SECURITY REPORT

2025

SEP

2025年09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08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。

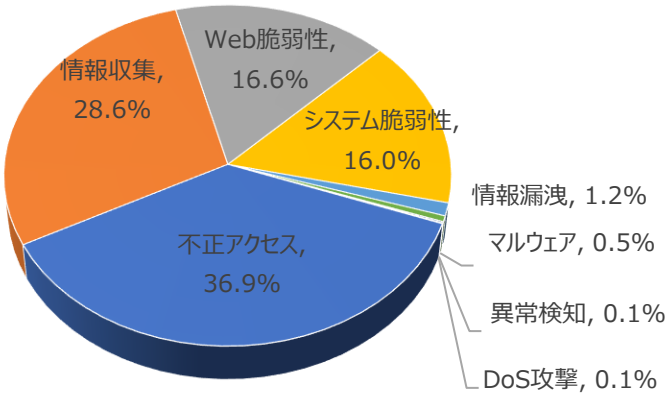
01. 月次攻撃類型

パターン	比率(%)	比較
不正アクセス(Unauthorized access)	36.9%	-
情報収集(Information Gathering)	28.6%	-
Web脆弱性(Web Vulnerability)	16.6%	-
システム脆弱性(System Vulnerability)	16.0%	-
情報漏洩(Information Exposure)	1.2%	-
マルウェア(Malware)	0.5%	-
異常検知(Anomaly Detection)	0.1%	-
DoS攻撃(Denial of service attack)	0.1%	-

2025年08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1.36倍ぐらい増加した。

そのうち、不正アクセスに関する攻撃は先月比べて約3,798件ほど増加し、これは主要サービスポートアクセス試みの攻撃件数の増加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2,983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。

