第二章　用語解説

AWS環境構築に向けた各種情報

用語解説

※クリックで該当ページにジャンプします。

1．テクノロジー

リージョン
アベイラビリティーゾーン

2．コンピューティングサービス

EC2
EC2のインスタンスタイプ
EC2の購入オプション
インスタンスへの接続方法
AMI
Auto Scaling
スケールアウトとスケールイン
スケールアップとスケールダウン
Lambda

3．ストレージサービス

EBS
S3

4．ネットワークサービス

Amazon VPC
サブネット
AWS Internet Gateway
NATゲートウェイ
セキュリティグループ

5．データベースサービス

RDS
RDSとRDB on EC2の違い

用語解説

※クリックで該当ページにジャンプします。

６．管理サービス

SessionManager
CloudWatch
SQS
ACM
Route53
SNS

７．その他

SSH

1.テクノロジー

【リージョン】

- リージョンとは

　AWSでは地域を物理的なロケーションに分割してサービスを提供しており、その物理的なロケーション分割単位が**リージョン**です。
　以下に記載する考慮すべきポイントに沿って、リージョンを選定します。

- 考慮すべきポイント

料金　　：リージョンによって異なる。最安と比較して6割～7割程度割高となる場合もある。

サービス：リージョン毎に対応しているサービスが異なる。
「アジアパシフィック（大阪）」は非常に少ない。

安定性　：統計的な数値は公表されていないがリージョンによって安定性が異なる。

スピード：利用者からの物理的距離に影響される。一般的には日本国内からのアクセスであれば、「アジアパシフィック（東京）」が安定して速度がでる。

【アベイラビリティーゾーン】

- アベイラビリティーゾーンとは

　リージョン内に必ず複数個存在し、物理的、ソフトウェア的に自律しているデータセンターの集合の単位が**アベイラビリティーゾーン（AZ）**です。

　アベイラビリティゾーンは、互いに影響を受けないように、地理、電源、ネットワーク的に分離されており、各アベイラビリティゾーンは高速専用線で接続されています。

　複数の異なるアベイラビリティーゾーンを利用することで、簡単に冗長構成を組むことが可能になります。（**マルチAZ**）

- マルチAZにおける考慮すべきポイント

レイテンシ：マルチAZ環境の場合、アベイラビリティゾーン間のレイテンシ（通信遅延）を考慮する必要があります。

安全性　　：マルチAZ環境においてもリージョン全体に影響を及ぼす障害が発生した場合には影響を受ける場合があります。

2. コンピューティングサービス

【EC2】

- EC2とは

　EC2は**「Amazon Elastic Compute Cloud」の略称**で、AWSで利用できるシステムのひとつです。

　ユーザーの必要に応じてサーバースペックを簡単に変更することが可能というメリットがあり、従量課金であることから必要なスペックを維持することで、コストメリットを得ることができます。

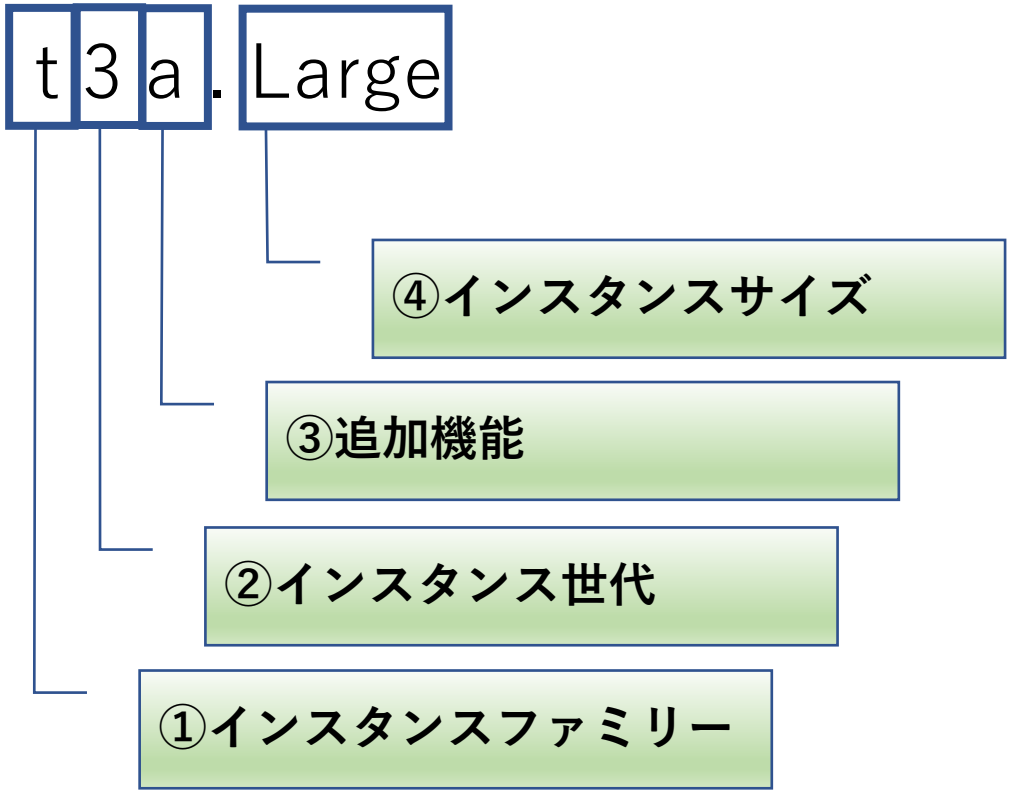
　ハードウェア設定が必要な物理サーバーなどを使う場合には、設定完了まで数日のタイムラグが発生しますが、EC2によって構築されるシステムはわずか数分あれば立ち上げが完了します。

