

ネットワークとは そもそも何？

ここで学ぶこと

- ・ ノード
- ・ リンク
- ・ フロー

ネットワーク (network) という言葉は、コンピューターを使ったもの以外でも使われる言葉です。それは **(ノード node)** と **リンク (link)** からなり、**フロー (flow)** があるものです。

1 ネットワークとは

ネットワークとは、「net」(網)と「work」(働き)が組み合わさった用語で、「モノ」が網状につながっており、そのつながったモノの間で何かは流れてやりとりされるもののことを指します。

つながるモノは**ノード**、ノードをつなげるものを**リンク**、ノードとノードをつなぐリンクで、ノード間で何かは流れることを**フロー**と呼びます。

たとえば、都市というノードを道路というリンクでつなぎ、荷物がフローする「物流ネットワーク」、人というノードを会話というリンクでつなぎ、情報がフローされる「連絡ネットワーク」などが、イメージとしてわかりやすいでしょう。

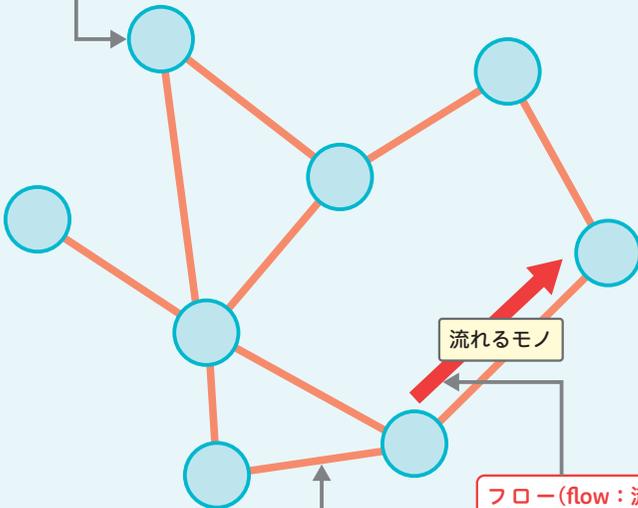
重要用語 ノード

ノードは、ネットワークでの接続点や端を指します。コンピューターネットワークでは、ネットワーク機器(ルーターやハブなど)やコンピューターのことです。

重要用語 フロー

フローは「流れ」のことで、リンク上をノードからノードへ向かって「データが流れること」を表します。

ノード (node : 節)
ネットワーク上のモノ



流れるモノ

リンク (link : 線)
ノードとノードをつなぐ

フロー (flow : 流れ)
ノードとノード間の
リンク上で何かを運
んで流れる

インターネットとは？

ここで学ぶこと

- インターネット
- 自律システム
- インターネットサービスプロバイダー

もっとも有名なWANとして、世界中のネットワークをつなげたインターネットがあります。インターネットに接続するということは、**インターネットサービスプロバイダー (ISP : Internet Service Provider)** との接続を行うということになります。

1 インターネットは世界中のLANやWANをつなげたもの

インターネット (the Internet) は世界最大のWANで、統一したルールと技術を用いた、世界中のWANやLANを相互につなげたネットワークです。インターネットには、WANやLANなどのネットワークの集合体である**自律システム (AS : Autonomous System)** が複数あります。これらがつながり合うことで、インターネットという1つの大きなWANを作り出しています。

重要用語 自律システム (AS)

