



Born2beRoot

概要:

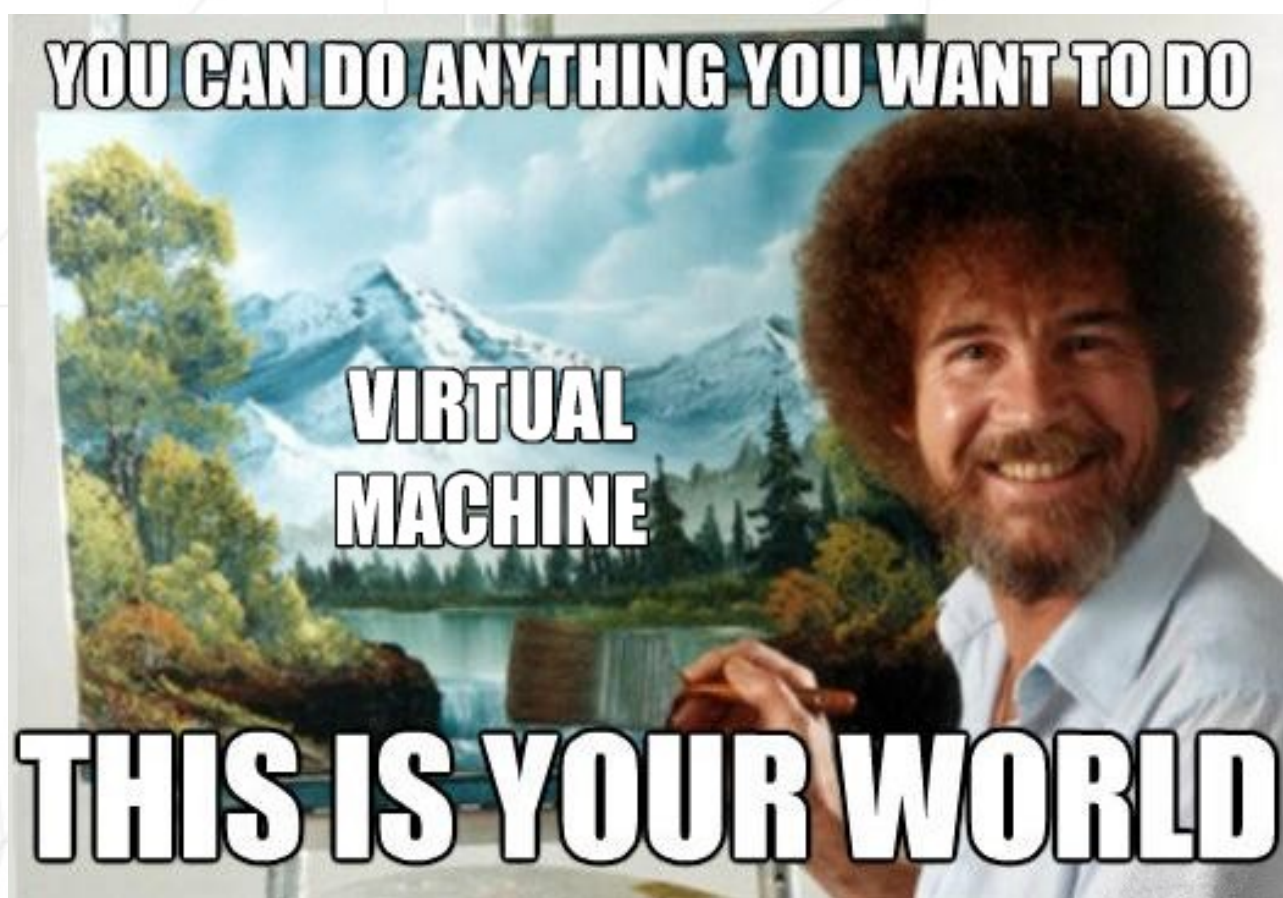
この文書はシステム管理関連の演習です。

バージョン: 4

目次

I	前文	2
II	はじめに	3
III	一般的なガイドライン	4
IV	AI指示	5
V	必須部分	7
VI	ボーナス部分	12
VII	提出とピア評価	14

第I章 前文



第II章 序論

このプロジェクトは、仮想化の素晴らしい世界を紹介することを目的としています。

VirtualBox（VirtualBoxが使用できない場合はUTM）で、特定の指示に従って最初のマシンを作成します。その後、このプロジェクトの終了時には、厳格なルールを適用しながら独自のオペレーティングシステムを設定できるようになります。

