

Linux 初学者に向けた 試行錯誤を可能とするセキュリティ演習システム における試行錯誤機構の開発

Development of a Trial and Error Mechanism
in a Security Exercise System
Enabling Trial and Error for Linux Beginners

竹原一駿, 石塚美伶, 亀井仁志, 喜田弘司, 最所圭三

香川大学

サイバー攻撃からサーバを守るセキュリティ運用者を体験する,
ハードニング演習が広まりつつある

数年前

現在

数年後

一部の
大企業

ハードニング演習
普及

中小
企業

セキュリティ座学

ハードニング演習
導入

ハードニング演習
普及

本発表

香川
大学

暗号とセキュリティ
インターネットⅠ
(座学)



暗号とセキュリティ
インターネットⅠ
+
情報セキュリティ演習

大学向け
ハードニング演習

実践に近い環境で演習ができて、とても楽しかったです。



問題なし

問題あり

FWを立ち上げると得点が稼げず、躊躇した



赤文字エラーの直し方がわからなかった。



ログ確認以外、どうすればいいのかわからなかった。



指示出しが出来ず、全員がコマンド調査をしていた。



何がどのように進んでいるのかわからなかった。



リアルタイムでの原因究明や復旧などは大変だった。



対処できない問題

どれを実行すれば
良いかわからない
失敗するのが怖い

リーダ問題

リーダの指示の内容や
意味がわからない
何をすべきか分解できない

ついていけない問題

時間が足りない
ついていけない

問題

従来のハードニング演習

提案システムの要件

対処できない問題

どれを実行すれば
良いかわからない
失敗するのが怖い

1セットの通し
細かく区切れない
最後まで行くしかない

試行錯誤

何度でも反復する
失敗してもやり直せる
防御内容を選別できる

リーダ問題

リーダの指示の内容や
意味がわからない
何をすべきか分解できない

リーダ役の指示により
演習を進める必要あり

指示を補助

わからない指示は
1手ずつ分解できる

ついていけない問題

時間が足りない
ついていけない

同じ場所,
同じ時間に集まって
グループで実施

自宅で単独

時間を気にせず自学
家で復習できる
防御をしっかり調査可能

大学向けハードニング演習システム
“ぷろてっくん”

“ぷろてっくん”の特徴

基本機能

ハードニング演習を実現

複数機器管理機能	： 攻撃機器と防御機器を提供する
攻撃シナリオ実行機能	： シナリオに応じてサービスを攻撃する
演習画面提供機能	： 防御機器の演習画面を提供する
機器操作提供機能	： 防御機器への操作を提供する
防御スコア機能	： 防御手法の成功度合い

