セキュリティコンテストでの試行過程の可視化による問題の分析と復習の支援

2024 年度 明星大学 情報学部 情報学科

丸山研究室

21J5-023 遠藤 裕太

背景

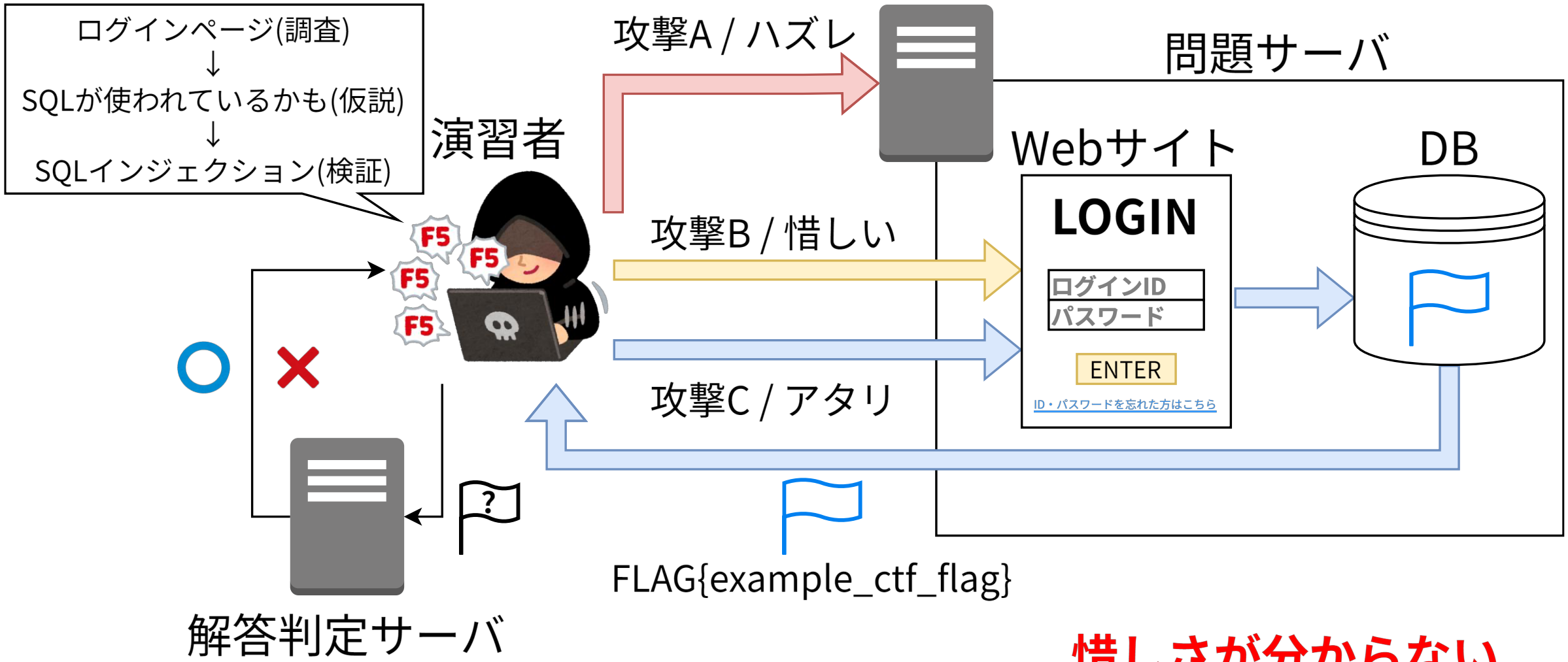
- 実践力や高度な知識を持ったセキュリティ人材が必要
  - 実践力→脅威に対する策を実際のシステムに適用する能力
  - 高度な知識→基礎から応用までを網羅した幅広い知識
- 人材育成において実践的なプログラムなどが提供されている
  - IPAの施策
    - RISS講習 / セキュリティキャンプ / 中核人材育成プログラム
  - NICTの施策
    - CYDER / SecHack365
  - 民間資格
    - OSCP+ / CEH
  - セキュリティコンテスト(CTFなど)

CTF(Capture The Flag)とは

- 対象を攻撃し，隠されたフラッグ(文字列)を取得する競技
  - 正しいフラッグの提出によりスコアを得る
  - 対象はWebシステム・アプリケーション・暗号文など