第III章 一般的なガイド

ライン

- VirtualBox（VirtualBoxが使用できない場合はUTM）の使用は必須です。
- リポジトリのルートディレクトリにsignature.txtファイルを提出するだけでよい。このファイルには仮想マシンの仮想ディスクの署名を貼り付ける必要がある。詳細は「提出とピア評価」を参照のこと。
- スナップショットの使用は禁止されています。

第4章

AI 指示

● 背景

このプロジェクトは、ICTトレーニングの基礎的な構成要素を発見する手助けとなるよう設計されています。

重要な知識とスキルを確実に定着させるには、AIツールと支援を慎重に活用する姿勢が不可欠である。

真の基礎的学習には、挑戦、反復練習、仲間との学び合いを通じた、本物の知的努力が不可欠です。

学習ツールとしてのAI、ICTカリキュラムの一部としてのAI、そして就職市場における期待としてのAIに関する当社の立場について、より包括的な概要については、イントラネット上の専用FAQをご参照ください。

● 主なメッセージ

- ➡ 近道なしで強固な基礎を築く。
- ➡ 技術力とパワースキルを真に育成する。
- ➡ 真の仲間との学びを経験し、学び方と新たな問題解決法を習得する。
- ➡ 学習の過程は結果よりも重要である。
- ➡ AIに関連するリスクを理解し、効果的な管理手法と対策を開発して、よくある落とし穴を回避する。

● 学習者ルール：

- 割り当てられたタスクには、特にAIに頼る前に、論理的思考を適用すべきです。

- AIに直接的な答えを求めるべきではありません。
- AIに関する42のグローバルアプローチについて学ぶべきです。

● フェーズ成果:

この基礎フェーズでは、以下の成果を得られます：

- 適切な技術とコーディングの基礎を習得する。
- このフェーズにおいて、AIがなぜ、どのように危険になり得るかを理解する。

● コメントと例：

- はい、AIが存在することは承知しています。そして、確かにAIはあなたの課題を解決できます。しかし、あなたがここにいるのは学ぶためであって、AIが学んだことを証明するためではありません。AIが与えられた問題を解決できることを示すためだけに、あなたの時間（そして私たちの時間）を無駄にしないでください。
- 42での学びは答えを知るのではなく、答えを見つける能力を育むことです。AIは直接答えを与えてしまいますが、それはあなた自身の推論を構築する機会を奪います。推論には時間と努力が必要であり、失敗も伴います。成功への道は容易であるべきではないのです。
- 試験中はAIが使えないことを忘れないでください——インターネットもスマートフォンも使えません。学習過程でAIに依存しすぎていると、すぐに気づくでしょう。
- 仲間との学びは多様な考え方やアプローチに触れさせ、対人スキルや発散的思考力を高めます。これは単なるボットとの会話よりもはるかに価値があります。だから遠慮せず、話し合い、質問し、共に学びましょう！
- はい、AIはカリキュラムの一部となります——学習ツールとして、またそれ自体がテーマとしてです。ご自身でAIソフトウェアを構築する機会も得られます。当社の段階的アプローチについてさらに学ぶため、イントラネットで公開されている資料をご確認ください。

✓ 効果的な実践例：

新しい概念で詰まってしまった。近くの人にどう取り組んだか尋ねる。10分間話し合うと——突然ピンとくる。理解できた。

✗ 悪い実践例:

こっそりAIを使い、見た目が良さそうなコードをコピーする。ピアレビューでは何も説明できず、失敗する。試験ではAI禁止——また行き詰まり、失敗する。

第V章 必須課題

このプロジェクトは、特定のルールに従って初めてのサーバーを構築することから成る。



サーバー構築が目的であるため、最小限のサービスのみをインストールする。このため、グラフィカルインターフェースは不要である。したがって、X.orgや同等のグラフィックスサーバーのインストールは禁止する。違反した場合、成績は0点とする。

