SECURITY REPORT

2025

FEB

2025年02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01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。

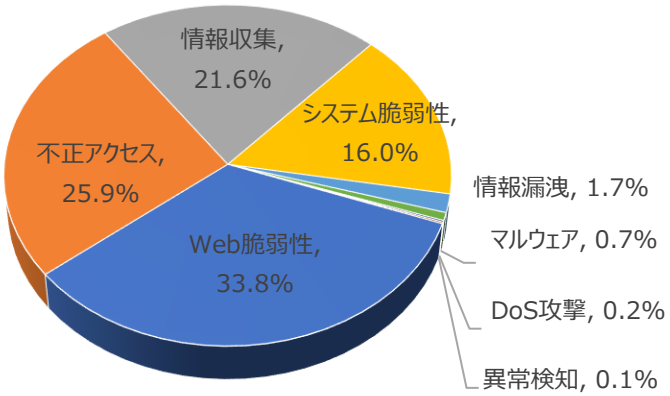
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	33.8%	-
不正アクセス(Unauthorized access)	25.9%	▲1
情報収集(Information Gathering)	21.6%	▲1
システム脆弱性(System Vulnerability)	16.0%	▼2
情報漏洩(Information Exposure)	1.7%	-
マルウェア(Malware)	0.7%	-
DoS攻撃(Denial of service attack)	0.2%	▲1
異常検知(Anomaly Detection)	0.1%	▼1

2025年01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0.85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861件ほど増加し、主要さーびすポートへのアクセス試み攻撃件数の増加によるものだと確認できた。

また、システム脆弱性に関する攻撃は先月と比べて約906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。

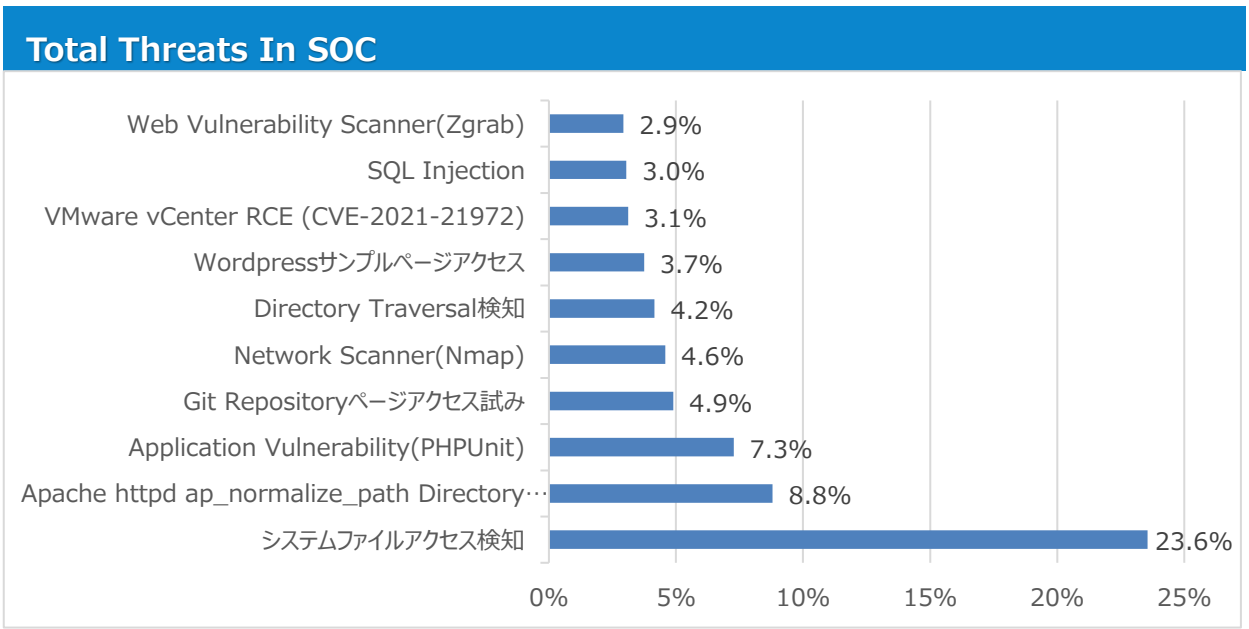


月次攻撃サービスの統計及び分析 - 2025年01月

02. 月次脆弱性攻撃TOP10

2025年01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、特にシステム脆弱性の攻撃件数が先月と比べて約2,902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	23.6%	▲1
2	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	8.8%	▼1
3	Application Vulnerability(PHPUnit)	7.3%	-
4	Git Repositoryページアクセス試み	4.9%	▲3
5	Network Scanner(Nmap)	4.6%	▲4
6	Directory Traversal検知	4.2%	NEW
7	Wordpressサンプルページアクセス	3.7%	NEW
8	VMware vCenter RCE (CVE-2021-21972)	3.1%	NEW
9	SQL Injection	3.0%	▼4
10	Web Vulnerability Scanner(Zgrab)	2.9%	▼6



月次攻撃サービスの統計及び分析 - 2025年01月

03. 月次ブラックリストIPアドレスTOP 10

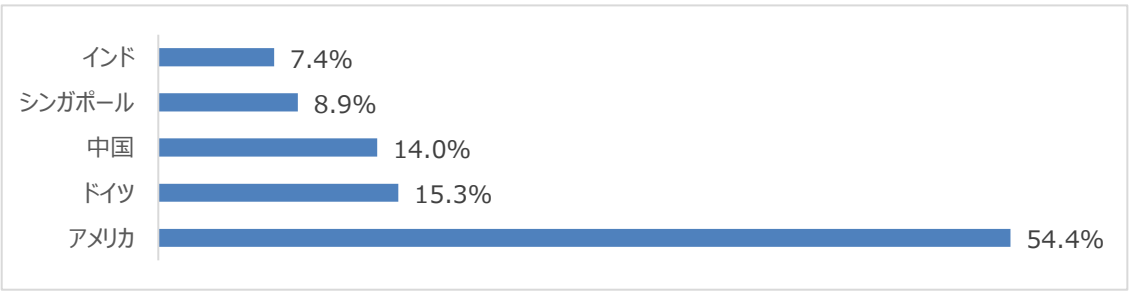
2025年01月についてTOP10を確認した結果、アメリカとドイツの攻撃比率減少し、特にアメリカの攻撃比率が約54.4%を超えていることが確認できた。

