03 サーバーの役割

サーバーの概要が理解できたところで、次はサーバーが担う具体的な役割と、代表的なサーバーについて解説していきます。

サーバーは今や生活に欠かせない大切なインフラ

サーバーは、ネットワークを介してクライアントに様々なサービスを提供します。普段の生活を考えてみてください。ニュースを見る時も、調べ事をする時も、買い物をする時も、PCやスマートフォンなどのクライアントからサーバーにアクセスすれば事足りてしまうのではないでしょうか。そうです、我々が日々利用するこれらのサービスを裏で支えているのがサーバーなのです。今やサーバーは水道や電気のように、**私たちの生活には欠かせないインフラとなっているのです**。

■サーバーも生活に欠かせない大切なインフラ

サーバーの役割は提供するサービスによってたくさんある

1-01 のネットショッピングの例にある図で、改めてサーバーの種類について確認してみましょう。

■表　代表的なサーバー

サーバー	内容
Webサーバー	ショッピングサイトのWebページを提供する
データベースサーバー	顧客データや商品データなどの大切なデータを管理する
認証サーバー	利用者（ユーザー）を識別し、認証する
監視サーバー	必要なサービスが提供できているかサーバーを監視する

このように、**提供するサービスによって様々な役割を持つサーバーが存在するのです**。なお、1台のサーバーで複数のサーバー機能を持つことも可能です。

■提供するサービスに応じて、サーバーには役割がある

まとめ

- **提供するサービスの種類によって様々なサーバーが存在する**
- **1台のサーバーで複数のサービスを提供することもある**

06 サーバーとネットワーク

ネットワークを活用することで、複数のサーバーやクライアントをつなぎ、それらのコンピュータ間でデータを送ったり、資源を共有したりすることができます。ここでは、サーバーとネットワークについて解説します。

情報のやりとりはネットワークが支えている

情報化社会にはネットワークが必要不可欠です。ネットワークを利用することで、コンピュータは互いに情報のやりとりをしたり、資源を共有したりすることができます。そして、**ネットワークの中で最も代表的なものが「インターネット」です**。

サーバーは、インターネットにより、世界中のコンピュータやモバイル端末、他のサーバーなどと通信を行うことができます。つまり、インターネットというネットワークにより、サーバーは世界中のあらゆるユーザーに様々なサービスを提供することが可能となっているのです。

ちなみに、**インターネットのように広い地域に敷設されたネットワークをWAN（Wide Area Network）と呼びます。これに対し、企業内などの狭い範囲に敷設されたネットワークをLAN（Local Area Network）と呼びます**。

サーバーとネットワークの基本構成

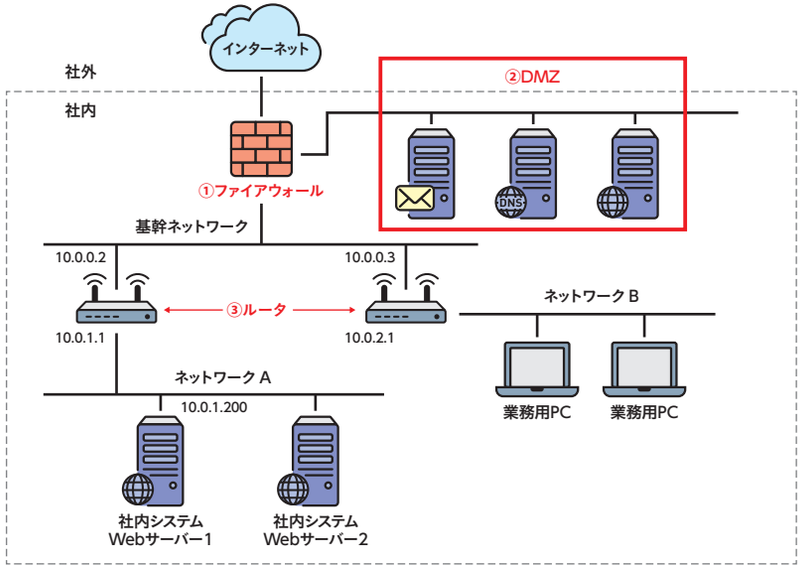
企業における社内LAN、インターネット、各種サーバーの基本構成は図の通りです。

①ファイアウォール
ファイアウォールと呼ばれる専用のネットワーク機器を利用して、インターネットからの不正侵入を防ぎます。

②DMZ
DMZ(DeMilitarized Zone非武装地帯)と呼ばれる特別なネットワーク領域を構築し、インターネットと内部のネットワークを直接接続しないようにします。