- 対象に存在する脆弱性への攻撃や解析を行う
  - 情報科学や脆弱性の幅広く高度な知識が必要
  - 知識を活用し実践する力が必要

Webセキュリティ分野のCTFの例



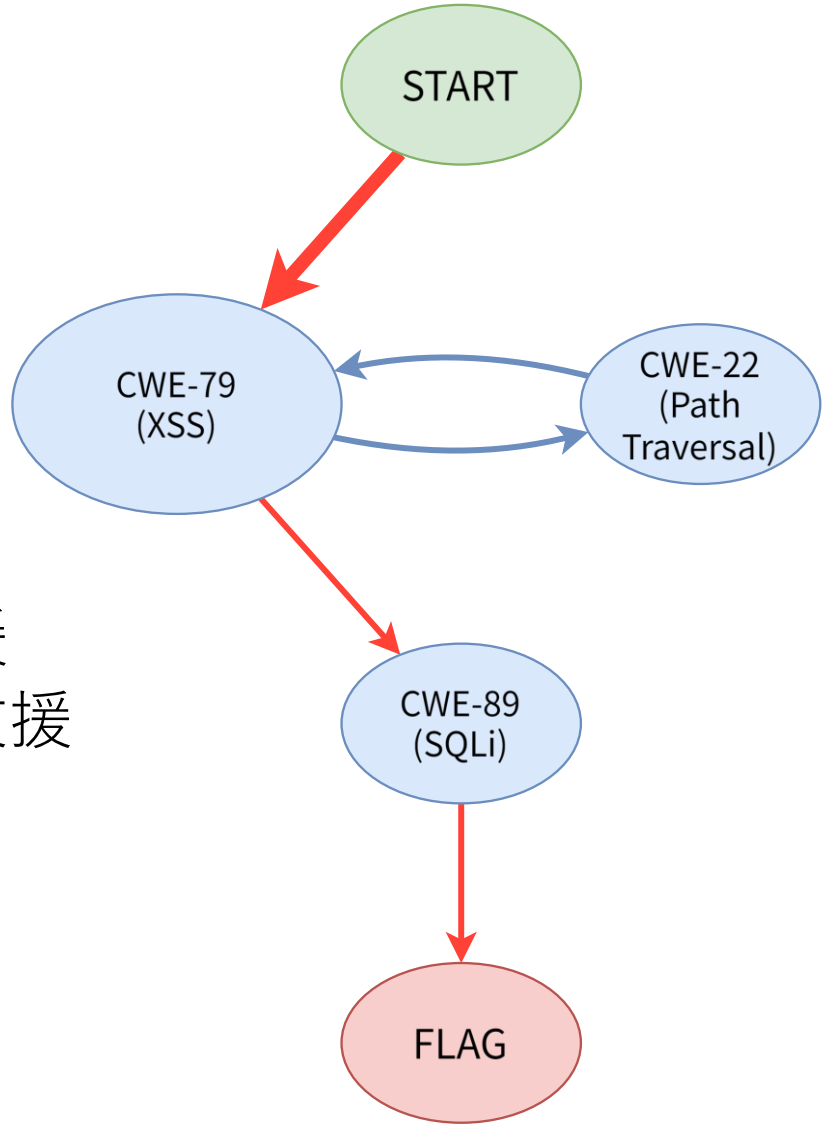
惜しさが分からない

目的

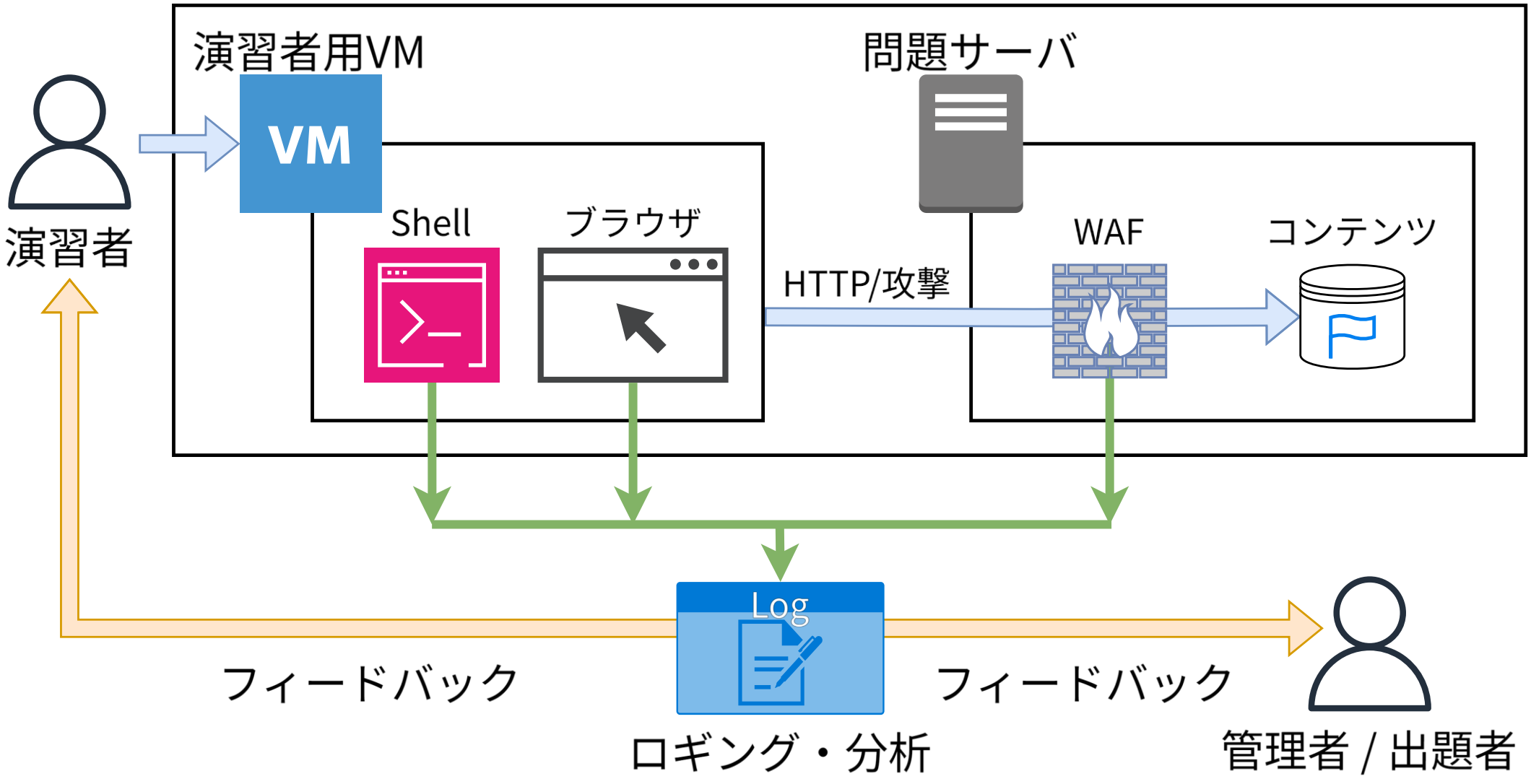
- CTF演習後にフィードバックを行う
  - 全演習者の攻撃行動の詳細表示
    →付随する各種行動も表示
  - 演習者全体の攻撃遷移の可視化

