SECURITY REPORT

2025

OCT

2025年10月
攻撃統計情報

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

月次攻撃サービスの統計及び分析 - 2025年09月

株式会社サイバーフォートレスでは攻撃情報を収集し、分析しています。
分析内容から、月次攻撃類型、脆弱性攻撃、ブラックリストのTOP10を確認し、過去データと比較し、
攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てて頂ければと思います。

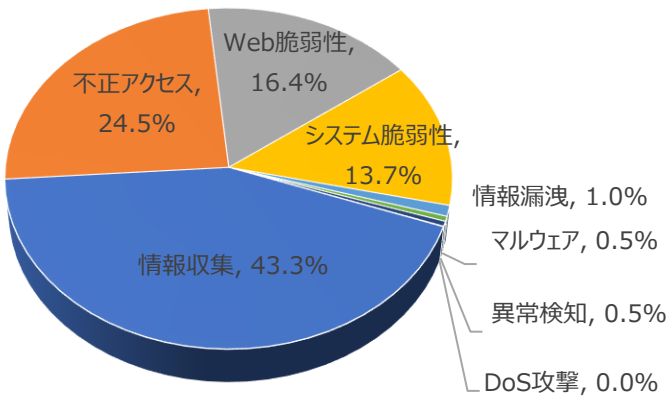
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	43.3%	▲1
不正アクセス(Unauthorized access)	24.5%	▼1
Web脆弱性(Web Vulnerability)	16.4%	-
システム脆弱性(System Vulnerability)	13.7%	-
情報漏洩(Information Exposure)	1.0%	-
マルウェア(Malware)	0.5%	-
異常検知(Anomaly Detection)	0.5%	-
DoS攻撃(Denial of service attack)	0.0%	-

2025年09月の攻撃類型を確認した結果、全体の攻撃合計が先月と比べて約0.89倍ぐらい減少した。

そのうち、不正アクセスに関する攻撃は先月比べて約4,295件ほど減少し、これは主要サービスポートアクセス試みの攻撃件数の減少によるものだと確認できた。

また、情報収集に関する攻撃は先月と比べて約2,985件ぐらい増加し、これは、Network Scan、ポートスキャンの攻撃件数増加によるものだと確認できた。

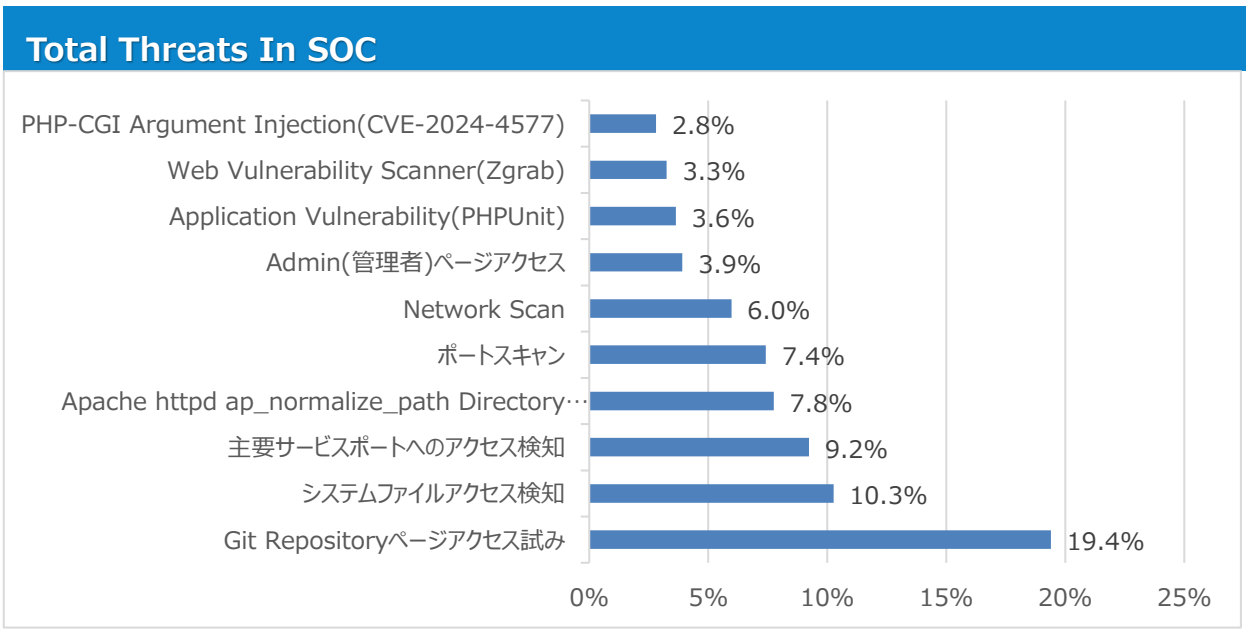


月次攻撃サービスの統計及び分析 - 2025年09月

02. 月次脆弱性攻撃TOP10

2025年09月の月次脆弱性TOP10を確認した結果、Web脆弱性攻撃がTOP10に登場した。
全体的な攻撃件数は減少した。特にGit Repositoryページアクセス試み数が先月と比べて約1,547件ぐらい増加したことが確認できた。

