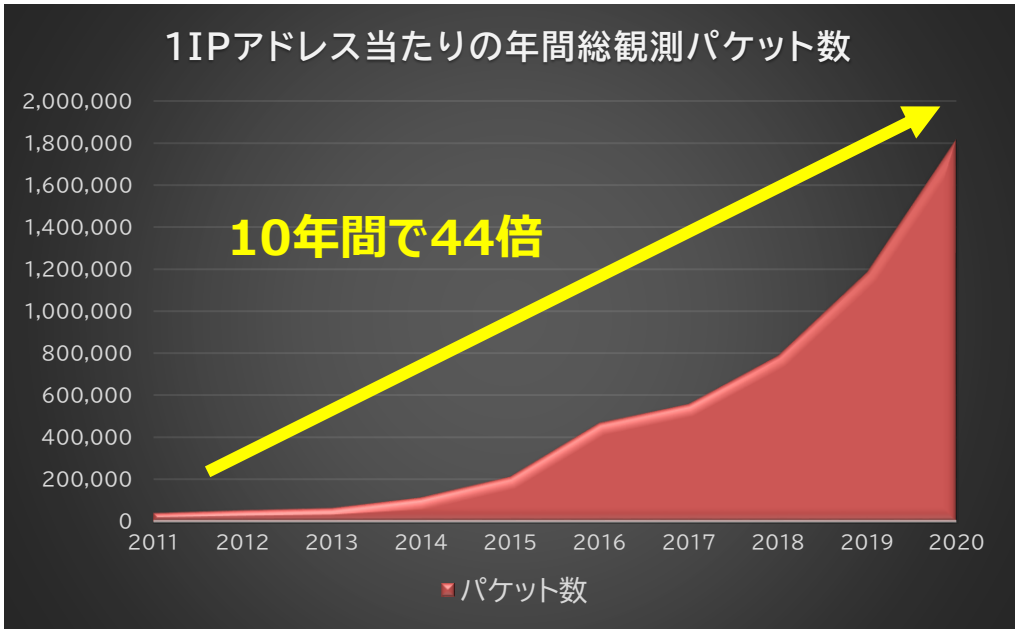
Confidencal

NET ASSIST
24/7 Guardian Deity

# サイバー攻撃の現状
# と
# セキュリティ対策の必要性

Confidencal

# 通信量でみるサイバー攻撃の脅威の増加




ある１IP* 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年間で約**44倍**になりました。

これは**サイバー攻撃の規模、脅威**が10年前の**44倍**になったということを意味しています。

企業の知名度や事業規模に関わらず、**全てのサーバは サイバー攻撃の脅威にさらされています**。

*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です。

未使用のIPアドレスであるため本来はパケットが観測されないはずですが、実際にはサイバー攻撃に関連する探索活動(スキャン)や送信元IPアドレスを詐称したDDoS攻撃の跳ね返り(バックスキャッタ)等が多く観測されます。
このパケットを分析することにより, インターネット上で発生しているサイバー攻撃の兆候や傾向等を把握することができます。

| 年 | 2011年 | 2012年 | 2013年 | 2014年 | 2015年 | 2016年 | 2017年 | 2018年 | 2019年 | 2020年 |
|---|---|---|---|---|---|---|---|---|---|---|
| パケット数 | 40,654 | 53,085 | 63,655 | 115,323 | 213,523 | 469,104 | 559,125 | 789,876 | 1,187,935 | 1,820,722 |