- 期待される効果
  - 演習者→自身と他人の行動比較・振り返りを支援
  - 出題者→問題分析・演習者の解法の評価などを支援

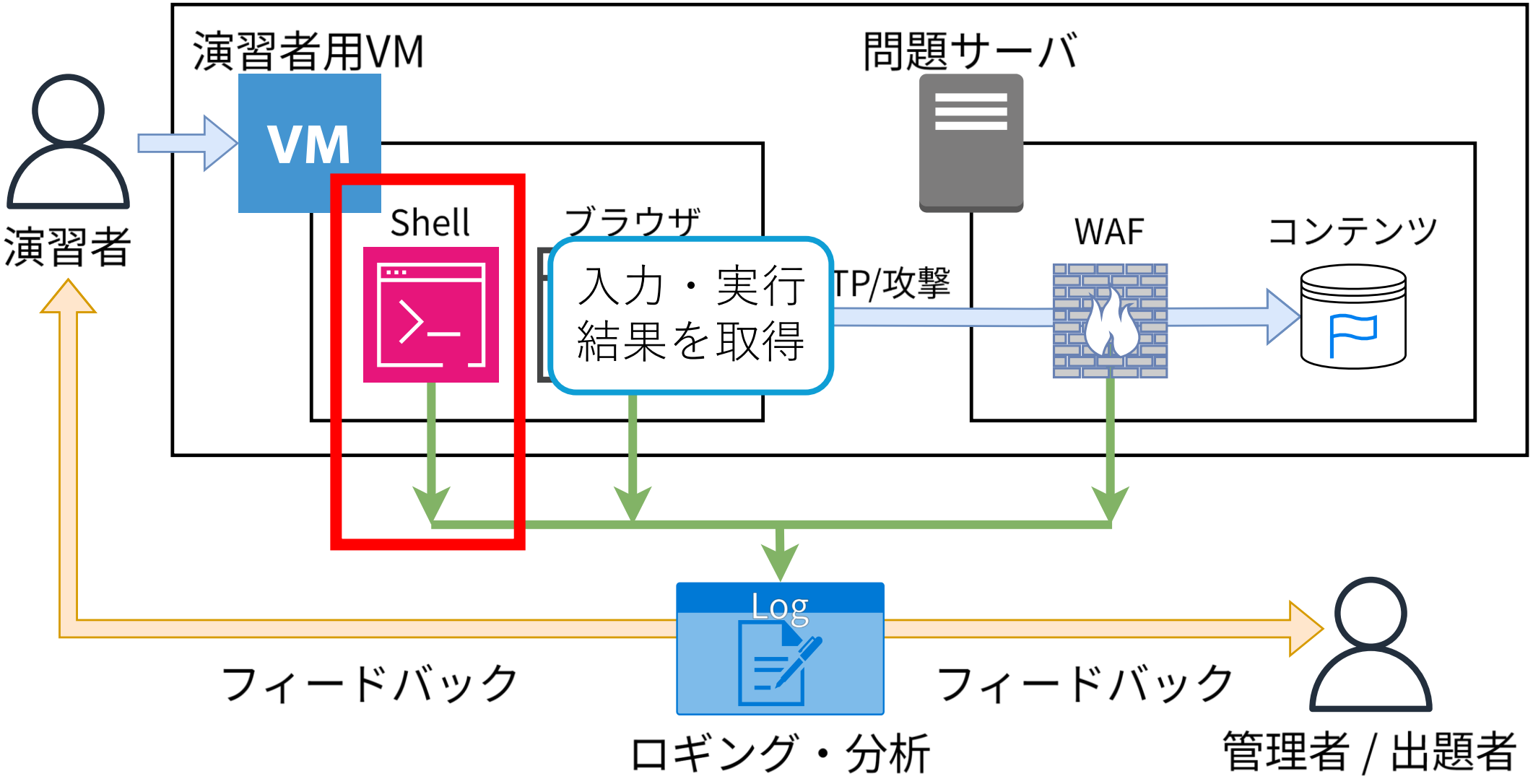
- Webセキュリティ分野を対象



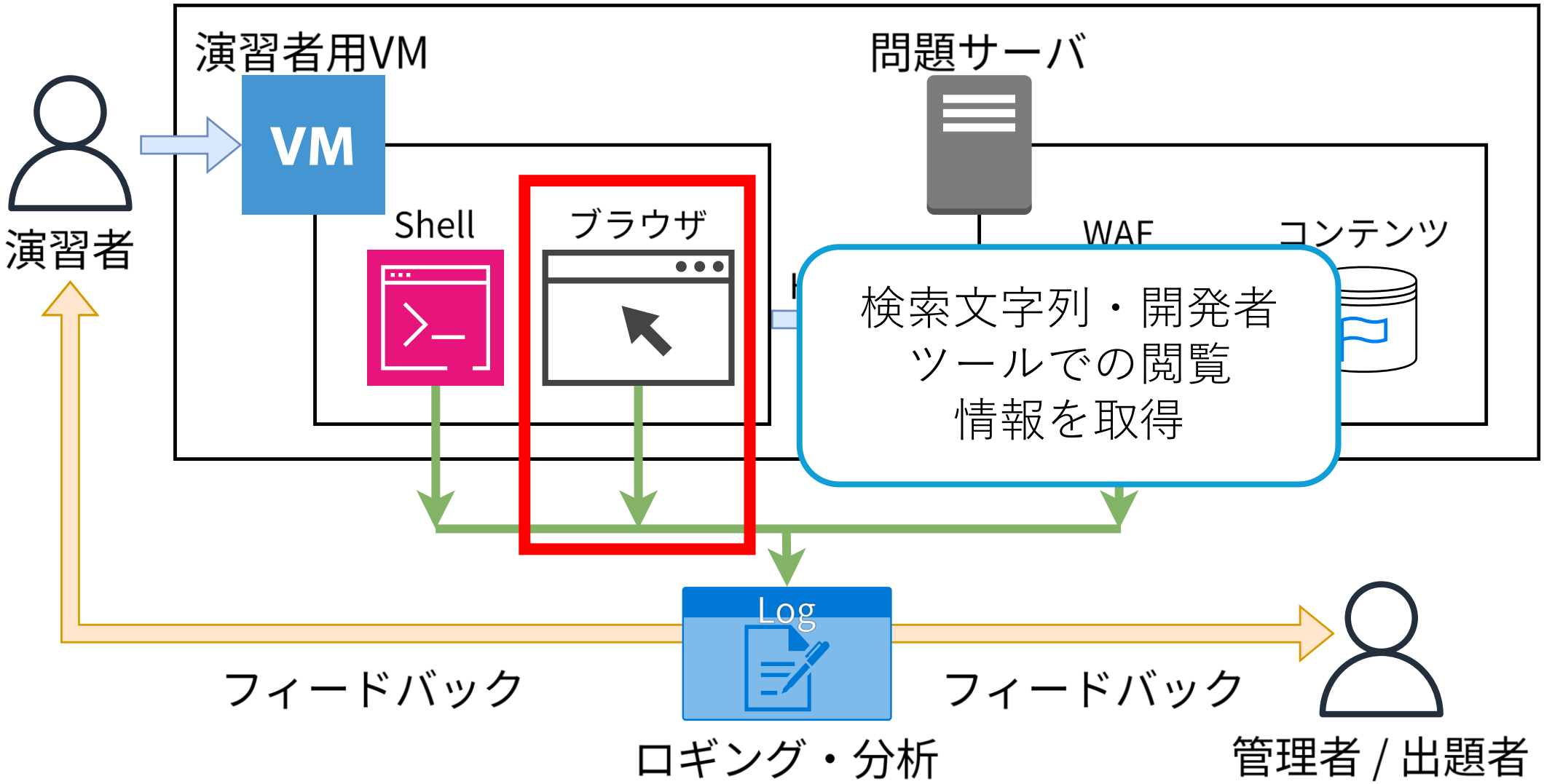
提案手法 - 概要図


演習者用VM
問題サーバ
VM
演習者
Shell
ブラウザ
WAF
コンテンツ
HTTP/攻撃
Log
フィードバック
フィードバック
ロギング・分析
管理者 / 出題者

