LogiScope

情報セキュリティ学習のための
アクセスログ監視ゲーム

ゲームの使い方①｜ゲームモード選択画面

チュートリアルモード

解説を見ながら、不正アクセスについて学習するモード（初心者向け）

テストモード

解説無しで、不正アクセスを見抜く力を試すモード（チャレンジ向け）

ゲームの使い方②｜チュートリアルモード

ログ一覧

解説ボタン

解答エリア

前提条件

不正アクセスの解説

ゲームの使い方③｜チュートリアルモード

行	アクセス時間	IPアドレス	ログの種類	ステータスコード	詳細	アクセスしたファイル	解説
1	2024-01-04T19:26:54.983Z	190.2.146.119	認証	200			解説
2	2024-01-04T19:26:54.983Z	195.91.253.99	アクセス	200	取得 /?file=../../etc/system.log	system.log	解説
3	2024-03-06T09:02:34.983Z	190.2.146.119	通信	200			解説
4	2024-03-06T09:02:34.983Z	2.57.0.255	アクセス	500	ロシア からのアクセス	index.html	解説
5	2024-03-29T16:50:12.983Z	109.206.244.37	認証	429	ユーザーumiri2323がログインを試行しました。状態:429		解説
6	2024-03-29T16:50:12.983Z	109.206.244.37	認証	429	ユーザーumiri2323がログインを試行しました。状態:429		解説
7	2024-03-29T16:50:12.983Z	109.206.244.37	認証	429	ユーザーumiri2323がログインを試行しました。状態:429		解説
8	2024-03-29T16:50:12.983Z	109.206.244.37	認証	429	ユーザーumiri2323がログインを試行しました。状態:429		解説
9	2024-03-29T16:50:12.983Z	109.206.244.37	認証	429	ユーザーumiri2323がログインを試行しました。状態:429		解説

1. 各ログについて、解説ボタンを押して**解説を見る**
2. 前提条件と、解説に書かれた「ログの特徴」を合わせながら**怪しいログを押す**(複数選択可能)
3. 解答エリアで、**該当する不正アクセス名を選ぶ**
4. 「**リストに追加**」ボタンを押す
5. 全ての不正アクセスを報告できたと思ったら、「**最終報告**」ボタンを押して結果を見る

ゲームの使い方④｜テストモード

ー テストモード ー　日本語　English　チュートリアルモード>>

行	アクセス時間	IPアドレス	ログの種類	ステータスコード	詳細	アクセスしたファイル
1	2024-01-02T16:37:12.199Z	66.102.12.218	エラー	404	ファイルが見つかりません: /var/../../../login/etc/404 Not Found: secret.pdf	404 Not Found: secret.pdf
2	2024-01-28T17:08:09.199Z	195.91.253.99	エラー	404	ファイルが見つかりません: /var/../../../login/etc/404 Not Found: secret.pdf	404 Not Found: secret.pdf
3	2024-02-01T20:02:32.199Z	83.169.216.11	認証	200	構文エラー: 'OR 1=1' 付近	
4	2024-02-01T20:02:32.199Z	185.199.108.153	操作	403	403 エラー: ユーザーringo2020はapi_file.docxへのアクセスを禁止されました	api_file.docx
5	2024-02-01T20:02:32.199Z	195.91.253.99	イベント	400	<img src=x onerror=alert("XSS")>	index.html
6	2024-02-25T13:15:42.199Z	185.199.108.153	認証	401	401 エラー: ユーザー'anonymous'はdata.csvへのアクセスに失敗しました	data.csv
7	2024-03-16T14:33:37.199Z	168.63.120.45	操作	200		
8	2024-03-27T20:42:55.199Z	95.216.11.43	操作	400	構文エラー: '; DROP TABLE users; --' 付近	
9	2024-03-27T20:42:55.199Z	178.62.219.100	認証	401	401 エラー: ユーザー'anonymous'はdata.csvへのアクセスに失敗しました	data.csv
10	2024-03-31T11:13:09.199Z	145.132.44.199	アクセス	200	シドニー、オーストラリアからのアクセス	profile.jpg

行目が

アクセス権がない、または認証されていない

の疑いがある　リストに追加する　最終報告をする

《現在の状況》

2行目が不正解

《前提条件》

- **就業時間**：8時～22時
- **支店**：沖縄・シドニー・北京
- **ランサムウェアの可能性のある拡張子**：「.Phobos」「.eking」「.faust」
- 以前ロシア・チリからサイバー攻撃を受けたことがあり、利用を制限している
- 5回以上連続のログイン認証はブルートフォース攻撃と見なす

※チュートリアルモードの解説が無いバージョン

ゲームの使い方⑤｜テストモード

行	アクセス時間	IPアドレス	ログの種類	ステータスコード	詳細	アクセスしたファイル
1	2024-01-09T19:35:37.960Z	145.132.44.199	認証	200		
2	2024-01-15T17:25:05.960Z	102.165.44.233	イベント	400	<img src=x onerror=alert("XSS")>	profile.jpg
3	2024-03-01T13:48:45.960Z	5.8.69.255	アクセス	500	チリ からのアクセス	index.html
4	2024-05-15T17:03:13.960Z	190.2.146.119	操作	200		
5	2024-05-18T17:52:57.960Z	66.102.12.218	エラー	404	ファイルが見つかりません: /var/../../../login/etc/404 Not Found: secret.pdf	404 Not Found: secret.pdf
6	2024-05-18T17:52:57.960Z	203.0.113.42	認証	401	401 エラー: ユーザー'anonymous'はdata.csvへのアクセスに失敗しました	data.csv
7	2024-07-27T11:39:46.960Z	190.2.146.119	アクセス	200	沖縄県, 日本 からのアクセス	script.js
8	2024-07-28T21:07:23.960Z	66.102.12.218	操作	400	構文エラー: '; DROP TABLE users; --' 付近	
9	2024-08-12T13:47:02.960Z	82.94.231.14	アクセス	200	北京, 中国 からのアクセス	profile.jpg
10	2024-08-12T13:47:02.960Z	83.169.216.11	通信	200	IP (83.169.216.11) の接続試行が検出されました	meeting_notes.docx.faust
11	2024-08-12T13:47:02.960Z	2.57.0.255	アクセス	500	ロシア からのアクセス	index.html

1. 前提条件を見ながら**怪しいログを押す**(複数選択可能)
2. 解答エリアで、**該当する不正アクセス名を選ぶ**
3. 「**リストに追加**」ボタンを押す
4. 全ての不正アクセスを報告できたと思ったら、「**最終報告**」ボタンを押して結果を見る