※出典：情報通信研究機構（ＮＩＣＴ） ＮＩＣＴＥＲ 観測レポート ２０２０

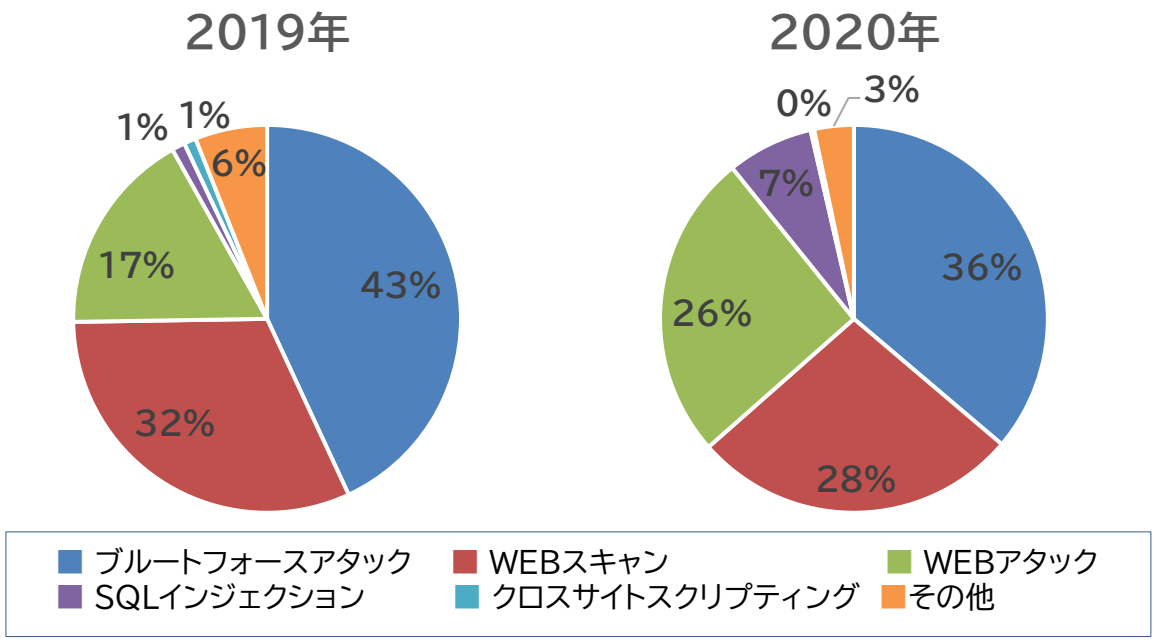
この表はNICTERのダークネット観測網(約30万IPアドレス)において2020年に観測されたサイバー攻撃関連通信の1IPアドレス当たりの年間総観測パケット数をグラフ化したものです。

企業の知名度や事業規模は問わず、サイバー攻撃の脅威は10年前の**44倍。**
IoT機器やリモートワークの普及などにより、サイバー攻撃は**今後も増加し続ける**ことが予想されています。

