SECURITY REPORT

2025

JAN

2025年01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 - 2024年12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。

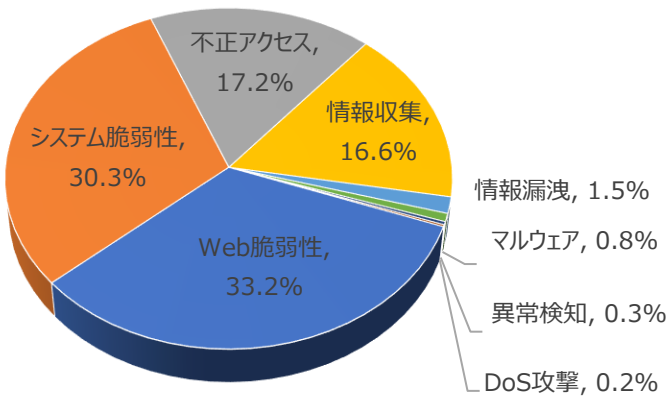
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	33.2%	▲1
システム脆弱性(System Vulnerability)	30.3%	▼1
不正アクセス(Unauthorized access)	17.2%	-
情報収集(Information Gathering)	16.6%	-
マルウェア(Malware)	1.5%	-
情報漏洩(Information Exposure)	0.8%	-
異常検知(Anomaly Detection)	0.3%	-
DoS攻撃(Denial of service attack)	0.2%	-

2024年12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0.76倍ぐらい減少した。

そのうち、Web脆弱性に関する攻撃は先月比べて約296件ほど減少し、PHPUnit, PHP-CGI Argument Injection攻撃件数の減少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5,067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。

