SECURITY REPORT

2025

NOV

2025年11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。

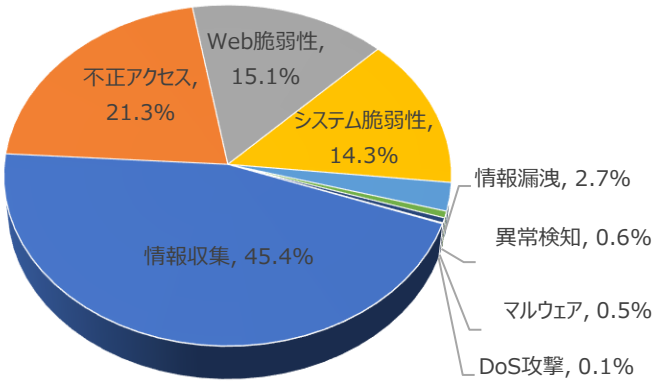
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	45.4%	-
不正アクセス(Unauthorized access)	21.3%	-
Web脆弱性(Web Vulnerability)	15.1%	-
システム脆弱性(System Vulnerability)	14.3%	-
情報漏洩(Information Exposure)	2.7%	-
異常検知(Anomaly Detection)	0.6%	▲1
マルウェア(Malware)	0.5%	▼1
DoS攻撃(Denial of service attack)	0.1%	-

2025年10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0.7倍ぐらい減少した。

そのうち、不正アクセスに関する攻撃は先月比べて約2,929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、不正アクセスに関する攻撃は先月と比べて約2,468件ぐらい増加し、これは、主要サービスポートアクセス試み攻撃件数減少によるものだと確認できた。



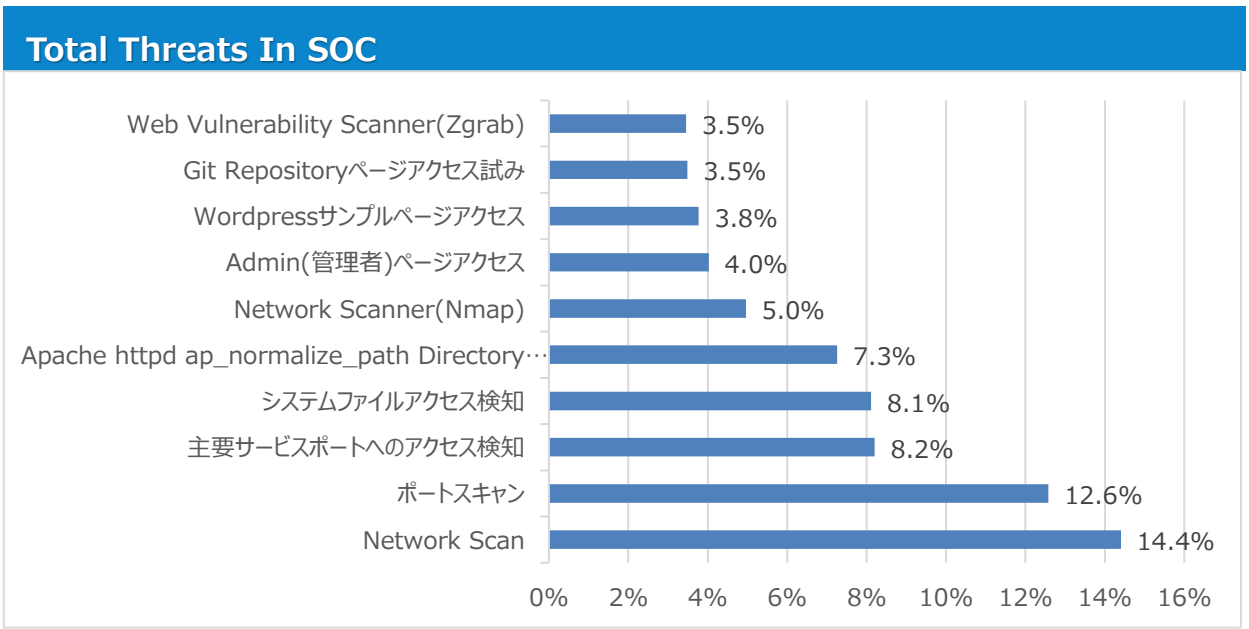
Copyright © Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2025年10月

02. 月次脆弱性攻撃TOP10

2025年10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減少した。Network Scan、ポートスキャンのような情報収集、不正アクセスの攻撃件数が先月と比べて約5,397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	Network Scan	14.4%	▲5
2	ポートスキャン	12.6%	▲3
3	主要サービスポートへのアクセス検知	8.2%	-
4	システムファイルアクセス検知	8.1%	NEW
5	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	7.3%	▼1
6	Network Scanner(Nmap)	5.0%	NEW
7	Admin(管理者)ページアクセス	4.0%	-
8	Wordpressサンプルページアクセス	3.8%	NEW
9	Git Repositoryページアクセス試み	3.5%	▼8
10	Web Vulnerability Scanner(Zgrab)	3.5%	▼1



