SECURITY REPORT

2025

APR

2025年04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03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。

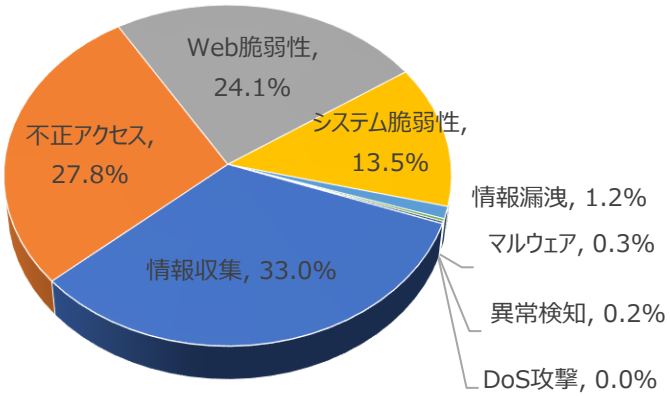
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	33.0%	▲3
不正アクセス(Unauthorized access)	27.8%	▼1
Web脆弱性(Web Vulnerability)	24.1%	▼2
システム脆弱性(System Vulnerability)	13.5%	▼1
情報漏洩(Information Exposure)	1.2%	-
マルウェア(Malware)	0.3%	-
異常検知(Anomaly Detection)	0.2%	-
DoS攻撃(Denial of service attack)	0.0%	-

2025年03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1.85倍ぐらい増加した。

そのうち、情報収集に関する攻撃は先月比べて約5,098件ほど増加し、これはGit Repositoryページアクセス試み、Web Scanner攻撃件数の増加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2,601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。

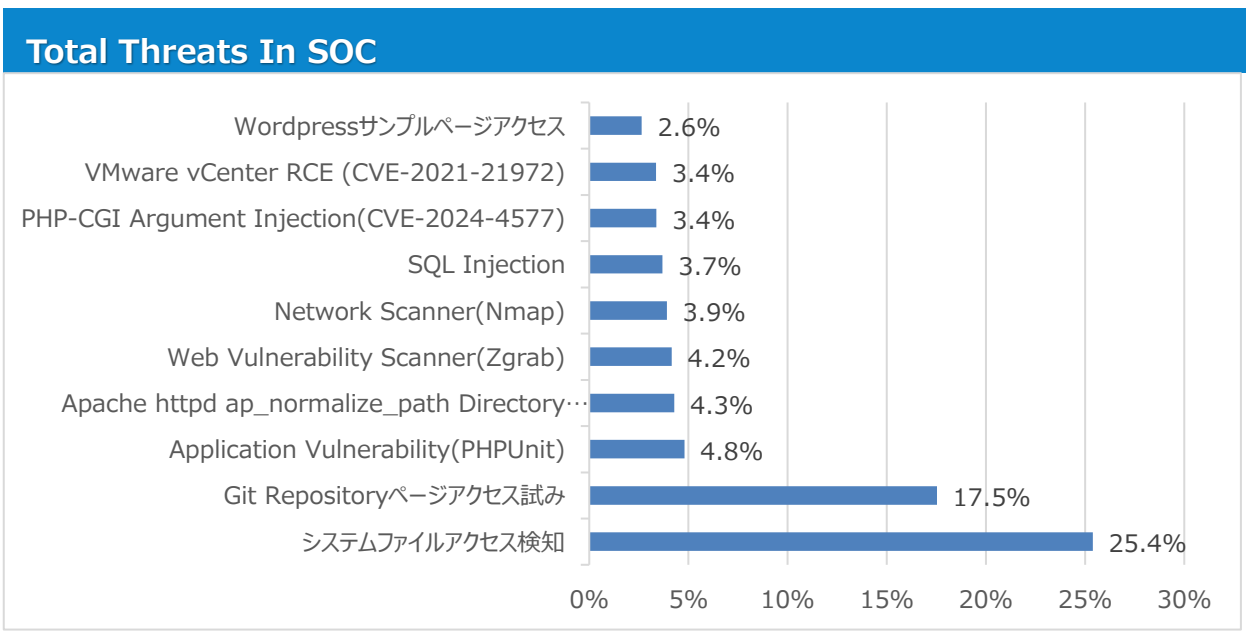


月次攻撃サービスの統計及び分析 - 2025年03月

02. 月次脆弱性攻撃TOP10

2025年03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5,098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	システムファイルアクセス検知	25.4%	-
2	Git Repositoryページアクセス試み	17.5%	▲6
3	Application Vulnerability(PHPUnit)	4.8%	▲4
4	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	4.3%	▼1
5	Web Vulnerability Scanner(Zgrab)	4.2%	NEW
6	Network Scanner(Nmap)	3.9%	▼1
7	SQL Injection	3.7%	▼5
8	PHP-CGI Argument Injection(CVE-2024-4577)	3.4%	NEW
9	VMware vCenter RCE (CVE-2021-21972)	3.4%	-
10	Wordpressサンプルページアクセス	2.6%	NEW