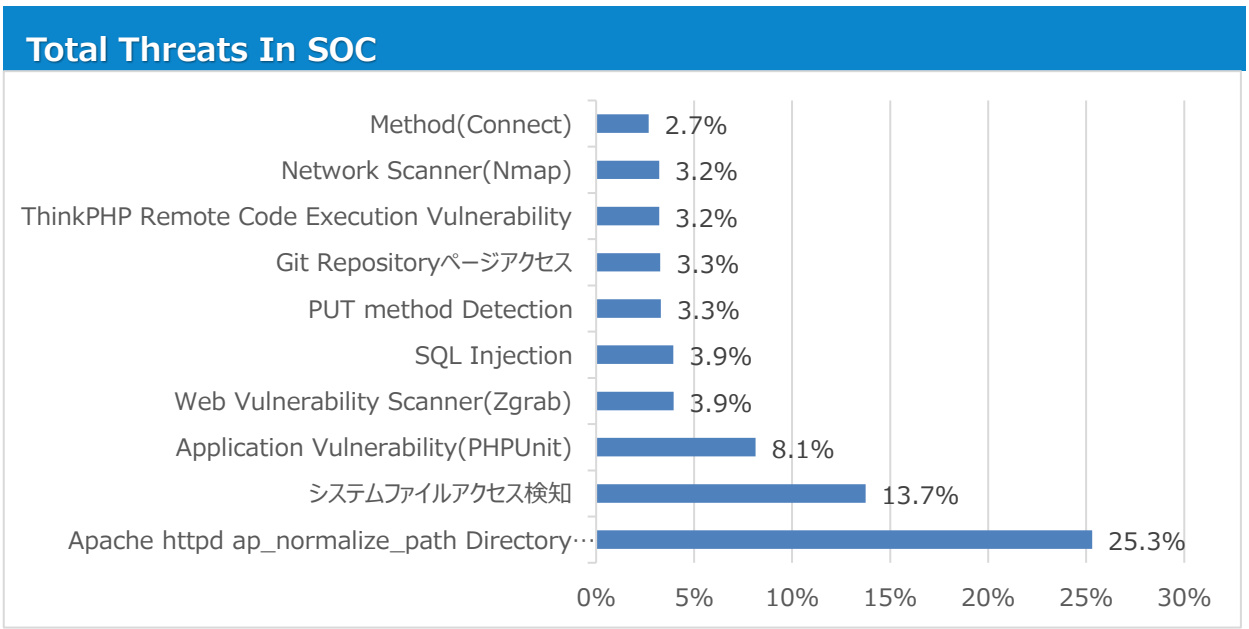


月次攻撃サービスの統計及び分析 - 2024年12月

02. 月次脆弱性攻撃TOP10

2024年12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5,067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	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	40.9%	-
2	システムファイルアクセス検知	13.1%	▲2
3	Application Vulnerability(PHPUnit)	8.2%	▼1
4	Web Vulnerability Scanner(Zgrab)	3.3%	▲1
5	SQL Injection	2.8%	NEW
6	PUT method Detection	2.8%	NEW
7	Git Repositoryページアクセス	2.3%	▲1
8	ThinkPHP Remote Code Execution Vulnerability	2.3%	▼4
9	Network Scanner(Nmap)	2.0%	-
10	Method(Connect)	1.9%	NEW



月次攻撃サービスの統計及び分析 - 2024年12月

03. 月次ブラックリストIPアドレスTOP 10

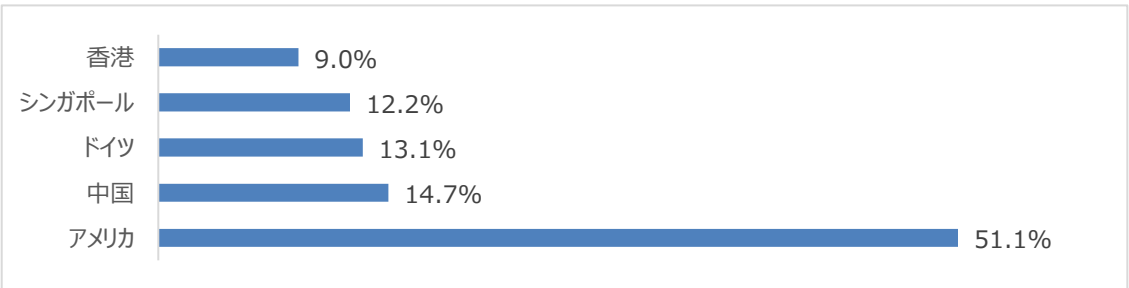
2024年12月についてTOP10を確認した結果、中国とシンガポールの攻撃比率が増加し、特にアメリカの攻撃比率が約39.9%を超えていることが確認できた。

※ 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	47.251.103.74	US	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
2	47.237.24.160	HK	PHP-CGI Argument Injection(CVE-2024-4577)
3	87.120.115.119	BG	システムファイルアクセス検知
4	8.209.204.4	JP	Application Vulnerability(PHPUnit)
5	47.237.94.12	SG	ThinkPHP Remote Code Execution Vulnerability
6	47.76.72.62	HK	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
7	87.120.115.34	BG	Git Repositoryページアクセス
8	47.236.232.202	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
9	8.219.136.232	SG	PHP-CGI Argument Injection(CVE-2024-4577)
10	47.237.6.119	SG	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
1	47.251.103.74	US
2	47.237.24.160	HK
3	87.120.115.119	BG
4	8.209.204.4	JP
5	47.237.94.12	SG

Rank	Source IP	Country
6	47.76.72.62	HK
7	87.120.115.34	BG
8	47.236.232.202	SG
9	8.219.136.232	SG
10	47.237.6.119	SG

