SECURITY REPORT

2025

MAY

2025年05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04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。

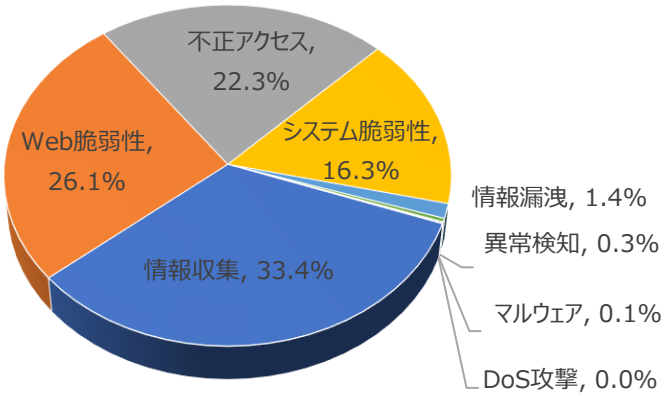
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	33.4%	-
Web脆弱性(Web Vulnerability)	26.1%	▲1
不正アクセス(Unauthorized access)	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%	▲1
マルウェア(Malware)	0.1%	▼1
DoS攻撃(Denial of service attack)	0.0%	-

2025年04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0.80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1,494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738件ぐらい減少し、これはSQL Injectionなどの攻撃件数減少によるものだと確認できた。