順位	検知名	比率(%)	比較
1	Git Repositoryページアクセス試み	19.4%	▲4
2	システムファイルアクセス検知	10.3%	-
3	主要サービスポートへのアクセス検知	9.2%	▼2
4	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	7.8%	▲2
5	ポートスキャン	7.4%	▼1
6	Network Scan	6.0%	▼3
7	Admin(管理者)ページアクセス	3.9%	-
8	Application Vulnerability(PHPUnit)	3.6%	-
9	Web Vulnerability Scanner(Zgrab)	3.3%	▼4
10	PHP-CGI Argument Injection(CVE-2024-4577)	2.8%	NEW



月次攻撃サービスの統計及び分析 - 2025年09月

03. 月次ブラックリストIPアドレスTOP 10

2025年09月についてTOP10を確認した結果、アメリカとドイツの攻撃比率が減少し、特にアメリカの攻撃比率が約67.4%を超えていることが確認できた。

※ 下記の表を参考にしたファイウォールやセキュリティ機器からの遮断を推奨します。

順位	ブックリストIP	国	攻撃情報
1	38.211.193.130	US	Directory Traversal検知
2	207.180.211.42	GE	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
3	34.123.181.51	US	Application Vulnerability(PHPUnit)
4	123.253.22.8	MM	Application Vulnerability(PHPUnit)
5	125.17.108.32	IN	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
6	103.251.93.98	IN	PHP-CGI Argument Injection(CVE-2024-4577)
7	5.104.86.61	DE	PHP-CGI Argument Injection(CVE-2024-4577)
8	212.113.102.147	RO	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
9	89.248.164.165	NE	ポートスキャン
10	185.250.36.134	GE	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)

Total Countries

今月攻撃IP, 国家順位の詳細TOP10の表及び比率

Rank	Source IP	Country
1	38.211.193.130	US
2	207.180.211.42	GE
3	34.123.181.51	US
4	123.253.22.8	MM
5	125.17.108.32	IN

Rank	Source IP	Country
6	103.251.93.98	IN
7	5.104.86.61	DE
8	212.113.102.147	RO
9	89.248.164.165	NE
10	185.250.36.134	GE

