SECURITY REPORT

2025

AUG

2025年08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07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。

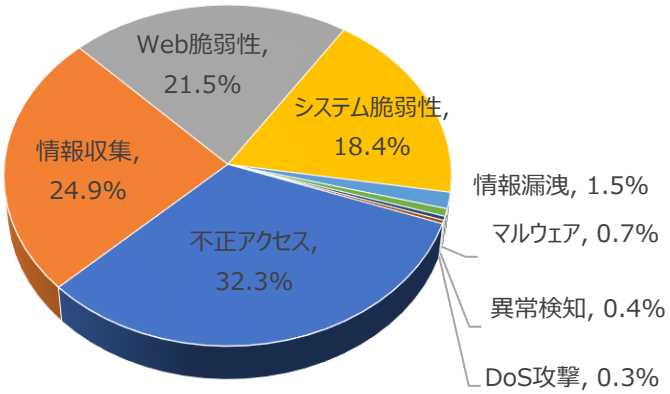
01. 月次攻撃類型

パターン	比率(%)	比較
不正アクセス(Unauthorized access)	32.3%	-
情報収集(Information Gathering)	24.9%	-
Web脆弱性(Web Vulnerability)	21.5%	-
システム脆弱性(System Vulnerability)	18.4%	-
情報漏洩(Information Exposure)	1.5%	-
マルウェア(Malware)	0.7%	▲1
異常検知(Anomaly Detection)	0.4%	▼1
DoS攻撃(Denial of service attack)	0.3%	-

2025年07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1.30倍ぐらい増加した。

そのうち、不正アクセスに関する攻撃は先月比べて約1,363件ほど増加し、これはAdmin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増加によるものだと確認できた。

また、情報収集に関する攻撃は先月と比べて約1,243件ぐらい増加し、これは,Network Scannerの攻撃件数増加によるものだと確認できた。



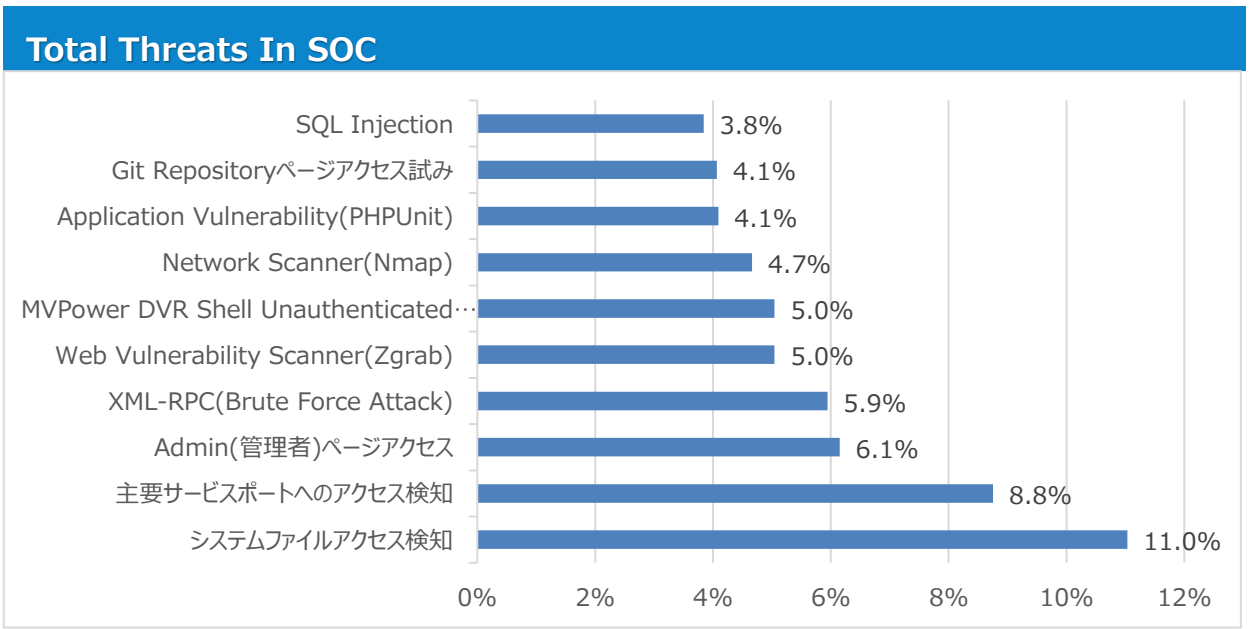
Copyright © Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2025年07月