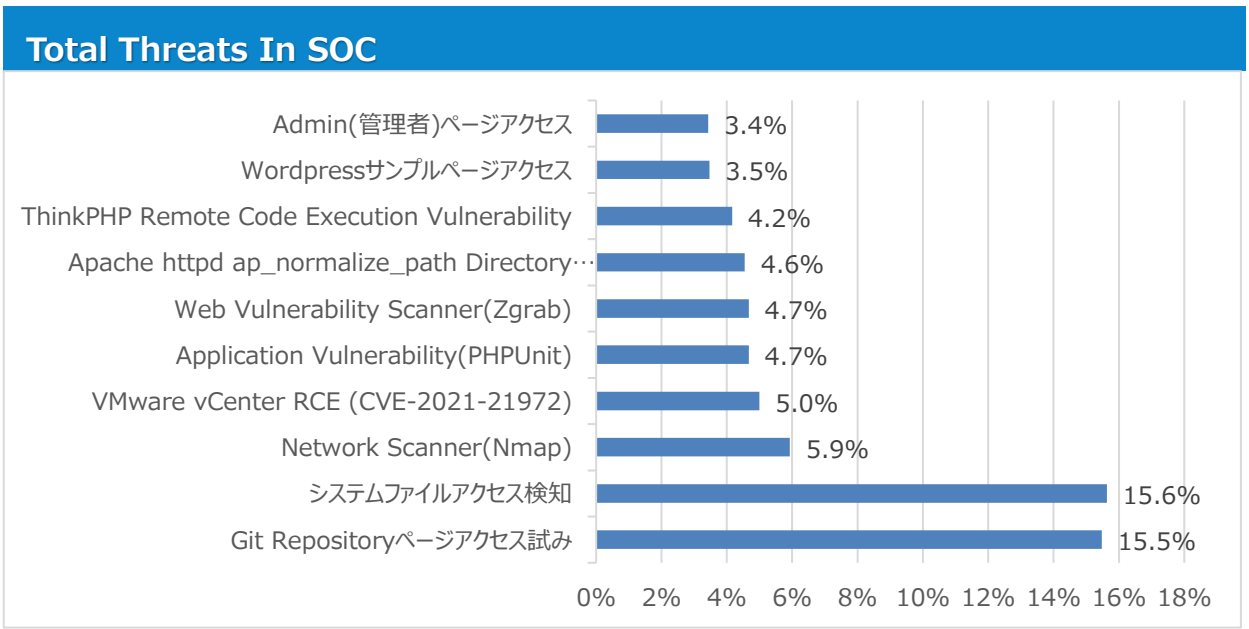


月次攻撃サービスの統計及び分析 - 2025年04月

02. 月次脆弱性攻撃TOP10

2025年04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増加した。特に不正アクセスの攻撃件数が先月と比べて約4,750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	Git Repositoryページアクセス試み	15.5%	▲1
2	システムファイルアクセス検知	15.6%	▼1
3	Network Scanner(Nmap)	5.9%	▲3
4	VMware vCenter RCE (CVE-2021-21972)	5.0%	▲5
5	Application Vulnerability(PHPUnit)	4.7%	▼2
6	Web Vulnerability Scanner(Zgrab)	4.7%	▼1
7	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	4.6%	▼2
8	ThinkPHP Remote Code Execution Vulnerability	4.2%	NEW
9	Wordpressサンプルページアクセス	3.5%	▲1
10	Admin(管理者)ページアクセス	3.4%	NEW



月次攻撃サービスの統計及び分析 - 2025年04月

03. 月次ブラックリストIPアドレスTOP 10

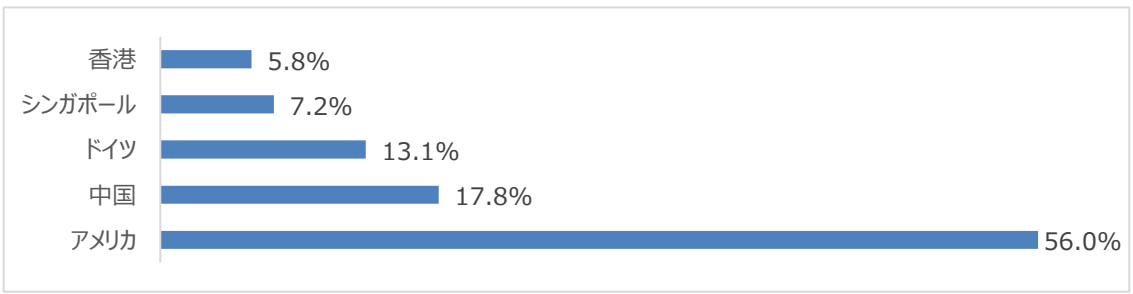
2025年04月についてTOP10を確認した結果、アメリカと中国の攻撃比率が増加し、特にアメリカの攻撃比率が約56.0%を超えていることが確認できた。

※ 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	195.178.110.164	BG	Git Repositoryページアクセス試み
2	195.178.110.159	BG	Git Repositoryページアクセス試み
3	35.195.46.0	BE	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
4	8.137.10.102	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
5	47.121.125.190	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
6	154.83.103.108	SC	Git Repositoryページアクセス試み
7	196.240.54.120	LV	Apache Tomcatから発生するリモートコード実行脆弱性 (CVE-2025-24813)
8	188.213.161.98	IT	Apache Tomcatから発生するリモートコード実行脆弱性 (CVE-2025-24813)
9	140.143.182.115	CN	Apache Tomcatから発生するリモートコード実行脆弱性 (CVE-2025-24813)
10	176.65.138.172	CY	Apache Tomcatから発生するリモートコード実行脆弱性 (CVE-2025-24813)

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	195.178.110.164	BG
2	195.178.110.159	BG
3	35.195.46.0	BE
4	8.137.10.102	CN
5	47.121.125.190	CN

Rank	Source IP	Country
6	154.83.103.108	SC
7	196.240.54.120	LV
8	188.213.161.98	IT
9	140.143.182.115	CN
10	176.65.138.172	CY

