

不審な IP アドレスに関するレポート

昨今発生している、[.env]や[/admin]などの探索を行っている可能性のある IP アドレスを公表いたします。

なお本件は下記条件下に当てはまるものを調査対象としています。

調査対象と内容

- ・ *.[.]studioaster[.]net に対してサーバが記録したログファイルをもとに、9 月のデータから抽出し、本来アクセスするものではないパスに対してのアクセスが継続的または集中的に発生している IP アドレスを公表します。
- ・ 管理者が指定する施設等の IP アドレスは除外した数値を掲載します。除外する施設名についてはこれを公表しませんが、3 施設です。
- ・ 本書は 10 月 9 日 0 時～3 時までのデータを参照しているため、一部 IP アドレスはメガクラウドの規約に基づき閉鎖された場合があります。

備考

なお、不審な Bot の活動により、重要なファイルやパスへのアクセスは確認されませんでした。

本書の責任者等

任意団体 スタジオアステル

責任者 びじゅママ

■ 9月のアクセス状況

■ ステータスコード別

ステータスコード	リクエスト数		IP アドレス数	
	件数(件)	割合(%)	件数(件)	割合(%)
200 番台	8,684	4.71	2,248	33.40
300 番台	21,379	11.60	1,348	20.03
400 番台	154,021	83.57	3,041	45.19
500 番台	215	0.12	93	1.38
合計	184,299	100.00	6730	100.00

※1:IP アドレス件数はステータスコード重複のため延べ数です。総リクエスト IP アドレス数は 4,784 件となります。

■ ステータスコード内訳

ステータスコード		件数	ステータスコードの意味
200 番台	200	8,536	リクエストが正常に処理され、要求されたデータを正常に返した
	206	148	要求されたデータの一部だけを正常に返した
300 番台	301	21,213	要求されたページが恒久的に別の URL へ移動した
	302	166	要求されたページが一時的に別の URL へ移動している
400 番台	404	94,752	要求されたページやリソースが見つからない
	401	53,199	認証が必要、または認証に失敗してアクセスできない
	403	4,530	アクセス権限がなく、サーバーからアクセスを拒否された
	400	1,485	リクエストの内容が不正で、サーバーが処理できない
	405	38	要求された HTTP メソッドが、そのリソースで許可されていない
	429	16	短時間に大量のリクエストが送られ、アクセス制限された
	499	1	クライアント側が待機中に接続を切断した
500 番台	501	96	サーバーが要求された機能や HTTP メソッドに対応していない
	500	80	サーバー内部で予期しないエラーが発生した
	503	39	サーバーが一時的に利用できない状態

■ 不審なリクエスト件数

[.env]を含むリクエスト	93,427 件（なお、IP アドレスは 597 件）
※クエリパラメータ含めます ※なお、[.env]ファイルへのアクセスはすべてエラーを返しており侵入は確認されませんでした	

[.git]を含むリクエスト	3,127 件（なお、IP アドレスは 660 件）
※なお、[.git]ファイルへのアクセスはすべてエラーを返しており侵入は確認されませんでした	

[wp-content]を含むリクエスト	1,337 件（なお、IP アドレスは 78 件）
※なお、WordPress を利用しているウェブサイトがないためはなから侵入されるわけありません	

※2:その他、[login]、[admin]等のアクセスも確認されましたが、いずれも不審な IP アドレスからの侵入は認められませんでした。

■ 9 月に 1,000 件を超えるリクエストがあった不審と判断された IP アドレス

IP アドレス	リクエスト	ホストネーム	ロケーション	ISP	UA 例
34.153.215.84	2,263	84.215.153.34.bc.googleusercontent.com	Tokyo, Tokyo, JP	Google LLC	Mozilla/5.0 (compatible; Meta-ExternalAgent/1.0; +https://developers.facebook.com/docs/sharing/webmasters/crawler) Mozilla/5.0 (compatible; Google-Extended; +http://www.google.com/bot.html) DuckAssistBot/1.1 (https://duckduckgo.com/duckassistbot) Mozilla/5.0 (compatible; GrokBot/1.0; +https://x.ai/) Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible; GPTBot/1.4; +https://openai.com/gptbot
34.21.208.252	2,248	252.208.21.34.bc.googleusercontent.com	Singapore, , SG	Google LLC	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Perplexity-User/1.0; +https://perplexity.ai/perplexitybot) CCBot/2.0 (https://commoncrawl.org/faq/) Mozilla/5.0 (compatible; Qwenbot/1.0; +https://qwen.alibaba.com/) Mozilla/5.0 (compatible; Kimi-SearchBot/1.0; +https://kimi.ai/) Mozilla/5.0 (compatible; xAI-Grok/1.0; +https://x.ai/)
34.73.244.84	2,098	84.244.73.34.bc.googleusercontent.com	North Charleston, South Carolina, US	Google LLC	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Mobile Safari/537.36 Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Mobile Safari/537.36 Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Mobile Safari/537.36 Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Mobile Safari/537.36 Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/147.0.0.0 Mobile Safari/537.36
4.224.45.129	1,784		Pune, Maharashtra, IN	Microsoft Corporation	
195.178.110.22	1,687		Amsterdam, North Holland, NL	TECHOFF SRV LIMITED	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