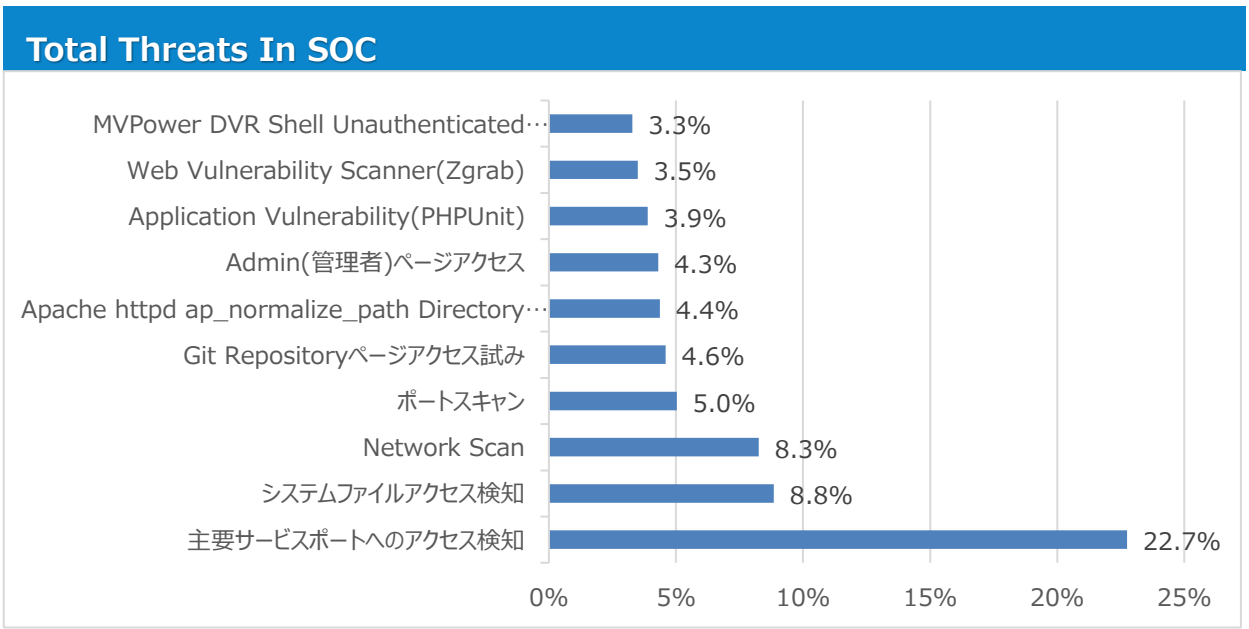


月次攻撃サービスの統計及び分析 - 2025年08月

02. 月次脆弱性攻撃TOP10

2025年08月の月次脆弱性TOP10を確認した結果、多数の不正アクセス攻撃がTOP10に登場した。
全体的な攻撃件数は増加した。特に主要サービスポートへのアクセス検知件数が先月と比べて約4,240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	主要サービスポートへのアクセス検知	22.7%	▲1
2	システムファイルアクセス検知	8.8%	▼1
3	Network Scan	8.3%	NEW
4	ポートスキャン	5.0%	NEW
5	Git Repositoryページアクセス試み	4.6%	▲4
6	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	4.4%	NEW
7	Admin(管理者)ページアクセス	4.3%	▼4
8	Application Vulnerability(PHPUnit)	3.9%	-
9	Web Vulnerability Scanner(Zgrab)	3.5%	▼4
10	MVPower DVR Shell Unauthenticated Command Execution	3.3%	▼4



月次攻撃サービスの統計及び分析 - 2025年08月

03. 月次ブラックリストIPアドレスTOP 10

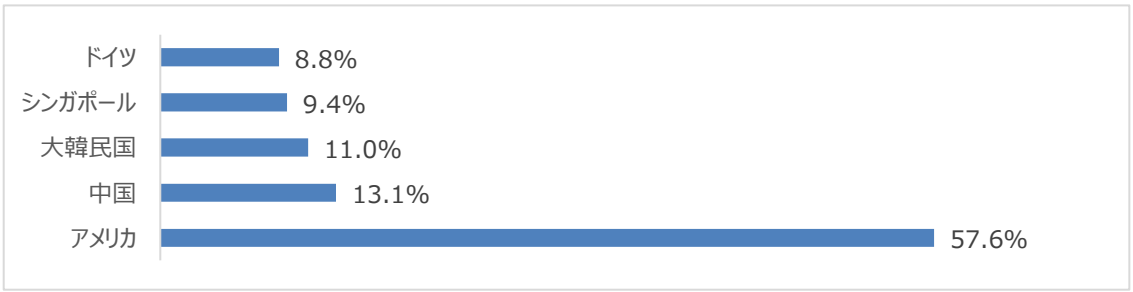
2025年08月についてTOP10を確認した結果、アメリカと中国の攻撃比率が増加し、特にアメリカの攻撃比率が約57.6%を超えていることが確認できた。

※ 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	PHP-CGI Argument Injection(CVE-2024-4577)
2	111.119.234.186	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
3	197.220.93.115	SO	ThinkPHP lang Remote Code Execution
4	45.131.108.170	NL	ThinkPHP Remote Code Execution Vulnerability
5	93.123.109.245	DE	Git Repositoryページアクセス試み
6	119.8.169.21	SG	PHP-CGI Argument Injection(CVE-2024-4577)
7	197.220.93.100	SO	Application Vulnerability(PHPUnit)
8	197.220.93.117	SO	Application Vulnerability(PHPUnit)
9	124.71.231.117	CN	ThinkPHP Remote Code Execution Vulnerability
10	115.248.8.65	IN	PHP-CGI Argument Injection(CVE-2024-4577)

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	111.119.234.186	SG
3	197.220.93.115	SO
4	45.131.108.170	NL
5	93.123.109.245	DE

Rank	Source IP	Country
6	119.8.169.21	SG
7	197.220.93.100	SO
8	197.220.93.117	SO
9	124.71.231.117	CN
10	115.248.8.65	IN