オペレーティングシステムとして、Debianの最新安定版（テスト版/不安定版ではない）またはRockyの最新安定版のいずれかを選択する必要があります。システム管理が初めての場合はDebianを強く推奨します。



Rockyの設定は非常に複雑です。そのため、KDUMPの設定は不要です。ただし、SELinuxは起動時に動作している必要があり、その設定はプロジェクトの要件に合わせて調整する必要があります。DebianのAppArmorも起動時に動作している必要があります。

LVMを使用して少なくとも2つの暗号化パーティションを作成する必要があります。以下に可能なパーティション分割の例を示します:

```
wil@wil:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0    0   8G  0 disk
├─sda1                              8:1    0 487M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0   7.5G  0 part
│   └─sda5_crypt                    254:0    0   7.5G  0 crypt
│       ├─wil--vg-root               254:1    0   2.8G  0 lvm    /
│       ├─wil--vg-swap_1             254:2    0   976M  0 lvm    [SWAP]
│       └─wil--vg-home               254:3    0   3.8G  0 lvm    /home
sr0                                  11:0    1 1024M  0 rom
```



防御中に、選択したオペレーティングシステムに関するいくつかの質問がされます。例えば、aptitude と apt の違い、SELinux や AppArmor とは何かを知っている必要があります。要するに、自分が使用しているものを理解してください！

仮想マシンでは、必須ポート4242でSSHサービスが稼働している必要があります。
セキュリティ上の理由から、root ユーザーとして SSH 接続することは絶対に許可されてはいけません。



SSHの使用は、新しいアカウントの設定を通じて審査中にテストされます。したがって、その仕組みを理解しておく必要があります。

オペレーティングシステムにUFW（Rockyの場合はfirewalld）ファイアウォールを設定し、仮想マシンでポート4242のみを開いた状態に保つ必要があります。



例示されているディスクサイズは任意のものです。適切な動作を確保しつつ不要なディスク使用を避けるため、各パーティションに適したサイズを決定する必要があります。



仮想マシン起動時にはファイアウォールが有効である必要があります。Rockyの場合、UFWではなく firewalld を使用してください。

- 仮想マシンのホスト名は、ログイン名に「42」を付加したもの（例: wil42）でなければなりません。評価期間中にこのホスト名を変更する必要があります。
- 強力なパスワードポリシーを実装する必要があります。
- sudo は厳格なルールに従ってインストールおよび設定する必要があります。
- root ユーザーに加えて、ログイン名をユーザー名とするユーザーが存在する必要があります。
- このユーザーは user42 グループと sudo グループに属している必要があります。



防御中に、新しいユーザーを作成し、それをグループに割り当てる必要があります。

強力なパスワードポリシーを設定するには、以下の要件を満たす必要があります：

- パスワードは30日ごとに失効する必要があります。
- パスワード変更までの最小日数は2日に設定されます。

- パスワード有効期限の7日前までに警告メッセージをユーザーに通知すること。
- パスワードは10文字以上でなければなりません。大文字、小文字、数字をそれぞれ1つ以上含める必要があります。また、3文字以上連続で同じ文字が続いてはいけません。
- パスワードにはユーザー名を含めることはできません。
- 以下のルールは root パスワードには適用されません：パスワードは、以前のパスワードに含まれていなかった文字を少なくとも 7 文字以上含める必要があります。
- もちろん、root パスワードもこのポリシーに準拠する必要があります。



設定ファイルの設定後、仮想マシン上のすべてのアカウント（rootアカウントを含む）のパスワードを変更する必要があります。

sudoグループの強固な設定を構築するには、以下の要件を満たす必要があります：

- sudoによる認証は、パスワードが間違っている場合に3回までしか試行できません。
- sudo使用時にパスワード誤りによるエラーが発生した場合、任意のカスタムメッセージを表示する必要があります。
- sudoを使用した各操作は、入力と出力の両方を記録する必要があります。ログファイルは /var/log/sudo/ フォルダに保存する必要があります。
- セキュリティ上の理由から、TTYモードを有効にする必要があります。
- 同様にセキュリティ上の理由から、sudo が使用できるパスを制限する必要があります。例：
`/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin`