③ルーター
ルーターと呼ばれる機器を利用することで、LANをさらにいくつかのネットワークに分割することができます。

■ネットワークの基本構成



まとめ

- ネットワークを活用することで、サーバーはより様々なサービスを提供できる
- 企業におけるサーバーとネットワークの基本構成は、社内LAN、DMZ、インターネットであり、ファイアウォールやルーターなどのネットワーク機器で実現する

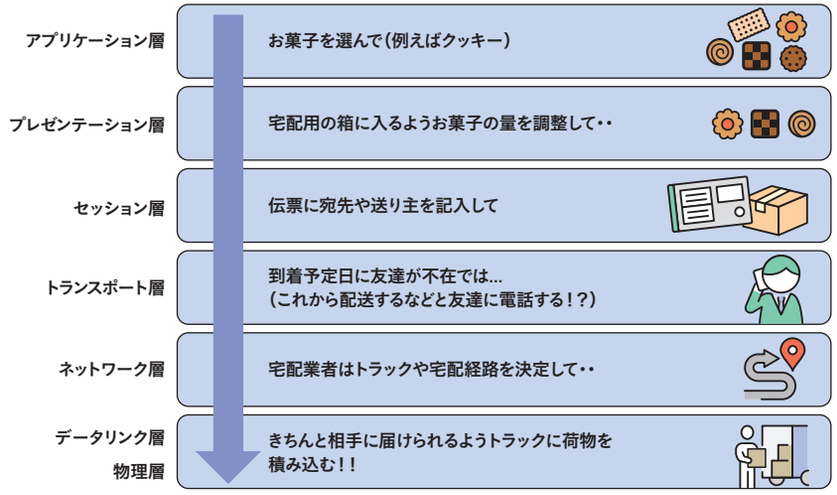
03 OSI参照モデルにおけるデータ転送

2-02で紹介したOSI参照モデルについて、ここでは、同モデルを宅配便に例えてデータ転送の仕組みをイメージしていきましょう。

OSI参照モデルを宅配便に置き換える

2-02では、OSI参照モデルを宅配便に例えましたが、OSI参照モデルを宅配便に対応させたイメージが以下の図です。

■OSI参照モデルを宅配便として考える



OSI参照モデルにおけるデータ転送の仕組み

データを配送するときも、宅配便の流れとほぼ同様です。アプリケーション層で管理されていた様々なデータは、次の図のように階層ごとに必要な処理を行い、最終的には物理層で電気信号に変換されネットワーク上を流れます。

上の階層は下の階層の機能（サービス）を利用し、逆に下の階層は上の階層に機能を提供する仕組みとなっています。

アプリケーション層では、アプリケーションサービスを提供します。プレゼンテーション層ではデータを配送するためにデータ形式を汎用的なものに変換します。セッション層は一連のセッションの管理を行い、トランスポート層は高品質なデータ伝送を実現するための仕組みを持ちます。ネットワーク層で伝送経路を選択し、パケットを別のネットワークに伝送、データリンク層では同じネットワーク内での伝送を実現します。最終的には、物理層が電気信号である0と1のデータに変換し、ケーブル内に伝送されます。

■宅配便とデータ転送のモデルは一緒

まとめ

- **第1～7層はそれぞれ役割があり、隣接する層同士でデータをやりとりする**

10 サーバーコンテナ

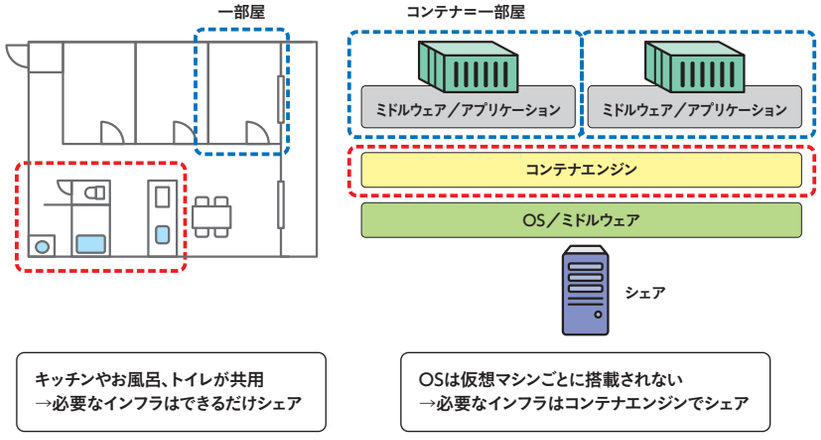
3-07～3-09では、サーバー仮想化について解説してきました。ここでは、サーバー自体を仮想化するのではなく、利用するアプリケーションだけを仮想化するサーバーコンテナという方法について紹介します。