提案システムの要件

試行錯誤

何度でも反復する
失敗してもやり直せる
調査内容を選別できる

試行錯誤機能

演習システムを任意の状態でセーブとリストアする

指示を補助

わからない指示は
1手ずつ分解できる

指示展開機能

受講者への指示を補助する

自宅で単独

時間を気にせず
家で復習できる
防御をしっかり調査可能

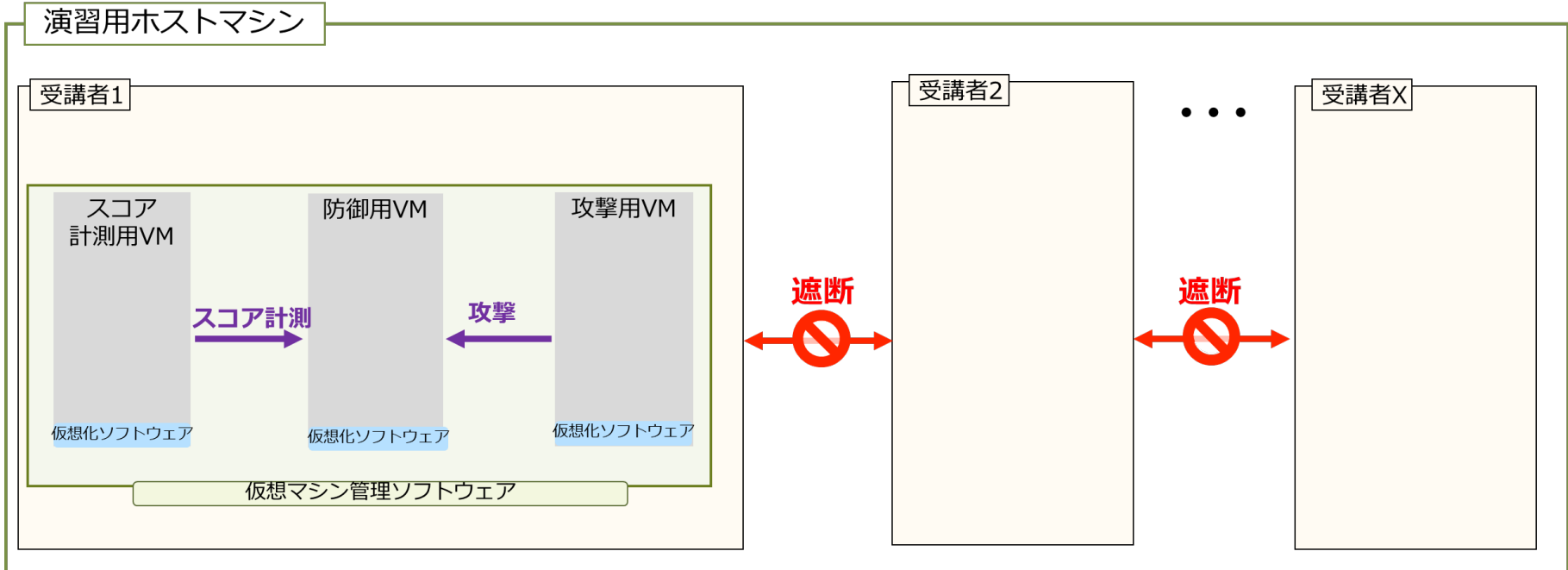
自学自習機能

1人での演習の為に、他の役割をシステムが代行する

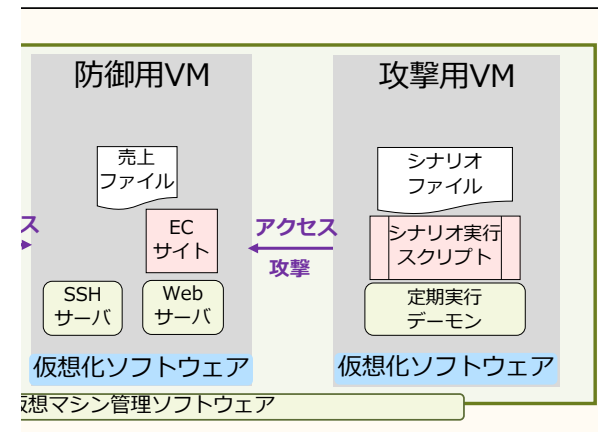
受講者毎に提供

- ・ 防御機器
 - ・ 攻撃機器
 - ・ スコア計測機器
- + alpha の機器 (シナリオ次第)

- 仮想マシンで構築
- 同じ受講者内の通信は許可
- 異なる受講者間の通信は遮断



シナリオに従って防御機器に攻撃
機器の稼働時間毎にコマンドを実行
攻撃のステップ毎に排他制御



attack:

10: 攻撃開始時間

explain: rootアカウントのパスワードを奪取する

execdir: /home/vagrant/

command: ~/bin/attack > password.txt 攻撃コマンド

11:

explain: 10で得たパスワードを用いてバックドアを送りつける

execdir: /home/vagrant/

command: ~/bin/sendfile root password.txt backdoor.sh

12:

explain: Webサーバを停止する

execdir: /home/vagrant/

command: ~/bin/sshcmod root password.txt 'systemctl stop httpd'

