

2021 年 2 月 25 日
株式会社ネットアシスト

ネットアシスト、さくらインターネットと提携し、 「攻撃遮断くん（サーバセキュリティタイプ）」の提供を開始

2021 年 2 月 25 日より「さくらのクラウド」にて提供

<https://www.netassist.ne.jp/news/?p=1#1614141937-597022>

MSP サービス（サーバやネットワークの運用・監視・保守）を提供する【株式会社ネットアシスト】（本社：東京都豊島区、代表取締役：伊藤 誠史）は、インターネットインフラサービスを提供する【さくらインターネット株式会社】（本社：大阪府大阪市、代表取締役社長：田中 邦裕）と提携し、株式会社サイバーセキュリティクラウドが開発する「攻撃遮断くん」のサーバセキュリティタイプを、さくらインターネットの IaaS 型クラウド「さくらのクラウド」においてマーケットプレイス※1 商材として 2021 年 2 月 25 日より提供を開始します。

※1 マーケットプレイスとは、さくらインターネット社が他社と協業し、他社の技術を用いて商材を提供する取り組みを指す。

■サイバー攻撃の規模、脅威が 10 年間で 44 倍

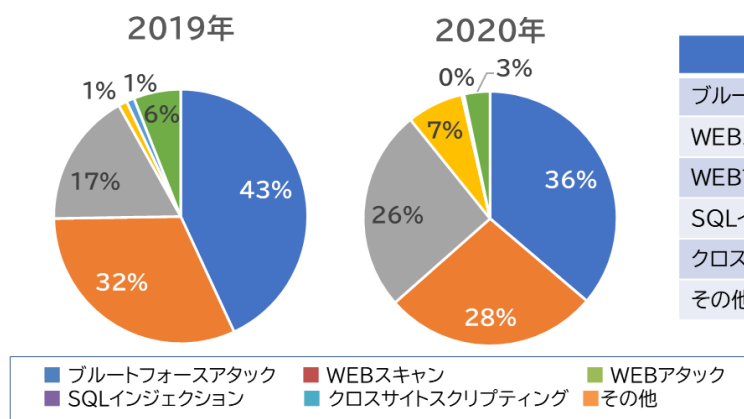
新型コロナへの対応として、テレワークの普及拡大や社会全体のデジタル・トランスフォーメーション（DX）が進みつつある中、サイバー攻撃も増加しています。国立研究開発法人情報通信研究機構の NICTER 観測レポート※2 のダークネット観測※3 によると、ある 1 IP に向けられたサイバー攻撃関連の通信量（パケット）は 2011 年からの 10 年間で 44 倍になりました。これはサイバー攻撃の規模、脅威が 10 年間で 44 倍になったということを意味しています。

※2 出典元「NICTER 観測レポート 2020」<http://www.nict.go.jp/cyber/report.html>

※3 ダークネット観測とはインターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを収集する手法。

下表は当社提供のセキュリティサービス（WAF※4）で実際にブロックしたサイバー攻撃の種別です。

■WEBサービスに対するサイバー攻撃種別（2019年と2020年）



	2019年	2020年
ブルートフォースアタック	43.0%	36.2%
WEBスキャン	31.6%	27.3%
WEBアタック	17.1%	25.7%
SQLインジェクション	1.1%	7.2%
クロスサイトスクリプティング	1.0%	0.3%
その他	6.0%	3.3%

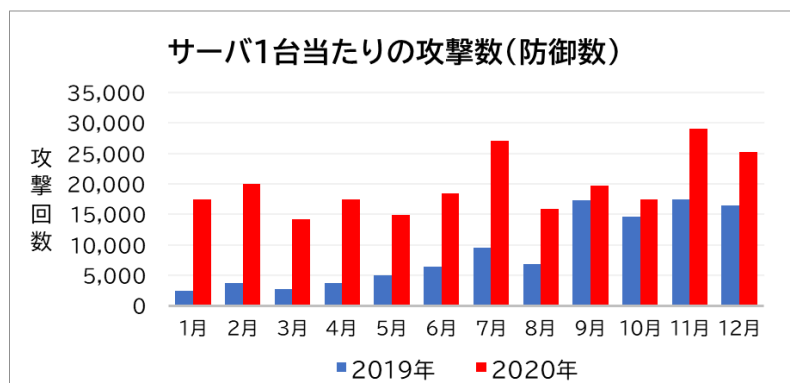
※ネットアシスト社提供のWAFでブロックしたサイバー攻撃の種別

※4 WAFとは「Web Application Firewall」の略称で、Webアプリケーションの脆弱性を突いた攻撃からWebサイトを守るためのセキュリティ対策を指す。

1位のブルートフォース攻撃は「総当たり攻撃」とも呼ばれ、管理画面などのログインページに対してパスワード入力を順に入力し続ける攻撃です。2位のWEBスキャンはアクセス制限が行われていないポートを見つけるための攻撃前に調べるチェックで、この結果セキュリティ対策が甘いとみられたサーバはサイバー攻撃の対象となる可能性が高まります。

下グラフは同じく当社のWAFで実際にブロックした攻撃回数の平均（サーバ1台あたり）です。企業の知名度や事業規模を問わずインターネットに公開されている全てのサーバが同様の攻撃を受けています。セキュリティソリューション未導入のサーバではこれらの攻撃を受け続ける事になり、脆弱性やパスワード設定に不備があった場合、不正侵入を許す可能性があります。

