

2022年12月  
攻撃統計情報

RISK

Threat

hacker



CyberFortress

# 月次攻撃サービスの統計及び分析 - 2022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。

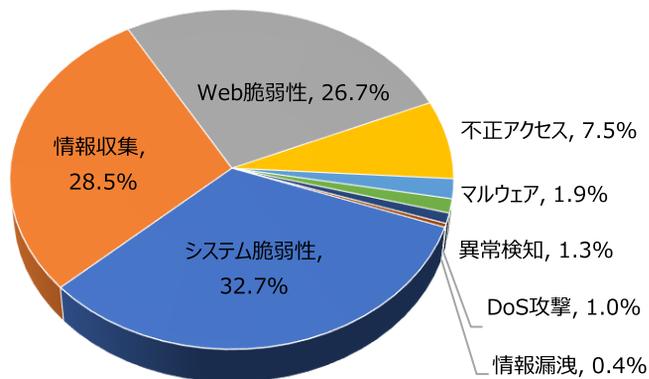
## 01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	32.7%	-
情報収集(Information Gathering)	28.5%	-
Web脆弱性(Web Vulnerability)	26.7%	-
不正アクセス(Unauthorized access)	7.5%	-
マルウェア(Malware)	1.9%	-
異常検知(Anomaly Detection)	1.3%	-
DoS攻撃(Denial of service attack)	1.0%	-
情報漏洩(Information Exposure)	0.4%	-

2022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0.75倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、システム脆弱性に関する攻撃は先月比べて約900件ほど減少し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数の減少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1,100件ぐらい減少し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数減少によるものだと確認できた。



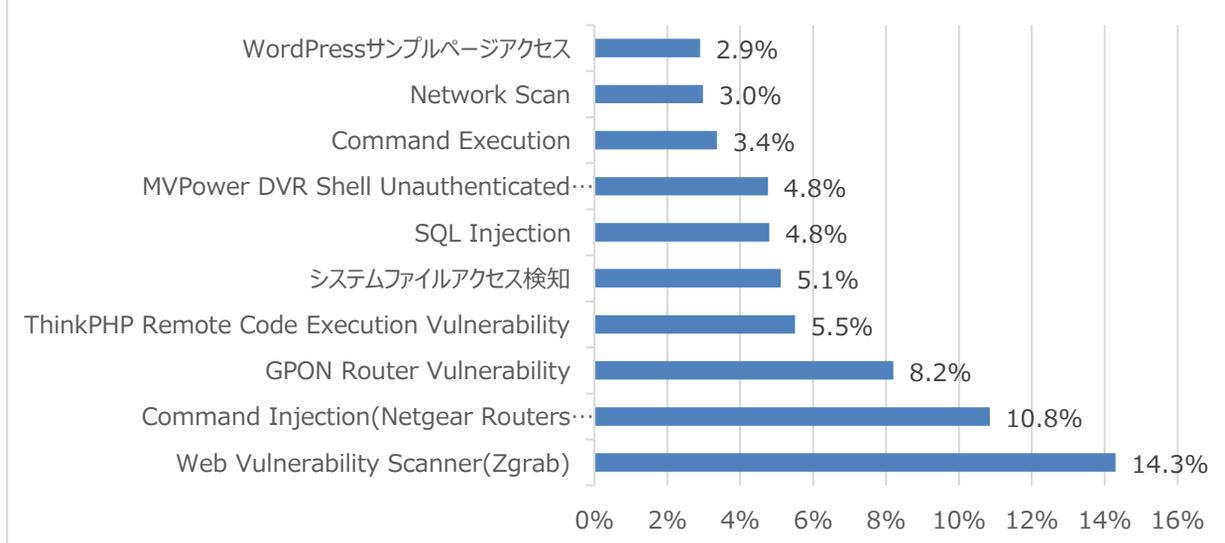
# 月次攻撃サービスの統計及び分析 - 2022年12月

## 02. 月次脆弱性攻撃TOP10

2022年12月の月次脆弱性TOP10を確認した結果、Command Execution, WordPressサンプルページアクセス攻撃が新たにTOP10に登場し、全体的な攻撃件数が減少したことが確認できた。特にWeb Vulnerability Scanner(Zgrab)攻撃が先月と比べて500件ぐらい大幅に減少した。