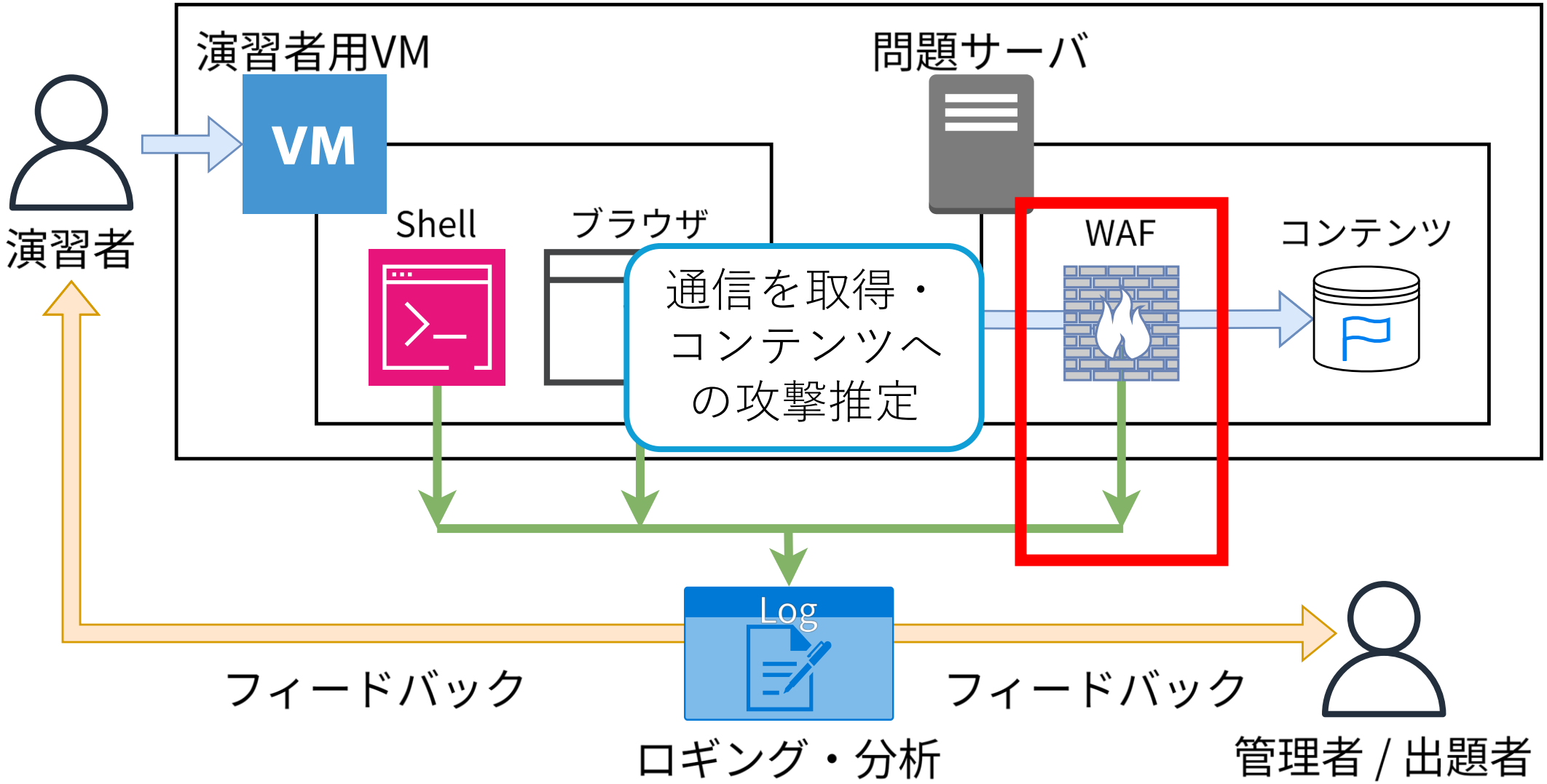
提案手法 - Shell


演習者用VM
問題サーバ
VM
演習者
Shell
ブラウザ
入力・実行
結果を取得
TP/攻撃
WAF
コンテンツ
Log
フィードバック
フィードバック
ロギング・分析
管理者 / 出題者

提案手法 - ブラウザ


演習者用VM
問題サーバ
VM
演習者
Shell
ブラウザ
WAF
コンテンツ
検索文字列・開発者
ツールでの閲覧
情報を取得
Log
フィードバック
フィードバック
ロギング・分析
管理者 / 出題者

提案手法 - Web Application Firewall



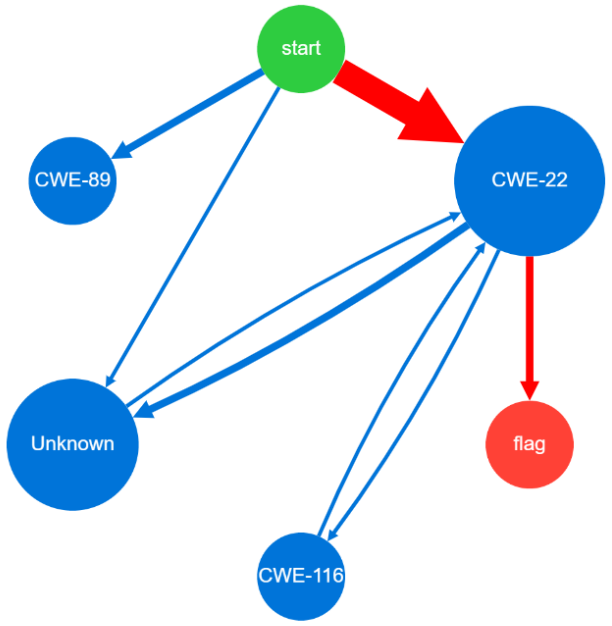
実装 – 攻撃手法の推定・分析

- 仮想環境上での各種情報をロギング
  - 演習者VM
    - コマンド入力・実行結果・ブラウジング情報
  - 問題サーバVM
    - 問題サーバへのHTTPリクエスト

- ログデータから攻撃分類・遷移を推定
  - 問題サーバへのHTTPログを利用
    →WAF(ModSecurity)で攻撃検出・攻撃名称を取得
  - 分類基準に共通脆弱性タイプ一覧(CWE)を利用
  - CWEを基にした辞書を作成し，ログにCWE-IDを紐づける

実装－フィードバック

192.168.178.121



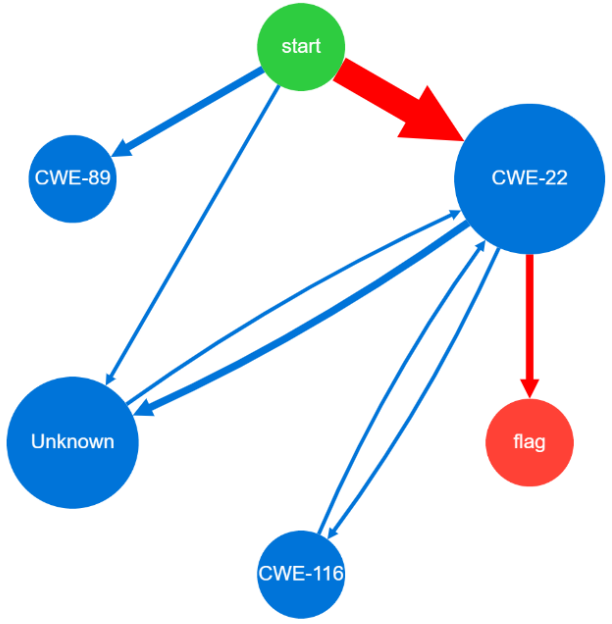
ブラウザ検索ログ

client_ip	query	time
filter data...		
192.168.178.121	zipファイル　攻撃	2024-12-26 18:33:35
192.168.178.121	ubuntu テキストファイル 作成	2024-12-26 18:36:24
192.168.178.121	ubuntu テキストファイル 作成	2024-12-26 18:36:30
192.168.178.121	zipファイルにパスを含ませる	2024-12-26 18:44:03
192.168.178.121	zip slip やり方	2024-12-26 18:49:23
192.168.178.121	7zip	2024-12-26 18:53:50
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:01:08
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:01:37
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:01:59
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:39:10
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:39:49
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:39:51
192.168.178.121	zip slip やり方	2024-12-26 19:39:53

client_ip	prev	next	unique_id	uri	message	time
121						
192.168.178.121	start	CWE-22	173520763296.620096	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:12
192.168.178.121	CWE-22	CWE-22	173520764640.324145	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:26
192.168.178.121	CWE-22	CWE-22	173520937889.638779	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:18
192.168.178.121	CWE-22	CWE-22	173520939449.586298	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:34
192.168.178.121	CWE-22	CWE-22	17352094543.222612	/?filename=..%2F..%2F	Path Traversal Attack (/../)	2024-12-26 19:37:34
192.168.178.121	CWE-22	CWE-22	173520953677.324551	/?filename=..%2F	Path Traversal Attack (/../)	2024-12-26 19:38:56
192.168.178.121	CWE-22	CWE-22	173520965044.424002	/?filename=..%2F..%2F..%2FGO.txt	Path Traversal Attack (/../)	2024-12-26 19:40:50