02. 月次脆弱性攻撃TOP10

2025年07月の月次脆弱性TOP10を確認した結果、多数のWeb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/情報収集の攻撃件数が先月と比べて約2,606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	11.0%	-
2	主要サービスポートへのアクセス検知	8.8%	-
3	Admin(管理者)ページアクセス	6.1%	-
4	XML-RPC(Brute Force Attack)	5.9%	NEW
5	Web Vulnerability Scanner(Zgrab)	5.0%	▼1
6	MVPower DVR Shell Unauthenticated Command Execution	5.0%	NEW
7	Network Scanner(Nmap)	4.7%	▼2
8	Application Vulnerability(PHPUnit)	4.1%	-
9	Git Repositoryページアクセス試み	4.1%	▼3
10	SQL Injection	3.8%	NEW



Copyright © Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2025年07月

03. 月次ブラックリストIPアドレスTOP 10

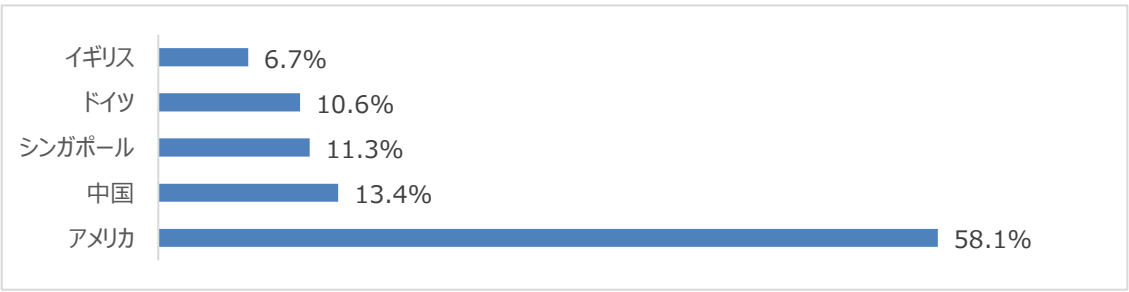
2025年07月についてTOP10を確認した結果、アメリカと中国の攻撃比率が減少し、特にアメリカの攻撃比率が約58.1%を超えていることが確認できた。

※ 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	47.99.40.17	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
2	46.19.141.90	CH	Method(Connect)
3	47.121.210.129	CN	TBK DVR-4104/DVR-4216 MDB/MDC OS Command Injection(CVE-2024-3721)
4	197.220.93.117	SO	ThinkPHP lang Remote Code Execution
5	38.211.193.130	AR	Application Vulnerability(PHPUnit)
6	212.113.102.147	SE	PHP-CGI Argument Injection(CVE-2024-4577)
7	152.32.145.205	JP	Application Vulnerability(PHPUnit)
8	80.75.212.17	DE	TP-Link Router Remote Code Execution(CVE-2023-1389)
9	139.162.124.188	JP	Network Scanner(Nmap)
10	92.55.190.215	KZ	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	47.99.40.17	CN
2	46.19.141.90	CH
3	47.121.210.129	CN
4	197.220.93.117	SO
5	38.211.193.130	AR

Rank	Source IP	Country
6	212.113.102.147	SE
7	152.32.145.205	JP
8	80.75.212.17	DE
9	139.162.124.188	JP
10	92.55.190.215	KZ