順位	検知名	比率(%)	比較
1	Web Vulnerability Scanner(Zgrab)	14.3%	-
2	Command Injection(Netgear Routers Vulnerability)	10.8%	▲1
3	GPON Router Vulnerability	8.2%	▲3
4	ThinkPHP Remote Code Execution Vulnerability	5.5%	▲3
5	システムファイルアクセス検知	5.1%	▼1
6	SQL Injection	4.8%	▲2
7	MVPower DVR Shell Unauthenticated Command Execution	4.8%	▼5
8	Command Execution	3.4%	NEW
9	Network Scan	3.0%	▲1
10	WordPressサンプルページアクセス	2.9%	NEW

### Total Threats In SOC



# 月次攻撃サービスの統計及び分析 - 2022年12月

## 03. 月次ブラックリストIPアドレスTOP 10

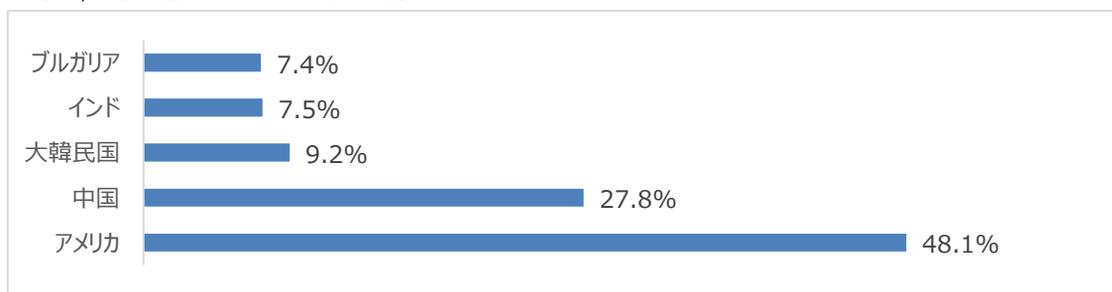
2022年12月についてTOP10を確認した結果、大韓民国とブルガリアの攻撃比率が増加し、一方アメリカと中国、インドの攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約50%で、半分ぐらい占めていることが確認できた。

※ 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	ブラックリストIP	国	攻撃情報
1	152.89.196.23	GB	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
2	152.89.196.211	GB	Application Vulnerability(PHPUnit)
3	185.7.214.218	RU	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
4	204.48.24.100	US	Apache Log4j RCE(CVE-2021-44228)
5	49.143.32.6	KR	GPON Router Vulnerability
6	193.142.146.35	DE	Command Injection(D-Link HNAP Vulnerability)
7	82.99.217.202	IR	Apache Log4j RCE(CVE-2021-44228)
8	123.157.222.168	CN	phpMyAdminサンプルページアクセス
9	195.178.120.33	US	Netgear Command Injection(CVE-2016-6277)
10	45.134.144.203	US	SIP Vulnerability Scanner(Sipvicious)

## 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	185.7.214.218	RU	6	14.36.39.167	KR
2	85.31.44.178	US	7	18.163.206.128	HK
3	85.31.44.156	US	8	193.47.61.99	US
4	193.47.61.60	US	9	176.65.137.5	DE
5	109.237.97.180	GB	10	59.3.64.13	KR