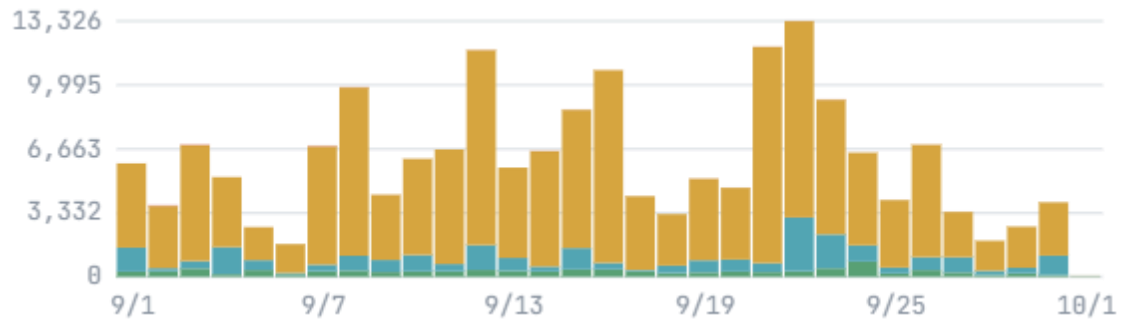
IP アドレス	リクエスト	ホストネーム	ロケーション	ISP	UA 例
34.24.135.198	1,604	198.135.24.34.bc.googleusercontent.com	North Charleston, South Carolina, US	Google LLC	Mozilla/5.0 (compatible; Amazonbot/0.1; +https://developer.amazon.com/support/amazonbot) Mozilla/5.0 (compatible; GrokBot/1.0; +https://x.ai/) Mozilla/5.0 (compatible; YouBot/1.0; +https://you.com/bot) Mozilla/5.0 (compatible; DeepSeekBot/1.0; +https://www.deepseek.com/) Mozilla/5.0 (compatible; Bytespider; spider-feedback@bytedance.com) AppleWebKit/537.36
34.21.168.36	1,575	36.168.21.34.bc.googleusercontent.com	Singapore, , SG	Google LLC	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36; compatible; OAI-SearchBot/1.4; +https://openai.com/searchbot Mozilla/5.0 (compatible; KimiBot/1.0; +https://kimi.ai/) Mozilla/5.0 (compatible; Qwenbot/1.0; +https://qwen.alibaba.com/) Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) DuckAssistBot/1.1 (https://duckduckgo.com/duckassistbot)
34.169.34.210	1,462	210.34.169.34.bc.googleusercontent.com	The Dalles, Oregon, US	Google LLC	Mozilla/5.0 (compatible; DeepSeekBot/1.0; +https://www.deepseek.com/) Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; PerplexityBot/1.0; +https://perplexity.ai/perplexitybot) Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html) Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Claude-User/1.0; +claudebot@anthropic.com) Mozilla/5.0 (compatible; KimiBot/1.0; +https://kimi.ai/)
34.19.91.56	1,182	56.91.19.34.bc.googleusercontent.com	The Dalles, Oregon, US	Google LLC	Mozilla/5.0 (compatible; DeepSeekBot/1.0; +https://www.deepseek.com/) Mozilla/5.0 (compatible; xAI-Grok/1.0; +https://x.ai/) Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36; compatible; OAI-SearchBot/1.4; +https://openai.com/searchbot Mozilla/5.0 (compatible; YouBot/1.0; +https://you.com/bot) Mozilla/5.0 (compatible; cohere-ai; +https://cohere.com/crawler)
103.168.67.253	1,145	253.67.168.103.in-addr.arpa.digivps.com	Dallas, Texas, US	DiGiVPS.com	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Mozilla/5.0 (Linux; Android 13; SM-S918B) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Mobile Safari/537.36 python-requests/2.32.4 WordPress/6.4.3 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

IP アドレス	リクエスト	ホストネーム	ロケーション	ISP	UA 例
8.234.57.103	1,108	103.57.234.8.bc.googleusercontent.com	Columbus, Ohio, US	Google LLC	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
31.59.160.3	1,105	hosted-by.server.express	Stockholm, Stockholm, SE	ServerExpress	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0 curl/8.6.0
34.186.178.170	1,044	170.178.186.34.bc.googleusercontent.com	Los Angeles, California, US	Google LLC	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; GPTBot/1.3; +https://openai.com/gptbot) Mozilla/5.0 (compatible; Bytespider; spider-feedback@bytedance.com) AppleWebKit/537.36 Mozilla/5.0 (compatible; GrokBot/1.0; +https://x.ai/) Mozilla/5.0 (compatible; MistralAI-User/1.0; +https://mistral.ai/) Mozilla/5.0 (compatible; Kimi-SearchBot/1.0; +https://kimi.ai/)
20.205.12.169	1,036		Hong Kong, , HK	Microsoft Corporation	
34.169.36.129	1,019	129.36.169.34.bc.googleusercontent.com	The Dalles, Oregon, US	Google LLC	Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Claude-User/1.0; +claudebot@anthropic.com) Mozilla/5.0 (compatible; MistralAI-User/1.0; +https://mistral.ai/) Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36; compatible; OAI-SearchBot/1.4; +https://openai.com/searchbot Mozilla/5.0 (compatible; YouBot/1.0; +https://you.com/bot) Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)

※3:ロケーション、ISP は IPinfo [<https://ipinfo.io/>]及び AbuseIPDB [<https://www.abuseipdb.com/>]から取得しています。誤りの場合があります。

※4:UA 例は 5 件を無作為抽出します。同じ UA が表示される場合があります。

■ リクエストグラフ



※5:緑色 200 番台、青色 300 番台、オレンジ色 400 番台、赤色 500 番台を返し、1 日ごとのデータです。