シェアハウスのメリットを考えてみよう

住居に例えるなら、サーバーコンテナはシェアハウスタイプであると言えます。

シェアハウスでは、キッチンやお風呂などの共用部分については自分専用として利用することはできませんが、掃除の手間やリフォーム時のコストなどを考えると、住民がやらなければいけないことは少ないでしょう。

■サーバーコンテナはシェアハウスのイメージ



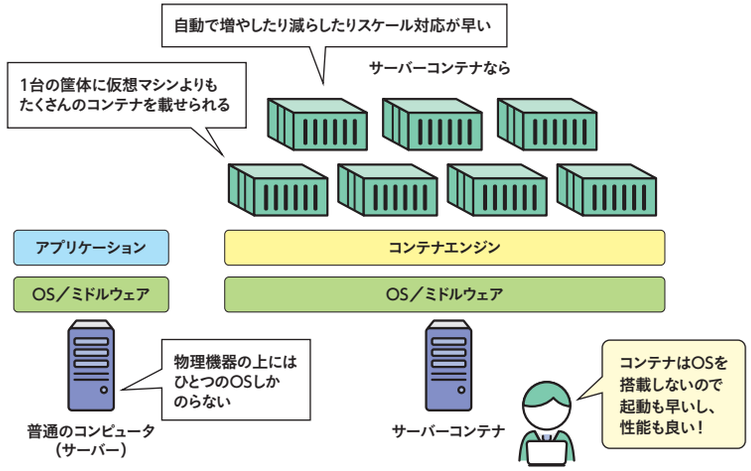
OSは同じで良いけれど、ミドルやアプリは別々に準備したい

従来のサーバー仮想化は、一台のホストの中に複数台の仮想マシンを構築することで、コスト削減、運用の効率化などを実現しました。仮想マシンはOS、ミドルウェア、アプリケーションをすべて搭載していて、マシン自体を仮想化していました。例えば違うOSを使いたい場合、OSレベルで設定をカスタマイズしたい場合などはとても有益な方法といえます。

しかし、「OSは同じで良いけれどミドルウェアやアプリケーションは独立した環境を準備したい」という場合があります。このような場合、仮想マシンにOSを搭載せず、ミドルウェアやアプリケーションだけをひとかたまりとして、仮想化することができます。このような技術を**サーバーコンテナ**といいます。

サーバーコンテナでも、サーバー仮想化で得られるコスト削減や運用の効率化などのメリットを同じように享受することができます。サーバー仮想化との違いは、ゲストにOSを搭載するかどうか、という点です。ちなみに、サーバーコンテナの場合、「仮想マシン」にあたるかたまりのことを「**コンテナ**」と呼びます。

■サーバーコンテナのメリット



まとめ

- **物理サーバーのOS上でコンテナエンジンが動作し、その上にコンテナを構築するタイプの仮想環境をコンテナ仮想化という**

05 DNSと名前解決

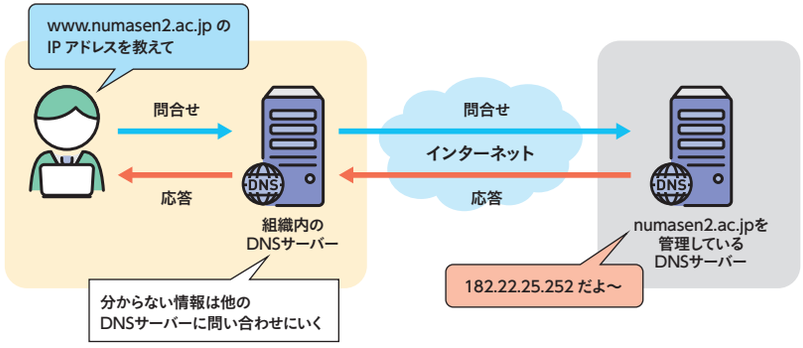
Webサーバーへの通信はURL（ドメイン）で行われますが、DNSと呼ばれるサーバーが名前解決をすることで、URLをIPアドレスに変換して通信が可能となるのです。