いくつものネットワークを持つ組織(大学・企業・プロバイダーなど)のことで、インターネットの運用単位がASです。

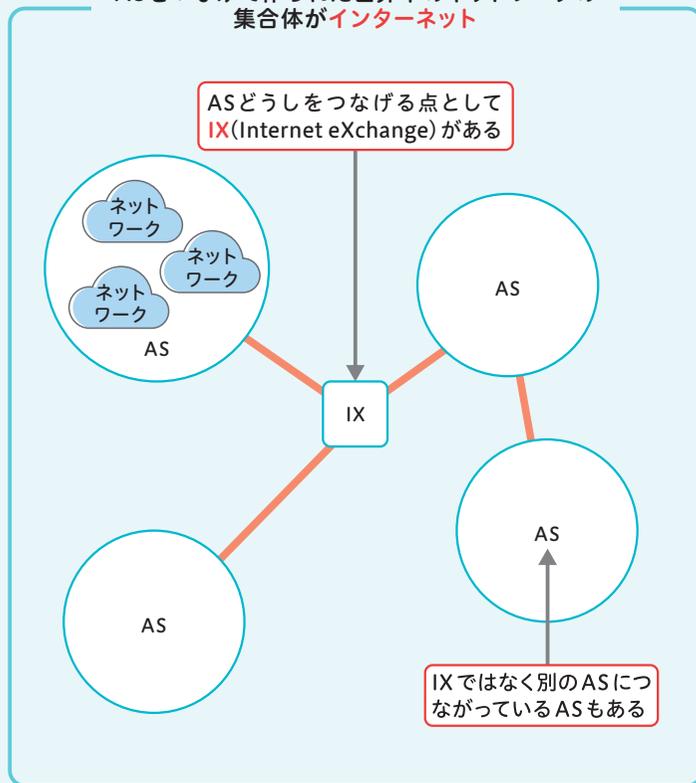
重要用語 IX(Internet eXchange)

ASどうしを相互につなげるためには多くの回線が必要となり、コストがかかるため、複数の回線をまとめてつなげるためにIXが使われています。インターネットの事実上のバックボーンとなっています。

補足 インターネットの記述

インターネットを「internet」と記述する場合は、「ネットワーク間接続」という意味になります。固有名詞のインターネットは「the」を付けたり、「INTERNET」など大文字を使います。

ASをつなげて作られた世界中のネットワークの集合体がインターネット



LAN回線からインターネットまでの流れ

ここで学ぶこと

- プロバイダー
- ルーティング
- 経路

自宅のブロードバンドルーターは、契約したWAN回線につながっています。このWAN回線を経由して、プロバイダーまでデータが届くことになります。その後、プロバイダーのルーターは**あて先IPアドレス**を確認し、**ルーティングを実施**します。

1 データをプロバイダーへ送信する

ブロードバンドルーターは、届いたデータ（フレーム）であて先として指定されているMACアドレスが、**ブロードバンドルーターのMACアドレスと一致するかどうか**を確認します。

その後、契約している回線、たとえば光回線のような回線にデータを送り出しますが、その際に、**プロバイダーとの通信**が行われます。

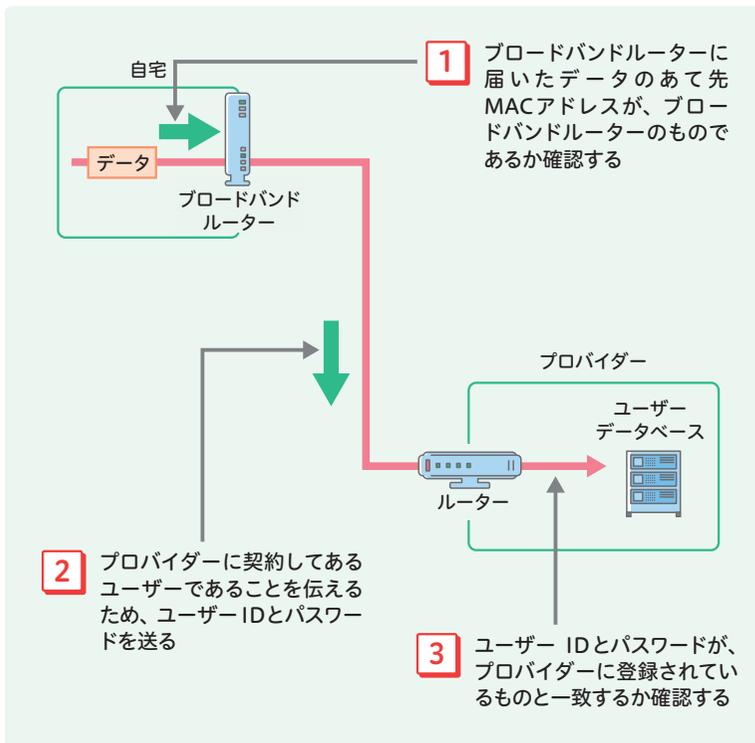
ブロードバンドルーターに設定されているプロバイダーのユーザーIDとパスワードが、プロバイダーに登録されているものと一致しているかを確認し、正しいユーザーIDとパスワードなら指定したプロバイダーへ接続されます。プロバイダーに接続されると、**データがプロバイダーの持つルーターへと送信**されます。