Copyright © Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2025年10月

03. 月次ブラックリストIPアドレスTOP 10

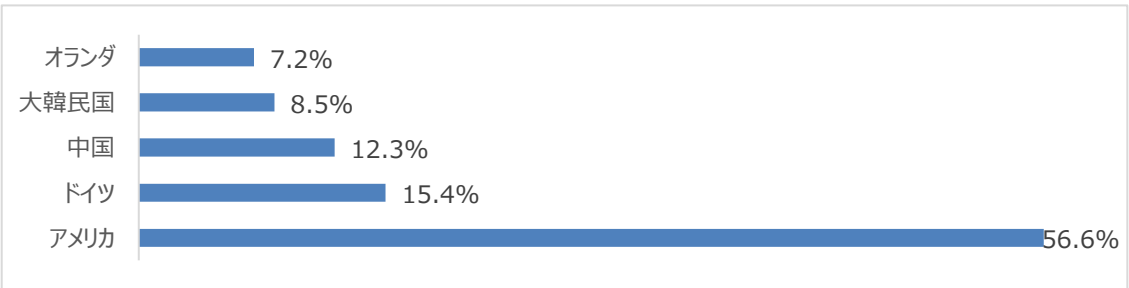
2025年10月についてTOP10を確認した結果、アメリカとドイツの攻撃比率が減少し、特にアメリカの攻撃比率が約56.6%を超えていることが確認できた。

※ 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	139.162.119.196	JP	Network Scanner(Nmap)
2	34.59.175.189	US	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
3	172.232.232.10	ID	ポートスキャン
4	20.249.104.159	US	phpinfoページ漏洩
5	139.162.119.146	JP	ポートスキャン
6	4.230.144.132	KR	phpinfoページ漏洩
7	192.210.160.141	NL	Application Vulnerability(PHPUnit)
8	172.236.137.159	US	ポートスキャン
9	139.162.3.144	SG	Network Scanner(Nmap)
10	124.198.131.83	US	GPON Router Vulnerability

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	139.162.119.196	JP
2	34.59.175.189	US
3	172.232.232.10	ID
4	20.249.104.159	US
5	139.162.119.146	JP

Rank	Source IP	Country
6	4.230.144.132	KR
7	192.210.160.141	NL
8	172.236.137.159	US
9	139.162.3.144	SG
10	124.198.131.83	US

Copyright © Cyberfortress, Inc. 2020. All rights reserved

攻撃パターン毎の詳細分析結果

10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。

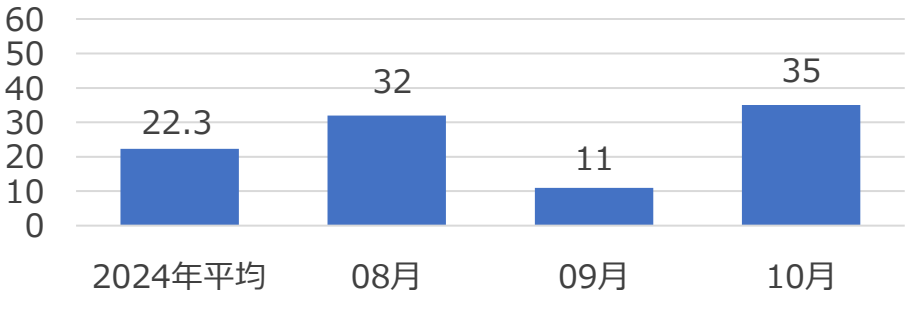
攻撃パターン	詳細分析結果
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行われる攻撃である。
ポートスキャン	主要ポートへのアクセスを試みしてからアクセス情報を奪取するためのBrute Force攻撃が行われ、アカウント情報が一致した場合、ウェブ改ざんや情報窃取などの被害が発生する可能性がある。アカウント情報の定期的な変更、文字・数字・特殊文字を組み合わせたパスワードの使用、外部からの全サービスポートへのアクセスポリシーの禁止、指定管理者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。
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。
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。
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 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。
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。
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。
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。
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。

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10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35件である。
10月1か月の間、 Microsoft(CVE-2025-59287), Redis(CVE-2025-49844)などに対する検知ポリシーが配布された。



3か月間件数

6,829
全体配布量

35
今月配布量

11
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 -> $HOME_NET [8530,8531] (msg:"IGRSS.1.06848 os-windows_microsoft_WindowsServer_WSUS_cve-2025-59287_Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/ReportingWebService/ReportingWebService.asmx"; fast_pattern:only; http_uri; content:"<ReportingEvent"; nocase; http_client_body; content:"SynchronizationUpdateErrorsKey"; nocase; http_client_body; content:"m_serializedClaims"; nocase; http_client_body; sid:106848;)	Microsoft Windows Server Update Serviceの脆弱性であるCVE-2025-59287を悪用した逆直列化攻撃を検知するポリシー	os-windows,microsoft,WindowsServer,WSUS,cve-2025-59287
alert tcp $EXTERNAL_NET any -> $HOME_NET 6379 (msg:"IGRSS.2.06851 server-other_redis_cve-2025-49844_Attempted User Privilege Gain"; flow:to_server,established; content:"$4|0D 0A|EVAL|0D 0A|"; nocase; content:"string.rep("; distance:0; fast_pattern; nocase; content:"string.rep("; distance:0; nocase; content:"string.rep("; distance:0; nocase; content:"string.rep("; distance:0; nocase; pcre:"/^((?:(?!¥r¥n).)*?¥bstring¥x2erep¥x28){10}/ims"; sid:206851;)	Redisの脆弱性であるCVE-2025-49844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	server-other,redis,cve-2025-49844
alert tcp any any -> any any (msg:"IGRSO.10.06867 server-webapp_Microsoft_Windows_CVE-2025-59287_Web Application Attack"; flow:established,to_server; content:"/ReportingWebService/ReportingWebService.asmx"; fast_pattern; content:"/SoftwareDistribution/ReportEventBatch"; content:"MiscData"; content:"Administrator|3d|"; content:"SynchronizationUpdateErrorsKey";)	Microsoft Windows Server Update Services (WSUS)の脆弱性であるCVE-2025-59287を悪用した逆直列化攻撃を検知するポリシー	server-webapp,Microsoft,Windows,CVE-2025-59287

Copyright © Cyberfortress, Inc. 2020. All rights reserved