# WEBサービスに対するサイバー攻撃種別【2019年・2020年】

Confidencal

弊社提供のセキュリティサービス（WAF）で実際にブロックしたサイバー攻撃の種別を取りまとめたグラフです。




| | 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% |

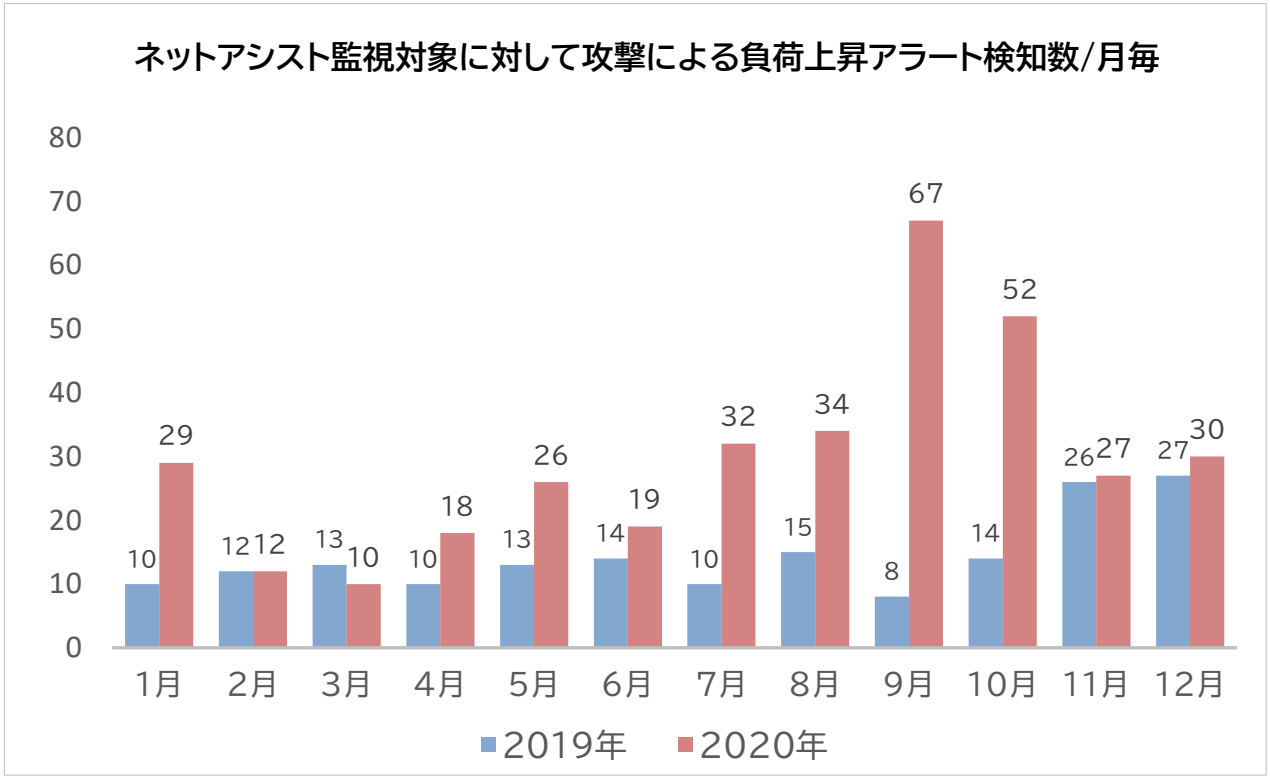
1位のブルートフォースアタックは「総当たり攻撃」とも呼ばれ、管理画面などのログインページに対してパスワード入力を順に入力し続ける攻撃です。
2位のWEBスキャンは攻撃を行う前の調査です。FWによってアクセス制限が行われていないポートを見つけるために行われ、この結果セキュリティ対策が甘いとみられたサーバーはサイバー攻撃の対象となる可能性が高まります。
割合は多くないもののSQLインジェクション、クロスサイトスクリプティングといった攻撃も続いており、様々な脆弱性を狙った多角的な攻撃がサーバに向けられていることが分かります。このようなサイバー攻撃に対して**適切なセキュリティサービスを導入していない場合には不正侵入を許す恐れがあります。**

様々な脆弱性を狙った**多角的なサイバー攻撃**に対して**最適なセキュリティ対策**の実施が必要とされています。

Confidencal

# 攻撃によるサーバーの異常検知数【2019年・2020年】

2019年・2020年の1年間で、弊社監視対象（約2000台）に対してサイバー攻撃が原因と思われる異常を検知した件数です。
高負荷やサイトの表示遅延など異常をきたすほどの攻撃は、サーバー監視で検知が可能ですが、負荷が上がらない程度の攻撃については、サーバー監視で検知できません。
**「障害を検知しない＝攻撃を受けていない」**という事ではなく、**公開サーバーは常に攻撃を受け続けている**事を認識する必要があります。