最後に、monitoring.sh というシンプルなスクリプトを作成する必要があります。これは bash で開発されなければなりません。

サーバー起動時、および10分ごとに（wallコマンドを参照）、このスクリプトは全端末に以下の情報を表示します。バナーは任意です。エラーは一切表示されてはいけません。

スクリプトは常に以下の情報を表示できる必要があります：

- オペレーティングシステムのアーキテクチャとカーネルバージョン。
- 物理プロセッサの数。
- 仮想プロセッサの数。
- サーバーの現在の利用可能なRAMとその使用率（パーセンテージ）。
- サーバー上の現在の利用可能ストレージ容量とその使用率（パーセンテージ）。
- プロセッサの現在の使用率（パーセンテージ）。
- 最後の再起動の日時。
- LVMが有効かどうか。
- アクティブな接続数。
- サーバーを利用しているユーザー数。
- サーバーのIPv4アドレスとそのMAC（メディアアクセス制御）アドレス。
- sudoプログラムで実行されたコマンドの数。



防御中に、このスクリプトの動作説明を求められます。また、スクリプトを変更せずに中断させる必要があります。cronを確認してください。

スクリプトの動作例は以下の通りです：

```
root@wil (tty1) からのブロードキャストメッセージ (2021年4月25日 15:45:00):
```

```
#アーキテクチャ: Linux wil 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux #物理CPU数 : 1
#vCPU : 1
#メモリ使用量: 74/987MB (7.50%) #ディスク
使用量: 1009/2Gb (49%) #CPU負荷: 6.7%
#最終起動: 2021-04-25 14:45
#LVM使用: はい
#接続 TCP : 1 確立済み#ユーザーログ: 1
#ネットワーク: IP 10.0.2.15 (08:00:27:51:9b:a5)
#Sudo : 42 cmd
```


対象の要件を確認するために使用できる2つのコマンドを以下に示します:Rockyの場合:

```
[root@wil will]# head -n 2 /etc/os-release
NAME="Rocky Linux"
VERSION="8.7 (Green Obsidian)"
[root@wil will]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[root@wil will]# ss -tunlp
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp    LISTEN 0      128      0.0.0.0:4242 0.0.0.0:*      users:((("sshd",pid=28429,fd=6))
tcp    LISTEN 0      128      [::]:4242 [::]:*        users:((("sshd",pid=28429,fd=4))
[root@wil will]# firewall-cmd --list-service
ssh
[root@wil will]# firewall-cmd --list-port
4242/tcp
[root@wil will]# firewall-cmd --state
running
[root@wil will]# _
```

Debianの場合:

```
root@wil:~# head -n 2 /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
root@wil:/home/wil# /usr/sbin/aa-status
apparmor module is loaded.
root@wil:/home/wil# ss -tunlp
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
tcp    LISTEN 0      128      0.0.0.0:4242 0.0.0.0:*      users:((("sshd",pid=523,fd=3))
tcp    LISTEN 0      128      [::]:4242 [::]:*        users:((("sshd",pid=523,fd=4))
root@wil:/home/wil# /usr/sbin/ufw status
Status: active

To Action From
--
4242 ALLOW Anywhere
4242 (v6) ALLOW Anywhere (v6)
```


第VI章 ボーナスパー

ト

ボーナスリスト：

- パーティションを正しく設定し、以下のような構造を実現してください：

```
# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0    0 30.8G  0 disk
├─sda1                              8:1    0   500M  0 part  /boot
├─sda2                              8:2    0     1K  0 part
└─sda5                              8:5    0 30.3G  0 part
   └─sda5_crypt                     254:0    0 30.3G  0 crypt
      ├─LVMGroup-root               254:1    0   10G  0 lvm    /
      ├─LVMGroup-swap               254:2    0    2.3G  0 lvm    [SWAP]
      ├─LVMGroup-home               254:3    0     5G  0 lvm    /home
      ├─LVMGroup-var                254:4    0     3G  0 lvm    /var
      ├─LVMGroup-srv                254:5    0     3G  0 lvm    /srv
      ├─LVMGroup-tmp                254:6    0     3G  0 lvm    /tmp
      └─LVMGroup-var--log           254:7    0     4G  0 lvm    /var/log
sr0                                  11:0    1 1024M  0 rom
```