攻撃パターン毎の詳細分析結果

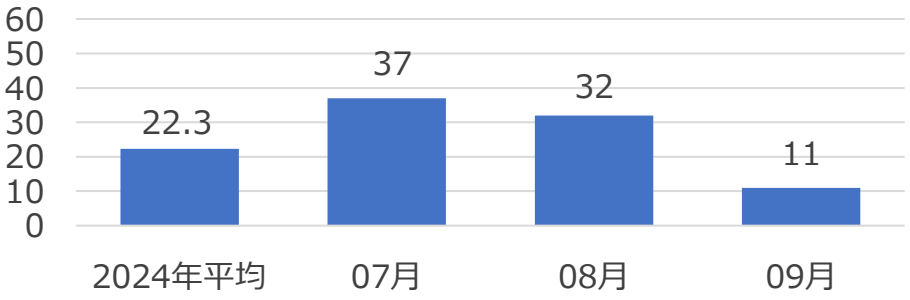
09月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
Git Repository ページアクセス	ソースコードのバージョン管理のためにGit Repository(/.git/)をホスティングする場合、存在するソースコード及び重要情報を確認するためにconfigやHEADなどのデフォルトパスの存在有無及びレポジトリのパスをスキャンする攻撃である。
システムファイルアクセス検知	Directory Traversalの脆弱性などを利用し、「/etc/passwd」や「*.conf /.env」などの構成情報を含む主要なシステムファイルにアクセスを計る。
主要サービスポートアクセス検知	主要ポートにアクセス試み後、アクセス情報を奪取するための総当たり攻撃後、アカウント情報が一致する場合、ウェブ改ざん、情報奪取などの被害が発生しうる。アカウント情報対する周期的な変更及び文字、数字、特殊文字が入っているパスワードの使用と外部からすべてのサービスポートへのアクセス可能ポリシー使用禁止、指定された管理者のIPのみ特定のサービスポートへアクセス可能ポリシーしようなどを推奨する。
Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	Apache httpdにDirectory Traversal脆弱性が存在する。当該の脆弱性は「ap_normalize_path」関数でURIぱすに対する不適切な有効性検証から発生する。リモートの攻撃者は悪意的に改ざんされたHTTPリクエストを送信して攻撃できる。攻撃に成功すると情報が漏洩される。
ポートスキャン	主要ポートへのアクセスを試みしてからアクセス情報を奪取するためのBrute Force攻撃が行われ、アカウント情報が一致した場合、ウェブ改ざんや情報窃取などの被害が発生する可能性がある。アカウント情報の定期的な変更、文字・数字・特殊文字を組み合わせたパスワードの使用、外部からの全サービスポートへのアクセスポリシーの禁止、指定管理者IPからのみ特定サービスポートへのアクセスポリシーの使用などを推奨する。
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行われる攻撃である。
Admin(管理者)ページアクセス	ウェブアプリケーションの適切なアクセス制御が設定されていない場合「/admin」、「/manager」などの一般ユーザーには提供していない管理者ページが外部に漏洩される可能性が存在する。管理者おページが外部に漏洩された場合、総当たり攻撃などでadminアカウントが漏洩される可能性がある。
Application Vulnerability(PHPUnit)	PHPUnitはユニットテストフレームワークで/phpunit/src/Util/PHP/eval-stdin.phpファイルに存在す る脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は<?phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)は、Webサーバの設定ページや許可方法、許可されていないWebページ、ライセンスのないポートなど、脆弱性部分の存在を判断するために使用される。
PHP-CGI Argument Injection(CVE-2024-4577)	CVE-2024-4577脆弱性はPHPのCGIモードからWindowsの「Best-Fit」機能が間違ったエンコードが行われて発生するリモートコード実行(RCE)脆弱性である。WindowsのOSからPHPがCGIモードで実行されたり、XAMPPのような開発環境でデフォルト設定でPHPバイナリが漏出された場合脆弱である。この脆弱性を悪用すると攻撃者は改ざんされたURLぱらめーたで任意のこーどが実行できる。今まで確認されたことは、特定のシステムロケール(中国語の繁体字及び簡体字、日本語)を使用する場合エクスプロイトができることが確認されたが、他のロケールも場合によっては影響を受ける可能性があるため、パッチバージョンでアップデートすることを推奨する。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年09月の1か月間で共有されたサイバー脅威検知ポリシーは11件である。
09月1か月の間、Citrix(CVE-2024-8068), Sangoma(CVE-2025-57819), CrushFTP(CVE-2025-54309)などに対する検知ポリシーが配布された。



3か月間件数

6,794
全体配布量

11
今月配布量

32
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06821 server-webapp,Citrix,cve-2024-8068,cve-2024-8069, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/msmq/queue_name"; fast_pattern:only; http_uri; content:"SOAPAction"; nocase; http_header; content:"MSMQMessage"; distance:0; nocase; http_header; content:"Binary"; nocase; http_client_body; content:"|00 01 00 00 00 FF FF FF FF 01 00 00 00 00 00 00|"; http_client_body; content:"System.Diagnostics"; distance:0; nocase; content:"Process"; nocase; content:"Start"; nocase; sid:106821;)	Citrixの脆弱性であるCVE-2024-8068を悪用した逆直列化試みを検知するポリシー	server-webapp,Citrix,cve-2024-8068,cve-2024-8069
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06825 server-webapp_Sangoma_FreePBX_cve-2025-57819_Web Application Attack"; flow:to_server,established; content:"/admin/ajax.php"; nocase; http_uri; content:"module=FreePBX"; fast_pattern; nocase; http_client_body; content:"modules"; within:15; nocase; http_client_body; content:"endpoint"; within:15; nocase; http_client_body; content:"ajax"; within:15; nocase; http_client_body; pcre:"/(^|&)module=FreePBX(¥x5c|%(25)?5c){2}modules(¥x5c|%(25)?5c){2}endpoint(¥x5c|%(25)?5c){2}ajax/Pim"; sid:1006825;)	Sangoma FreePBXの脆弱性であるCVE-2025-57819を悪用した認証バイパス攻撃を検知するポリシー를 악용한 인증 우회 공격을 탐지하는 정책	server-webapp,Sangoma,FreePBX,cve-2025-57819
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06830 server-webapp_CrushFTP_cve-2025-54309_Web Application Attack"; flow:to_server,established; content:"/WebInterface/function"; fast_pattern:only; http_uri; content:"AS2-TO"; nocase; http_header; detection_filter:track by_src, count 30, seconds 5; sid:1006830;)	CrushFTPの脆弱性であるCVE-2025-54309を悪用したリモートコード実行攻撃を検知するポリシー	server-webapp,CrushFTP,cve-2025-54309