攻撃パターン毎の詳細分析結果

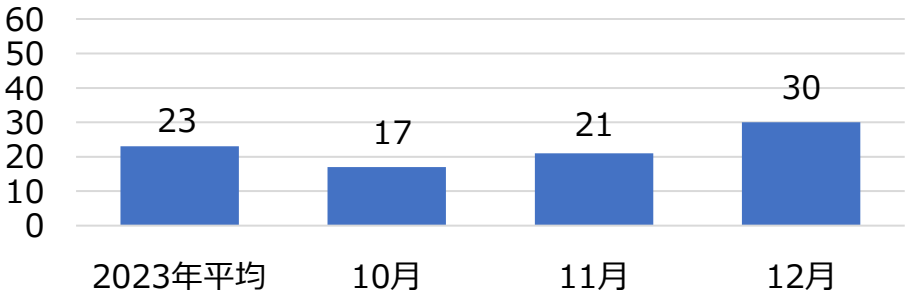
12月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
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。
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。
PUT method Detection	Methodはウェブアプリケーションからデフォルトで提供するクライアントと通信をするためのツールでGET,POST, PUT, MOVE, DELETEなど様々なMethodがある。Methodに対する制限がない場合ファイル生成 (PUT)、削除(DELETE)、トンネリングアクセス(CONNECT)などの動作ができる。
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、存在するソース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。
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。
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。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security)トンネリングは内部にアクセ スをする。このため、Connect Methodを使用していて、脆弱性が存在する場合、中間経由地として使 用される可能性がある。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年12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30件である。
12月1か月の間、Fortinet(CVE-2024-47575), VMware(CVE-2021-39144), CyberPanel(CVE-2024-51378), PaloAltoNetworks(CVE-2024-9463)などに対する検知ポリシーが配布された。



3か月間件数

6,580
全体配布量

30
今月配布量

21
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 541 (msg:"IGRSS.1.06588 server-other,fortinet,FortiManager,cve-2024-47575, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"|36 E0 11 00|"; depth:4; content:"channel"; distance:4; nocase; content:"som/export"; fast_pattern:only; content:"|22|file|22|"; nocase; pcre:"/¥x22file¥x22¥s*¥x3a¥s*¥x22((?!(?<!¥x5c)¥x22).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/i"; sid:106588;)	Fortinet FortiMangerの脆弱性であるCVE-2024-47575を悪用したCommand Injection攻撃を検知するポリシー	server-other,fortinet,FortiManager,cve-2024-47575
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06598 server-webapp,VMware,NSX Manager, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/services/usermgmt/password/"; fast_pattern:only; http_uri; content:"java|2E|"; nocase; file_data; pcre:"/<¥w+¥s+class¥s*?¥x3D¥s*?[¥x22¥x27]java¥x2e/i"; sid:106598;)	VMware NSX Manager Xstreamの脆弱性であるCVE-2021-39144を悪用したCommand Injection攻撃を検知するポリシー	server-webapp,VMware,NSX Manager
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06615 server-webapp,CyberPanel,cve-2024-51378, Web Application Attack"; flow:to_server,established; content:"/"; http_uri; content:"/getresetstatus"; within:15; distance:3; nocase; http_uri; file_data; content:"|22|statusfile|22|"; nocase; pcre:"/¥x22statusfile¥x22¥s*¥x3a¥s*¥x22((?!(?<!¥x5c)¥x22).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/i"; sid:1006615;)	CyberPanelの脆弱性であるCVE-2024-51378を悪用したCommand Injection攻撃試みを検知するポリシー	server-webapp,CyberPanel,cve-2024-51378
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06616 server-webapp,PaloAltoNetworks,Expedition,cve-2024-9463, Web Application Attack"; flow:to_server,established; content:"/API/convertCSVtoParquet.php"; fast_pattern:only; http_uri; content:"ram="; nocase; http_client_body; pcre:"/(^|&)ram=[^&]*?([¥x60¥x3b¥x7c¥x23]|%(25)?(60|3b|7c|23|26|0a)|([¥x3c¥x3e¥x24]|%(25)?(3c|3e|24))(¥x28|%(25)?28))/Pim"; sid:1006616;)	PaloAltoNetworksのExpedition脆弱性である CVE-2024-9463を悪用したCommand Injection攻撃試みを検知するポリシー	server-webapp,PaloAltoNetworks,Expedition,cve-2024-9463