# SECURITY REPORT

# 2021 OCT


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 - 2021年10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いただければと思います。

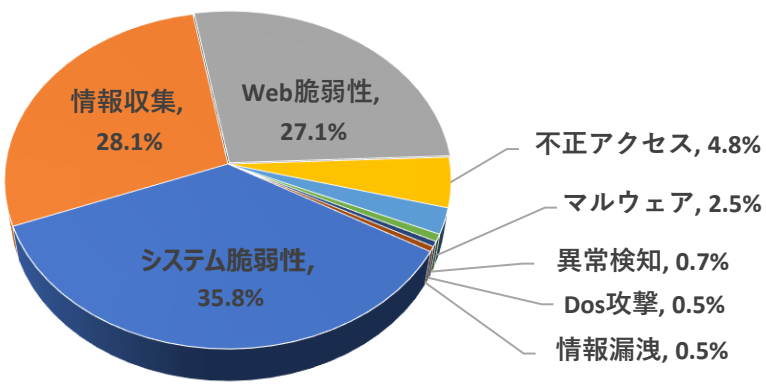
## 01. 月次攻撃類型

| パターン | 比率(%) | 比較 |
|---|---|---|
| システム脆弱性(System Vulnerability) | 35.8% | - |
| 情報収集(Information Gathering) | 28.1% | ▲1 |
| Web脆弱性(Web Vulnerability) | 27.1% | ▼1 |
| 不正アクセス(Unauthorized access) | 4.8% | - |
| マルウェア(Malware) | 2.5% | - |
| 異常検知(Anomaly Detection) | 0.7% | - |
| Dos攻撃(Denial of service attack) | 0.5% | ▲1 |
| 情報漏洩(Information Exposure) | 0.5% | ▼1 |

2021年10月の月次攻撃の類型を確認した結果、情報収集やWeb脆弱性を除き、攻撃の種類とランキングが前月とほぼ同様であることが確認できた。

情報収集は前年から着実に増加しており、Web脆弱性のランキングを追い越している。

また、Dos攻撃が前月より僅かに増加し、ランキング上昇したことも分かる。

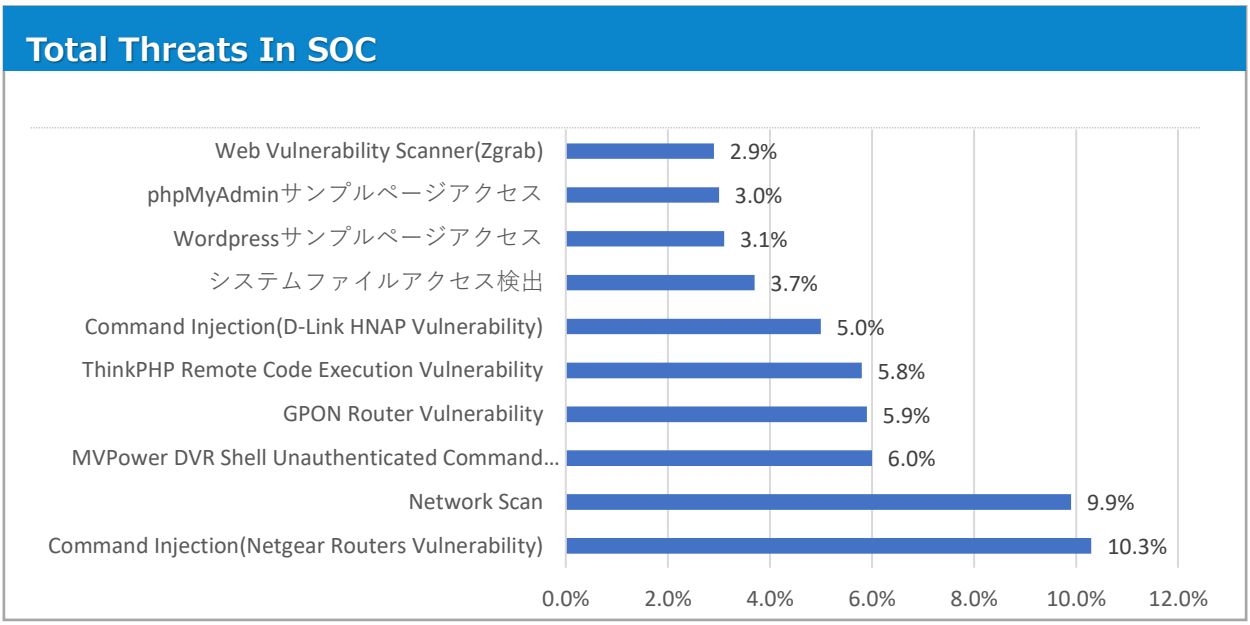


# 月次攻撃サービスの統計及び分析 - 2021年10月

## 02. 月次脆弱性攻撃TOP10

2021年10月の月次脆弱性TOP10を確認した結果、システムファイルアクセス検出が新たにトップ10入りし、前月から比べて攻撃数は1.5倍に増加しました。
Network Scan件数も前月から更に増加が続き、前月比約2倍の増加にて2位にランキングしています。