補足 MACアドレスの確認

LANのようなマルチアクセスネットワークでは、すべての機器が送信するデータがルーターに届くため、自分あてかどうかをMACアドレスで確認します。

2

データはネットワークをどう流れる？



補足 ユーザーIDとパスワードの確認

プロバイダーへの接続には、プロバイダーとの契約時に与えられたユーザーIDとパスワードが必要です。ブロードバンドルーターにはこれを設定する必要があります。

なお、ユーザーIDとパスワードによる認証は、プロバイダーとの接続を確立する際に行われ、接続が切断されない限り、データの送受信のたびに行う必要はありません。

ネットワークモデルとは？

ここで学ぶこと

- ベンダー
- スタンドアード
- ネットワークモデル

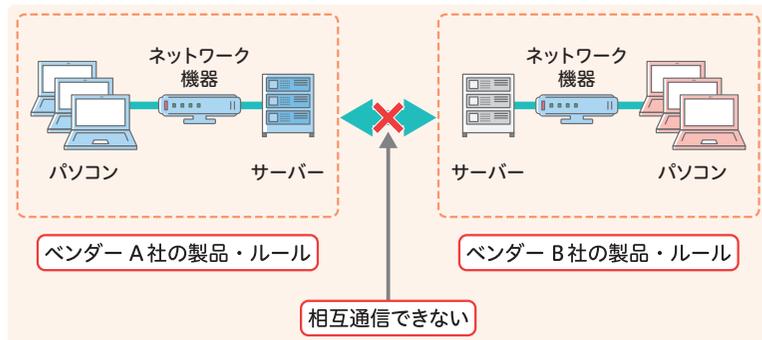
ネットワークは物理的なパソコンやサーバー、ネットワーク機器の構成だけで成り立っているわけではありません。それらも含めた**ネットワークを構成する「モデル」**が存在しています。この章ではそのモデルについて説明します。

1 かつてのネットワークはベンダーごとの独自規格

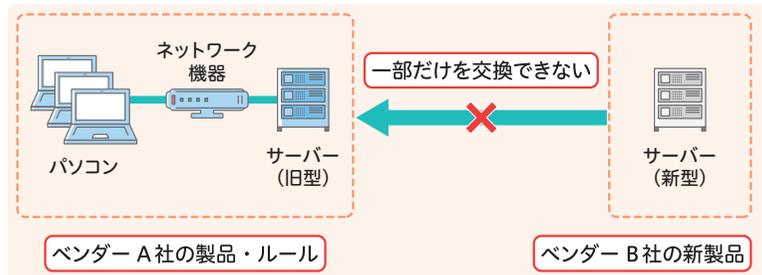
かつてのネットワークは、多くの場合は1社の**ベンダー**（製造メーカー、販売会社のこと）によって独自規格で作られた製品や、通信ルールなどでネットワークが構築されていました。そのため、一度構築したネットワークには他ベンダーの機器を使用することができない（互換性がまったくない）状態となっていました。

この状態では、ユーザー側がもし新たに他ベンダーの機器を導入したいと思っても、ネットワークごと一斉入れ替えが必要となるか、2つのネットワークを並列で使用する必要がありました。これは、ユーザー側の不利益がとて大きい状態といえます。

