

10 秒で始める AI プログラミング学習サービス「Aidemy」

新コース「ブロックチェーン発展 I」を開設

－ 暗号通貨におけるセキュリティの理解から実装まで －

東大発スタートアップの株式会社アイデミー(本社:東京都渋谷区、代表取締役 CEO 石川聡彦)が提供する AI プログラミング学習サービス「Aidemy」(<https://aidemy.net/>)は、2018 年 7 月 4 日(水)より、新コース「ブロックチェーン発展 I」コースの提供を開始しましたのでお知らせいたします。



【「ブロックチェーン発展 I」コース概要】

暗号通貨のセキュリティ面から理解し実装をしていきます。ビットコインの所有権は、秘密鍵、公開鍵、ビットコインアドレス、署名を基に成り立っています。中でも秘密鍵に関してはビットコインネットワークから独立していて、ウォレットと呼ばれる秘密鍵を保管する単純なデータベースの中に保持されています。このコンテンツでは、主に秘密鍵・公開鍵・ビットコインアドレスの生成、ウォレットの実装をしていきます。

なお、このコンテンツは3部に渡るブロックチェーン発展講座の1つ目の講座となります。

■ブロックチェーン発展 Iコース: <https://aidemy.net/courses/7110>

■コース内容

1. 基礎講座の復習

このコースは無料で公開しているブロックチェーン基礎講座を基に説明を進めます。今回の発展 I 講座を理解していただく上で必要なブロックチェーン基礎講座の要素を復習します。

2. 公開鍵暗号方式

ビットコインのセキュリティモデルにおいて、根本原理である公開鍵暗号方式について理解していきます。その上で秘密鍵、公開鍵、ビットコインアドレスの生成を行います。

3. ウォレットの実装

ウォレットは鍵を管理するための容器であり、簡単なデータベースとして実装されています。ここではいくつかのウォレットの型について説明した後、HD ウォレット(階層的決定性ウォレット)という、現在もっとも実用的とされるウォレットを実装していきます。

The screenshot shows the Aidemy web interface. On the left, there is a navigation pane with the title "ブロックチェーン発展I" and a sub-section "1.3.2 階層的決定性ウォレット". Below the text, there is a diagram illustrating the generation of keys from a seed. The diagram shows a "シード" (Seed) leading to a "マスター鍵" (Master key) labeled 'k'. From this master key, three "子鍵" (Child keys) labeled 'k' are generated. Each child key further generates three "孫鍵" (Grandchild keys) labeled 'k'. The text explains that a hierarchical deterministic wallet (HD wallet) is a type of deterministic wallet where a single seed can generate many keys, and each key is derived from the previous one in a hierarchical structure.

図1.3.2 -1 階層的決定性ウォレット

それではシードから秘密鍵を作成する手順を学びましょう。

```
script.py
1 import os
2 import binascii
3 import hmac
4 import hashlib
5
6 secret_key = os.urandom(32)
7 root_seed = secret_key
8
9 # ASCII形式でメッセージに任意の文字列を代入しています
10 message = b"random_seed"
11
12 # hmac関数を適応してください
13 hmac_hash =
14
15 # master_secret_keyに前半32bitを
16 # master_chain_codeに後半32bitを代入してください
17
18 master_secret_key =
19 master_chain_code =
20
21 print(binascii.hexlify(master_secret_key))
22 print(binascii.hexlify(master_chain_code))
```

RESET RUN

> コンソール

▲「ブロックチェーン発展 I」の画面▲

■価格:980 円

【Aidemy の概要】

Aidemy は正式公開から3ヶ月で会員登録ユーザー数1万人以上、コード実行回数100万回以上を記録した、日本最大級の先端技術のラーニングサービスです。 <https://aidemy.net/>

1. 10秒で演習開始 - PCへの環境構築は不要で、インターネットブラウザ上でプログラミングができます。
2. 今話題の技術を習得可能 - ディープラーニングや自然言語処理など、いま話題の技術を習得できます。
3. 無料から始められる - 一部の講座は完全無料にてご受講いただけます。



▲Aidemy の演習画面の例(左:コードを書きながら学習する問題, 右:クイズに答えながら学習する問題)▲

【Aidemy の教材の特徴】

1. 業界トップシェア技術を採用 – Python/numpy/pandas/scikit-learn/tensorflow などの技術が学べます。
2. 理論より実践重視 – 難しい数学の知識や理論もできるだけ直感的に理解できるような教材です。
3. 自動採点システム – 書いたプログラムは仮想環境上で自動的に採点されます。



▲Aidemy の教材(左:受講ルートページ, 右:受講コースページ)▲

【株式会社アイデミーについて】

株式会社アイデミー(旧社名 Goods 株式会社)は「社会とテクノロジーをつなぐ。」をミッションとする、2014 年創業のベンチャー企業です。大学での機械学習応用系の研究、クライアント企業のアプリケーション制作・データ解析を経て、2017 年 12 月に「10 秒で始める AI プログラミング学習サービス Aidemy」をリリースしました。Aidemy はサービス開始 3 ヶ月で会員数 1 万名超、コード実行回数 100 万回を突破した日本最大級の先端技術のラーニングサービスです。また、早稲田大学リーディング理工学博士プログラムでの AI 入門特別実践セミナーも担当し、代表取締役 石川聡彦の著書「人工知能プログラミングのための数学がわかる本」が KADOKAWA より 2018 年 2 月に発売されました。こうした事業を通じて、「世界 100 万人規模の先端 IT 人材の不足」という社会課題の解決に貢献して参ります。



▲株式会社アイデミー 代表取締役 CEO 石川 聡彦▲

【株式会社アイデミー概要】

会社名:株式会社アイデミー

所在地:東京都渋谷区道玄坂 2-16-8 渋谷坂本ビル 6 階

代表者:代表取締役 CEO 石川 聡彦

設立:2014 年 6 月

URL:<https://aidemy.net/>

株主:経営陣, Skyland Ventures, UTEC, エンジェル投資家 他

事業内容:エンジニアのための AI プログラミング学習サービス「Aidemy」の提供



【本件に関する報道関係者からのお問合せ先】

株式会社アイデミー

代表取締役 CEO 石川 聡彦

TEL:03-6868-0998 (平日 9:00-18:00)

e-mail: support@aidemy.net