SECURITY REPORT

2025

JUL

2025年07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06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。

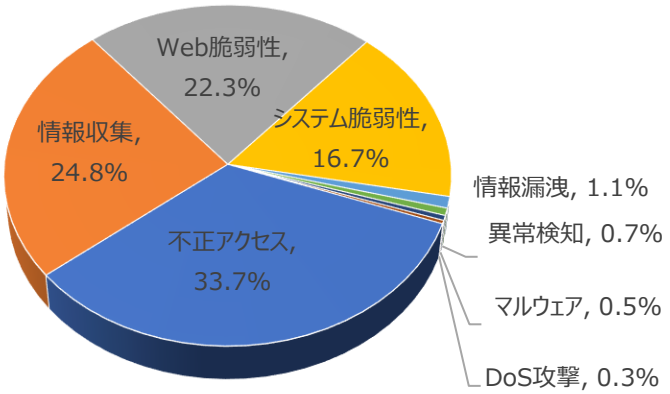
01. 月次攻撃類型

パターン	比率(%)	比較
不正アクセス(Unauthorized access)	33.7%	▲1
情報収集(Information Gathering)	24.8%	▼1
Web脆弱性(Web Vulnerability)	22.3%	-
システム脆弱性(System Vulnerability)	16.7%	-
情報漏洩(Information Exposure)	1.1%	-
異常検知(Anomaly Detection)	0.7%	-
マルウェア(Malware)	0.5%	-
DoS攻撃(Denial of service attack)	0.3%	-

2025年06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0.98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1,180件ほど増加し、これはAdminページアクセス試み、システムファイルアクセス検知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842件ぐらい減少し、これは,Netowrk Scannerの攻撃件数減少によるものだと確認できた。

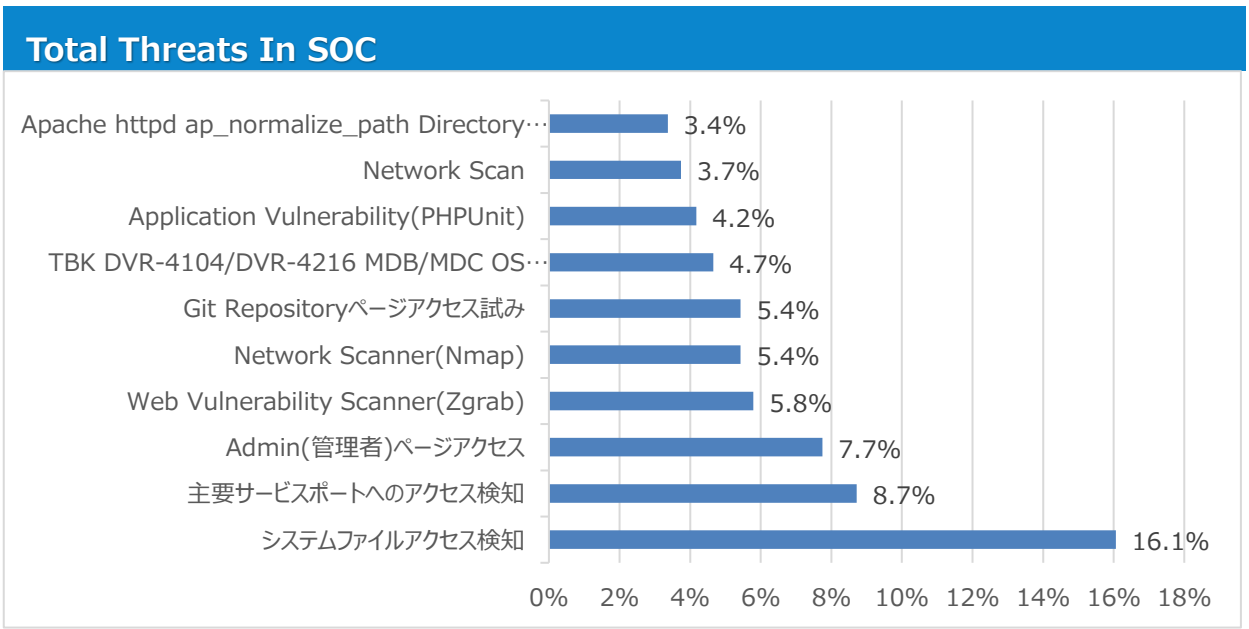


月次攻撃サービスの統計及び分析 - 2025年06月

02. 月次脆弱性攻撃TOP10

2025年06月の月次脆弱性TOP10を確認した結果、多数のシステム脆弱性攻撃がTOP10に登場した。
全体的な攻撃件数は減少した。特に情報収集の攻撃件数が先月と比べて約824件ぐらい減少
したことが確認できた。