　そのためスピードが求められる事業においても、便利に利用することが可能です。

【EC2のインスタンスタイプ】

- EC2のインスタンスタイプについて

  EC2インスタンスタイプには非常に多くの種類があり、以下の書式で表現されます。



①インスタンスファミリー

大きく分けて5種類のユースケース(汎用、ストレージ最適化、コンピューティング最適化、メモリ最適化、高速コンピューティング)に適したファミリーに分類されます。

②インスタンス世代

数値が大きい方が新しい世代になります。

③追加機能

CPUのIntel製からの変更や、リソースの強化・追加等を表します。

④インスタンスサイズ

nano→micro→medium→small→largeの順で、CPU / メモリ / ネットワーク帯域上限等が大きくなります。

【EC2の購入オプション】

- EC2の購入オプションについて

EC2には3つの購入オプションが用意されており、それぞれ異なる料金形態が採用されています。

・オンデマンドインスタンス

サーバーの利用時間によって料金が発生する従量課金のスタイルです。

短時間の限られたタイミングでだけ利用したいときに適しています。

・リザーブドインスタンス

稼働時間を事前に設定して、料金を先に支払う方法です。

常にインスタンスを利用したいが、予算が決められている場合に適しています。

・スポットインスタンス

AWS内で使われていないコンピューティングリソースを利用する方法です。

条件を満たすことで大幅に割引されるため、コスト重視での利用に適しています。

【インスタンスへの接続方法】

- 接続方法

EC2インスタンスへの接続方法は対象となるOSによってことなりますが、代表的なOS「Amazon Linux」、「Windows」への接続方法を以下にまとめます。

接続方式	OS	設定範囲	操作性	ネットワーク利用	条件・制限等
RDPクライアント	Windows	◎	◎	あり	–
SSHクライアント	Linux	◎	◎	あり	–
Instance Connect	Linux	◎	○	あり	※1
シリアルコンソール	Windows Linux	△(制限あり) △(制限あり)	△(SAC) ○	なし なし	※2
セッションマネージャー	Windows Linux	○ ○	△(PowerShell) ○	あり あり	※3

※1：パブリックネットワーク接続が必要

※2：リージョン・インスタンスの設定に制限あり

※3：443ポートアウトバウンド許可が必要

【AMI】

- AMIとは

AMIは**「Amazonマシンイメージ」の略称**で、**EC2インスタンスの構築に必要な情報がまとめられた起動テンプレート**を指します。

AMIには「OS」、「ミドルウェア」、「ルートデバイスのストレージ」、「起動許可」といった要素があり、それぞれの要素を組み合わせた状態の事前に用意されたAMIを利用することにより、EC2インスタンス作成時の工数を削減することが可能です。

また、AMIを使用することでEC2インスタンスをバックアップとして保存することができ、EC2インスタンスの障害発生時に作成していたAMIを利用することで、特定の状態にまで復帰させることが可能です。