# 攻撃パターン毎の詳細分析結果

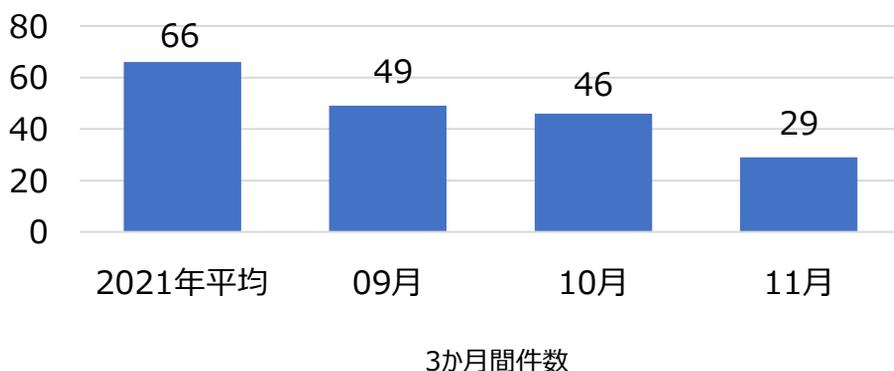
12月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。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。この脆弱性は家庭用ルータにて発見された。
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。
システムファイル アクセス検出	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。
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。
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。
Command Execution	適切な認証が行われていないユーザーの入力値がOSコマンドの一部、もしくはその他のコマンドで構成され実行される場合、意図しないシステムコマンドが実行され、不正に権限が変更されたり、システム動作及び運用に悪影響を及ぼす可能性がある。一般的なコマンドラインのパラメータやストリーム入力など、外部入力を使用しシステムコマンドを生成するプログラムはたくさん存在するが、この場合、外部の入力文字列は信頼できないため、適切な処理（チェック処理）をしないと攻撃者が望むコマンドが実行可能になる。
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行われる攻撃である。
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。

# 検知ポリシー

## ▶ 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーにて、2022年11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29件である。11月1か月の間、OpenSSL(CVE-2022-3602, CVE-2022-3786), WordPress(WordPress Plugin)(CVE-2022-2840), GLPI htmlawed(CVE-2022-35914)などに対する検知ポリシーが配布された。



**6,014**  
全体配布量

**29**  
今月配布量

**46**  
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 -> any any (msg:"IGRSS.2.06022 OpenSSL, CVE-2022-3602, Attempted User Privilege Gain"; flow:established; content:" 06 03 55 1D 1E 01 "; content:" 04 82 "; within:2; distance:1; content:" 30 82 "; within:2; distance:2; content:" 82 "; within:1; distance:3; content:" 30 82 "; within:2; distance:2; content:" 81 82 "; within:2; distance:2; byte_test:2,>,500,0,relative; content:"xn--"; within:4; distance:2; fast_pattern; sid:206022;)	OpenSSLのCVE-2022-3602脆弱性を悪用したパッファオーバーフロー攻撃を検知するポリシー	OpenSSL, CVE-2022-3602
alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"IGRSS.10.06027 GLPI, htmlawed, CVE-2022-35914, Web Application Attack"; flow:to_server,established; content:"/vendor/htmlawed/htmlawed/htmlawedTest.php"; fast_pattern:only; http_uri; content:"hhook"; nocase; http_uri; sid:1006027;)	GLPI htmlawedのCVE-2022-35914脆弱性を悪用したリモートコード実行攻撃を検知するポリシー	GLPI, htmlawed, CVE-2022-35914
alert tcp any any -> any any (msg:"IGRSS.2.06028 OpenSSL, CVE-2022-3602, CVE-2022-3786, Attempted User Privilege Gain"; flow:established; content:" 06 03 55 1D 1E "; content:" 04 82 "; within:5; content:" 30 82 "; within:2; distance:2; content:" 82 "; within:1; distance:3; content:" 30 82 "; within:2; distance:2; content:" 81 82 "; within:2; distance:2; byte_test:2,>,500,0,relative; content:"xn--"; within:4; distance:2; fast_pattern; sid:206028;)	OpenSSLの(CVE-2022-3602, CVE-2022-3786)脆弱性を悪用した攻撃を検知するポリシー	OpenSSL, CVE-2022-3602, CVE-2022-3786
alert tcp \$EXTERNAL_NET any -> \$HOME_NET \$HTTP_PORTS (msg:"IGRSS.10.06044 WordPress, Zephyr Project Manager Plugin, CVE-2022-2840, Web Application Attack"; flow:to_server,established; content:"/wp-admin/admin-ajax.php"; fast_pattern:only; http_uri; content:"zpm_view_project"; nocase; http_client_body; pcre:"/^(^ &)(project(?:%5f (25)?f)id)=[^&]*?([%x27]*x22*x3b*x23*x28 )%{(2-5)?(27 22 3b 23 28)}(?:%x2f (25)?f)(%x2a (25)?2a) (%x2d (25)?2d){2}"/; im"; sid:1006044;)	WordPress Zephyr Project Managerの CVE-2022-2840脆弱性を悪用したSQL Injection攻撃を検知するポリシー	WordPress, Zephyr Project Manager Plugin, CVE-2022-2840