名前はIPアドレスに変換されて、通信が始まる

クライアントがWebサイトにアクセスする流れを考えてみます。

クライアントが「https://www.numasen2.ac.jp」にアクセスするために、まずはこの名前のIPアドレスがいくつなのか、組織内のDNSサーバーに問い合わせます。なお、**DNS「Domain Name Service」とは、URLや電子メールのアドレスをIPアドレスに変換する仕組みやサーバー**のことを意味します。

■DNSサーバーは分からない情報を別のサーバーに問い合わせる



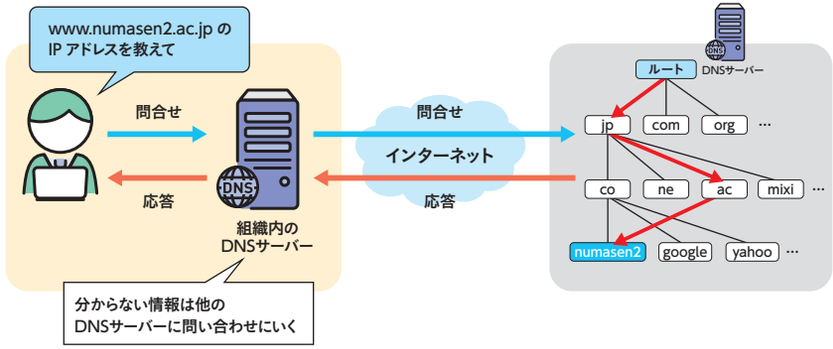
DNSサーバーには、インターネット上のすべての情報が設定されているわけではないので、わからないIPアドレスもあるでしょう。その場合には、図で示したように、「numasen2.ac.jp」を管理している別のDNSサーバーに問い合わせを行い、名前解決を試みます。

名前解決を行う仕組み

DNSサーバーはどのように「numasen2.ac.jp」を管理するサーバーを探すのかもう少し詳しく解説します。

名前解決ができなかった組織内のDNSサーバーは、今度は自身がクライアントとなって最上位のドメインを管理するDNSサーバーに問い合わせを行います。最上位のドメインを管理するサーバーを**ルートDNS**といいます。このルートDNSに、ドメインのピリオドで区切られた一番右の部分、「numasen2.ac.jp」であれば「jp」を管理するDNSサーバーの情報を訪ねます。次に教えてもらったサーバーに対して、「ac.jp」を管理するサーバーを訪ねます。これを繰り返して、「numasen2.ac.jp」を管理するサーバーを見つけるのです。

■名前解決を行う仕組み



まとめ

- **IPアドレスとURLの紐づけを管理することを名前解決という**
- **DNSサーバーは名前解決のサービスを提供するサーバーである**

02 DNS キャッシュサーバー

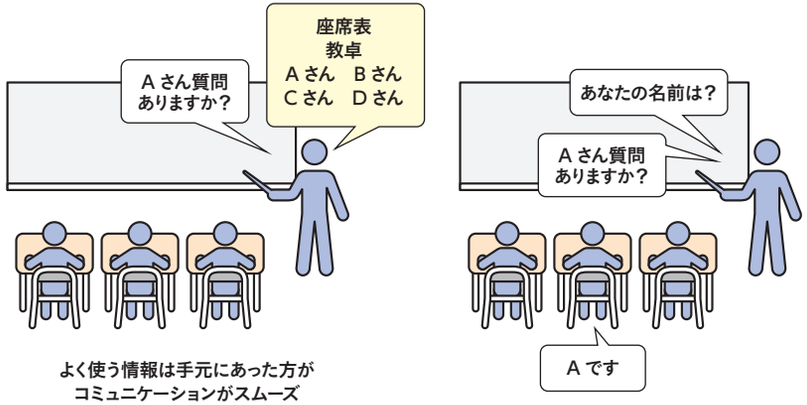
DNSキャッシュサーバーはクライアントからのDNS問合せに対し、DNSサーバーの「メモ帳」として情報取得を代行するサービスです。