実装－フィードバック

192.168.178.121



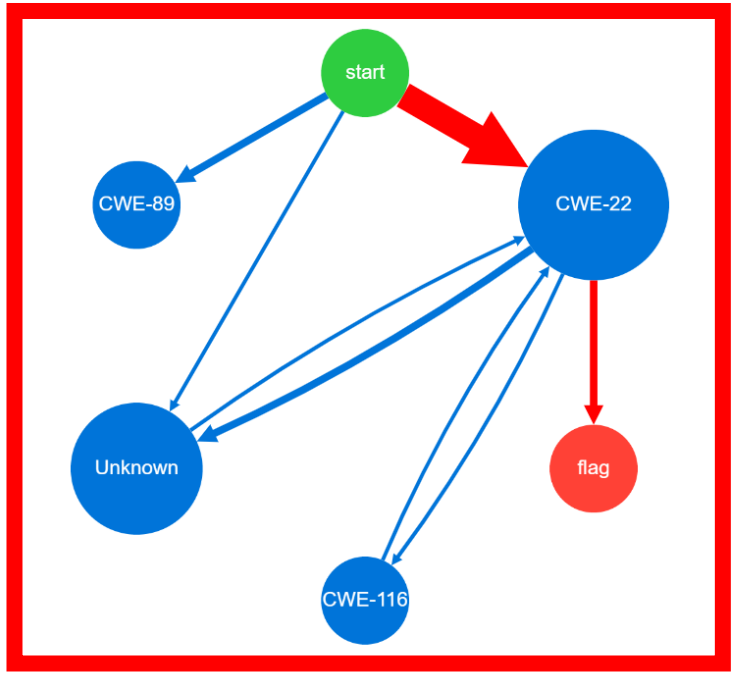
選択したユーザの
攻撃遷移をハイライト

client_ip	query	time
		2024-12-26 18:33:35
		2024-12-26 18:36:24
		2024-12-26 18:36:30
		2024-12-26 18:44:03
		2024-12-26 18:49:23
		2024-12-26 18:53:50
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:01:08
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:01:37
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:01:59
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:39:10
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:39:49
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:39:51
192.168.178.121	zip slip やり方	2024-12-26 19:39:53

client_ip	prev	next	unique_id	uri	message	time
121						
192.168.178.121	start	CWE-22	173520763296.620096	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:12
192.168.178.121	CWE-22	CWE-22	173520764640.324145	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:26
192.168.178.121	CWE-22	CWE-22	173520937889.638779	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:18
192.168.178.121	CWE-22	CWE-22	173520939449.586298	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:34
192.168.178.121	CWE-22	CWE-22	17352094543.222612	/?filename=..%2F..%2F	Path Traversal Attack (/../)	2024-12-26 19:37:34
192.168.178.121	CWE-22	CWE-22	173520953677.324551	/?filename=..%2F	Path Traversal Attack (/../)	2024-12-26 19:38:56
192.168.178.121	CWE-22	CWE-22	173520965044.424002	/?filename=..%2F..%2F..%2FGO.txt	Path Traversal Attack (/../)	2024-12-26 19:40:50