異なるベンダーの機器間では相互通信できない



製品の交換なども自由にできない



重要用語 互換性

互換性とは、ある製品などに対して置き換えが可能になる性質のことです。たとえばA社の製品に使われているA社のケーブルを、B社のケーブルに置き換えても問題なく動作する場合、「B社のケーブルはA社のケーブルに対し互換性がある」と表現します。

重要用語 ベンダーロックイン

複数のメーカー（ベンダー）で構成せず、1つのベンダーの製品や規格で構成されたシステムで、他社への切り替えが困難になる状況のことを、ベンダーロックインといいます。

プロトコルとは？

ここで学ぶこと

- プロトコル
- プロトコルスイート
- TCP/IPプロトコルスイート

OSI参照モデルでは、それぞれの層ごとにすべき機能と手順があります。この機能と手順を実行するために必要なルールのことを、**プロトコル** (protocol) と呼びます。プロトコルは、通信上のすべての機器で**同一のものを使う必要**があります。

1 プロトコルは通信の機能を果たすためのルール

OSI参照モデルは、通信全体のモデルを7つの層に分割しています。それぞれの層には**機能と手順を実行するためのルール**があり、これを**プロトコル**と呼びます。

プロトコルは、具体的にいくつかの物事を決めています。たとえば、データを送る際に付加する通信に必要なデータの中身や、そのデータの構造を決めています。ほかにもデータをやりとりする際の手順(たとえば、「Aというデータを受信したらBというデータを返す」など)を決めています。

補足 プロトコルの意味

本来のプロトコルは、規定や議定書などの意味で使われます。外交儀礼とその手順、外交の議定書などで使われる言葉です。

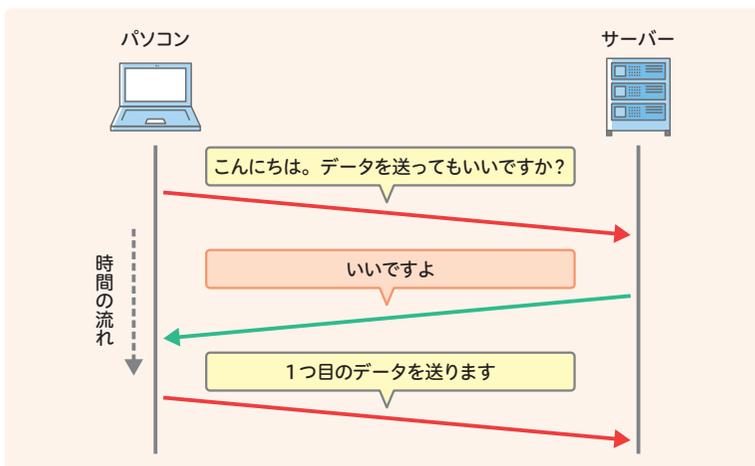
3

ネットワークモデルを知ろう

「データの中身や付加する情報」を決めている



「データをやりとりする際の手順」を決めている



補足 RETR

図にあるRETRは、FTP (File Transfer Protocol) で使用される命令です。ファイルのダウンロード命令がRETR、アップロード命令がSTORとなります。

IPv6とは？

ここで学ぶこと

- IPv4アドレスの枯渇
- IPv6アドレス
- ヘッダーの簡略化

IPv6は現在IPv4に置き換わりつつある、新たなIPのバージョンです。IPv4が抱えていた問題を解決し、新たな技術に対応するバージョンとして策定され、実際に運用されています。

1 IPv6はIPv4アドレスの枯渇を解決する

IPv4の問題点の1つは、**アドレスの数**です。IPv4のアドレス（IPv4アドレス）は32ビットで、約43億個しかありません。インターネットの急速な普及により、以前から不足することが予測されており、実際に2015年にインターネットで使用可能なIPv4アドレスはすべて使われ、**枯渇**しました。

これに対し、IPv6アドレスは**128ビット**あり、利用できるアドレスの数は32ビットの4乗ですので、43億の4乗個という膨大な数になります。これにより、パソコンだけでなく、さまざまな機器にもIPアドレスが利用できるようになります。