AMIはアカウント間で共有可能であり、他のアカウントIDを指定して共有先のアカウントにてEC2インスタンスを起動できます。

なお長期間使用しないEC2インスタンスはAMIを取得し、インスタンス自体を削除しておくことでコストを削減することが可能となります。

【Auto Scaling】

- Auto Scalingとは

Auto Scalingとは、インスタンスの負荷の**しきい値をあらかじめ設定**することで、しきい値に達した際に**自動的にクラウドサーバーの台数やスペックを増減させる**機能のことです。

Auto Scaling導入のメリットには以下のようなものがあります。

・突発的なサーバー負荷にも耐えられるシステムの構築が可能

・運用リスクを軽減できる

・インフラの運用コストを最適化できる

Auto Scalingを活用する場合には、**インスタンスをステートレス化**しておくか、ユーザーがどこまで操作したかを**サーバー間で共有する仕組み**を用意しておく必要があります。

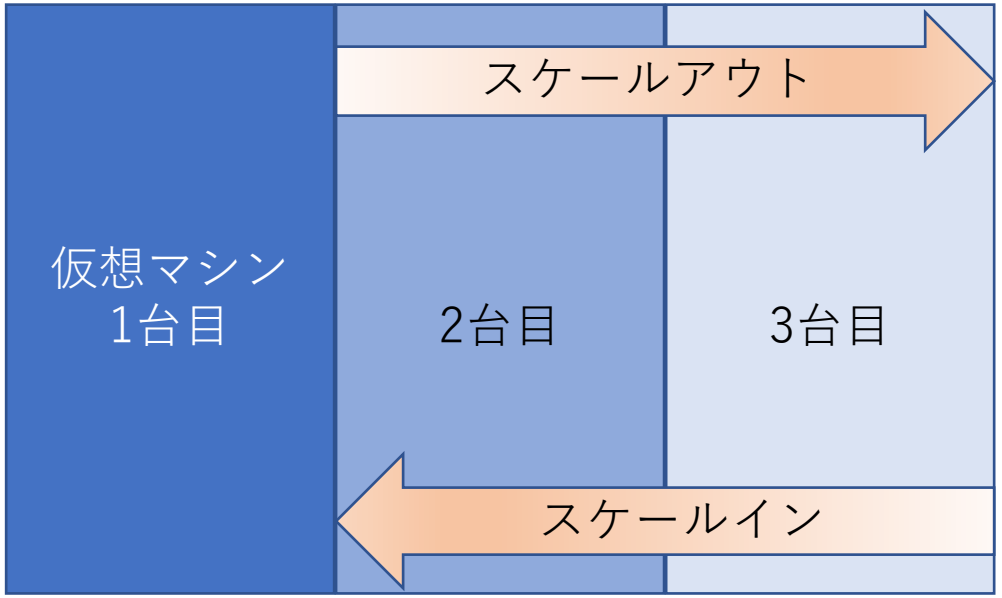
【スケールアウトとスケールイン】

- スケールアウトとスケールインとは

　スケールアウトとスケールインは、システムを構成する**<u>サーバの台数を増減させる</u>**ことを示します。

　スケールアウトであればサーバの台数を増やし、スケールインであればサーバの台数を減らします。

　比較的単純な処理で、複数サーバー間でのデータ連携が多くなく、多数の処理を同時並行で行う必要があるシステムに向いています。



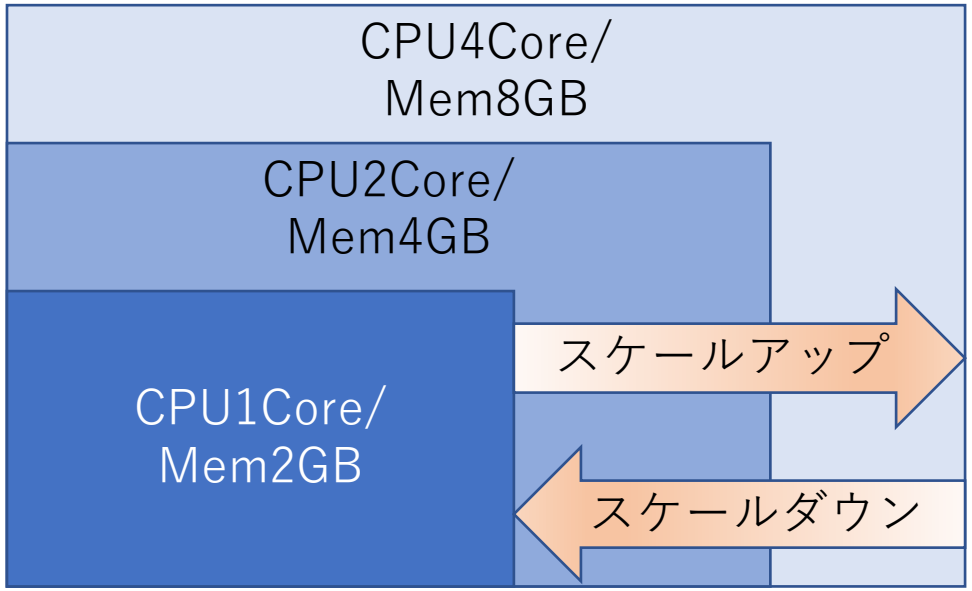
【スケールアップとスケールダウン】

- スケールアップとスケールダウンとは

　スケールアップとスケールダウンは、システムを構成する**サーバのスペック（CPUのCore数、メモリサイズ等）を増減させる**ことを示します。

　スケールアップであればサーバのスペックを増やし、スケールダウンであればサーバのスペックを減らします。

　複数サーバーが同期して動くようなサーバー間データ連携があり、データの整合性に高い信頼性を求められるシステムに向いています。



【Lambda】

- Lambdaとは

Lambdaは**サーバレスのFaaS(Function as a Service)**で、**クラウド上にプログラムを定義し、インターネットを通じて実行できるサービス**です。

Lambdaには以下のような**メリット**があります。

・コストが低い。
・準備したコードを実行するだけのため高速で開発が可能。
・サーバの保守・運用が不要。
・AWSのサービス間を疎結合可能。
・疎結合で障害が起きても影響を極小化可能。
・実行トリガーとなる関数が多くSNS、DataDog（監視サービス）と連携可能。
・選択できるプログラミング言語が豊富。

