SECURITY REPORT

2024

AUG

# 2024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 - 2024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。

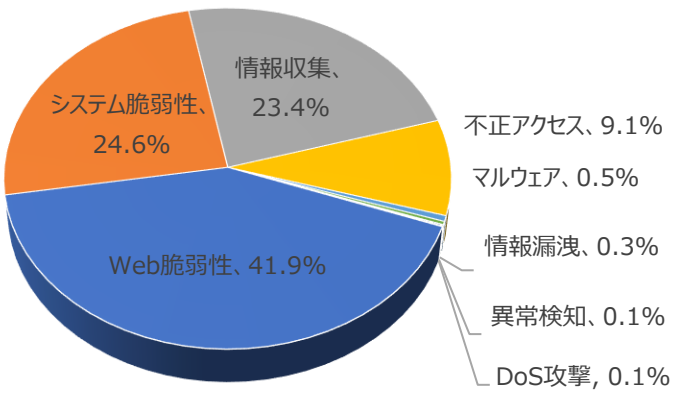
## 01. 月次攻撃類型

| パターン | 比率(%) | 比較 |
|---|---|---|
| Web脆弱性(Web Vulnerability) | 41.9% | - |
| システム脆弱性(System Vulnerability) | 24.6% | - |
| 情報収集(Information Gathering) | 23.4% | - |
| 不正アクセス(Unauthorized access) | 9.1% | - |
| マルウェア(Malware) | 0.5% | - |
| 情報漏洩(Information Exposure) | 0.3% | - |
| 異常検知(Anomaly Detection) | 0.1% | - |
| DoS攻撃(Denial of service attack) | 0.1% | - |

2024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0.8倍ぐらい減少した。

そのうち、システム脆弱性に関する攻撃は先月比べて約2,377件ほど減少し、これはDicrectory Traversal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106件ぐらい減少し、これは,Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃件減少加によるものだと確認できた。