Copyright © Cyberfortress, Inc. 2020. All rights reserved

攻撃パターン毎の詳細分析結果

07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。

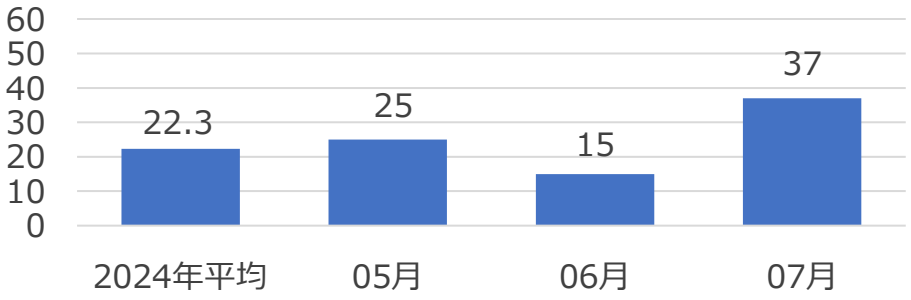
攻撃パターン	詳細分析結果
システムファイルアクセス検知	Directory Traversalの脆弱性などを利用し、「/etc/passwd」や「*.conf /.env」などの構成情報を含む主要なシステムファイルにアクセスを計る。
主要サービスポートアクセス検知	主要ポートにアクセス試み後、アクセス情報を奪取するための総当たり攻撃後、アカウント情報が一致する場合、ウェブ改ざん、情報奪取などの被害が発生しうる。アカウント情報対する周期的な変更及び文字、数字、特殊文字が入っているパスワードの使用と外部からすべてのサービスポートへのアクセス可能ポリシー使用禁止、指定された管理者のIPのみ特定のサ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。
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。
XML-RPC(Brute Force Attack)	XML-RPC(Brute Force Attack)はリモートブログページXML-RPCを利用して総当たり攻撃のログイン攻撃ができる。攻撃者は「¥“system.multicall¥”」メソッドを呼び出して一つのリクエストパケットに数百のID/PWを挿入して攻撃を試みる。
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。
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥‘shell¥’」ファイルを利用することでクエリの文字列の中から任意のシステムコマンドが実行できるようになる。
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。
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。
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。

Copyright © Cyberfortress, Inc. 2020. All rights reserved

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025年07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37件である。
07月1か月の間、MS Windows(CVE-2025-47981), MS SharePoint(CVE-2025-49704), WingFTP(CVE-2025-47811, CVE-2025-47812)脆弱性とspinstallウェブシェルなどに対する検知ポリシーが配布された。



3か月間件数

6,751
全体配布量

37
今月配布量

15
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 any -> $HOME_NET 445 (msg:"IGRSS.2.06753 os-windows,microsoft,windows,SPENGO,cve-2025-47981, Attempted User Privilege Gain"; flow:to_server,established,only_stream; content:"|FE|SMB"; content:"|01 00|"; within:2; distance:8; content:"NEGOEXTS|04 00 00 00|"; distance:0; fast_pattern; byte_extract:4,44,byte_offset,relative, little; byte_extract:4,0,byte_length,relative, little; byte_jump:0,-64,relative; isdataat:byte_offset,relative; byte_jump:0,byte_offset,relative; isdataat:!byte_length,relative; sid:206753;)	Microsoft Windowsの脆弱性であるCVE-2025-47981を悪用したリモートコマンド実行攻撃を検知するポリシー	os-windows,microsoft,windows,SPENGO,cve-2025-47981
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06755 server-webapp,Microsoft,SharePoint,cve-2025-49704, Attempted User Privilege Gain"; flow:to_server,established; content:"/_layouts/"; nocase; http_uri; content:"toolpane.aspx"; distance:0; fast_pattern; nocase; http_uri; content:"DisplayMode=Edit"; distance:0; nocase; http_uri; content:"toolpane.aspx"; distance:0; nocase; http_uri; content:!"|26|"; distance:0; http_uri; content:"Referer|3A|"; nocase; http_header; content:"/SignOut.aspx"; within:50; nocase; http_header; sid:206755;)	Microsoft SharePointの脆弱性であるCVE-2025-49704を悪用したリモートコマンド実行攻撃を検知するポリシー	server-webapp,Microsoft,SharePoint,cve-2025-49704
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06761 server-webapp,WingFTP,cve-2025-47811,cve-2025-47812, Web Application Attack"; flow:to_server,established; content:"/loginok.html"; fast_pattern:only; http_uri; content:"username="; nocase; http_uri; pcre:"/[?&]username=[^&]*?¥x00/Ui"; sid:1006761;)	WingFTPの脆弱性であるCVE-2025-47811, CVE-2025-47812を悪用したリモートコマンド実行攻撃を検知するポリシー	server-webapp,WingFTP,cve-2025-47811,cve-2025-47812
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.06778 malware-backdoor,asp,webshell,spinstall, A Network Trojan was detected"; flow:to_server,established; content:"/_layouts/"; nocase; http_uri; content:"/spinstall0.aspx"; fast_pattern:only; http_uri; sid:806778;)	ToolShell攻撃チェーンでアップロードされるspinstall.aspxウェブシェルのネットワーク通信を検知するポリシー	malware-backdoor,asp,webshell,spinstall

Copyright © Cyberfortress, Inc. 2020. All rights reserved