**2020年1年間で**
**サイバー攻撃による異常を検知した回数**

**356回　／4.1億＊**

＊サーバー1台当たりの年間攻撃観測数（208,313回）
× 監視対象（2000台）

※上記はネットアシストの監視環境における観測結果です。

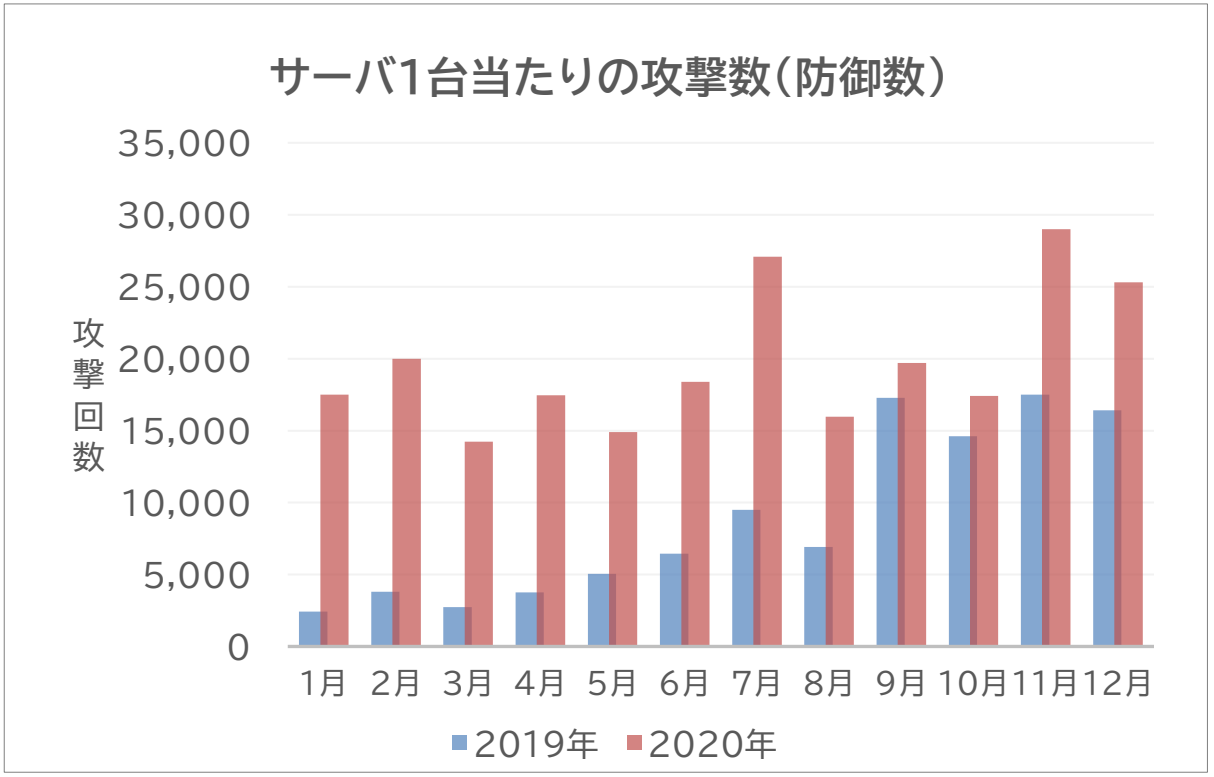
サーバーへ負荷がかかるサイバー攻撃は攻撃全体の割合からみるとごく僅かです。
**「稼働やリソース状況が安定している＝サイバー攻撃を受けていない」**ということではありません。

Confidencal

# サーバ 1台当たりの攻撃件数の比較【2019年・2020年】

下記のグラフは弊社提供のセキュリティサービス（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**全てのサーバーが同様の攻撃**を受けています。

セキュリティソリューション導入済のサーバーであればブロックを行いますが、**未導入のサーバー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。