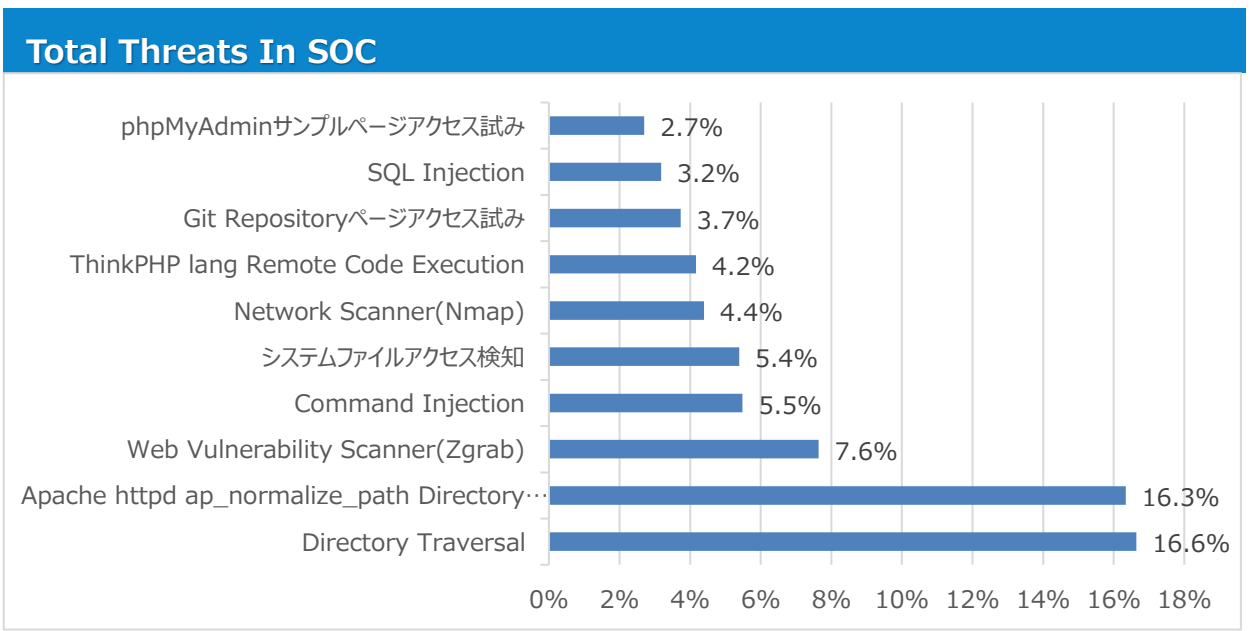


# 月次攻撃サービスの統計及び分析 - 2024年07月

## 02. 月次脆弱性攻撃TOP10

2024年07月の月次脆弱性TOP10を確認した結果、 SQL Injection攻撃が新たにTOP10に登場した。
全体的な攻撃件数は減少し、特にDirectory Traversal攻撃件数は先月と比べて約2,410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 | Directory Traversal | 16.6% | ▲1 |
| 2 | Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773) | 16.3% | ▼6 |
| 3 | Web Vulnerability Scanner(Zgrab) | 7.6% | - |
| 4 | Command Injection | 5.5% | ▲6 |
| 5 | システムファイルアクセス検知 | 5.4% | ▼1 |
| 6 | Network Scanner(Nmap) | 4.4% | ▲3 |
| 7 | ThinkPHP lang Remote Code Execution | 4.2% | ▼2 |
| 8 | Git Repositoryページアクセス試み | 3.7% | - |
| 9 | SQL Injection | 3.2% | NEW |
| 10 | phpMyAdminサンプルページアクセス試み | 2.7% | ▼4 |



# 月次攻撃サービスの統計及び分析 - 2024年07月

## 03. 月次ブラックリストIPアドレスTOP 10

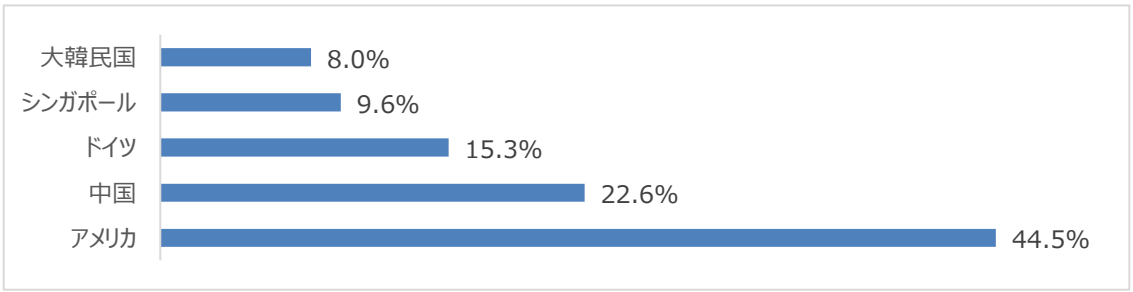
2024年07月についてTOP10を確認した結果、アメリカ、中国、ドイツの攻撃比率が増加し、特にアメリカの攻撃比率が44%を超えていることが確認できた。

※ 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 | 110.14.63.54 | KR | Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773) |
| 2 | 78.153.140.177 | GB | システムファイルアクセス |
| 3 | 51.158.205.47 | FR | Network Scanner(masscan) |
| 4 | 8.213.41.202 | SA | Application Vulnerability(PHPUnit) |
| 5 | 114.205.92.219 | KR | Directory Traversal検知 |
| 6 | 83.222.191.62 | BG | Apache OFBiz Auth Bypass/RCE(CVE-2023-51467) |
| 7 | 206.189.233.163 | US | Directory Traversal検知 |
| 8 | 91.92.244.183 | BG | phpinfo()ページ漏洩 |
| 9 | 78.153.140.179 | GB | システムファイルアクセス |
| 10 | 198.7.123.235 | DE | Directory Traversal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 | 110.14.63.54 | KR | 6 | 83.222.191.62 | BG |
| 2 | 78.153.140.177 | GB | 7 | 206.189.233.163 | US |
| 3 | 51.158.205.47 | FR | 8 | 91.92.244.183 | BG |
| 4 | 8.213.41.202 | SA | 9 | 78.153.140.179 | GB |
| 5 | 114.205.92.219 | KR | 10 | 198.7.123.235 | DE |

# 攻撃パターン毎の詳細分析結果

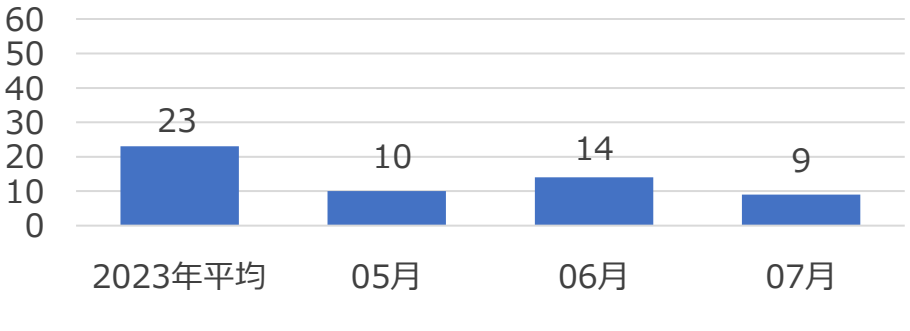
07月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

