SECURITY REPORT

2025

DEC

2025年12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11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。

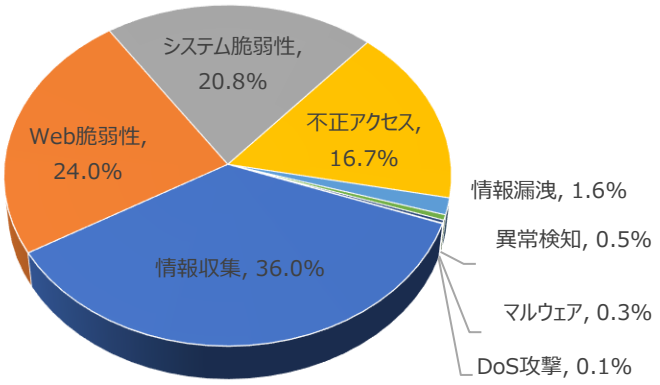
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	36.0%	-
Web脆弱性(Web Vulnerability)	24.0%	▲1
システム脆弱性(System Vulnerability)	20.8%	▲1
不正アクセス(Unauthorized access)	16.7%	▼2
情報漏洩(Information Exposure)	1.6%	-
異常検知(Anomaly Detection)	0.5%	-
マルウェア(Malware)	0.3%	-
DoS攻撃(Denial of service attack)	0.1%	-

2025年11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1.06倍ぐらい増加した。

そのうち、情報収集に関する攻撃は先月比べて約1,302件ほど減少し、これはNetwork Scan、ポートスキャン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1,907件ぐらい増加し、これは、이는 Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)のような攻撃件数増加によるものだと確認できた。

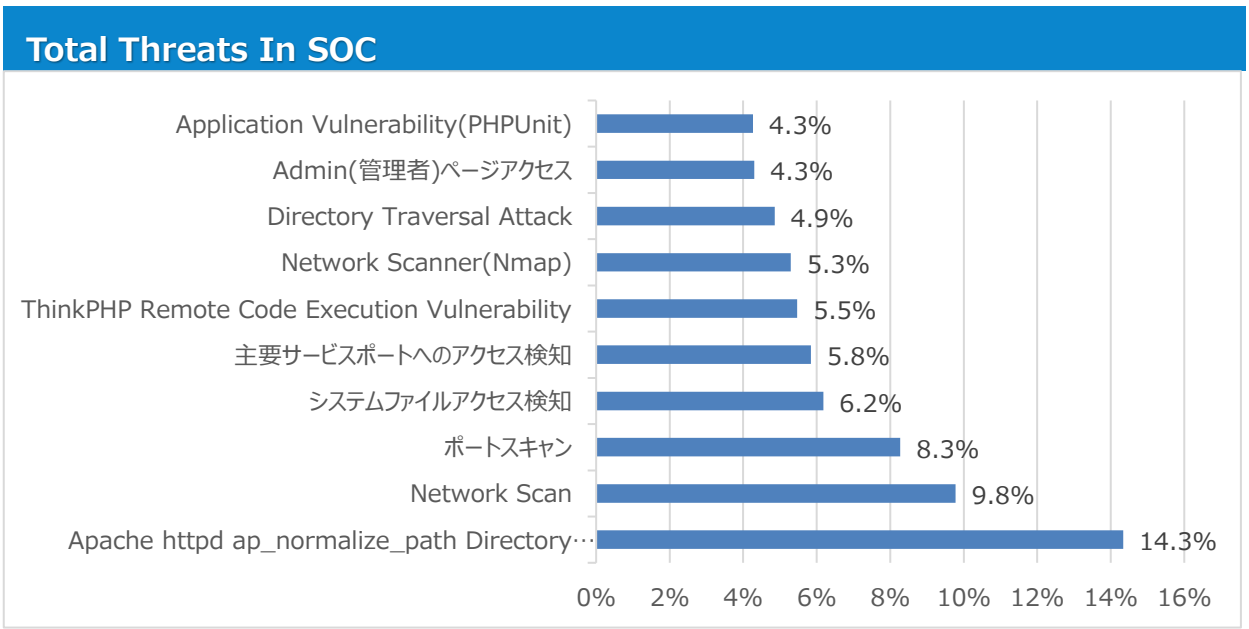


月次攻撃サービスの統計及び分析 - 2025年11月

02. 月次脆弱性攻撃TOP10

2025年11月の月次脆弱性TOP10を確認した結果、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。Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)のような攻撃件数が先月と比べて約1,907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	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	14.3%	▲4
2	Network Scan	9.8%	▼1
3	ポートスキャン	8.3%	▼1
4	システムファイルアクセス検知	6.2%	-
5	主要サービスポートへのアクセス検知	5.8%	▼2
6	ThinkPHP Remote Code Execution Vulnerability	5.5%	NEW
7	Network Scanner(Nmap)	5.3%	▼1
8	Directory Traversal Attack	4.9%	NEW
9	Admin(管理者)ページアクセス	4.3%	▼2
10	Application Vulnerability(PHPUnit)	4.3%	NEW