重要用語 グローバルルーティングプレフィックス

グローバルルーティングプレフィックスとは、IPv6アドレスの先頭48ビットの部分で、世界の中での管理団体（日本ならばAPNIC）と、アドレスを提供するプロバイダーを示す部分です。

4

IPv4アドレスの表記と構成



- 前半はネットワークを示す**ネットワーク番号**
- 後半はホストを示す**ホスト番号**
- ネットワーク番号のビット数は、サブネットマスクや**プレフィックス長**で明示

重要用語 サブネットID

サブネットIDとは、IPv4アドレスのサブネット番号の役割を果たす部分です。IPv6アドレスでは16ビットあります。

IPv6アドレスの表記



重要用語 インターフェイスID

インターフェイスIDとは、IPv4アドレスのホスト番号の役割を果たす部分です。通常はMACアドレス48ビットを、EUI-64という変換を使って64ビットにして使います。

IPv6アドレスの構成



前半64ビットはネットワークを識別する部分、後半64ビットは機器を識別する部分

データベースサーバーの働きを知ろう

ここで学ぶこと

- データベース
- データベース管理システム
- レプリケーション

データベースとは、アプリケーションなどで**使用するデータを集合させたもの**で、データの管理や操作には、データベース管理システムが使われます。多くの場合は、データベースサーバーで運用し、ネットワークを介して共有されます。

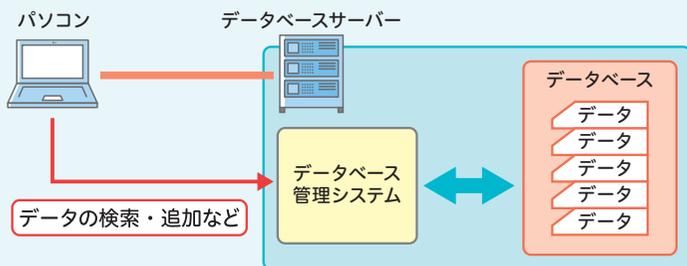
1 データベースサーバーはデータの保持と管理を行う

検索サーバー、ネットショッピング、ネットゲームなどのネット上のサービスは、ほとんどがユーザーや顧客のデータを保持することを前提としています。そのデータは、**データベース**という形で保持され、その運用には**データベース管理システム**と、**データベースサーバー**が欠かせません。

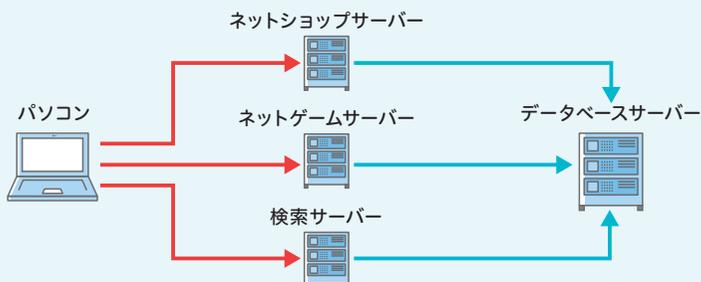
データベースサーバーは、データベースとその管理システムのアプリケーションを持っています。そして、管理システムが持つネットワーク機能により、データに対する検索、閲覧、追加、削除、修正などの処理をネットワーク経由で受け持つことができます。

補足 代表的なデータベース管理システム

代表的なデータベース管理システム(データベースサーバー)としては、OracleのOracle Database、MicrosoftのSQL ServerやAccess、IBMのDB2などがあります。



データベースサーバーは、データを格納する**データベース**と、格納されたデータを管理し、検索や追加や修正などの要求に応じる**データベース管理システム**を持つ



数多くのサーバーの後ろでデータを管理するためにデータベースサーバーが使われている

重要用語 SQL

データベース操作言語の1つで、現在のデータベース管理システムでもっともよく使われています。SQLを使うことで、データベースのデータの参照や検索、追加、削除などを行います。

