Clustering ≫ Protocol Fault Isolation
Administration & Authentication	≫ Integrated CLI ≫ Web GUI ≫ Vyatta Remote Access API	≫ Telnet ≫ SSHv2 / SSH Public Key ≫ Binary Image Install	≫ RADIUS ≫ TACACS+* ≫ Single Configuration File
Diagnostics & Logging	≫ tcpdump ≫ Wireshark Packet Capture ≫ BGP MD5 Support	≫ Serial Loopback Commands ≫ Netflow / sFlow ≫ LLDP	≫ Syslog ≫ SNMPv2c ≫ SNMP for IPv6

1.4 Vyattaの入手と情報収集

これらのVyatta製品の入手にはいくつかの方法があります。

Vyatta Coreについては，VyattaのWebページからダウンロードできます。詳しい方法については「第3章　クイックスタートガイド」で解説します。Vyatta SEおよびVyatta PLUSは有償製品です。日本の正規代理店またはVyatta Associate Partnerから購入できます。日本の正規代理店，Associate Partnerについては，VyattaのWebページの問い合わせフォームを利用するのがよいでしょう（なお，日本では「株式会社まほろば工房」がVyatta Associate Partnerです。日本語で問い合わせたい場合は便利です）。

また，日本では「日本Vyattaユーザー会」が2010年6月に発足しました。日本Vyattaユーザー会では，Vyatta Coreだけでなく，Vyatta製品全般について使用方法やトラブルシューティングについて情報交換を行っているほか，定期的に会合を行っています。メーリングリスト登録で簡単に参加できますので，まずはこちらで質問してみてもよいでしょう。

- Vyattaホームページ（http://www.vyatta.com/）
- 日本Vyattaユーザー会（http://www.vyatta-users.jp/）
- 株式会社まほろば工房（http://www.ate-mahoroba.jp/）