| 攻撃パターン | 詳細分析結果 |
|---|---|
| Directory Traversal | 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。 |
| 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。 |
| Command Injection | システムコマンドが含まれている入力値が適切な検証プロセスを通らない場合、入力されたコマンドが実行 しうる。この脆弱性が存在する場合、攻撃者がシステムに直接コマンド送信できるため、ファイルの閲覧、 ダウンロード、実行などで追加被害が発生する可能性がある。 |
| 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。 |
| 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。 . |
| ThinkPHP lang Remote Code Execution | 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。 |
| Git Repository ページアクセス試み | 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。 |
| phpMyAdminサンプル ページ アクセス | phpMyAdminはMySQLをWebサーバで管理する目的にてPHPで作成されたオープンソースツールである。MySQLサーバを対象に脆弱性を見つけ、データベースの作成/削除、テーブルの作成/削除、フィールドの生成/削除、SQL文の実行など、権限を利用した管理機能実行による攻撃が可能となる。その脆弱性が存在する場合、phpMyAdminのscript/setup.phpファイルに `?` 引数を使用して任意の関数を挿入し、システム命令を実行できる。 |

# 検知ポリシー

## ▶ 月間サイバー脅威検知ポリシー統計

2024年06の月の1か月間で共有されたサイバー脅威検知ポリシーは9件である。07月1か月間Fortinet(CVE-2024-23108, CVE-2023-34992), MS Office(CVE-2024-38021), Moveit(CVE-2024-5806)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、461**
全体配布量

**9**
今月配布量

**14**
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 7900 (msg:"IGRSS.10.06490 server-webapp,fortinet,fortisiem,cve-2024-23108,cve-2023-34992, Web Application Attack"; flow:to_server,established; content:"\|51 00 00 00\|"; depth:4; content:"<server_ip"; distance:8; nocase; content:"<mount_point"; distance:0; nocase; pcre:"/<(server_ip\|mount_point)[^>]*?>[^<]*?([¥x60¥x3b¥x7c¥x26¥x23]\|¥x24¥x28)/i"; sid:1006490;) | Fortinet FortiSIEMの脆弱性であるCVE-2024-23108, CVE-2023-34992を悪用したInjection攻撃を検知するポリシー | server-webapp,fortinet,fortisiem,cve-2024-23108,cve-2023-34992 |
| alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS [25,587] (msg:"IGRSS.2.06491 file-office,ms,office,cve-2024-38021, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"<img"; nocase; content:"src"; within:100; nocase; content:"file\|3A\|//\|5C 5C\|"; within:100; nocase; content:"\|21\|"; distance:0; pcre:"/<img[^>]*?src¥s*=¥s*[¥x22¥x27]file¥x3a¥x2f¥x2f¥x2f¥x5c¥x5c[^¥x22¥x27]*?¥x21/i"; sid:206491;) | MS Officeの脆弱性であるCVE-2024-38021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 | file-office,ms,office,cve-2024-38021 |
| alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.06495 malware-tools,trojan,plugx, A Network Trojan was detected"; flow:to_client,established; flowbits:isset,file.exe; file_data; content:"\|56 57 48 33 C9 6A 30 5E 65 48 8B 36 48 8B 76 60 48 8B 76 18 48 8B 76 10 48 8B 46 30 48 8B 7E 60 48 8B 36 66 39 4F 18 75 EF 80 3F 6B 74 05 80 3F 4B 75 E5 5F 5E C3\|"; sid:806495;) | PlugX Malwareのネットワーク通信を検知するポリシー | malware-tools,trojan,plugx |
| alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06496 server-webapp,progress,moveit,cve-2024-5806, Attempted User Privilege Gain"; flow:to_server,established; content:"/guestaccess.aspx"; fast_pattern:only; http_uri; content:"Arg12"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?Arg12((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?(PuTTY-User-Key-File-3\|¥x2d{4,5}¥s*BEGIN)/Pims"; sid:206496;) | Progress MOVEitの脆弱性であるCVE-2024-5806を悪用した権限上昇試みを検知するポリシー | server-webapp,progress,moveit,cve-2024-5806 |