月次攻撃サービスの統計及び分析 - 2025年03月

03. 月次ブラックリストIPアドレスTOP 10

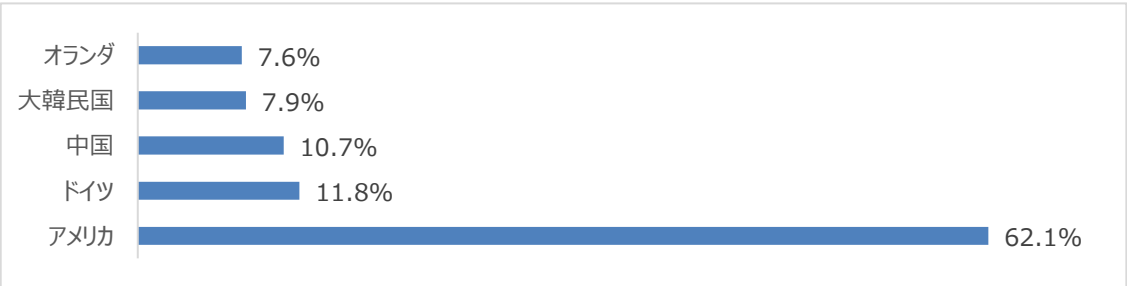
2025年03月についてTOP10を確認した結果、アメリカとオランダの攻撃比率が増加し、特にアメリカの攻撃比率が約62.1%を超えていることが確認できた。

※ 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	45.148.10.90	NL	Git Repositoryページアクセス試み
2	45.148.10.35	NL	Git Repositoryページアクセス試み
3	195.178.110.163	US	Git Repositoryページアクセス試み
4	45.148.10.34	NL	システムファイルアクセス検知
5	35.195.46.0	BG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
6	195.178.110.164	US	システムファイルアクセス検知
7	195.178.110.159	US	システムファイルアクセス検知
8	4.230.144.132	US	Git Repositoryページアクセス試み
9	20.249.104.159	US	Git Repositoryページアクセス試み
10	20.249.139.38	US	Git Repositoryページアクセス試み

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	45.148.10.90	NL
2	45.148.10.35	NL
3	195.178.110.163	US
4	45.148.10.34	NL
5	35.195.46.0	BG

Rank	Source IP	Country
6	195.178.110.164	US
7	195.178.110.159	US
8	4.230.144.132	US
9	20.249.104.159	US
10	20.249.139.38	US

攻撃パターン毎の詳細分析結果

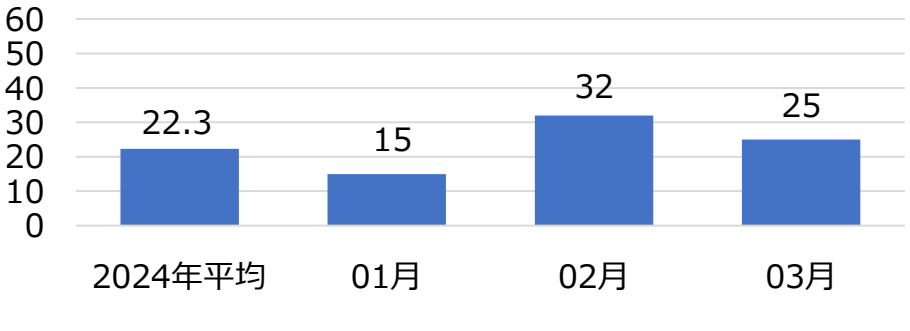
03月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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03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。
03月1か月の間Oracle(CVE-2023-21931), SAP(CVE-2022-22536), Mitel(CVE-2024-41710), PaloAltoNetworks(CVE-2025-0108)などに対する検知ポリシーが配布された。



3か月間件数

6,652
全体配布量

25
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 any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06671 server-webapp,Apache,Camel,cve-2025-27636, Attempted User Privilege Gain"; flow:to_server,established; content:"org.apache.camel."; fast_pattern:only; http_header; pcre:"/^(?!org¥x2eapache¥x2ecamel¥x2e)(?i)org¥x2eapache¥x2ecamel¥x2e/Hm"; sid:206671;)	Apache Camleの脆弱性であるCVE-2025-27636を悪用したバイパス試みを検知するポリシー	server-webapp,Apache,Camel,cve-2025-27636
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06673 server-webapp,Apache,Camel,cve-2025-27636, Attempted User Privilege Gain"; flow:to_server,established; content:"CamelExec"; fast_pattern:only; http_header; pcre:"/^CamelExec(Command|Exit|Stderr|Use)/Him"; sid:206673;)	Apache Camleの脆弱性であるCVE-2025-27636を悪用したバイパス試みを検知するポリシー	server-webapp,Apache,Camel,cve-2025-27636
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06681 server-webapp,Next.js,cve-2025-29927, Web Application Attack"; flow:to_server,established; content:"x-middleware-subrequest|3A|middleware|3A|middleware|3A|middleware|3A|middleware"; fast_pattern:only; http_header; sid:1006681;)	Next JSの脆弱性であるCVE-2025-29927を悪用したバイパス攻撃を検知するポリシー	server-webapp,Next.js,cve-2025-29927
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06685 server-webapp,Next.js,cve-2025-29927, Web Application Attack"; flow:to_server,established; content:"x-middleware-subrequest|3A|src/middleware|3A|src/middleware|3A|src/middleware|3A|src/middleware|3A|src/middleware"; fast_pattern:only; http_header; sid:1006685;)	Next JSの脆弱性であるCVE-2025-29927を悪用したバイパス攻撃を検知するポリシー	server-webapp,Next.js,cve-2025-29927