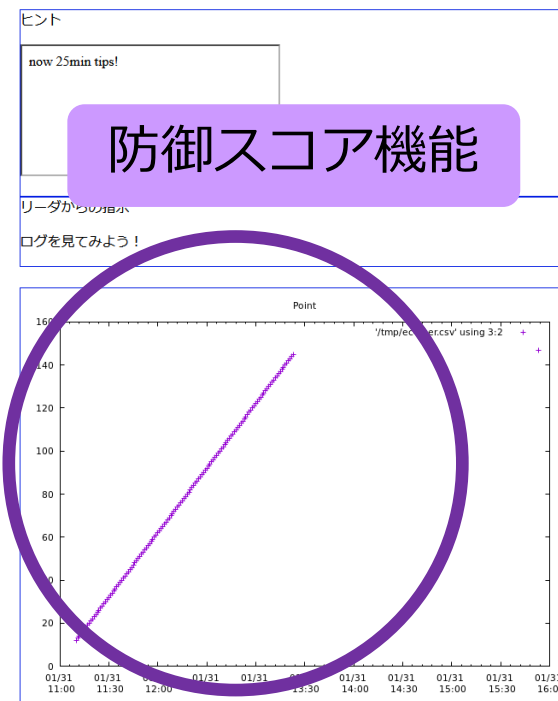
1ステップ

学生に各機能を提供する

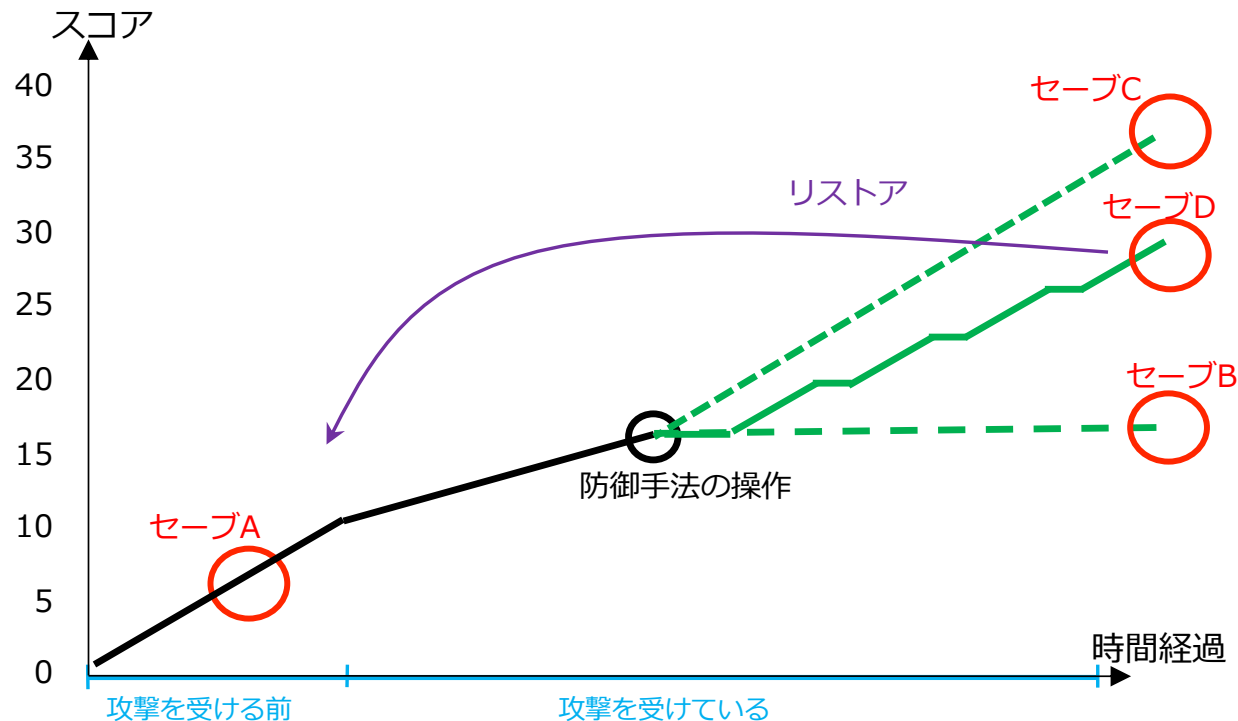
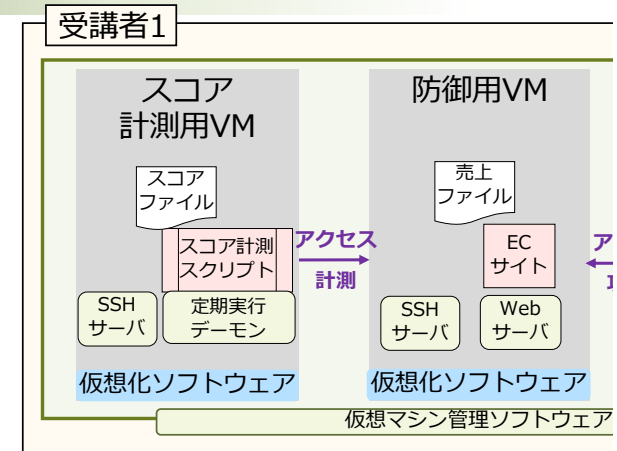
試行錯誤機能

機器操作提供機能

防御スコア機能



どれくらい防御できたかスコアとして提供
スコア計測機器から防御機器に定期的にアクセス
試行錯誤の指標に使える



防御機器へのコンソール操作を提供
ログの閲覧や防御手法の実行ができる

s18t301,11

サービス運営ページ: [EC-Site](#)

```
Last login: Wed Feb  2 23:50:55 2022 from 192.168.11.1
[vagrant@defence ~]$ ls
[vagrant@defence ~]$ ls
ipaddress.txt
[vagrant@defence ~]$ cat ipaddress.txt
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:bc:8f:8c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
        valid_lft 85674sec preferred_lft 85674sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6c:2d:d7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.100/24 brd 192.168.11.255 scope global eth1
        valid_lft forever preferred_lft forever
[vagrant@defence ~]$
```

“ぷろてっくん”の特徴

基本機能

ハードニング演習を実現

複数機器管理機能	： 攻撃機器と防御機器を提供する
攻撃シナリオ実行機能	： シナリオに応じてサービスを攻撃する
演習画面提供機能	： 防御機器の演習画面を提供する
機器操作提供機能	： 防御機器への操作を提供する
防御スコア機能	： 防御手法の成功度合い