実装－フィードバック

192.168.178.121



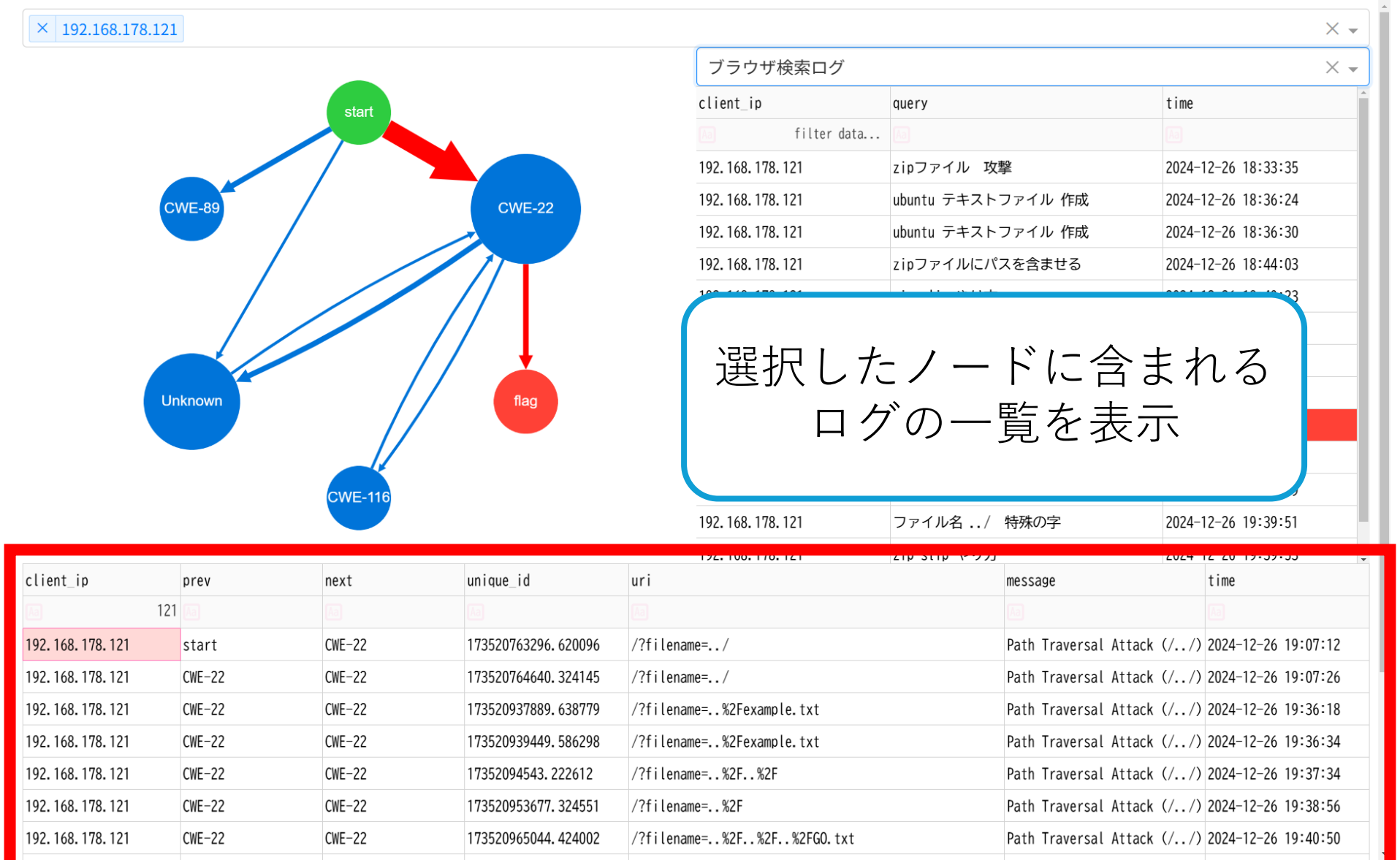
攻撃手法遷移をグラフ化
ノード・矢印の大きさで
該当数の多さを示す

ブラウザ検索ログ

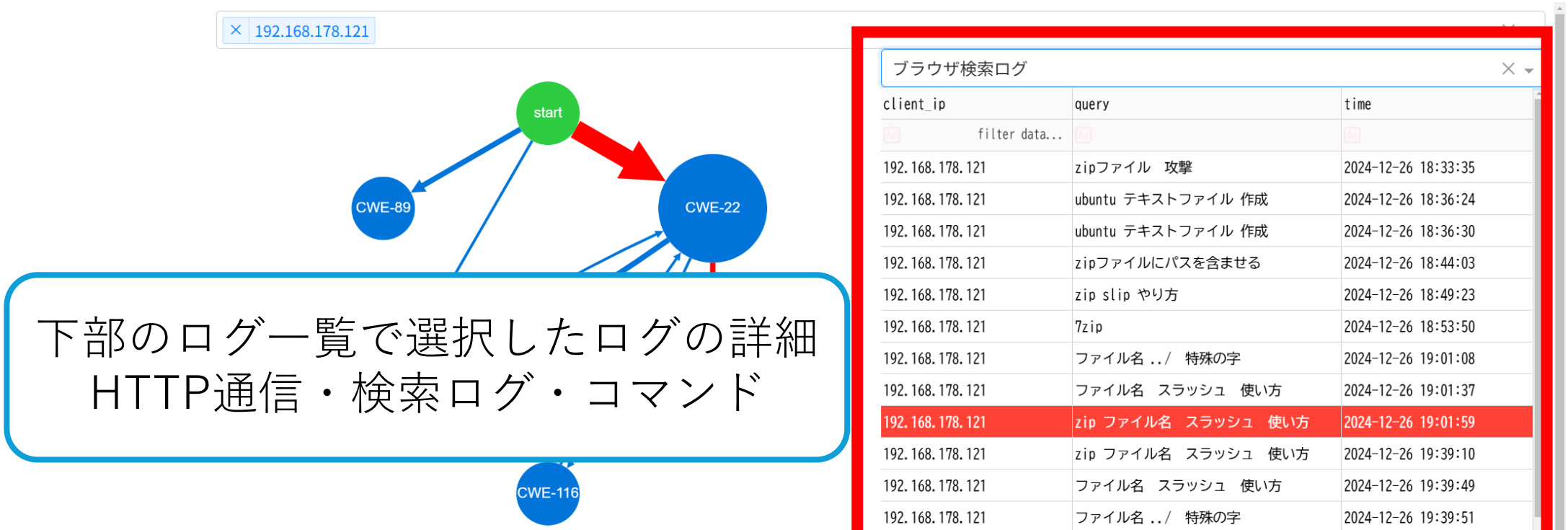
client_ip	query	time
filter data...		
		18:33:35
		:36:24
		:36:30
		:44:03
		:49:23
		:53:50
		19:01:08
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:01:37
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:01:59
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:39:10
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:39:49
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:39:51
192.168.178.121	zip slip やり方	2024-12-26 19:39:53

client_ip	prev	next	unique_id	uri	message	time
121						
192.168.178.121	start	CWE-22	173520763296.620096	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:12
192.168.178.121	CWE-22	CWE-22	173520764640.324145	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:26
192.168.178.121	CWE-22	CWE-22	173520937889.638779	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:18
192.168.178.121	CWE-22	CWE-22	173520939449.586298	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:34
192.168.178.121	CWE-22	CWE-22	17352094543.222612	/?filename=..%2F..%2F	Path Traversal Attack (/../)	2024-12-26 19:37:34
192.168.178.121	CWE-22	CWE-22	173520953677.324551	/?filename=..%2F	Path Traversal Attack (/../)	2024-12-26 19:38:56
192.168.178.121	CWE-22	CWE-22	173520965044.424002	/?filename=..%2F..%2F..%2FGO.txt	Path Traversal Attack (/../)	2024-12-26 19:40:50

実装－フィードバック


192.168.178.121
start
CWE-89
CWE-22
Unknown
flag
CWE-116
ブラウザ検索ログ
client_ip
query
time
filter data...
192.168.178.121
zipファイル　攻撃
2024-12-26 18:33:35
192.168.178.121
ubuntu テキストファイル 作成
2024-12-26 18:36:24
192.168.178.121
ubuntu テキストファイル 作成
2024-12-26 18:36:30
192.168.178.121
zipファイルにパスを含ませる
2024-12-26 18:44:03
192.168.178.121
ファイル名 ../　特殊の字
2024-12-26 19:39:51
選択したノードに含まれる
ログの一覧を表示
client_ip
prev
next
unique_id
uri
message
time
192.168.178.121
start
CWE-22
173520763296.620096
/?filename=../
Path Traversal Attack (/../)
2024-12-26 19:07:12
192.168.178.121
CWE-22
CWE-22
173520764640.324145
/?filename=../
Path Traversal Attack (/../)
2024-12-26 19:07:26
192.168.178.121
CWE-22
CWE-22
173520937889.638779
/?filename=..%2Fexample.txt
Path Traversal Attack (/../)
2024-12-26 19:36:18
192.168.178.121
CWE-22
CWE-22
173520939449.586298
/?filename=..%2Fexample.txt
Path Traversal Attack (/../)
2024-12-26 19:36:34
192.168.178.121
CWE-22
CWE-22
17352094543.222612
/?filename=..%2F..%2F
Path Traversal Attack (/../)
2024-12-26 19:37:34
192.168.178.121
CWE-22
CWE-22
173520953677.324551
/?filename=..%2F
Path Traversal Attack (/../)
2024-12-26 19:38:56
192.168.178.121
CWE-22
CWE-22
173520965044.424002
/?filename=..%2F..%2F..%2FGO.txt
Path Traversal Attack (/../)
2024-12-26 19:40:50