ネットワークの管理と運用とは？

ここで学ぶこと

- 24 × 365
- 5つの管理業務
- ネットワーク管理者

ネットワークそのものが必要ということはあまりなく、たとえば業務アプリケーションによるコストダウンのように、何かを実現するためのものがネットワークです。ネットワークはそのための**インフラとして常に動作している必要があります**。

1 合言葉は「24時間×365日」

業務などのインフラとして、ネットワークは常に正しく動作していることが必要とされます。それはよく**24 × 365**というキーワードで表されます。つまり、24時間 × 365日、常にいつでも、という意味です。

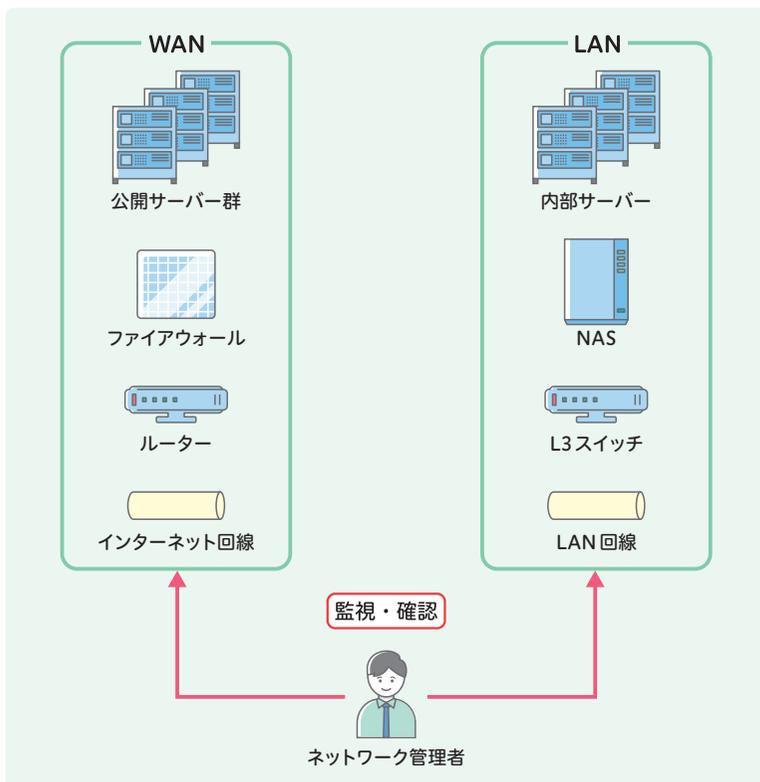
しかし、ネットワークを構築したからといって、それをそのままにしておいては24 × 365は実現できません。必要なのは、ネットワークの状態の**監視・確認**を行い、機器のアップデートや障害対応、セキュリティインシデントの防止などを行う「**管理**」と「**運用**」を常に行っていくことです。

補足 24×365

24 × 365 = 8,760時間となります。もし99.99%稼動したとしても、52分は停止することになります。よって、常に稼動しつづけることがネットワーク管理で重要となります。

6

ネットワークの管理と運用を学ぼう



重要用語 セキュリティインシデント

インシデントとは「出来事」「事件」などの意味があり、セキュリティインシデントはセキュリティを侵害する事象、ウイルス感染や不正侵入などのことを指します。

セキュリティとは？

ここで学ぶこと

- CIA
- リスク
- 脅威とぜい弱性

コンピューターのセキュリティでは、**脅威**という言葉がよく使われます。脅威はコンピューターシステムに対して何らかの「損害」を引き起こす「要因」のことで、悪意の有無や内部/外部は関係ありません。これを防ぐには**情報セキュリティ対策**が必要です。

1 セキュリティのCIAとは

「セキュリティ (情報セキュリティ)」という言葉が示すのは、「コンピューターシステムの**CIAを維持する**」ことです。CIAとは「機密性 (C: Confidentiality)」「完全性 (I: Integrity)」「可用性 (A: Availability)」の頭文字をとったものです。