| 順位 | 検知名 | 比率(%) | 比較 |
|---|---|---|---|
| 1 | Command Injection (Netgear Routers Vulnerability) | 10.3% | - |
| 2 | Network Scan | 9.9% | ▲3 |
| 3 | MVPower DVR Shell Unauthenticated Command Execution | 6.0% | - |
| 4 | GPON Router Vulnerability | 5.9% | - |
| 5 | ThinkPHP Remote Code Execution Vulnerability | 5.8% | ▼3 |
| 6 | Command Injection (D-Link HNAP Vulnerability) | 5.0% | - |
| 7 | システムファイルアクセス検出 | 3.7% | NEW |
| 8 | Wordpressサンプルページアクセス | 3.1% | ▲2 |
| 9 | phpMyAdmin サンプルページアクセス | 3.0% | ▼2 |
| 10 | Web Vulnerability Scanner(Zgrab) | 2.9% | ▼1 |



# 月次攻撃サービスの統計及び分析 - 2021年09月

## 03. 月次ブラックリストIPアドレスTOP 10

2021年10月はアメリカ、イギリス、ロシアでの攻撃率が増加し、特にイギリスは前月から約3.7の大幅な増加が見られた。

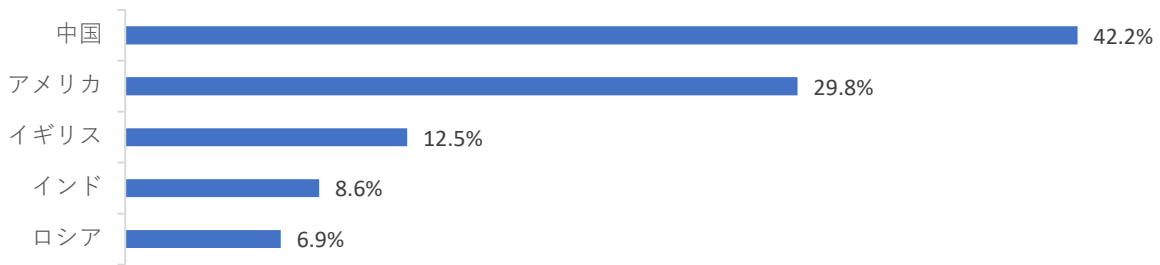
中国とインドの攻撃率については、わずかに低下が見られる。

下記の表を参考にしてファイウォールやセキュリティ機器からの遮断を推奨する。

| 順位 | ブックリストIP | 国 | 攻撃情報 |
|---|---|---|---|
| 1 | 45.146.164.110 | RU | Application Vulnerability(PHPUnit) |
| 2 | 217.112.83.246 | GB | Confluence Server Webwork OGNL injection (CVE-2021-26084) |
| 3 | 89.248.165.229 | GB | Network Scan |
| 4 | 91.132.58.33 | AU | Directory Traversal |
| 5 | 89.248.165.217 | GB | Network Scan |
| 6 | 89.248.165.219 | GB | Network Scan |
| 7 | 89.248.165.227 | GB | Network Scan |
| 8 | 89.248.165.162 | GB | Network Scan |
| 9 | 91.132.58.162 | AU | Fortinet FortiOS Directory Traversal (CVE-2018-13379) |
| 10 | 89.248.165.212 | GB | Network Scan |

## 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 | 45.146.164.110 | RU |
| 2 | 217.112.83.246 | GB |
| 3 | 89.248.165.229 | GB |
| 4 | 91.132.58.33 | AU |
| 5 | 89.248.165.217 | GB |

| Rank | Source IP | Country |
|---|---|---|
| 6 | 89.248.165.219 | GB |
| 7 | 89.248.165.227 | GB |
| 8 | 89.248.165.162 | GB |
| 9 | 91.132.58.162 | AU |
| 10 | 89.248.165.212 | GB |

# 攻撃パターン毎の詳細分析結果

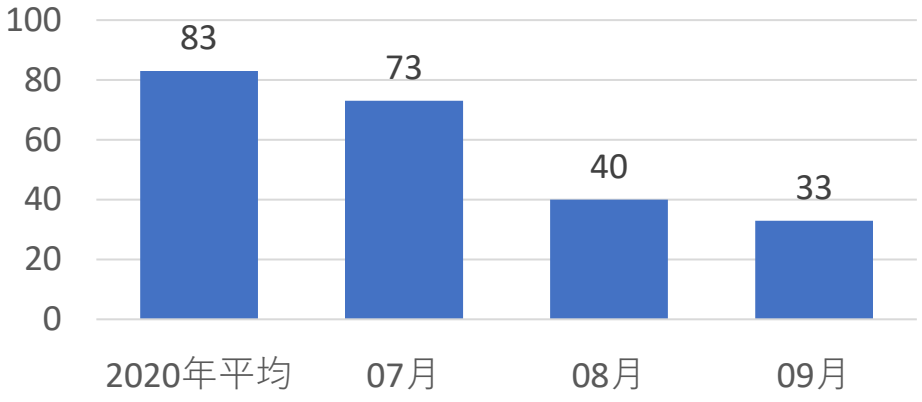
10月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