実装－フィードバック



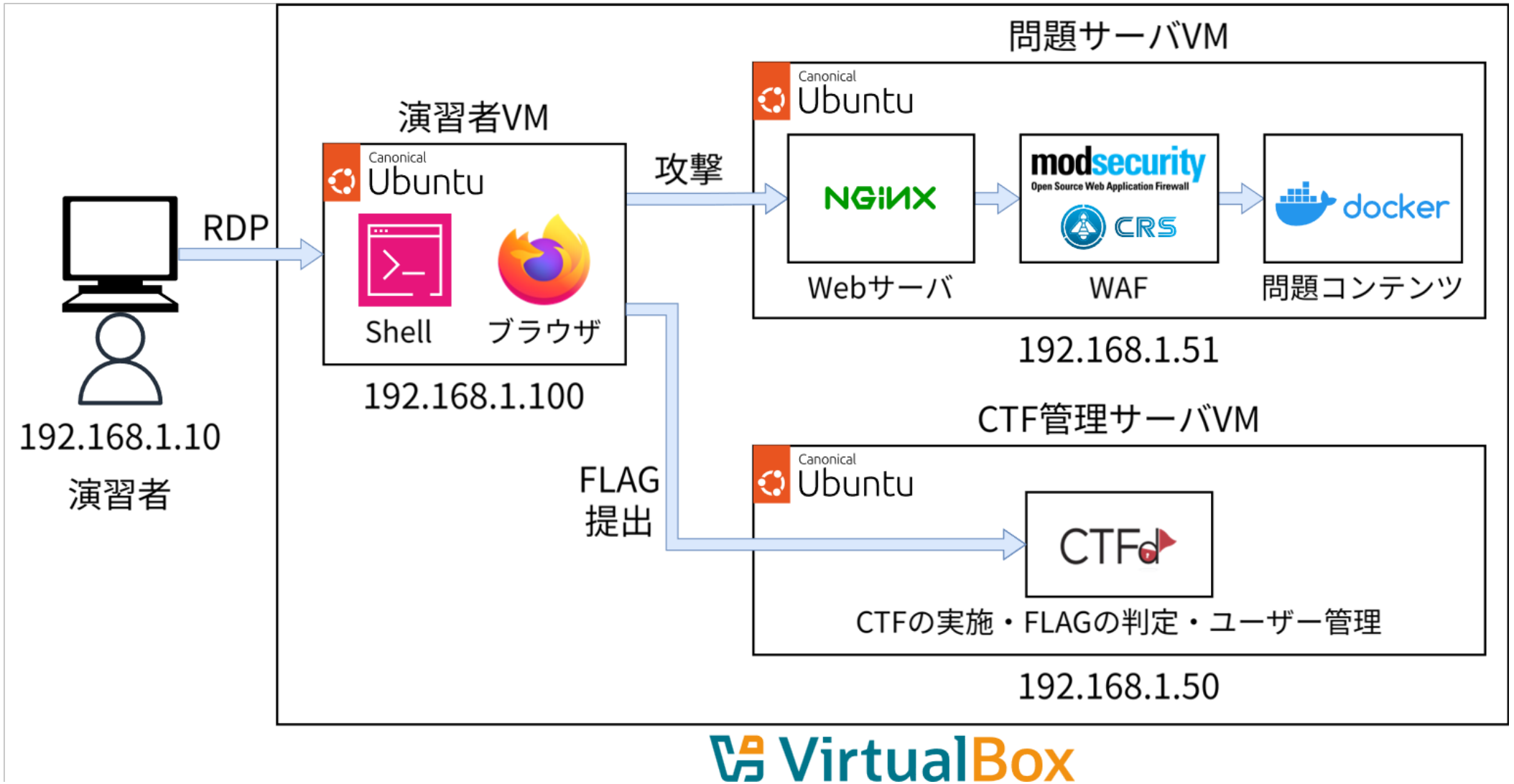
下部のログ一覧で選択したログの詳細
HTTP通信・検索ログ・コマンド

ブラウザ検索ログ

client_ip	query	time
filter data...		
192.168.178.121	zipファイル　攻撃	2024-12-26 18:33:35
192.168.178.121	ubuntu テキストファイル 作成	2024-12-26 18:36:24
192.168.178.121	ubuntu テキストファイル 作成	2024-12-26 18:36:30
192.168.178.121	zipファイルにパスを含ませる	2024-12-26 18:44:03
192.168.178.121	zip slip やり方	2024-12-26 18:49:23
192.168.178.121	7zip	2024-12-26 18:53:50
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:01:08
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:01:37
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:01:59
192.168.178.121	zip ファイル名　スラッシュ　使い方	2024-12-26 19:39:10
192.168.178.121	ファイル名　スラッシュ　使い方	2024-12-26 19:39:49
192.168.178.121	ファイル名 ../　特殊の字	2024-12-26 19:39:51
192.168.178.121	zip slip やり方	2024-12-26 19:39:53

client_ip	prev	next	unique_id	uri	message	time
121						
192.168.178.121	start	CWE-22	173520763296.620096	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:12
192.168.178.121	CWE-22	CWE-22	173520764640.324145	/?filename=../	Path Traversal Attack (/../)	2024-12-26 19:07:26
192.168.178.121	CWE-22	CWE-22	173520937889.638779	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:18
192.168.178.121	CWE-22	CWE-22	173520939449.586298	/?filename=..%2Fexample.txt	Path Traversal Attack (/../)	2024-12-26 19:36:34
192.168.178.121	CWE-22	CWE-22	17352094543.222612	/?filename=..%2F..%2F	Path Traversal Attack (/../)	2024-12-26 19:37:34
192.168.178.121	CWE-22	CWE-22	173520953677.324551	/?filename=..%2F	Path Traversal Attack (/../)	2024-12-26 19:38:56
192.168.178.121	CWE-22	CWE-22	173520965044.424002	/?filename=..%2F..%2F..%2FGO.txt	Path Traversal Attack (/../)	2024-12-26 19:40:50

実装 – 演習環境


問題サーバVM
Canonical
Ubuntu
演習者VM
Canonical
Ubuntu
攻撃
RDP
NGINX
modsecurity
Open Source Web Application Firewall
CRS
docker
Shell
ブラウザ
Webサーバ
WAF
問題コンテンツ
192.168.1.51
192.168.1.100
CTF管理サーバVM
192.168.1.10
演習者
FLAG
提出
Canonical
Ubuntu
CTFd
CTFの実施・FLAGの判定・ユーザー管理
192.168.1.50
VirtualBox

実験 – 本実験

- 提案システム(一部機能は無効化)の確認
  - 演習者側は，セキュリティ知識のない学生5名
  - 出題者側は，予備実験で演習を行った学生3名
  - セキュリティ学習コンテンツの実施
  - 予備実験で出題した問題から1問を出題
  - 有用性と有用なフィードバック項目などをアンケート評価