順位	検知名	比率(%)	比較
1	システムファイルアクセス検知	16.1%	-
2	主要サービスポートへのアクセス検知	8.7%	▲8
3	Admin(管理者)ページアクセス	7.7%	-
4	Web Vulnerability Scanner(Zgrab)	5.8%	▲2
5	Network Scanner(Nmap)	5.4%	-
6	Git Repositoryページアクセス試み	5.4%	▼2
7	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)	4.7%	NEW
8	Application Vulnerability(PHPUnit)	4.2%	▼1
9	Network Scan	3.7%	NEW
10	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	3.4%	▼8



月次攻撃サービスの統計及び分析 - 2025年06月

03. 月次ブラックリストIPアドレスTOP 10

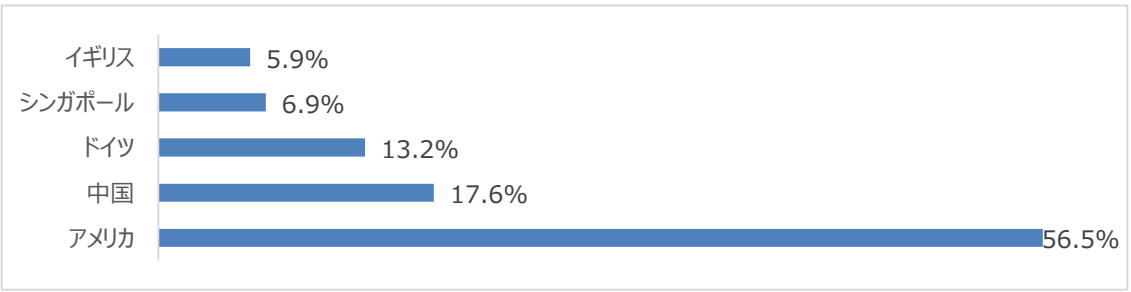
2025年06月についてTOP10を確認した結果、アメリカと中国の攻撃比率が減少し、特にアメリカの攻撃比率が約56.5%を超えていることが確認できた。

※ 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	45.207.195.204	MU	SQL Injection
2	39.103.62.205	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
3	118.194.253.212	TW	Application Vulnerability(PHPUnit)
4	117.48.157.75	HK	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
5	47.122.4.148	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
6	93.123.109.231	CN	Git Repositoryページアクセス試み
7	47.121.220.66	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
8	103.39.93.93	CN	ThinkPHP Remote Code Execution Vulnerability
9	47.121.210.129	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
10	112.120.228.189	CN	Application Vulnerability(PHPUnit)

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	Rank	Source IP	Country
1	45.207.195.204	MU	6	93.123.109.231	CN
2	39.103.62.205	CN	7	47.121.220.66	CN
3	118.194.253.212	TW	8	103.39.93.93	CN
4	117.48.157.75	HK	9	47.121.210.129	CN
5	47.122.4.148	CN	10	112.120.228.189	CN