**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）**

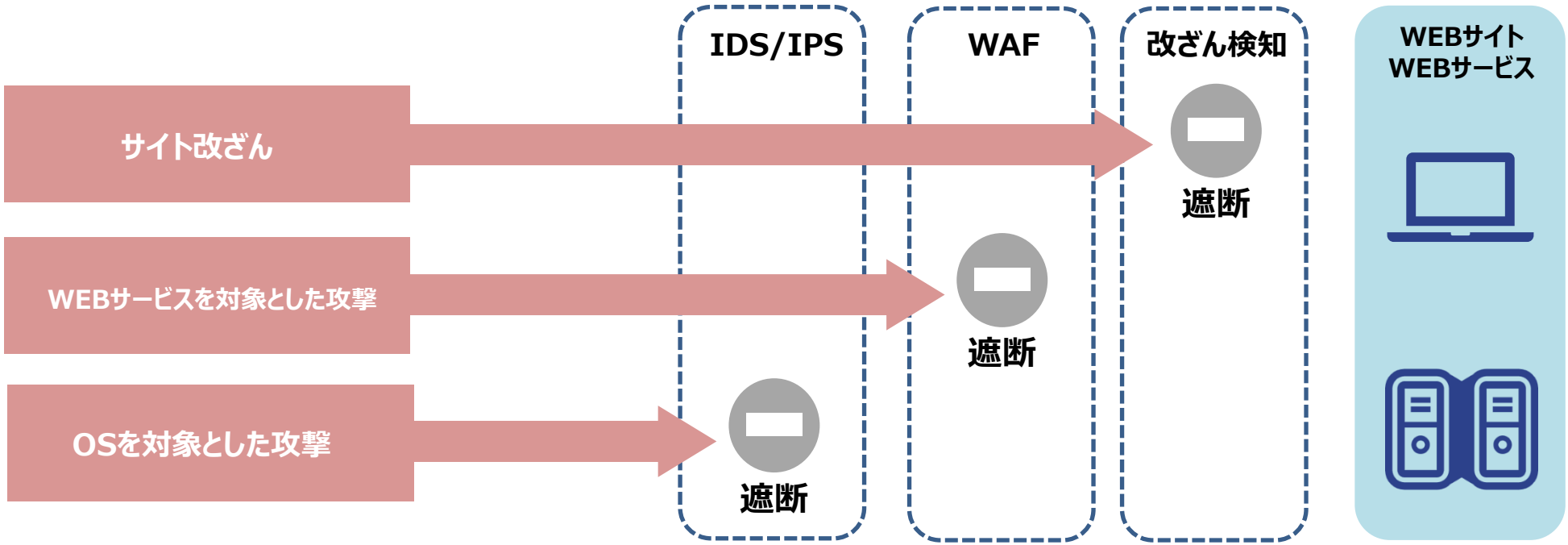
| | 2019年 | 2020年 |
|---|---|---|
| 年間合計 | 106,482回 | 208,313回 |
| 月間最大 | 17,289回 | 28,993回 |
| 月間平均 | 8,873回 | 19,749回 |

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。

サイバー攻撃は年々増加傾向にあり、弊社の調査環境では前年比約2倍となります。
IOT機器やリモートワークの普及によるオンライン化、国際的なイベントの開催など、今後も増加し続けることが予想されています。

Confidencal

## サイバー攻撃に対しての有効な対策とは




※上記全ての攻撃が各セキュリティサービスで防げるわけではありませんので予めご了承ください

**1つのセキュリティソリューションで全てのサイバー攻撃に対応することはできません。**

OSを対象とした攻撃には【 IDS/IPS 】、WEBサービスを対象とした攻撃には【WAF】、サイトの改ざんには【改ざん検知】の導入が必要となります。全てのソリューションを導入するには多大なコストが発生してしまいセキュリティ対策実現のハードルが高くなります。

そのため、まずは運用している自社のサーバーにておいて **1番リスクの高い箇所の対策をする**事をお勧めします。

Confidencal

# WAF
# (Web Application Firewall)


# WAF 攻撃遮断くんの特徴

Confidencal

攻撃遮断くん

国内導入社数・導入サイト数
クラウド型WAF No.1

※出典:「クラウド型WAFサービス」に関する市場調査(2019年6月16日現在)<ESP総研調べ>(2019年5月～2019年6月調査)

## サーバセキュリティタイプ　2大ポイント

**簡単！手放し運用** … シグネチャが自動更新の為、専任のセキュリティエンジニアが不要。

**安心！定額利用** … ドメイン数やネットワーク量に関わらず、固定料金での利用が可能。

## その他のおすすめポイント

- 導入時にサーバーの停止が不要
- リアルタイム攻撃情報、攻撃種別、攻撃元IP、攻撃元国、期間ごとの攻撃グラフが確認できる管理画面
- 日付別、時間帯別、攻撃種別ログ、攻撃種別割合、攻撃元ランキング等、 攻撃状況を一目で把握できる月次レポート