メモ帳を使うときってどんなとき

突然ですが、あなたは教員だとします。学生20名に対して授業を行う際に、教卓に座席表を準備し、どの学生がどこに座っているかわかるようにすると、学生とコミュニケーションをとるのに便利でしょう。座席表には学生について最低限必要な情報、氏名を書いておきます。

座席表を準備せずに、いちいち学生に氏名を聞いて、話しかけても良いわけですが、座席表を準備するのはなぜでしょうか。よく使う情報、この場合だと氏名を座席表としてすぐ手元に置いておくことで、直接学生に尋ねるよりも、スムーズにコミュニケーションが行えます。

■よく使う情報は手元のメモに

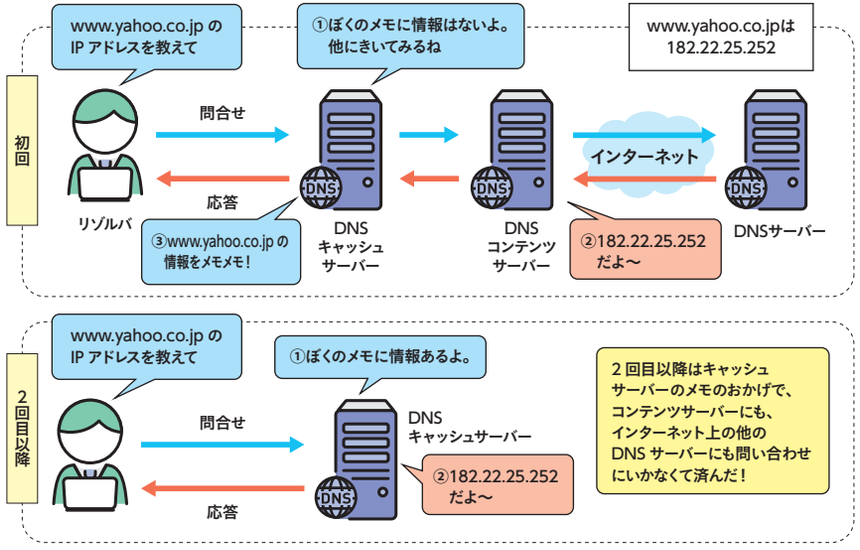


DNSキャッシュサーバーとは

DNSとは、4-05で説明した通りURLや電子メールのアドレスをIPアドレスに変換する仕組みのことで、DNSサーバーには、情報そのものを持つDNSコンテンツサーバーと、問い合わせた情報のメモだけを持つDNSキャッシュサーバーがあることを説明しました。DNSキャッシュサーバーは、**DNSコンテンツサーバーに問合せ（DNSクエリ）を実行して目的の情報を取得します**。そしてその**取得した情報を内部のデータベースにメモとして保持**します。

上記の例の通り、よく使う情報や一度利用した情報は手元にメモとして保持することで、名前解決レスポンス向上や、DNSクエリの通信量を低減することが期待できます。

■DNSキャッシュサーバーの仕組み



まとめ

- **DNSキャッシュサーバーは、DNSコンテンツサーバーに問い合わせた名前解決の情報のメモを持つサーバーである**

04 セキュリティゾーン

同等のセキュリティレベルをもつネットワークのことをセキュリティゾーンといいます。セキュリティゾーンにはコントロールできるゾーンとコントロールできないゾーンがあり、その考え方について解説します。

セキュリティゾーンとは

ネットワークは、インターネット上のネットワーク（WAN）と企業などの構内ネットワーク(LAN)に分けられます。LANは3章で解説した通り、DMZと内部ネットワークに分けられることが大半です。そして、分けたネットワークのことをそれぞれ、セキュリティゾーンと呼びます。**セキュリティゾーンはファイアウォールによって区切られ、同じセキュリティゾーン内のコンピュータは同じセキュリティレベル**といえます。

セキュリティゾーンごとのセキュリティレベルの違いは以下の通りです。インターネット上のネットワークは、コントロールできないため、セキュリティレベルが一番低いといえます。

