SECURITY REPORT

2025

JUN

2025年06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05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。

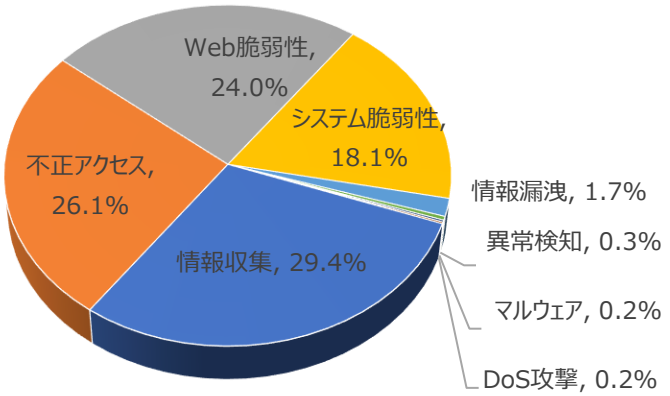
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	33.4%	-
不正アクセス(Unauthorized access)	26.1%	▲1
Web脆弱性(Web Vulnerability)	22.3%	▼1
システム脆弱性(System Vulnerability)	16.3%	-
情報漏洩(Information Exposure)	1.4%	-
異常検知(Anomaly Detection)	0.3%	-
マルウェア(Malware)	0.1%	-
DoS攻撃(Denial of service attack)	0.0%	-

2025年05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0.82倍ぐらい減少した。

そのうち、情報収集に関する攻撃は先月比べて約1,800件ほど検証し、これはGit Repository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減少によるものだと確認できた。

また、Web脆弱性に関する攻撃は先月と比べて約1,234件ぐらい減少し、これは、Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)などの攻撃件数減少によるものだと確認できた。

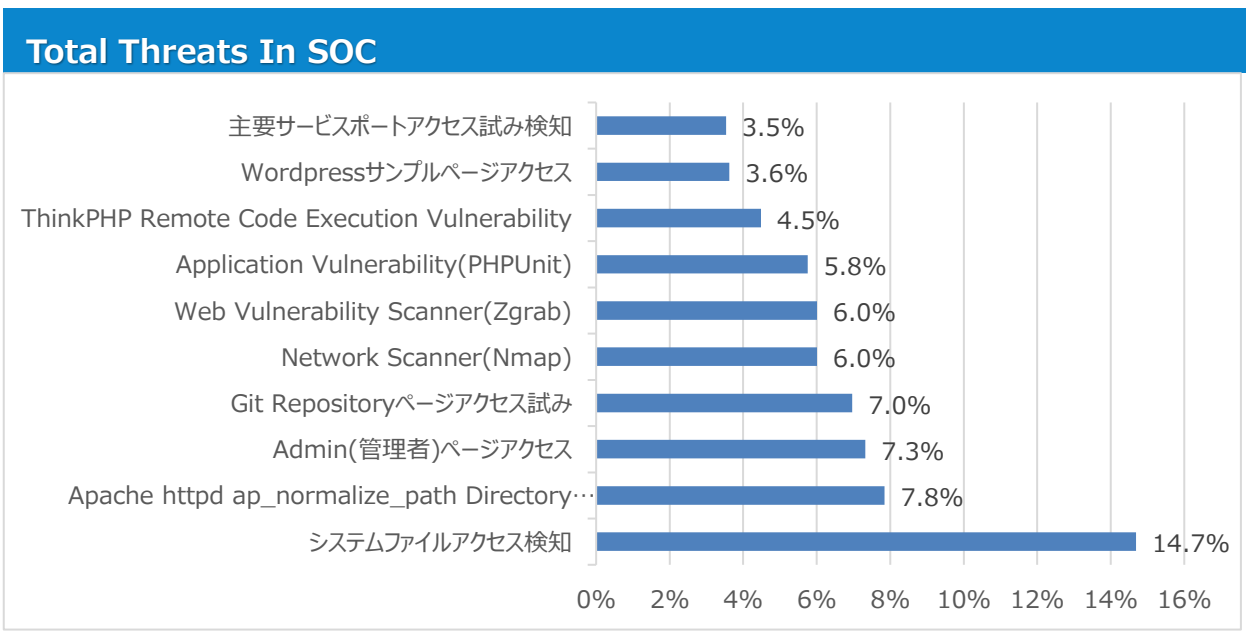


月次攻撃サービスの統計及び分析 - 2025年05月

02. 月次脆弱性攻撃TOP10

2025年05月の月次脆弱性TOP10を確認した結果、多数の新たな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3,420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	14.7%	▲1
2	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	7.8%	▲5
3	Admin(管理者)ページアクセス	7.3%	▲7
4	Git Repositoryページアクセス試み	7.0%	▼3
5	Network Scanner(Nmap)	6.0%	▼2
6	Web Vulnerability Scanner(Zgrab)	6.0%	-
7	Application Vulnerability(PHPUnit)	5.8%	▼2
8	ThinkPHP Remote Code Execution Vulnerability	4.5%	-
9	Wordpressサンプルページアクセス	3.6%	-
10	主要サービスポートアクセス試み検知	3.5%	NEW