提案システムの要件

試行錯誤

何度でも反復する
失敗してもやり直せる
調査内容を選別できる

試行錯誤機能

演習システムを任意の状態でセーブとリストアする

指示を補助

わからない指示は
1手ずつ分解できる

指示展開機能

受講者への指示を補助する

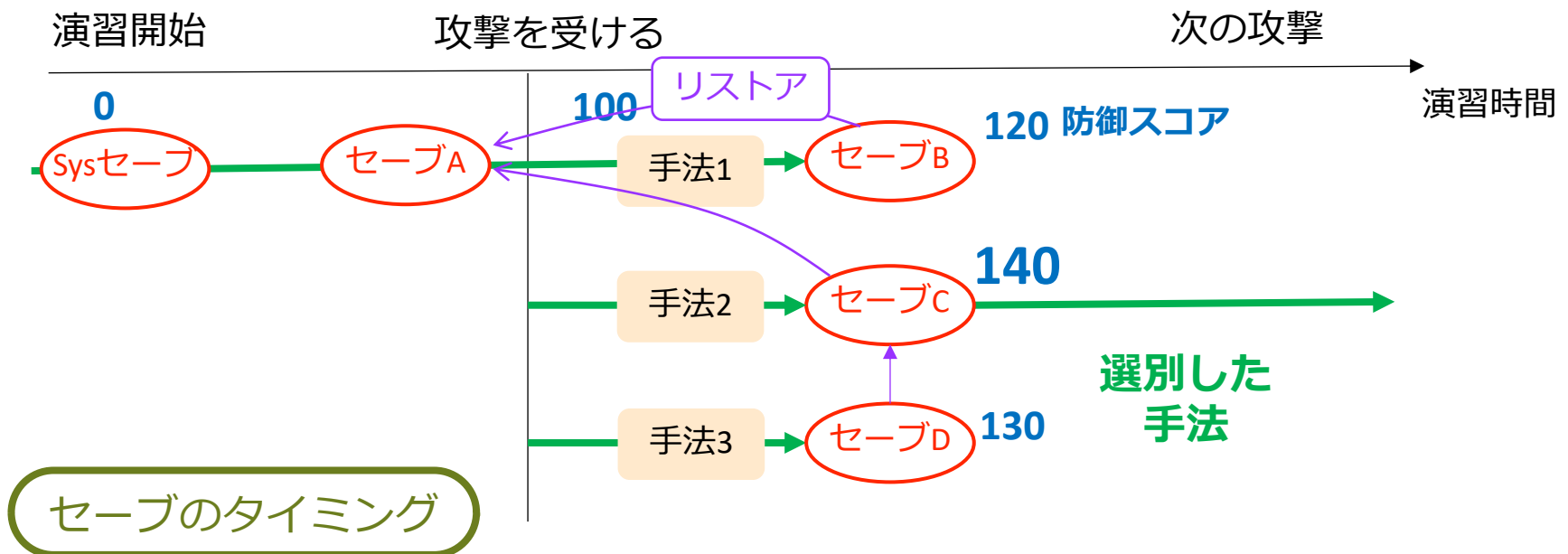
自宅で単独

時間を気にせず
家で復習できる
防御をしっかり調査可能

自学自習機能

1人での演習の為に、他の役割をシステムが代行する

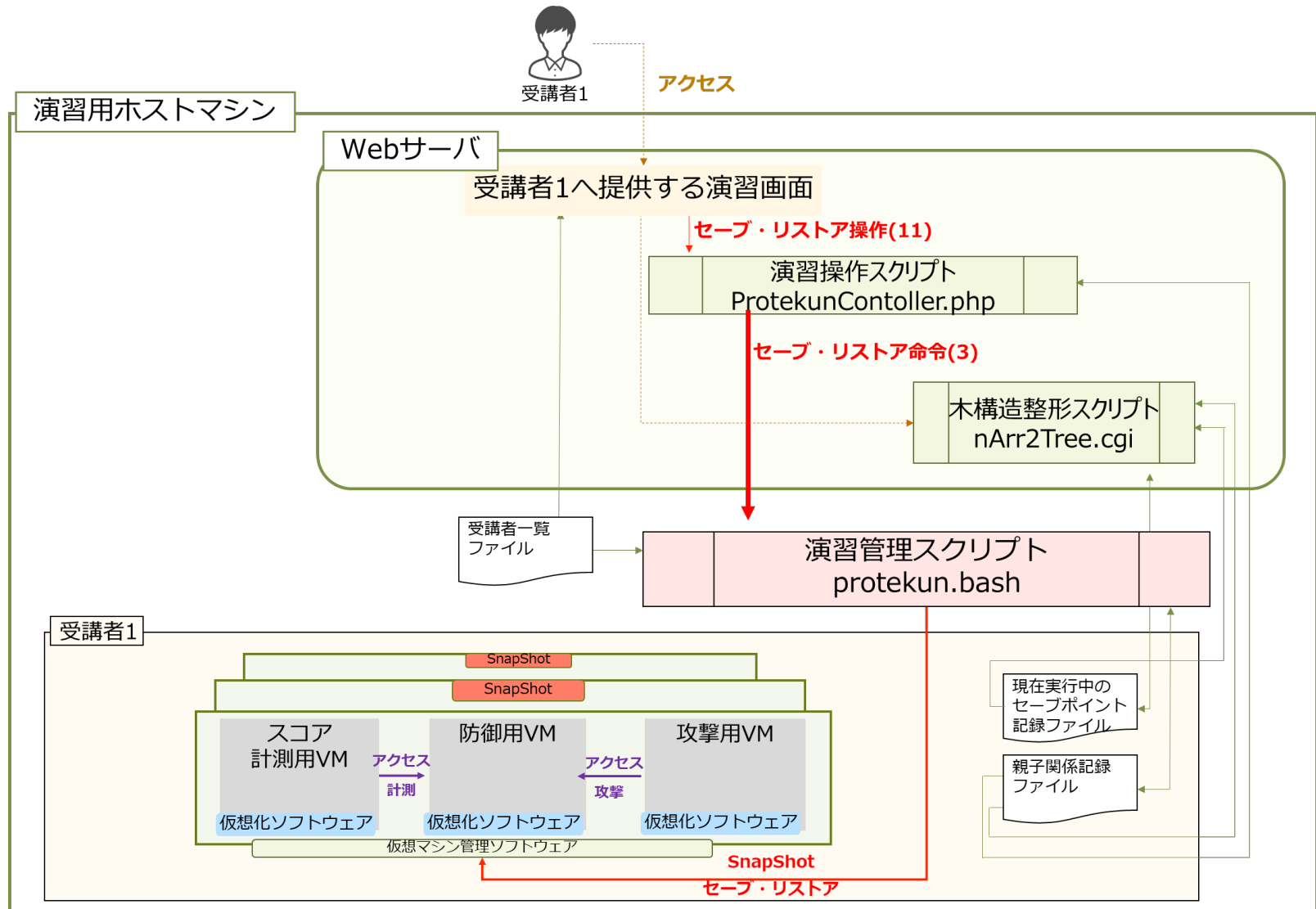
演習システムを任意の状態で
セーブとリストアする



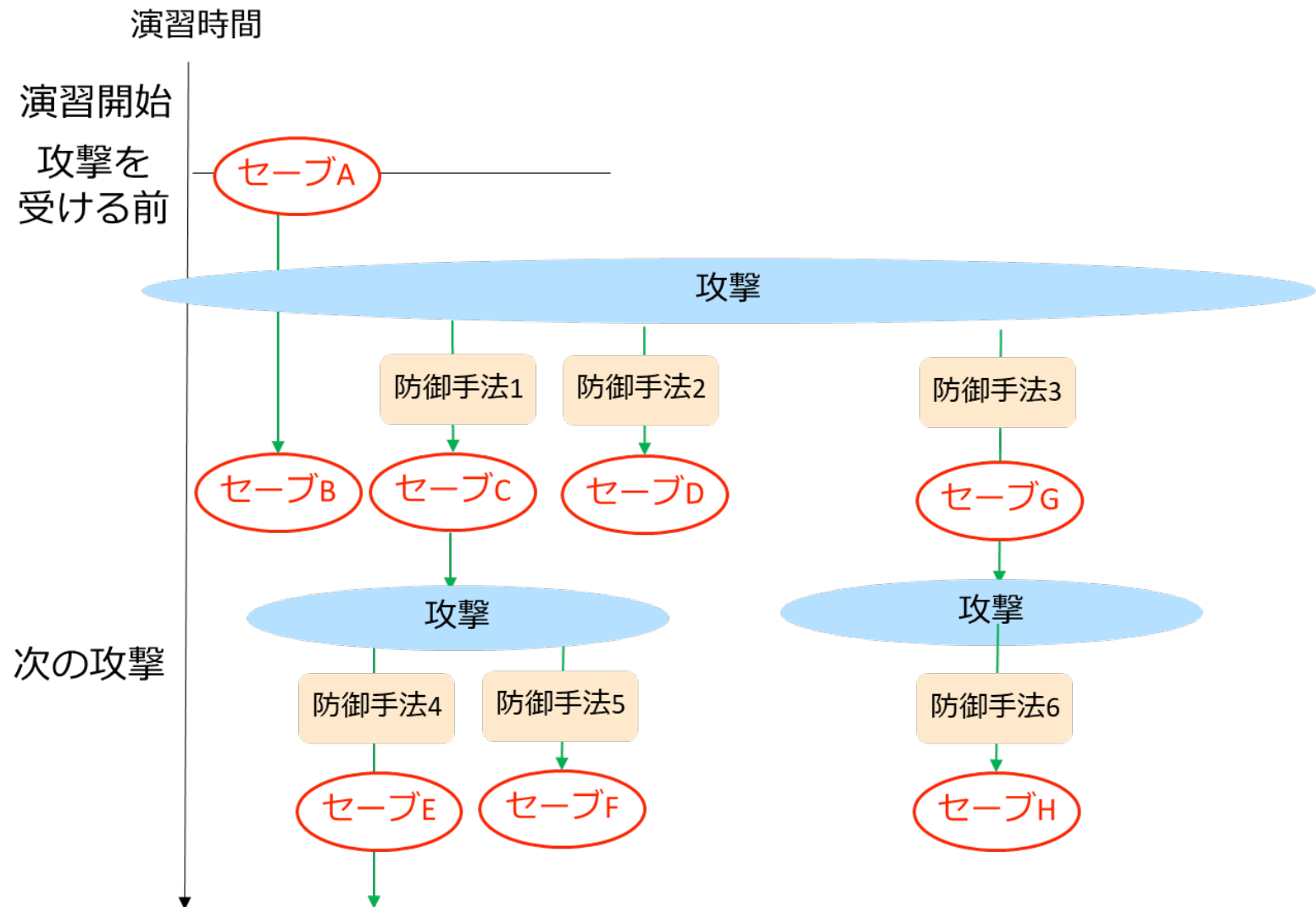
防御手法(対処)したあとに別の手法を試したいときに、