攻撃パターン毎の詳細分析結果

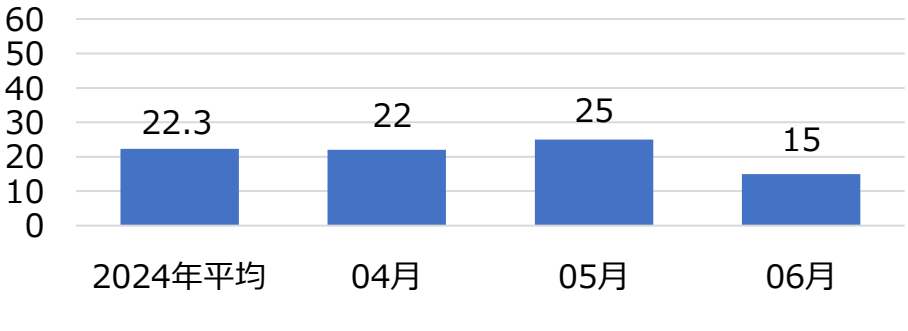
06月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
Network Scanner(Nmap)	代表的なNetwork Scanツールで、IP ScanとPort Scanの機能がある。ネットワーク脆弱性診断ツールとして活用されるが攻撃者から悪用されて攻撃ツールとして使用される。
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。
TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)	TBK DVR-4104およびDVR-4216バージョンから発見された深刻な脆弱性である。これは「/device.rsp?opt=sys&cmd= S_O_S_T_R_E_A_MAX」ファイルの「mdb/mdc」引数改ざんに関連する。これにより、OSコマンドがインジェクションされ、リモート攻撃が可能になる。
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。
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。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年06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15件である。
06月1か月の間、PaloAltoNetworks(CVE-2025-0108,CVE-2025-0111), Wazuh(CVE-2025-24016), CISCO(CVE-2025-20188), LG(CVE-2023-40504)などに対する検知ポリシーが配布された。



3か月間件数

6,714
全体配布量

15
今月配布量

25
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06747 server-webapp,PaloAltoNetworks,PAN-OS,cve-2025-0108,cve-2025-0111, Web Application Attack"; flow:to_server,established; content:"/unauth/"; fast_pattern:only; content:"/unauth/"; nocase; http_raw_uri; pcre:"/^¥x2funauth¥x2f[^¥x3f¥x26]*?(¥x2e|%(25)?2e){2}([¥x2f¥x5c]|%(25)?(2f|5c))/Ii"; sid:1006747;)	Palo Alto Networks PAN-OSの脆弱性であるCVE-2025-0108, CVE-2025-0111を悪用した認証バイパス試みを検知するポリシー	server-webapp,PaloAltoNetworks,PAN-OS,cve-2025-0108,cve-2025-0111
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06748 server-webapp,Wazuh,cve-2025-24016, Web Application Attack"; flow:to_server,established; content:"/security/user/authenticate/run_as"; fast_pattern:only; http_uri; content:"|22|__unhandled_exc__|22|"; http_client_body; content:"|22|__class__|22|"; http_client_body; pcre:"/¥x22__class__¥x22¥s*¥x3a¥s*¥x22((?!(?<!¥x5c)¥x22).)*?(¥w+¥s*¥x28|__¥w+__|¥x2e¥w+|exit|quit|eval|exec|compile|(get|set|has|del)attr|globals|locals|vars|dir|open|input|print)/P"; sid:1006748;)	Wazuhの脆弱性であるCVE-2025-24016を悪用したリモートコマンド実行攻撃を検知するポリシー	server-webapp,Wazuh,cve-2025-24016
alert tcp any any -> any any (msg:"IGRSK.10.06749 server-webapp_cisco_IOS_XE_WLC_cve-2025-20188_Web Application Attack"; flow:established,to_server; content:"POST"; content:"/upload/"; fast_pattern; content:"jwt="; content:"."; content:"cdb_token_request_id1";)	cisco IOS XE WLCの脆弱性であるCVE-2025-20188を悪用したファイルアップロード攻撃を検知するポリシー	server-webapp,cisco,IOS,XE,WLC,cve-2025-20188
alert tcp any any -> any any (msg:"IGRSK.10.06750 server-webapp_LG_SimpleEditor_cve-2023-40504_Web Application Attack"; flow:established,to_server; content:"POST"; content:"/uploadVideo.do"; fast_pattern; content:"|20|form-data|3b 20|"; pcre:"/^¥/?¥"¥s?&/m";)	LG Simple Editorの脆弱性であるCVE-2023-40504を悪用したリモートコマンド実行攻撃を検知するポリシ	server-webapp,LG,SimpleEditor,cve-2023-40504