3.ストレージサービス

【EBS】

- EBSとは

EBSは**Elastic Block Storeの略**でデータベースや、エンタープライズアプリケーション、コンテナ化されたアプリケーションなど、**多くのサービス向けに提供されたストレージサービス**です。

アベイラビリティゾーン内の複数のサーバーで自動的にレプリケート（複製）されます。

EBSには主に以下のような特徴があります。

・SSDタイプとHDDタイプの2種類のディスクタイプが存在している。

・データの耐久性が高く年間故障率（AFR）が0.1%～0.2%になるように設計されている。

・データのポイントインタイムスナップショットをAmazon S3に保存する機能が用意されている。

・EBSデータボリューム、ブートボリューム、およびスナップショットの暗号化を提供されている。

【S3】

- S3とは

  S3はデータを格納・管理できる**オブジェクトストレージサービス**です。

  S3に格納したデータは自動的に3つのデータセンターに複製されるため、**高いデータ耐久性を実現**しています。万一の障害やエラー、脅威などからデータを保護することができます。

  サービスは従量課金制で、「ストレージ容量」「リクエスト数」「データ転送量」といった**使用量に応じて料金が算出**されるため、コストを意識した利用が可能です。

容量制限が無く、データをいくらでもアップロードできる非常に大きなメリットがあります。

  保存するデータに「１ファイルにつき5TBまで」という制限はありますが、**サービス全体の容量制限がありません**。ストレージの残容量を気にすることなくデータを保存できるため、複数のデバイスにデータを分けて蓄積するといったことを検討する必要がありません。

4.ネットワークサービス

【Amazon VPC】

- Amazon VPCとは

　AWSアカウント内に構築できる仮想ネットワークで、仮想サーバ「EC2」などAWSのサービスが起動する環境が**Amazon VPC**※1です。

　1つのVPCを論理的なまとまりとして分離することが可能で、複数のVPC間の接続も可能です。

　インターネットに公開するパブリックなVPCや、VPNなどを使用して接続するプライベートなVPCの構築ができます。

- Amazon VPCを利用するメリット

　・クラウド上で仮想ネットワークを簡単に構築できる

　・インターネットを使わないセキュアな通信もできる

　・便利なコンポーネントが多くカスタマイズ性が高い

※1　VPC = Virtual Private Cloud

【サブネット】

- サブネットとは

　VPCのIPアドレスの範囲を分割して作成したネットワークです。VPCのIPアドレスの範囲内でサブネットを指定することができます。しかし1つのサブネットはVPCの複数アベイラビリティーゾーンをまたぐことはできません。