攻撃パターン毎の詳細分析結果

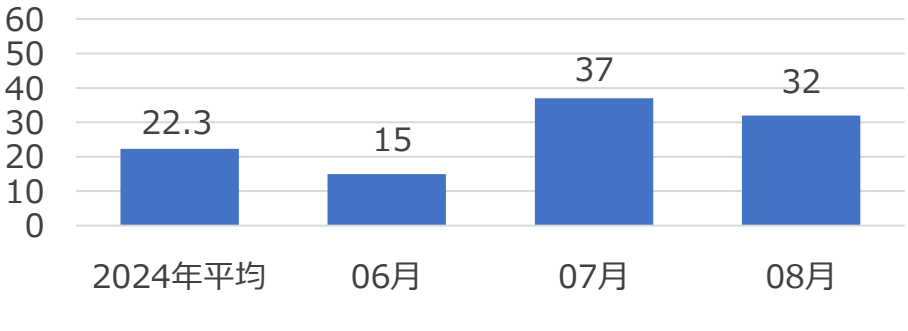
08月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
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。
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、存在するそーそ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。
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。
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。
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」ファイルを利用することでクエリの文字列の中から任意のシステムコマンドが実行できるようになる。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年08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32件である。
08月1か月の間、NimDoorマルウェアとAntropic(CVE-2025-6514), Fortinet(CVE-2025-32756, CVE-2025-25256)脆弱性などに対する検知ポリシーが配布された。



3か月間件数

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.06791 malware-other,torjan,NimDoor,DPRK, A Network Trojan was detected"; flow:to_client,established; flowbits:isset,file.macho64be|file.macho64le|file.machobe|file.machole|file.universalbinary; file_data; content:"/Users/artyom/Documents/gilly/InjectWithDyld/InjectWithDyldAmd64/InjectWithDyldAmd64/"; fast_pattern; sid:806791;)	NimDoor変種マルウェアダウンロード試みを検知するポリシー	malware-other,torjan,NimDoor,DPRK
alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"IGRSS.10.06802 server-webapp,Anthropic,MCP-Remote,cve-2025-6514, Web Application Attack"; flow:to_client,established; file_data; content:"|22|authorization_endpoint|22|"; fast_pattern:only; pcre:"/¥x22authorization_endpoint¥x22s*¥x3a¥s*¥x22(?!http(s)?:)((?!(?<!¥x5c)¥x22).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/i"; sid:1006802;)	Anthropic MCP-Remoteの脆弱性であるCVE-2025-6514を悪用したコマンドインジェクション攻撃を検知するポリシー	server-webapp,Anthropic,MCP-Remote,cve-2025-6514
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06803 server-webapp,Fortinet,cve-2025-32756, Attempted User Privilege Gain"; flow:to_server,established; content:"/module/admin.fe"; fast_pattern:only; http_uri; content:"APSCOOKIE"; nocase; http_cookie; content:"AuthHash"; distance:0; nocase; http_cookie; pcre:"/(¥x26|%(25)?26)AuthHash(¥x3d|%(25)?3d)[^&]{30}/Ci"; sid:206803;)	Fortinetの様々な製品から発見されたCVE-2025-32756を悪用したバッファオーバーフロー攻撃を検知するポリシー	server-webapp,Fortinet,cve-2025-32756
alert tcp $EXTERNAL_NET any -> $HOME_NET 7900 (msg:"IGRSS.1.06816 server-other,Fortinet,FortiSIEM,cve-2025-25256, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"<archive_nfs_"; fast_pattern:only; content:"<archive_storage_type"; nocase; pcre:"/<archive_nfs_(archive_dir|server_ip)[^>]*?>[^<]*?([¥x60¥x3b¥x7c¥x26¥x23]|¥x24¥x28)/i"; sid:106816;)	Fortinet FortiSIEMの脆弱性であるCVE-2025-25256を悪用したコマンドインジェクション試みを検知するポリシー	server-other,Fortinet,FortiSIEM,cve-2025-25256

CyberFortress