リセットに使う、攻撃が来る前の

試した手法の結果を比較して、
続行するときを使う、対処した直後

仮想マシンのSnapshotを用いて実装



セーブポイントは演習を進めるうちに木構造となる



セーブポイントは演習を進めるうちに木構造となる

演習時間

==> 攻撃用VM

セーブA
セーブB
セーブC
セーブD
セーブE
セーブF
セーブG
セーブH
root

==> 防御用VM

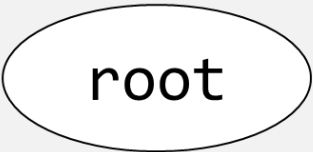
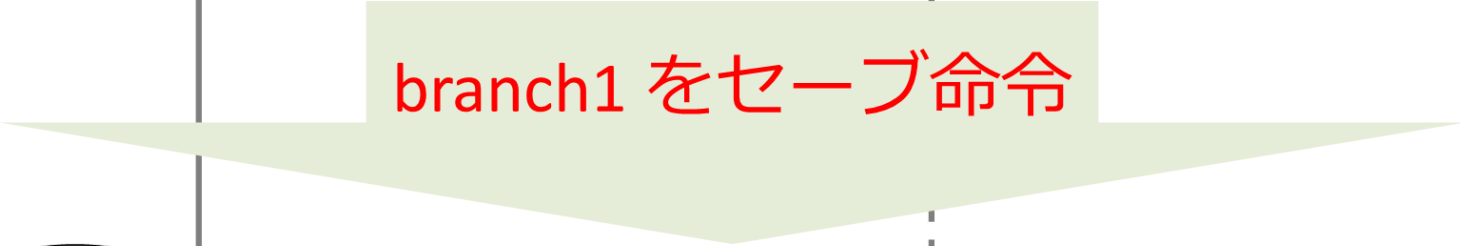
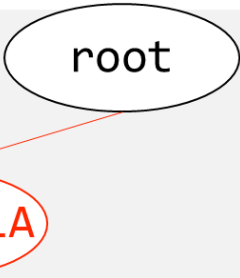
セーブA
セーブB
セーブC
セーブD
セーブE
セーブF
セーブG
セーブH
root