■インターネット上のネットワーク

ファイアウォールの外側に位置し、非コントロールゾーンとも呼ばれ、最もセキュリティレベルが低く信頼できないゾーンです。

■DMZ

インターネット上のネットワークと内部ネットワークとの間に配置され、内部ネットワークから見ると、セキュリティリスクを抑制させる役割を果たすゾーンです。

■社内ネットワーク

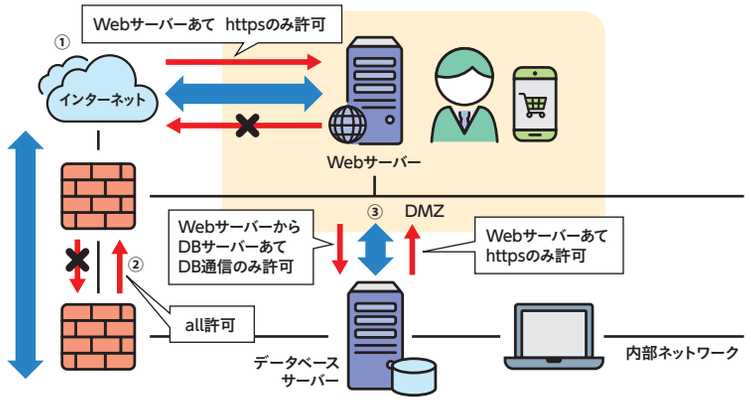
ファイアウォールの内側に配置する最もセキュリティレベルの高いゾーンです。データベースサーバーやファイルサーバーなど機密情報を扱うサーバーを配置します。

セキュリティゾーンにおけるパケットフィルタリングの設定

セキュリティゾーンを実現するためのパケットフィルタリング設定について、ネットショッピングを例に考えてみたいと思います。Webサーバーを DMZ、データベースサーバーを内部セグメントに配置することとします。

以下の図において、①インターネット⇔DMZ、②インターネット⇔内部ネットワーク、③DMZ⇔内部ネットワークの3つにわけて考えます。基本的には許可する通信を個別に記載し、それ以外の設定はすべて拒否するというような設定を入れます。

■パケットフィルタリングの設定例イメージ



まとめ

- **同じセキュリティゾーン内のコンピュータは同じセキュリティレベルである**
- **インターネット、DMZ、内部ネットワークの3構成を標準とし、パケットフィルタで通信制限をかける**

02 チーミング／ボンディング

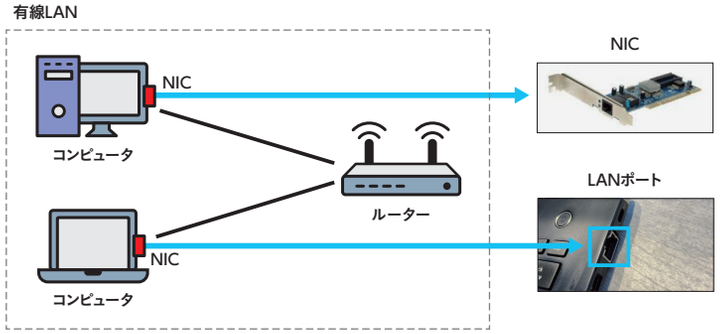
7-01で冗長化技術について解説しました。ここではネットワーク（NIC）の冗長化について解説します。サーバーの筐体自体を冗長化するのは、コストやスペースの点からも大がかりな作業となるため、ネットワークの冗長化が目的であれば、NICだけを冗長構成とするように考えることがあります。

NICとは

7-01では冗長化技術について解説しましたが、ここではNICの冗長化について考えてみます。

NICとは「Network Interface Card」の略で、LANポートのことをいいます。

■NICとは



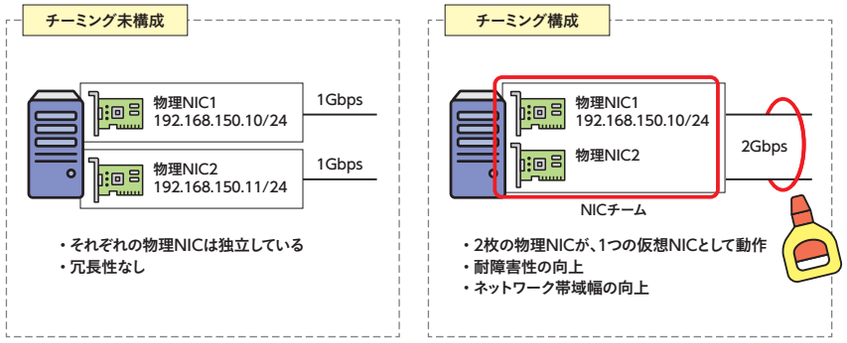
一般ユーザーが利用するノートPCなどでは、有線のLANポートが1つですが、サーバーではLANポートが複数ついている場合があります。この理由は、1台のサーバーが複数のネットワークに所属することがあったり、後述するNICの冗長構成をとったりするためです。NICは他にも、ネットワークカード、ネットワークアダプター、LANカード、LANボード、LANアダプタとも呼ばれます。