　サブネットには「**パブリックサブネット**」と「**プライベートサブネット**」があります。

パブリックサブネット　：関連付けられているルートテーブルのルートにインターネットゲートウェイがあることで、インターネット通信を可能にします。

プライベートサブネット：関連付けられているルートテーブルにインターネットゲートウェイのルートがないサブネットで、インターネット通信はできません。

【AWS Internet Gateway】

- AWS Internet Gatewayとは

　VPC内から**インターネットに接続するためのゲートウェイ**です。インターネットゲートウェイを使うことで、VPC内のシステムがグローバルIPを使えるようになります。

　作成手順としてはインターネットゲートウェイを作成した後にVPCに追加（アタッチ）する方法をとります。

　削除する場合には、アタッチを解除（デタッチ）した後、削除するという手順になります。

【NATゲートウェイ】

- NATゲートウェイとは**NAT ※1機能を提供**する、インターネット接続時に利用されるオブジェクトです。

  NATゲートウェイはプライベート IP とパブリック IP を多対 1 で変換します。

  変換と同時に動的に NAT エントリが生成されますが、インターネットからの通信は (NAT エントリが無いため) アクセスできません。

  このためNATゲートウェイの使い道は、主に「インターネットからはアクセスされたくないがインターネットへのアクセスは実施したい」というケース、具体的にはインターネット通信のできないプライベートサブネットからインターネットへアクセスしてソフトウェアのアップデートなどを行う際に利用します。

  インターネットとの接続にはインターネットゲートウェイが必要です。

※1　NAT = Network Address Translation
送信元や宛先の IP アドレスを、あらかじめ決められたルールに従い別の IP アドレスに変換する機能

【セキュリティグループ】

- セキュリティグループとは

　グループ外のインスタンスと通信を行う際のトラフィックを制御する**ファイアウォールの役割**を担います。セキュリティグループには以下の特徴があります。

・許可リストを設定することが可能、拒否リストは設定できない。

・インバウンド(受信)ルールとアウトバウンド(送信)ルールを設定可能。

・インバウンド(受信)ルールを追加するまで、全てのトラフィックを拒否する。

・アウトバウンド(送信)ルールを追加するまで、全てのトラフィックを許可する。

・インバウンドのトラフィックに対するレスポンスは、アウトバウンドのルールに関係なく許可される。

・許可リストを設定しなければ、セキュリティグループ内のインスタンスも互いにやりとりすることはできない。

・インスタンスの起動後、どのセキュリティグループに属するか変更することが可能。

5.データベースサービス

【RDS】

- RDSとは

RDSはRelational Database Serviceの略で、**DBをサービスとして提供**しており、以下のDBに対応しています。

・**Oracle**
・**MySQL**
・**MariaDB**
・**SQL Server**
・**PostgreSQL**
・**Amazon Aurora**