攻撃パターン毎の詳細分析結果

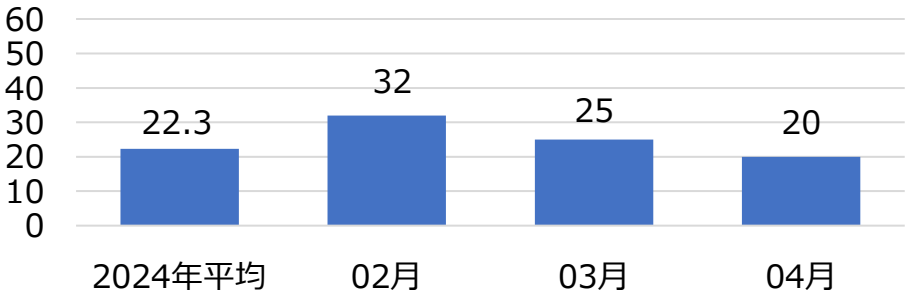
04月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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。
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。
SQL Injection	SQL Injection攻撃はウェブページから記号やUnion, Selectなどクエリで使用される文字列をフィルタリングせずに入力された値がクエリに使用される場合発生しうる。攻撃者はDBに繋がっているアカウントが持っている権限内で様々なクエリを使用して保存された情報の取得、修正、削除及びシステムアクセスなどが可能である。
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。
VMware vCenter RCE (CVE-2021-21972)	vSphere Client (HTML5)ではvCenter Serverプラグインのリモートコード実行脆弱性が含まれている。ポート443にたいするネットワークアクセス権限がある攻撃者がこの脆弱性を悪用してvCenter ServerをホスティングするOSで制限なくコマンドが実行できる。これはVMware vCenter Server (7.0 U1c以前7.x, 6.7 U3l以前6.7および6.5 U3n以前6.5)およびVMware Cloud Foundation (4.2以前4.xおよび3.10.1.2以前3.x)に影響を及ぼす。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年04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20件である。
04月1か月の間SAP(CVE-2017-12637), Ivanti(CVE-2025-22457), Erlang/OTP(CVE-2025-32433)脆弱性とLummaStealerマルウェアなどに対する検知ポリシーが配布された。



3か月間件数

6,672
全体配布量

20
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 -> any $HTTP_PORTS (msg:"IGRSS.10.06696 server-webapp,SAP,NetWeaver,cve-2017-12637, Web Application Attack"; flow:to_server,established; content:"/scheduler/ui/js/ffffffffbca41eb4/"; fast_pattern; nocase; http_uri; content:"root.js"; distance:0; nocase; http_uri; sid:1006696;)	SAP NetWeaverの脆弱性であるCVE-2017-12637を悪用したLFI(Local File Inclusion)試みを検知するポリシー	server-webapp,SAP,NetWeaver,cve-2017-12637
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06699 server-webapp,Ivanti,cve-2025-22457, Web Application Attack"; flow:to_server,established; content:"X-Forwarded-For|3A|"; fast_pattern:only; http_header; content:"X-Forwarded-For|3A|"; isdataat:512,relative; content:!"|0A|"; within:512; sid:1006699;)	Ivantiの脆弱性であるCVE-2025-22457を悪用したバッファオーバーフロー	server-webapp, Ivanti,cve-2025-22457
alert tcp any any -> $HOME_NET 22 (msg:"IGRSS.1.06703 server-other,Erlang/OTP,SSH,cve-2025-32433, Attempted Administrator Privilege Gain"; flow:to_server,established; flowbits:isset,erlang_ssh_banner; content:"|62|"; depth:1; offset:5; content:"|00 00 00 04|exec"; within:8; distance:4; sid:106703;)	Erlang/OTP SSHの脆弱性であるCVE-2025-32433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-other, Erlang/OTP,SSH, cve-2025-32433
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06704 malware-cnc,Infostealer,LummaStealer, A Network Trojan was detected"; flow:to_server; urilen:1,norm; content:"Content-Disposition:"; http_client_body; content:"name=|22|hwid|22|"; http_client_body; content:"name=|22|build_id|22|"; within:100; distance:50; fast_pattern; nocase; http_client_body; pcre:"/name¥x3d"hwid"(¥x0d¥x0a){2}[a-f0-9]{21}¥x2d[a-f0-9]{8}¥x2d[a-f0-9]{4}/Pi"; sid:806704;)	LummaStealerマルウェアのネットワーク通信を検知するポリシー	malware-cnc, Infostealer, LummaStealer