※ 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	178.215.236.132	US	Git Repositoryページアクセス試み
2	87.120.115.119	BG	システムファイルアクセス検知
3	47.76.72.62	HK	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
4	141.94.145.70	FR	システムファイルアクセス検知
5	39.103.191.118	CN	ThinkPHP Remote Code Execution Vulnerability
6	193.41.206.36	FR	Wordpressサンプルページアクセス
7	46.19.143.26	CH	Command Injection
8	92.255.57.58	HK	etcpasswd Detect
9	78.153.140.203	GB	Phpinfoページ漏洩
10	87.120.115.34	BG	システムファイルアクセス検知

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	178.215.236.132	US	6	193.41.206.36	FR
2	87.120.115.119	BG	7	46.19.143.26	CH
3	47.76.72.62	HK	8	92.255.57.58	HK
4	141.94.145.70	FR	9	78.153.140.203	GB
5	39.103.191.118	CN	10	87.120.115.34	BG

攻撃パターン毎の詳細分析結果

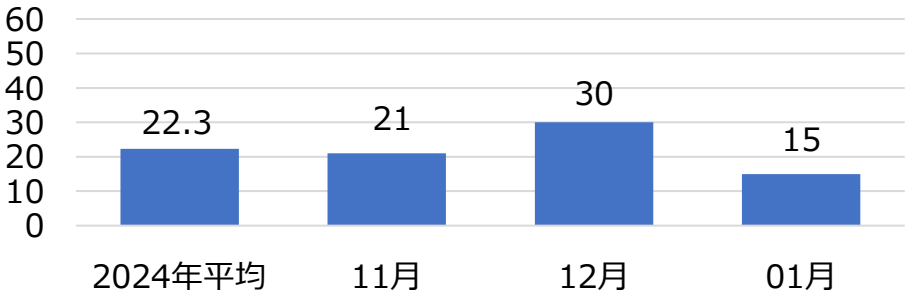
01月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
Directory Traversal 検知	ホームページの表示もしくはダウンロードページのURLを使用せず、Webサーバ上のhomeディレクトリ外の任意のディレクトリ上のファイル(/etc/passwdファイルなど)を参照またはダウンロードすることが出来る。内部情報については、システム情報を含む/etc/pass/shadow、/etc/hosts/hostsなどの主要ファイルをダウンロードすることが可能であり、システム侵入や内部データ漏洩などの二次的な攻撃 に悪用される可能性がある。
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。
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。
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。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年01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。
01月1か月の間Windows Server(CVE-2024-49112), Apache Struts(CVE-2024-53677), Aviartix(CVE-2024-50603)脆弱性とGamaredon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

6,595
全体配布量

15
今月配布量

30
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET [389,636] -> $HOME_NET any (msg:"IGRSS.11.06618 os-windows,windows,ldap,cve-2024-49112, Attempted Denial of Service"; flow:to_client,established; content:"|30|"; depth:1; content:"|02 04|"; within:2; distance:1; content:"|65|"; within:1; distance:4; content:"|0A 01 0A|"; within:3; distance:1; content:"ldap"; distance:8; fast_pattern; nocase; content:"://"; within:4; sid:1106618;)	Windows Serve LDAPの脆弱性であるCVE-2024-49112を悪用したサービス拒否攻撃を検知するポリシー	os-windows,windows,ldap,cve-2024-49112
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06622 server-webapp,Apache,Struts,cve-2024-53677, Web Application Attack"; flow:to_server,established; content:"uploadFileName"; fast_pattern:only; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?uploadFileName(¥x5b¥d+¥x5d)?((?!^--).)*?¥x2e¥x2e[¥x2f¥x5c]/Psim"; sid:1006622;)	Apache Strutsの脆弱性であるCVE-2024-53677を悪用したDirectory Traversal攻撃を検知するポリシー	server-webapp,Apache,Struts,cve-2024-53677
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06623 malware-cnc,Trojan,Gamaredon, A Network Trojan was detected"; flow:to_server,established; content:"User-Agent: Mozilla/4.0 (compatible|3B| Win32|3B| WinHttp.WinHttpRequest.5)"; http_header; content:"Content-Disposition"; nocase; content:"|0D 0A 0D 0A|MjAwMDo6"; fast_pattern:only; http_client_body; pcre:"/¥r¥n¥r¥nMjAwMDo6[A-Za-z0-9]{40,100}/P"; sid:806623;)	Gamaredonの変種Malwareのネットワーク通信を検知するポリシー	malware-cnc,Trojan,Gamaredon
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06624 server-webapp,Aviartix,cve-2024-50603, Web Application Attack"; flow:to_server,established; content:"/v1/api"; fast_pattern:only; http_uri; content:"action"; nocase; http_client_body; content:"flightpath"; distance:0; nocase; http_client_body; content:"cloud_type"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?(src_)?cloud_type((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/Psim"; sid:1006624;)	Aviartixの脆弱性であるCVE-2024-50603を悪用したCommand Injection攻撃を検知するポリシー	server-webapp,Aviartix,cve-2024-50603