**対応可能な主要なサイバー攻撃**

ブルートフォースアタック / SQLインジェクション / クロスサイトスクリプティング
ディレクトリトラバーサル / OSコマンドインジェクション / 改行コードインジェクション
LDAPインジェクション / ファイルインクルード / URLエンコード攻撃 / その他のWeb攻撃

# 主要なサイバー攻撃について

Confidencal

## 攻撃遮断くん(WAF)で対応可能な主要なサイバー攻撃概要

| | |
|---|---|
| ブルートフォースアタック | 「総当たり攻撃」とも呼ばれ、暗号解読方法のひとつであり、可能な組み合わせを全て試す攻撃手法です。<br>手軽に実行できるツールが普及しており、時間的制約がない限りは確実にパスワードを割り出して侵入することが可能です。 |
| SQLインジェクション | 攻撃者がWEBサイトのフォーム等に不正な内容を盛り込んだSQL文を入力し検索を行うことで、本来は隠されているはずのデータへのアクセスを可能にする攻撃手法です。 |
| クロスサイトスクリプティング | 脆弱性のある掲示板やSNSに投稿された【スクリプトが埋め込まれたリンク】をクリックする事により、攻撃者が作った不正なスクリプトを、<br>被害者のWebブラウザーで実行、閲覧者に情報を送信させる攻撃手法です。 |
| ディレクトリトラバーサル | 本来ユーザーのアクセスを意図していないファイルやディレクトリの場所を相対パスの指名などで場所を特定し、不正なアクセスをする攻撃手法です。 |
| OSコマンドインジェクション | ユーザーがデータ入力可能なWEBサイトで、本来アプリケーションに対して送るパラメータ情報の中に不正なOSコマンドを紛れ込ませて操作する攻撃手法です。 |
| 改行コードインジェクション | 「HTTPヘッダインジェクション」とも呼ばれ、ヘッダ内に改行コードを入れることで、本来製作者側が意図していない文字列を生成し、不正にアクセスをする攻撃手法です。 |
| LDAPインジェクション | SQLインジェクションやOSコマンドインジェクション　と同様に、LDAP（Lightweight Directory Access Protocol）と呼ばれる通信プロトコルに対して不正なコマンドを送り込む攻撃手法です。 |
| ファイルインクルード | ディレクトリトラバーサルと似た攻撃手法ですが、この攻撃はアプリケーションが使用するスクリプト言語の「include系関数」を利用して不正にアクセスを行います。 |
| URLエンコード攻撃 | URLの一部の文字を「%」を使ってエンコード（変換）をすることで、本来はアクセスできないはずのページ（ログイン後のユーザー情報など）にアクセスが可能になります。 |

これらのサイバー攻撃によって不正アクセスを許してしまった場合、個人情報を含むデータの流出や漏洩、サイトの改ざんやウィルス感染などの被害が予想されます。
サイバー攻撃の被害状況・原因・対策の実施など一連の対応が完了するまでの期間、**運営サイト/サービスの停止**を余儀なくされます。

また、サイバー攻撃の際に流失した個人情報を悪用されたてしまったり、他社のサーバへの攻撃の踏み台として自社サーバが乗っ取られ、迷惑メール配信など第3者のサイト/サービスへ影響をあたえてしまった場合には、サイバー攻撃の被害者としてだけではなく、今度は**加害者として「損害賠償請求」をされる可能性**があります。

# さくらのクラウドについて

Confidencal



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/

■ マーケットプレイス：攻撃遮断くん（サーバセキュリティタイプ）
https://cloud.sakura.ad.jp/specification/security/#shadan-kun
※ 2021年2月25日（木）から提供開始

Confidencal

# 本件に関するお問合せ、導入のご相談は下記まで

株式会社ネットアシスト　浅井

TEL:03-3985-6780

MAIL:sales@netassist.ne.jp

NET ASSIST
24/7 Guardian Deity