- 結果
  - 有用性について演習者・出題者の両方から高い評価を得る
  - 演習者・出題者共に，攻撃ログ一覧が一番有用と評価

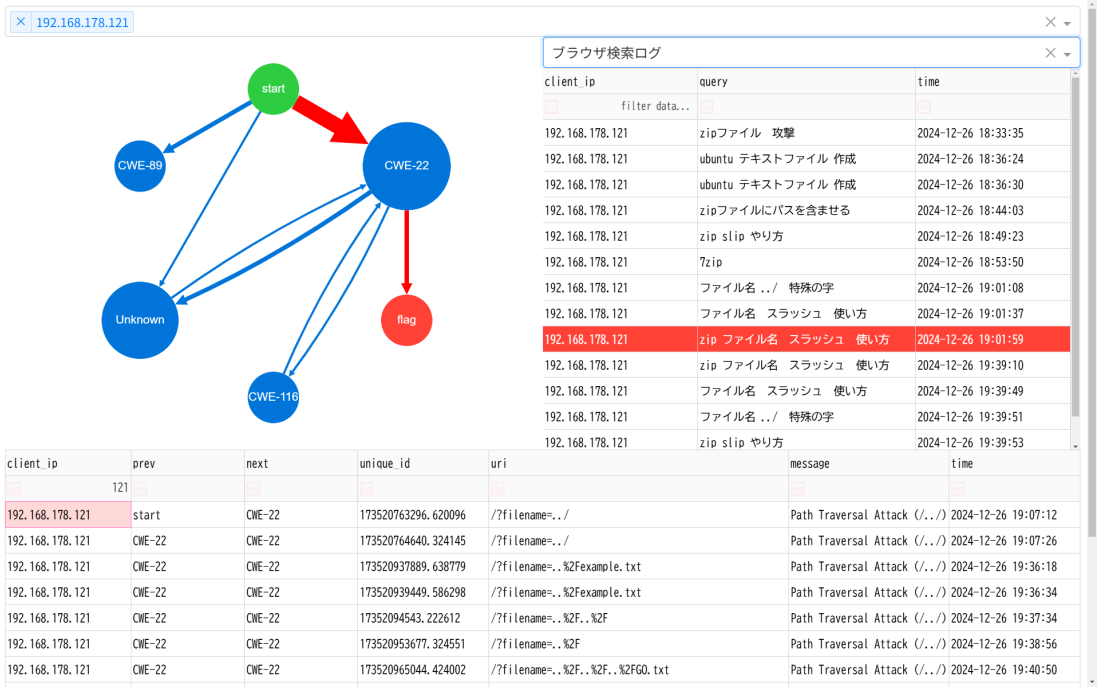
実験 - アンケート結果

- Q3 自身の攻撃や行動は網羅されていましたか？
- Q4 他人の行動は分かりやすいですか？
- Q5 自身の行動の振り返り・分析に役立ちましたか？

- 「とてもそう思う」を5 「とてもそう思わない」を1とした5段階の平均値

Q3 網羅されていたか	Q4 分かりやすいか	Q5 役立つか
4	4.4	4.4

考察(1)



- 提案システムの評価
  - ○分析・振り返り用途で高評価
    - →有用性がある
  - ○攻撃ログ一覧が高評価
    - →URLに攻撃の差が明確に表れる影響
- フィードバックシステムの表示
  - ×攻撃遷移グラフのCWE-ID表記が分かりにくい
    - →攻撃手法名でノードを示す
- 攻撃の推定における課題
  - Unknownラベルがついたものを分析
    - →CWE辞書の不足や，文字列的な攻撃手法の推定に課題がある

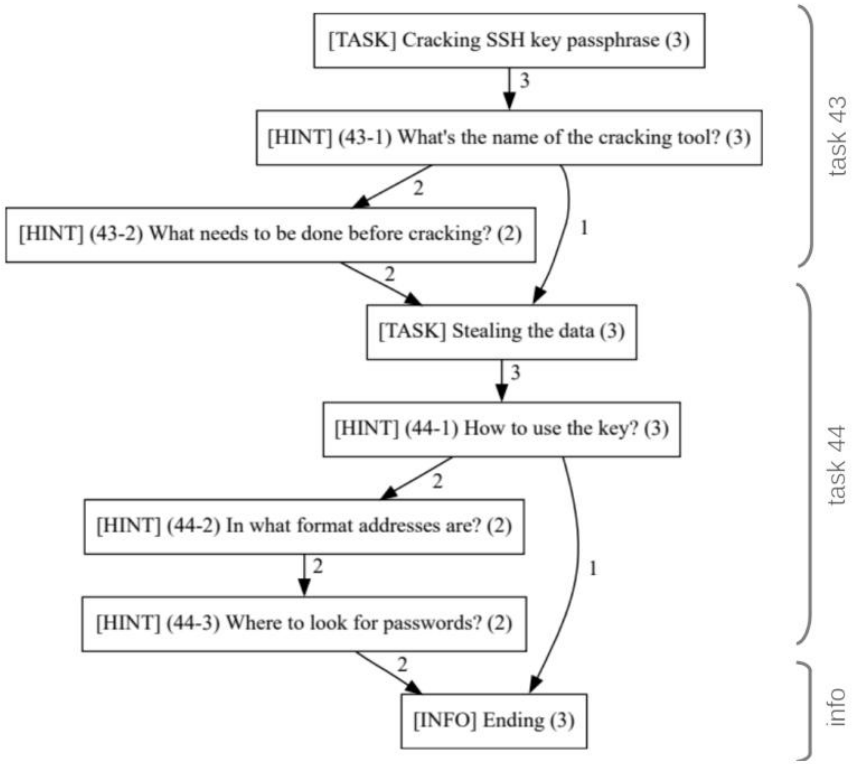
考察(2)

- ブラウザの開発者ツールでの利用情報の取得
  - VM上での動作速度から導入を断念
  - 開発者ツールを利用する演習者もいる
    →網羅性の向上が見込める
  - 解決策
    - クライアントサーバ型で構築
    - 演習者端末でログを取得し送信する

- ブラウザでの追加の情報取得
  - 開発者ツールでのWebアプリケーションのソース閲覧行動の分析
  - 攻撃と閲覧したソースコード部分の対応付け
    - 攻撃着目点ヒートマップを作製

関連研究(1)

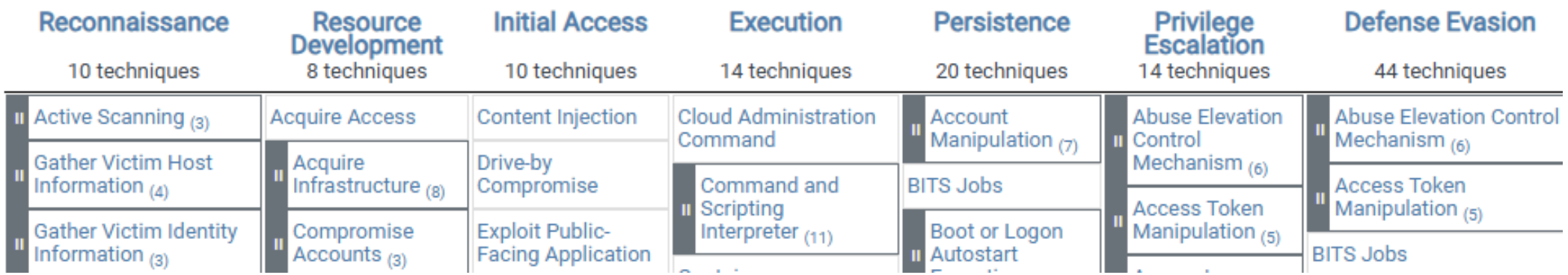
- Macakら[1]
  - CTF演習者の問題解決過程をプロセスマイニングで分析・可視化する手法を提案
  - サイバーレンジというセキュリティ演習環境において，CTFイベント・Bash・Metasploitなどのログを取得
  - プロセスマイニングを実施し行動を可視化
  - ログ分類にCWEを用いる点で相違



関連研究(2)

- Savinら[2]
  - CTF演習者のキーストローク・コマンド履歴からの分析
  - 演習者のコマンド操作をログから正確に復元
  - 演習者の行動をMITRE ATT&CKフレームワークを用いてラベリング

  - フィードバックを行う点で相違



MITRE ATT&CKフレームワーク(抜粋)

結論

- WAFを用いてCTFでの攻撃手法を推定できる
  - 一定の網羅性がある
- CTFにおいて追加のフィードバックを行う有用性がある
- 教育効果や，性能については検討を行う必要がある

今後の課題

- 開発者ツール利用情報のロギング
  - 現状のシステムでは動作性能に問題
  - Firefoxのビルド時に適切な最適化を行う必要

- 新たな情報の取得
  - ソースコードの閲覧情報の取得
    →着目点の把握

情報処理学会 インターネットと運用技術シンポジウム2024で発表