■サーバ1台当たりの攻撃件数の比較(2019年と2020年)



実際にネットアシストで観測した攻撃回数
(サーバ1台あたり)

	2019年	2020年
年間合計	106,482回	208,313回
月間最大	17,289回	28,993回
月間平均	8,873回	19,749回

2020年ではサーバ1台あたり、1年間で約21万回のサイバー攻撃を受けています。

これらサイバー攻撃に対して適切なセキュリティに対応していない場合には不正侵入を許す恐れがあり、様々な脆弱性を狙った多角的な攻撃に対して最適なセキュリティ対策が必要とされています。

■幅広い領域でWEBサーバやWEBサイトを保護する「攻撃遮断くん」

攻撃遮断くん

年々増加するサイバーセキュリティの脅威に対して、お客さまの大切な情報を預かるサーバセキュリティは、高いレベルが要求されるようになりました。「攻撃遮断くん」はウェブサイト・ウェブサーバへのサイバー攻撃を可視化・遮断するウェブセキュリティサービスです。今回提供するサーバセキュリティタイプは、クラウド上の監視センターにログを送信するためのエージェントをお客さまサーバへインストールし、送信されたログをもとに攻撃の検知・遮断命令を出します。

多くの企業のサーバを運用・保守・管理するネットアシストでは、さくらインターネットと提携し、さくらのクラウドにて「攻撃遮断くん」の提供を開始します。

■ 攻撃遮断くん（サーバセキュリティタイプ）について

<特徴>

クラウド上の監視センターにログを送信するためのエージェントをお客さまサーバへインストールし、送信されたログをもとに攻撃の検知・遮断命令を出します。

攻撃の検知・遮断の最中でも、WAF※5 導入によるサーバ性能の低下やサイトを訪れるユーザーへのレスポンス低下といった心配がありません。トラフィック容量の大きなコンテンツを提供しているウェブサービスを運営している方に特におすすめです。クラウド型のため、保守・運用に手間を掛ける事なく、24 時間 365 日の高セキュリティを実現しています。

※5 WAF とは Web Application Firewall の略称で、Web アプリケーションの脆弱性を突いた攻撃から Web サイトを守るためのセキュリティ対策を指す。

・サーバ単位で保護

サーバ OS 単位でエージェントをインストールすることでクラウド上の監視センターにログが送信されるようになり、攻撃の検知・遮断が可能になりサーバを保護します。DNS 切り替え型とは異なり、トラフィックによる従量課金を気にする必要が無いため、様々なサービスとの組み合わせが容易になります※6。

※6 ロードバランサー等の中間機器にエージェントをインストールしてご利用になる場合にはこの限りではありません。

・管理画面の提供

利用開始後、クラウドアカウントごとに管理画面を提供いたします。管理画面では、グラフィカルなマップとデータで攻撃状況を可視化します。攻撃元 IP アドレスや攻撃種別の確認、検知状況などの確認を、お客さま側で素早く行うことが可能です。

・初期費用無料

さくらのクラウドで提供する「攻撃遮断くん（サーバセキュリティタイプ）」は初期費用が発生いたしません。

<月額料金>

サービスプラン	単位	月額料金
サーバセキュリティタイプ	1 台/1 IP アドレス	¥ 44,000（税込）

※ 掲載プラン以外をご検討の場合は、以下記載のリクエストフォームからのお問い合わせとなります。

リクエストフォーム URL : https://www.sakura.ad.jp/request_form/service/cloud/

<提供開始日>

2021 年 2 月 25 日 (木)

<https://cloud.sakura.ad.jp/specification/security/#shadan-kun>

■さくらのクラウドについて

さくらのクラウドは、さくらインターネット株式会社が提供するサーバやストレージなどの多彩なサービスが利用できる IaaS 型クラウドです。インターネットサービスのインフラ基盤としてはもちろん、大規模法人・公的機関向け業務システムなど、幅広い業種に導入実績があります。時間割料金・日割料金・月額料金を設定しており、利用期間に応じて最安の価格が適用され、コストパフォーマンスに優れています。詳細は以下ウェブサイトをご覧ください。

さくらのクラウド サービスサイト

<https://cloud.sakura.ad.jp/>

■会社概要

株式会社ネットアシスト

<https://www.netassist.ne.jp/>

東京都豊島区南池袋 3-13-5 池袋サザンプレイス 7F

代表取締役 伊藤 誠史

■本件に関するお問い合わせ先

株式会社ネットアシスト

担当：浅井

TEL：03-3985-6780

MAIL：sales@netassist.ne.jp

※記載されている会社名、製品名は、各社の商標、もしくは登録商標です。

◆新型コロナウイルス感染症に関するリモートワーク実施について

2021 年 1 月 7 日に発令された日本政府の緊急事態宣言を受けまして当社では 2021 年 1 月 12 日より、一部スタッフを除き原則リモートワークを実施しております。

サービスのお問い合わせやメディアさまの取材等は電話やビデオ会議とさせていただきます。ご理解いただけますよう、よろしくお願い申し上げます。

PRESS RELEASE