月次攻撃サービスの統計及び分析 - 2025年11月

03. 月次ブラックリストIPアドレスTOP 10

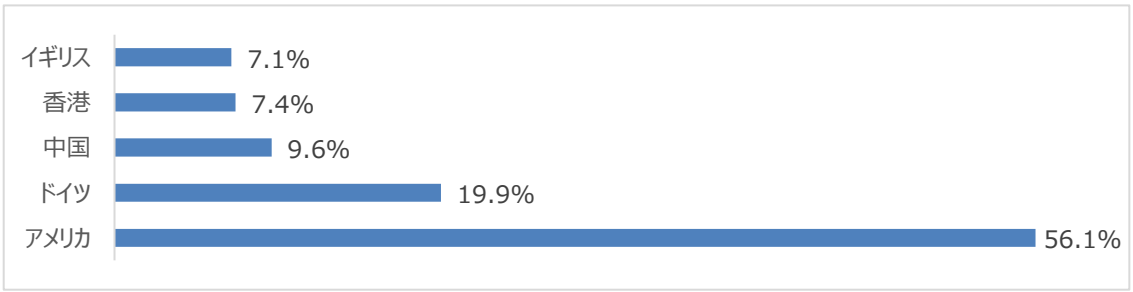
2025年11月についてTOP10を確認した結果、アメリカとドイツの攻撃比率が減少し、特にアメリカの攻撃比率が約56.1%を超えていることが確認できた。

※ 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	62.84.181.65	FR	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
2	128.14.227.179	TW	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
3	192.159.99.95	NL	Remote Code Execution Vulnerability
4	141.255.164.26	CH	Directory Traversal Attack
5	130.185.118.124	FR	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
6	178.18.251.197	FR	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
7	101.36.108.167	HK	Directory Traversal Attack
8	120.233.128.103	CN	ThinkPHP Remote Code Execution Vulnerability
9	91.232.238.112	UA	Network Scanner(masscan)
10	61.245.11.87	PH	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)

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	62.84.181.65	FR	6	178.18.251.197	FR
2	128.14.227.179	TW	7	101.36.108.167	HK
3	192.159.99.95	NL	8	120.233.128.103	CN
4	141.255.164.26	CH	9	91.232.238.112	UA
5	130.185.118.124	FR	10	61.245.11.87	PH

攻撃パターン毎の詳細分析結果

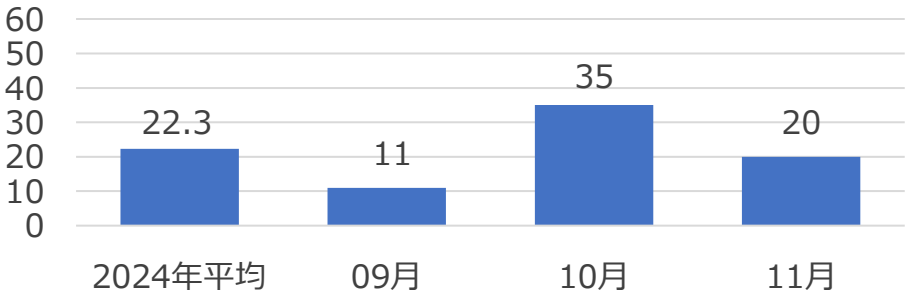
11月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
ポートスキャン	主要ポートへのアクセスを試みしてからアクセス情報を奪取するためのBrute Force攻撃が行われ、アカウント情報が一致した場合、ウェブ改ざんや情報窃取などの被害が発生する可能性がある。アカウント情報の定期的な変更、文字・数字・特殊文字を組み合わせたパスワードの使用、外部からの全サービスポートへのアクセスポリシーの禁止、指定管理者IPからのみ特定サービスポートへのアクセスポリシーの使用などを推奨する。
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。
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。
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。
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。
Directory Traversal Attack	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できる。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。
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。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2025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20件である。
11月1か月の間、Citrix (CVE-2025-12101)、GitLab (CVE-2025-25291)、Samsungデバイス (CVE-2025-21042)脆弱性とLandfallマルウェアなどに対する検知ポリシーが配布された。



3か月間件数

月間配布件数

検知ポリシー	説明	タグ
alert tcp any any -> any any (msg:"IGRSO.10.06874 server-webapp_Citrix_Netscaler_cve-2025-12101_Web Application Attack"; flow:established,to_server; content:"POST"; content:"/cgi/logout"; fast_pattern; content:"RelayState|3d|"; pcre:"/(?:(?:¥x0d|¥x250[dD])(?:¥x0a|¥x250[aA])){2}.*?(?:on(?:(?:s(?:elec|ubmi)|rese)t|d(?:blclick|ragdrop)|(?:mouse|key)[a-z]+|c(?:hange|lick)|(?:un)?load|focus|blur|error)|s(?:cript|tyle¥x3d))/";)	Citrix Netscalerの脆弱性であるCVE-2025-12101を悪用したXSS攻撃を検知するポリシー	server-webapp,Citrix,Netscaler,cve-2025-12101
alert tcp any any -> any any (msg:"IGRSO.10.06875 server-webapp_GitLab_cve-2025-25291_Web Application Attack"; flow:established,to_server; content:"/users/auth/saml/callback"; fast_pattern; content:"SAMLResponse|3d|"; content:"|3c 21|DOCTYPE|20|"; content:"|3e 3c 21 2d 2d|"; distance:0; content:"|3c 21|ENTITY|20|"; distance:0;)	GitLabの脆弱性であるCVE-2025-25291を悪用した認証バイパス試みを検知するポリシー	server-webapp,GitLab,cve-2025-25291
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"IGRSS.8.06880 malware-cnc_Trojan_Landfall_Samsung_mobile_A Network Trojan was detected"; flow:to_server,established; content:"type=MSG_TYPE_GET_AGENT"; fast_pattern:only; content:"protocol="; nocase; content:"agent_id="; nocase; content:"command_id="; nocase; content:"bh_path="; nocase; content:"runner="; nocase; sid:806880;)	Samsungモバイルファームウェアの脆弱性であるCVE-2025-21042を悪用してインストールされるLandfallマルウェアのネットワーク通信を検知するポリシー	malware-cnc,Trojan,Landfall,Samsung,mobile