チーミング／ボンディングとは

複数の物理NICを、論理的に1つのNICとしてまとめる技術のことをチーミング（teaming）やボンディング（bonding）といいます。チーミングはスポーツのチームなどで利用する「team」という言葉が語源で、複数のNICを束ねることを意味します。ボンディングは、文房具でものを貼り付けるときに使う「ボンド（bond）」が語源で、複数のNICを束ねてくっつける＝回線を増強することを意味します。

同じ意味として利用されることもありますが、チーミングは単にNICを束ねること、ボンディングは束ねたNICを1つのNICとして増強し、冗長化とスループット（処理能力）の向上を目的として利用されます。

■チーミング／ボンディング



まとめ

- チーミングやボンディングはNICの冗長化を実現する技術である
- NICを束ねることで、障害対策に加え性能の増強を実現できる

05 DNS ラウンドロビン

ここからは負荷分散の方法について解説します。Webシステムなどで、集中する負荷を軽減させるために同じ処理を行うサーバーを複数台準備し、処理を分散させる場合があります。DNSラウンドロビンについて解説します。

処理を振り分ける仕組み（負荷分散）

7-04で解説した通り、サーバーの冗長化は、単にサーバーの筐体を複数準備するだけでは実現できません。通信の流れを制御し、利用するサーバーを振り分ける仕組みが必要なのですが、このような仕組みを負荷分散と呼びます。負荷分散を図ることは、障害に備えることにつながるのです。

7-05〜7-09に渡り、下記に示す負荷分散の仕組みをいくつか紹介します。

- DNSラウンドロビン
- コンテンツ配信負荷分散
- データベース負荷分散
- ELB負荷分散

DNSラウンドロビンとは

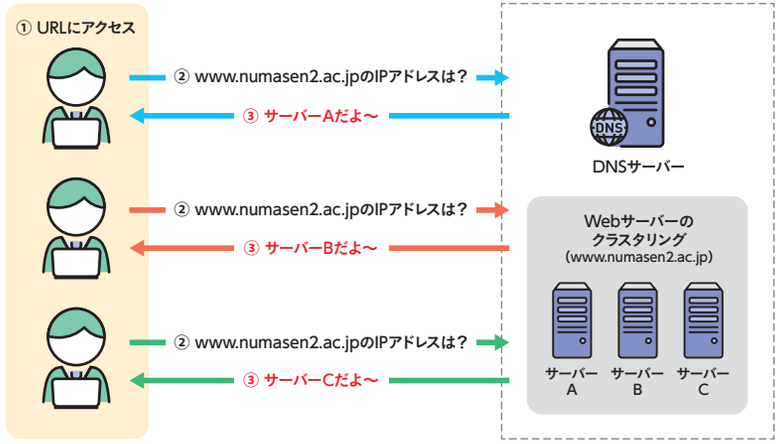
DNSラウンドロビンとは、DNSの問合せに対し、回答内容のサーバーを順繰りに変える仕組みのことをいいます。回答内容となる対象のサーバーはクラスタリング構成にしておきます。次に、ネットショッピングの例で考えてみましょう。

ネットショッピングを提供しているWebサーバーを1台だけで運用するのは、サービスの信頼性のためにも避けたいところでしょう。そのため、複数のWebサーバーを準備し、クラスタリング構成にした環境で、DNSラウンドロビンによる負荷分散を行うと、通信の流れは以下のようになります。

① クライアント端末はブラウザでURLにアクセスする
② URLに記載されたWebサーバーにあたるFQDN名（ホスト名（コンピュータの名前）とドメイン名（組織名）を組み合わせた名前）から、クライアントはDNSサーバーにIPアドレスの名前解決要求をする
③ DNSサーバーは最初要求に対する回答はWebサーバーA、次の要求にはWebサーバーB、その次はWebサーバーCのIPアドレス…といったように、クラスタリングの中から順繰りに各ノードのIPアドレスを応答する
④ クライアントは情報を得たIPアドレス宛にWeb通信を行う