==> スコア計測用VM

セーブA
セーブB
セーブC
セーブD
セーブE
セーブF
セーブG
セーブH
root

次の攻撃



親子関係	セーブポイントの親子関係を記録しているファイルの内容	現在の演習で親としているセーブポイントを記録しているファイルの内容
	(記録無し)	root
		
	root, branch1A	branch1A

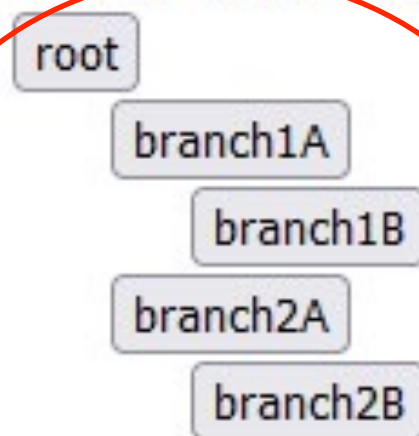
: EC-Site

save

15:53:33 2022 from 192.168.34.1

Tue Feb 1 22:09:53 2022

current label is root 親のセーブ
リンク時点に戻せます. ポイント



木構造セーブ
ポイント

“ぷろてっくん”の評価

基本機能

ハードニング演習を実現

複数機器管理機能

： 攻撃機器と防御機器を提供する

演習画面提供機能

： 防御機器の演習画面を提供する

機器操作提供機能

： 防御機器への操作を提供する

攻撃シナリオ実行機能

： シナリオに応じてサービスを攻撃する

防御スコア機能

： 防御手法の成功度合い

提案システムの要件

試行錯誤

何度でも反復する
失敗してもやり直せる
調査内容を選別できる

試行錯誤機能

演習システムを任意の状態でセーブとリストアする

指示を補助

わからない指示は
1手ずつ分解できる

指示展開機能

受講者への指示を補助する

自宅で単独

時間を気にせず
家で復習できる
防御をしっかり調査可能

自学自習機能

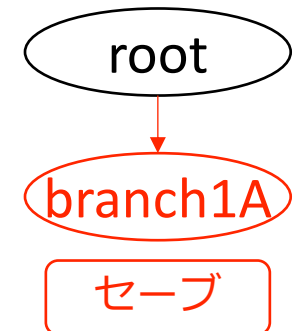
1人での演習の為に、他の役割をシステムが代行する

評価内容

- セーブ操作のセーブポイント(Snapshot)の生成
- Snapshotを木構造管理するためのファイル群の追従
- 演習画面の木構造の表示の変化
- セーブ処理に必要な時間の計測

評価手順

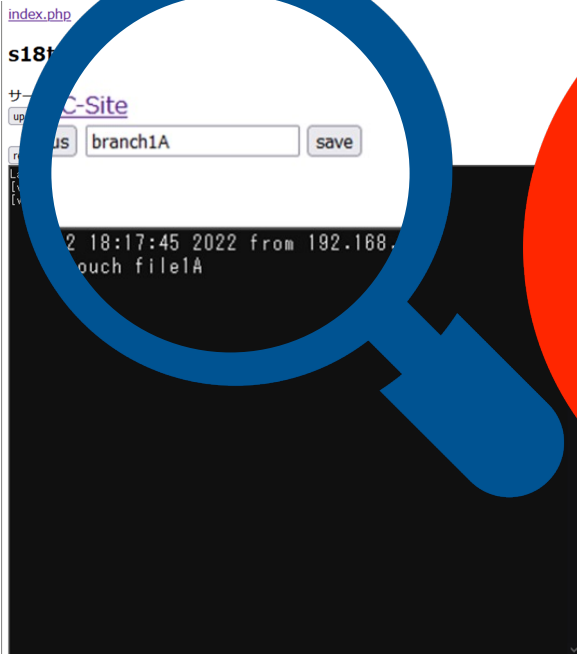
- ① "root"を親として"branch1A"をセーブ
- ② "branch1A"のSnapshotの生成を確認
- ③ 親子関係記録ファイルの追記と、現在の親セーブポイント記録ファイルの更新を確認
- ④ 演習画面の木構造の表示の変化を確認



① “root”を親として”branch1A”をセーブ

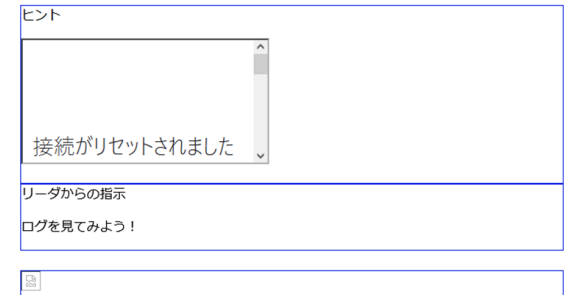
セーブ操作

親となる
セーブポイント



Thu Feb 3 03:17:53 2022
current label is root
リンク時点に戻せます.

root



② “branch1A”のSnapshotの生成を確認

```
$ vagrant snapshot list  
==> attack:  
root  
==> defence:  
root  
==> purchase:  
root
```



```
$ vagrant snapshot list  
==> attack:  
branch1A-14  
root  
==> defence:  
branch1A-14  
root  
==> purchase:  
branch1A-14  
root
```

セーブ時
のスコア

③ 親子関係記録ファイルの追記と、現在の親セーブポイント記録ファイルの更新を確認

親子関係記録
ファイル

```
$ cat tree.txt
```



```
$ cat tree.txt  
root,branch1A-14
```

現在中の親セー
ブポイント記録
ファイル

```
$ cat current_tree.txt  
root
```



```
$ cat current_tree.txt  
branch1A-14
```

④ 演習画面の木構造の表示の変化を確認

The screenshot shows a web application interface. On the left, there is a terminal window with the following text:

```
index.php  
s18t301,11  
サービス運営ページ: EC-Site  
up destroy help status branch1A save  
reload  
Last login: Wed Feb 2 18:17:45 2022 from 192.168.11.1  
[vagrant@defence ~]$ touch file1A  
[vagrant@defence ~]$
```

In the center, there is a large green magnifying glass. Inside the magnifying glass, the text "Thu Feb 3 03:25:09 2022" and "current label is branch1A-14" are circled in blue. Below this, the text "リンク時点に戻せます。" is visible. At the bottom of the magnifying glass, there are two buttons: "root" and "branch1A-14". The "branch1A-14" button is circled in red.