- 以下のサービスで機能する WordPress ウェブサイトを設定する: lighttpd、MariaDB、PHP。
- 有用と思われる任意のサービス（NGINX / Apache2を除く！）を設定してください。発表時にはその選択理由を説明する必要があります。



例示されているディスクサイズは任意のものです。適切な動作を確保しつつ、不要なディスク使用を避けるため、各パーティションの適切なサイズを決定する必要があります。



ボーナス部分を完了するには、追加のサービスを設定する可能性があります。この場合、必要に応じてより多くのポートを開くことができます。もちろん、UFW/Firewalldルールはそれに依拠して適応させる必要があります。



ボーナス部分は、必須部分が完璧である場合にのみ評価されます。完璧とは、必須部分が完全に実施され、不具合なく動作していることを意味します。必須要件をすべて満たしていない場合、ボーナス部分は一切評価されません。

第VII章

提出と相互評価

提出するのは、Gitリポジトリのルートディレクトリにあるsignature.txtファイルのみです。このファイルには、仮想マシンの仮想ディスクの署名を貼り付ける必要があります。この署名を取得するには、まずデフォルトのインストールフォルダ（仮想マシンが保存されているフォルダ）を開きます：

- Windows: %HOMEDRIVE%%HOMEPATH%\VirtualBox VMs\
- Linux: ~/VirtualBox VMs/
- MacM1: ~/Library/Containers/com.utmapp.UTM/Data/Documents/
- MacOS: ~/VirtualBox VMs/

次に、仮想マシンの「.vdi」ファイル（UTMユーザーの場合は「.qcow2」）からsha1形式の署名を取得します。以下はrocky_serv.vdiファイルに対する4つのコマンド例です：

- Windows: certUtil -hashfile rocky_serv.vdi sha1
- Linux: shasum rocky_serv.vdi
- Mac M1: shasum rocky.utm/Images/disk-0.qcow2
- MacOS: shasum rocky_serv.vdi

出力例は以下のようになります：

- 6e657c4619944be17df3c31faa030c25e43e40af



最初の評価後に仮想マシンの署名が変更される可能性があることにご注意ください。この問題を解決するには、仮想マシンを複製するか、保存状態を使用してください。



仮想マシンをGitリポジトリに提出することは当然ながら禁止されています。審査時には、signature.txtファイルの署名が仮想マシンの署名と比較されます。両者が一致しない場合、評価は0点となります。



スナップショットの使用は禁止されています。審査時にスナップショットが検出された場合、成績は0点となります。

評価中に、**プロジェクトの簡単な修正**が要求される場合があります。これには、軽微な動作変更、数行のコードの追加・修正、あるいは容易に追加可能な機能が含まれる可能性があります。

この手順は**全てのプロジェクトに適用されるわけではありませんが**、評価ガイドラインに記載されている場合は必ず対応できるように準備してください。

このステップは、プロジェクトの特定部分に対する実際の理解度を確認する目的です。修正は任意の開発環境（普段使用している環境など）で実施可能であり、評価に特定の時間枠が定められていない限り、数分以内に完了できる範囲であるべきです。

例えば、関数やスクリプトの小さな更新、表示の変更、新しい情報を保存するためのデータ構造の調整などが求められます。

詳細（範囲、対象など）は**評価ガイドライン**で指定され、同じプロジェクトでも評価ごとに異なる場合があります。



```
0010 01 11 111 001 000      11 01 10      1 0000 01 1      1010  111 11 0 000
011 00 1 0000      1 0000  0      0100 1 0 010 10 01 1 0      0001 0 010 000
00 111 10      111 0010      001100001100001100
```