このように、DNSラウンドロビンによって、Webサーバーは順繰りにアクセスされ、負荷分散されることになります。

■DNSラウンドロビンとは



まとめ

- DNSラウンドロビンとは、DNSの通信負荷分散を実現する技術である
- DNSラウンドロビンでは、名前解決要求に対して、順番に別のIPアドレスを回答することで負荷分散を実現する

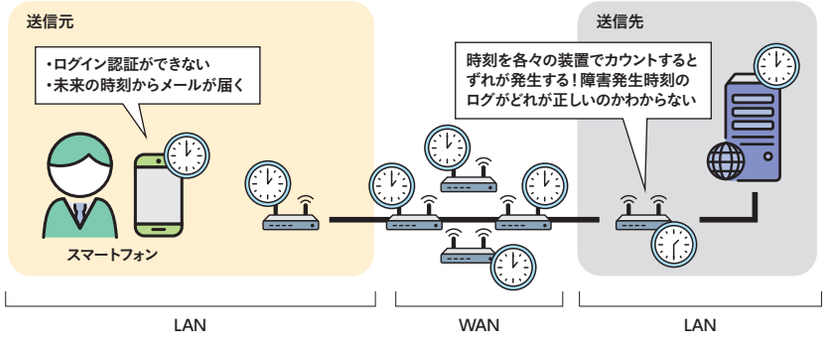
02 NTPサーバー

サーバーを構築するときに各サーバーで時間が同期されていることはとても大切です。時刻がずれると、ログ確認にも支障を及ぼすことがあります。海外でサーバーを展開する場合には、時差も考慮する必要があります。

時刻を合わせるということ

サーバーやネットワーク機器が複数台準備された環境において、それぞれの機器で時刻をカウントしている場合、時刻がずれる可能性があります。時刻がずれると、ログの確認や認証やログイン操作などに影響を及ぼす場合があります。メールにおいては、未来の時刻からメールが送信されたりする可能性もあり、システム全体の信頼性にも関わります。

■時刻同期の必要性

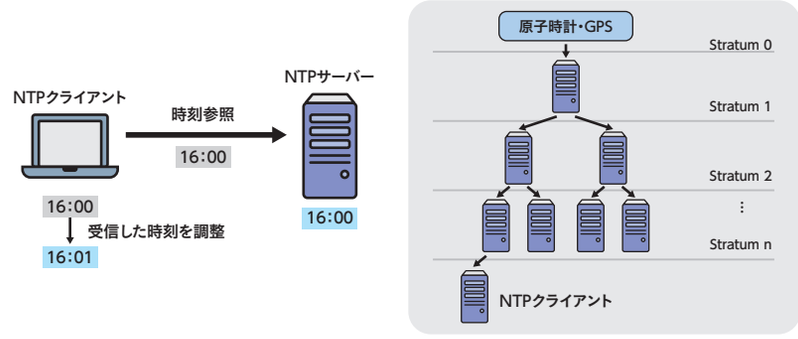


NTPとは

ネットワークの世界には、**時刻同期を行うプロトコルとしてのNTP（Network Time Protocol）があります**。NTPの前身として、TP（Time Protocol）がありますが、こちらは、1900年1月1日からどの程度時間が経過したのかという情報だけを通知する単純なプロトコルであり、情報を通知する際にかかる遅延などについては考慮されていません。したがって、何台もの機器を経由する環境では、利用が不向きであるといえます。

NTPはTPの問題を解決しているプロトコルです。したがって、相手サーバーとの通信の遅延を計測し、やりとりする時間に関する情報を補正することが可能です。また、階層構造を採用して、時刻の伝達方法についても制御する仕組みが備わっています。

■NTPと階層



NTPの階層のことをstratum（ストラタム）と呼びます。stratumは0から16までの階層で定義され、最上位であるstratum0は原子時計やGPS時刻のような正確な時刻源を指し、stratum0から時刻情報を受け取るサーバーがstratum1です。そして、stratum1から時刻情報を受け取るサーバーがstartum2、stratum2から時刻情報を受け取るサーバーがstratum3…というような階層構造となっています。ちなみに、stratum16からは時刻情報を受け取ることができません。

まとめ

- **NTPサーバーは時刻同期を実現する仕組みである**