機密性は「**情報の漏えいなどが無い**」こと、完全性とは「**情報が完全である**」こと、つまり改ざんや消去が勝手にされないことです。そして、可用性とは「**情報が必要なときに使える**」こと、つまり障害などが発生していないことを意味します。

7

ネットワークのセキュリティを強化しよう

情報セキュリティのCIA

- Confidentiality (機密性)
= 情報を閲覧・使用できるのは、許可のある人だけであること



許可がある人だけが情報を利用できるように制御する

- Integrity (完全性)
= 情報が改ざんされていない、消去や破壊もされていないこと



情報の改ざんや消去、破壊ができないように制御する

- Availability (可用性)
= 必要なときに情報が利用できること



バックアップや多重化などで障害に備える

補足 機密性

機密性については、Section 02の侵入対策やSection 07の流出対策、Section 08の暗号化の説明なども参照してください。

補足 完全性

完全性については、Section 09のデジタル署名の説明も参照してください。

補足 可用性

可用性については、第6章のネットワーク運用のうち、障害対応やバックアップの部分を参照してください。

SDN / OpenFlowとは？

ここで学ぶこと

- データセンター
- SDN
- OpenFlow

サーバー仮想化やネットワーク仮想化のときに、ネットワーク機器を1つ1つ設定していったら、その利点を失うことにもなりかねません。そこで、**ネットワーク機器の構成や機能をソフトウェアだけで設定できるようにするSDN**を使用することがあります。

1 SDN / OpenFlowとは

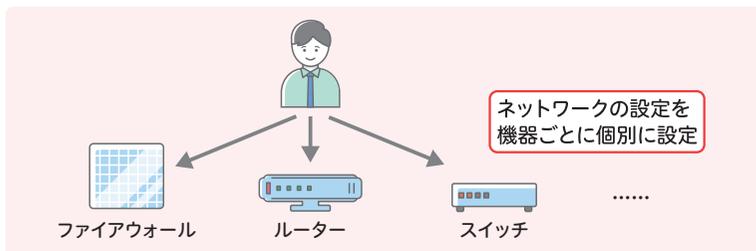
データセンターのように、サーバーを多く収容し、それぞれの企業に合わせたネットワーク構成を持つ必要がある場所では、企業ごとのネットワーク構成や、サーバーの高可用性を維持する必要があります。しかし、ネットワーク機器をそれに合わせて1つ1つ設定しては時間的に間に合わず、手間もかかります。

そこで生まれた、ネットワークの構成や機能などをソフトウェアで一括で設定できるようにする、という考え方がSDN (Software Defined Network) です。**SDN**により、ネットワークの構成が自動化され、構成の変更にも柔軟に対応できるようになります。SDNを実現するための技術として挙げられるのが**OpenFlow**です。

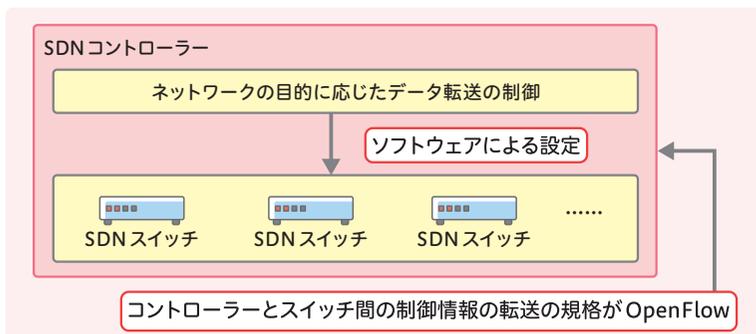
補足 SDN
コントローラー

SDNの制御を統合して行うソフトウェアのことを、SDNコントローラーといいます。1台または少数のコントローラーから、ネットワーク上の多くのSDNスイッチを一括して制御することができます。

従来



SDN



重要用語 SDNスイッチ

SDNスイッチは通常のスイッチとは異なり、スイッチ、ルーター、ファイアウォール、負分散装置など、さまざまなネットワーク機器の機能を持つスイッチです。SDNコントローラーからの指示により、使用する機能を定めることができます。