サービスは従量課金制ですが、以下の制限範囲内であれば**無料での利用も可能**です。

・750時間の使用時間（db.t2.microのみ）
・20GBのストレージ
・20GBのスナップショットと自動バックアップ

【RDSとRDB on EC2の違い】

- RDSとRDB on EC2

  AWSでDBを利用する場合、RDSを利用する方法以外にEC2上でRDBを利用する方法（RDB on EC2）があります。

  以下にRDSとRDB on EC2の特徴を記載します。

  ・**RDS**

  構築時のリードタイムが短くスナップショット機能でバックアップ取得可能。

  Amazon Auroraの利用が可能。

  Multi-AZ構成をとることが可能。

  ・**RDB on EC2**

  OSにログインする事が可能。

  RDSで提供されていないインスタンスタイプ/ストレージの利用が可能。

6.管理サービス

【SessionManager】

- SessionManagerとは

  SessionManagerは**フルマネージド**※1**型のAWS Systems Manager 機能**です。

  SessionManagerを利用することにより、以下のようなメリットがあります。

  ・IAMポリシーを使ったインスタンスのアクセス制御を一元的に行うことが出来る。

  ・踏み台ホストやSSHキーの管理をしたり、インバウンドポートを開いたりする必要が無い。

  ・コンソールやCLIからインスタンスにワンクリックアクセスが出来る。

  ・ポート転送が可能。

  ・LinuxとWindows両方でクロスプラットフォームのサポートが出来る。

※1　クラウド業者がすべての作業を行うサービス提供の形態

【CloudWatch】

- CloudWatchとは

  CloudWatchはAWS内で動作する仮想サーバーや各サービスを監視できるサービスです。
  以下のような機能が提供され、必要なものを組み合わせて利用します。

  ・AWS内に立てた仮想サーバーのCPU使用率、ディスクの読み書き回数、
  インターフェースの通信量などを監視する「**メトリクス**」。

  ・使用中のすべてのシステム、アプリケーション、AWS サービスのログファイルを監視する「**ログ監視機能**」。

  ・特定の閾値を超えた場合、下回った場合、監視ができなくなった場合などに設定した方法で通知する「**アラーム通知機能**」。

  ・状態が変化した場合や指定された時間にイベントを実行する
  「**イベント管理・自動化機能**」。

  ・メトリクス・ログ・イベントの状況を可視化し、一元的にダッシュボードへ表示する
  「**ダッシュボード機能**」。

【SQS】

- SQSとは

  SQSは「**Simple Queue Service**」の略でフルマネージド型のキューイングサービスです。
  異なるソフトウェア間でデータを送受信する手法の一つとして選択できます。

  SQSには以下2種類のキュータイプがあります。

  ・**標準キュー**

  スループットは無制限ですが、配信順序はベストエフォートで保証されません。
  メッセージは最低1回配信されるため、複数回同じメッセージを受け取っても悪影響が出ない構成にする必要があります。FIFOキューと比較すると安価です。

  ・**FIFO キュー**

  スループットは1秒あたり300件の制限がありますが、配信順序は保証されます。
  メッセージは必ず1回のみ配信されます。

【ACM】

- ACMとは

ACMは**「AWS Certificate Manager」**の略で、パブリックとプライベートの SSL/TLS 証明書を自動更新可能です。

SSL／TLS証明書の購入、アップロード、更新というプロセスを手動で行う必要がなくなります。

また、証明書をコンソールなどから一括で管理することができ、**実質無料で利用することが可能**ですが、ELB(Elastic Load Balancing)、Cloudfront(Amazon CloudFront)のサービスで使用する証明書のみプロビジョニング可能となっています。

【Route53】

- Route53とは

  Route53は**DNS（ドメインネームサービス）のフルマネージドサービス**です。

  Route 53 は下記3点の機能を使用できます。

  ・**ドメイン登録機能**

  ウェブサイトやウェブアプリケーションの名前（ドメイン名）を登録できます。

  ・**DNS ルーティング機能**

  ウェブブラウザにて登録されたドメイン名またはサブドメイン名を入力した場合に、Route 53 は接続するための支援を行います。

  ・**DNS ヘルスチェック機能**

  自動リクエストをインターネット経由でウェブサーバーなどのリソースに送信し、対象リソースが到達可能、使用可能、機能中であることを確認できます。

【SNS】

- SNSとは

SNSは「**Simple Notification Service**」の略でフルマネージド型のウェブサービスです。

論理アクセスポイントにメッセージを作成して送信することで、紐づけられた受信者に対してメッセージが非同期に一括で届けられる仕組みです。

以下のプロトコルがサポート対象です。

- **Amazon SQS(Simple Queue Service)**
- **AWS Lambda**
- **HTTP**
- **HTTPS**
- **Eメール**
- **SMS(Short Message Service)**

7.その他

【SSH】

- SSHとは

SSHとは「**Security Shell**」の略称で、**別のコンピューターに遠隔でログインしたり、特定のサーバに接続するためのプロトコルまたはソフトウェア**を指します。

サーバ接続時の代表的な認証方式には「**パスワード認証方式**」、「**公開鍵認証方式**」があります。

パスワード認証方式：パスワードは、サーバのユーザーアカウントに設定されます。
手軽ですがパスワードが流失すると悪意をもった第三者から
サーバにログインされてしまう危険性があります。

公開鍵認証方式　　：事前に公開鍵をサーバに格納し、クライアント側で保持する
秘密鍵と併せて情報を暗号化する方式です。
不正ログインに対しての安全性も高い方式です。