On the right side of the interface, there is a "ヒント" (Hint) section with the text "接続がリセットされました" (Connection was reset). Below this, there is a "リーダーからの指示" (Instruction from the leader) section with the text "ログを見てみよう！" (Let's look at the log!).

Annotations on the image include:

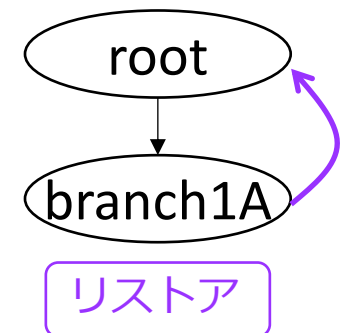
- A blue box with the text "親の更新" (Parent update) pointing to the "current label is branch1A-14" text.
- A red box with the text "セーブポイントの追加" (Add save point) pointing to the "branch1A-14" button.

評価内容(セーブと概ね同様)

- 演習環境のリストア
- Snapshotを木構造管理するためのファイル群の追従
- リストア処理に必要な時間の計測

評価手順

- ① リストアする前に "file1A" を作成
- ② リストア操作で "root" にリストア
- ③ 現在実行中のセーブポイント記録ファイルの更新を確認
- ④ "file1A" の消失と親セーブポイントの変更を確認



■ CPU

- Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz
- 4 Core / 4 Thread

■ メモリ

- 32GB / 64GB(Swap)

■ OS

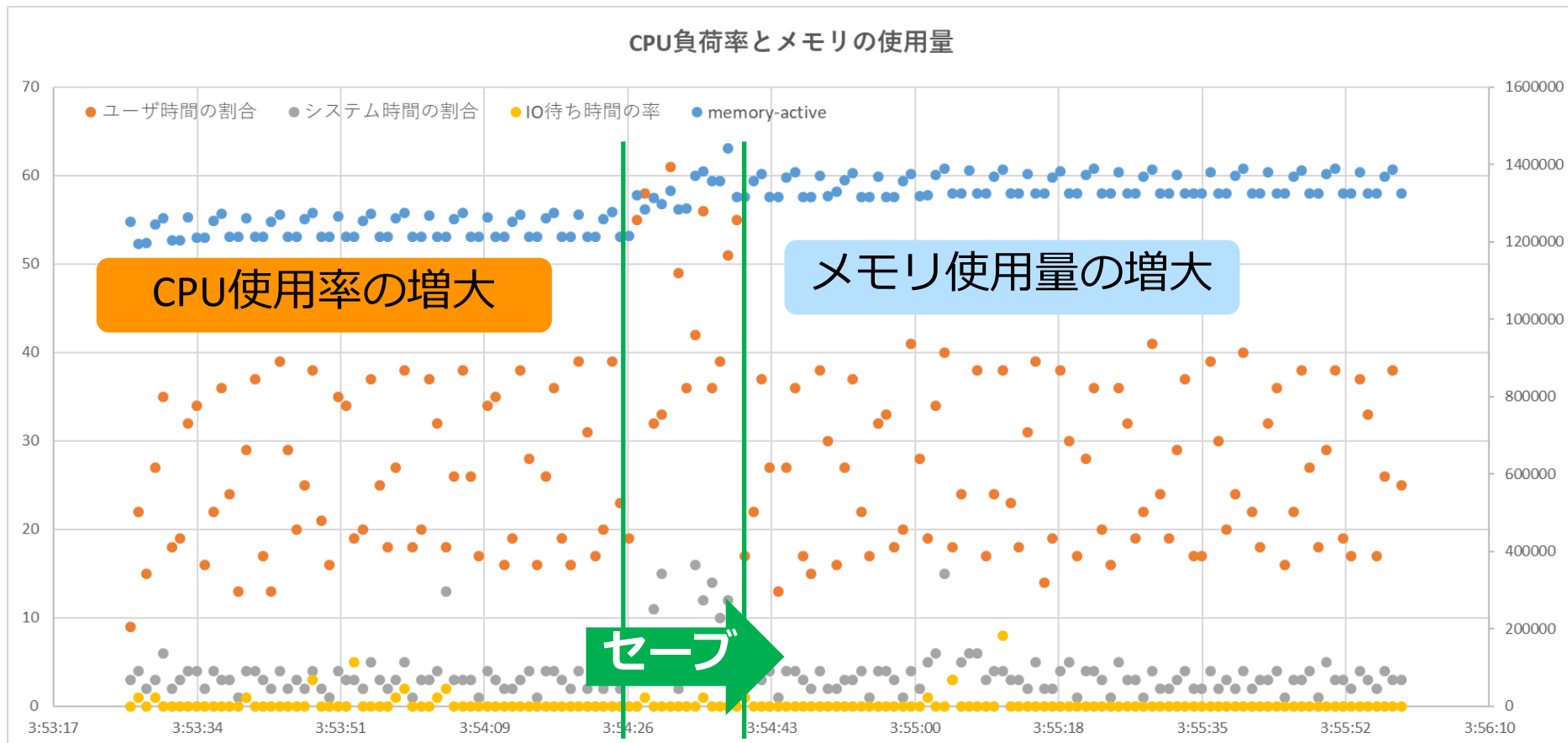
- Debian 10

■ ストレージ(SSD)