| 攻撃パターン | 詳細分析結果 |
|---|---|
| CommandInjection (Netgear Routers Vulnerability) | NetGear DGNシリーズのルータ内のウェブサーバが一部のURLに対して認証をせず、「setup.cgi」スクリプトの「syscmd」機能を活用して任意のコマンドを実行することができる。 |
| Network Scan | ネットワーク脆弱性スキャン攻撃はリモートからシステムのバグ、構成上の問題などハッキングできるセキュリティ脆弱性を確認するための攻撃であり、一番頻繁に発生する攻撃である。 |
| 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。 |
| GPON Router Vulnerability | Dasan GPON家庭用のルータから発見された脆弱性で「?images」の文字列を機器アクセス用URLに入力することで認証をスルー出来る脆弱性である。<br>当該の脆弱性を利用して認証されていない攻撃者が機器へリモートでコマンドを実行し、DNS設定修正などの様々な攻撃が可能である。 |
| ThinkPHP Remote Code Execution Vulnerability | ThinkPHP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。 |
| Command Injection (D-Link HNAP Vulnerability) | D-Link製品を設置する際に使用されるHNAP(Home Network Administration Protocol)に関するスクリプトに存在する脆弱性で認証を迂回してサービス中止、バックドアインストールなどのコマンドの実行が可能になる。<br>攻撃者は「Domain/HNAP1/GetDeviceSettings/」パスの後ろにコマンドを挿入し、「SOAPAction」フィールドを利用して実行を試みる。 |
| システムファイル アクセス検出 | Directory Traversalの脆弱性を利用し、「/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。 |
| 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。 |
| phpMyAdmin サンプルページ アクセス | phpMyAdminはウェブサーバーから MySQL を管理する目的で PHP で作成されているオープンソースツールで、この攻撃は My-SQL サーバを対象に脆弱性を探してデータベースの作成/削除、テーブルの作成/削除、フィールドの作成/削除、 SQL問い合わせ実行、実行権限管理機能などが実行できる脆弱性が存在している場合、phpMyAdminの「script/setup.php」ファイルに「?」因子を利用して任意の関数を挿入することでシステムコマンドが実行できる。 |
| Web Vulnerability Scanner(Zgrab) | Web Vulnerability Scanner(Zgrab)はウェブサーバの設定ページもしくは、許可メソッド、非認可ウェブページ、非許可ポートなど、脆弱なところの存在有無を確認するために使用する。 |

# 検知ポリシー

## ▶. 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーで、2021年09月の1か月間共有されたサイバー脅威検知ポリシーは33件である。
Atlassian Confluence(CVE-2021-26084)、MS Office(CVE-2021-40444)、
MS Windows(CVE-2021-36942)脆弱性に関する検知ポリシーが配布された。




3か月間件数

**5,239**
全体配布量

**33**
今月配布量

**40**
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 $HTTP_PORTS (msg:"IGRSS.1.05249 Atlassian Confluence, CVE-2021-26084, Attempted Administrator Privilege Gain"; flow:to_server,established; content:".action"; fast_pattern:only; http_uri; content:"u0027"; nocase; http_uri; pcre:"/[?&](featureKey\|token\|queryString\|linkCreation\|sourceTemplateId\|syncRev)=[^&]*?(¥x5C\|%(25)?5C)u0027/Ii"; sid:105249;) | Atlassian Confluence(CVE-2021-26084)<br>脆弱性から管理者特権での試行を<br>検知するポリシー | Atlassian<br>Confluence,<br>CVE-2021-26084 |
| alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.05257 MS, Office, CVE-2021-40444, Attempted User Privilege Gain"; flow:to_server,established; flowbits:isset,file.rtf; file_data; content:"\|7B 5C 2A 5C\|oleclsid"; fast_pattern:only; content:"\|5C\|objclass"; nocase; content:"\|5C\|objdata"; nocase; content:"d0cf11e"; nocase; sid:205257;) | MS Office(CVE-2021-40444)<br>MS OfficeのInternet Explorer利用に<br>関するMSHTML脆弱性でのユーザ権限<br>取り消し試行を検知するポリシー | MS, Office,<br>CVE-2021-40444 |
| alert tcp $EXTERNAL_NET any -> $HOME_NET [139,445] (msg:"IGRSS.2.05274 MS, Windows, CVE-2021-36942, Attempted User Privilege Gain"; flow:to_server,established; flowbits:isset,efsrpc; content:"\|FE\|SMB\|4000\|"; depth:6; offset:4; content:"\|09 00\|"; within:2; distance:6; byte_jump:2,52,relative,little,from_beginning,post_offset 4; content:"\|05 00 00\|"; within:3; content:"\|00 00\|"; within:2; distance:19; content:"\|5C 00 5C 00\|"; within:4; distance:12; fast_pattern; sid:205274;) | MS Windows(CVE-2021-36942)<br>Windows LSAの脆弱性を利用した<br>異常動作を検知するポリシー | MS, Windows,<br>CVE-2021-36942 |