月次攻撃サービスの統計及び分析 - 2025年05月

03. 月次ブラックリストIPアドレスTOP 10

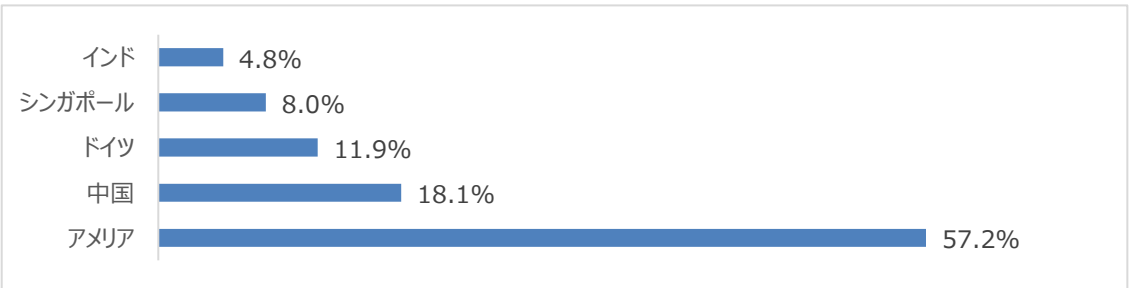
2025年05月についてTOP10を確認した結果、アメリカと中国の攻撃比率が減少し、特にアメリカの攻撃比率が約57.2%を超えていることが確認できた。

※ 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	93.123.109.231	BG	システムファイルアクセス検知
2	93.123.109.229	BG	Git Repositoryページアクセス試み
3	93.123.109.230	BG	システムファイルアクセス検知
4	93.123.109.228	BG	Git Repositoryページアクセス試み
5	47.122.4.148	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
6	47.121.186.223	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
7	8.137.10.102	SJ	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
8	47.121.210.129	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
9	194.50.16.252	NL	phpinfoページ漏洩
10	47.121.124.143	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)

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	93.123.109.231	BG
2	93.123.109.229	BG
3	93.123.109.230	BG
4	93.123.109.228	BG
5	47.122.4.148	CN

Rank	Source IP	Country
6	47.121.186.223	CN
7	8.137.10.102	SJ
8	47.121.210.129	CN
9	194.50.16.252	NL
10	47.121.124.143	CN

攻撃パターン毎の詳細分析結果

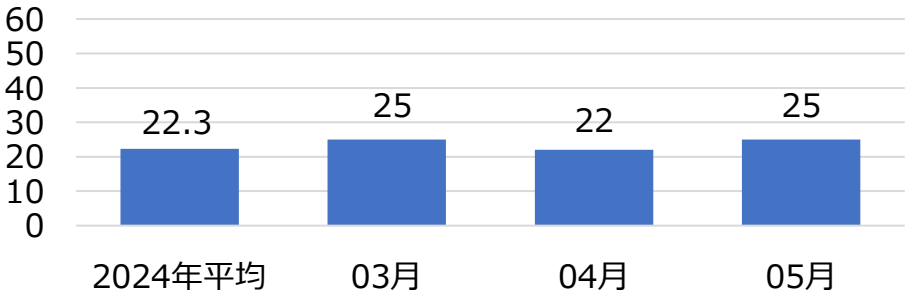
05月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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。
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。
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。
ThinkPHP Remote Code Execution Vulnerability	ThinThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。￥think￥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
Wordpressサンプルページアクセス	Wordpressのログインページである「wp-login.php, wp-admin.php, wp-config.php」やサ ンプルページにアクセスするイベントで主にページの有無を確認するためのアクセスである。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年05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25件である。
05月1か月の間SAP NetWeaver(CVE-2025-31324), Langflow(CVE-2025-3248), Ivanti(CVE-2025-4427,CVE-2025-4428), MS(CVE-2024-43451)などに対する検知ポリシーが配布された。



3か月間件数

6,699
全体配布量

25
今月配布量

22
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.1.06718 server-webapp,SAP,NetWeaver,cve-2025-31324, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/developmentserver/metadatauploader"; fast_pattern:only; http_uri; content:"<%"; http_client_body; sid:106718;)	SAP NetWeaverの脆弱性であるCVE-2025-31324を悪用したファイルアップロード試みを検知するポリシー	server-webapp,SAP,NetWeaver,cve-2025-31324
alert tcp $EXTERNAL_NET any -> $HOME_NET [$HTTP_PORTS,7860] (msg:"IGRSS.2.06723 server-webapp,Langflow,cve-2025-3248, Attempted User Privilege Gain"; flow:to_server,established; content:"POST /api/v1/validate/code"; depth:26; fast_pattern; nocase; content:"|22|code|22|"; nocase; pcre:"/^¥s*?¥x3a¥s*?¥x22((?!(?<!¥x5c)¥x22).)*?(@¥s*?(exec|eval|__import__)|def¥b[^:]*?=¥s*?(exec|eval|__import__))/Ri"; sid:206723;)	Langflowの脆弱性であるCVE-2025-3248を悪用したリモートコマンド実行試みを検知するポリシー	server-webapp,Langflow,cve-2025-3248
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06724 server-webapp,Ivanti,cve-2025-4427,cve-2025-4428, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/api/v2/featureusage"; fast_pattern:only; http_uri; content:"format="; nocase; http_client_body; pcre:"/(^|&)format=[^&]*?(¥x28|%(25)?28)/Pim"; sid:106724;)	Ivanti EPMMの脆弱性であるCVE-2025-4427, CVE-2025-4428を悪用したリモートコマンド実行試みを検知するポリシー	server-webapp,Ivanti,cve-2025-4427,cve-2025-4428
alert tcp any any -> any any (msg:"IGRSK.2.06734 os-windows_MS_Windows_NTLM_cve-2024-43451_Attempted User Privilege Gain"; flow:established; content:"|5b|InternetShortcut"; pcre:"/^(?:¥x2e[AW])¥x5d/R"; content:"|3d 5c 5c 5c 5c|";)	MS Windows NTLMの脆弱性であるCVE-2024-43451を悪用したNTLMハッシュ公開スプーフィング攻撃を検知するポリシー	os-windows,microsoft,Windows,NTLM,cve-2024-43451