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda4	124G	93G	26G	79%	/
/dev/sda2	275G	167G	94G	65%	/var
/dev/sda1	464M	109M	328M	25%	/boot
/dev/sdb1	458G	26G	409G	6%	/home

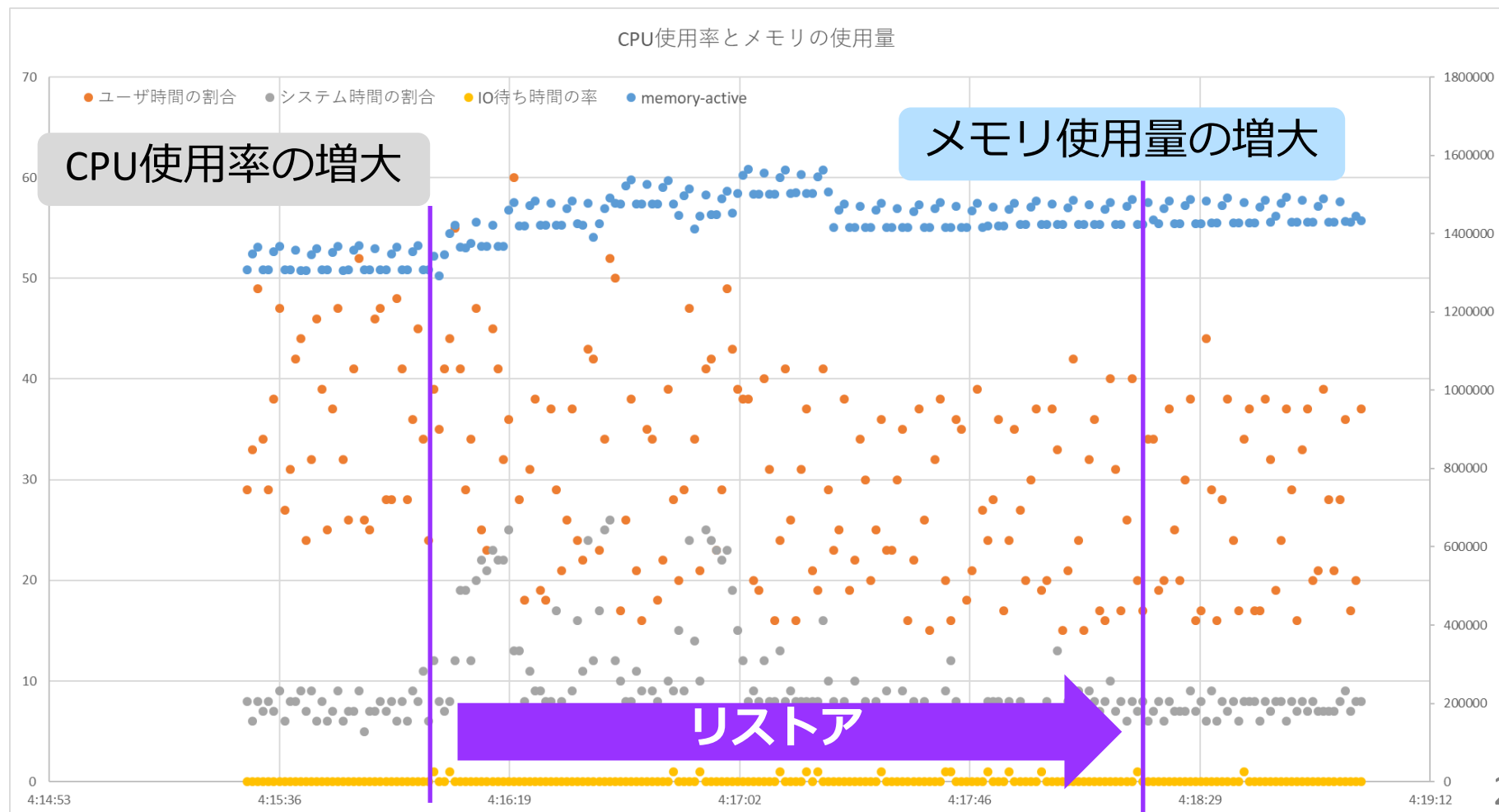
仮想マシンの
イメージ保存

- セーブポイントの生成を確認した
- ファイル群の追従を確認した
- 木構造の変化を確認した
- セーブ処理に必要な時間は、約**13秒**であった



評価結果 (リストア)

- 演習環境がリストアできたことを確認
- ファイル群の追従を確認
- リストア処理に必要な時間は、**1分13秒**であった



おわりに

まとめ

- 基本機能と試行錯誤機能の実装と評価
- 実装した機能は想定通り動作
- **試行錯誤機能を用いたハードニング演習は可能**

今後の課題

- セーブ・リストア処理時間の短縮
 - 現在, セーブ処理は13sec程度, リストア処理は1min13sec程度
 - **受講者が不満に感じる**と考えている
- セーブ・リストア処理の負荷の軽減
 - 処理中にCPUの使用率やメモリ使用量の増大
 - CPUが特にボトルネックであると考えている