

NEWS LETTER

2022.11

#19



TOPICS

TOPICS : #01 さくらインターネット石狩データセンター見学レポート!

TOPICS : #02 WAFサービス「攻撃遮断くん サーバセキュリティタイプ」
便利な機能を追加してリニューアルされました!

TOPICS : #03  12月14日📅
Web負荷テストに関するセミナーを開催!

さくらインターネット 石狩データセンター 見学レポート！



10月6日にさくらインターネットさんに招待いただき、石狩データセンターの見学をしてきました。データセンターはセキュリティの点から、なかなか見学ができない施設ですが、今回は特別にお時間をいただいたので、紹介したいと思います！当日はデータセンター見学前に講義形式で、石狩データセンターの特徴や機能などについて説明いただきました。実際にデータセンター内を歩いて、設備の説明をしていただきました。

石狩データセンターとは？

石狩データセンターは、クラウドコンピューティングに最適化された日本最大級の郊外型大規模データセンターです。北海道の冷涼な外気を活用した外気冷房によるエネルギー効率の向上、建物から設備にいたるまでの徹底したモジュール設計による柔軟性、東京ドームの約1.1倍という広大な敷地、などの特徴があります。1～3号棟で約3000ラックの対応が可能です。また、最終的には5号棟までに約6800ラックまで増設する予定とのことです。

1号棟/2号棟/3号棟と進むにつれ、配電設備が変わり、サーバー搬入がスムーズにできるよう搬入口が改良されるなど様々な箇所での進化を遂げていました。需要動向に応じた拡張を実施し、その時々最新の技術を採用しているとのことです。



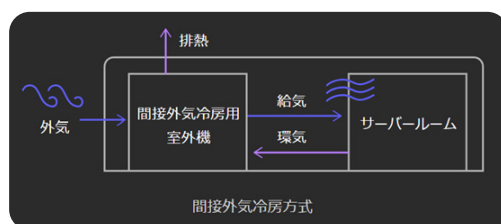
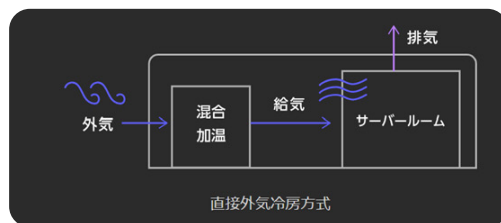
提供元: さくらインターネット株式会社

環境に配慮したデータセンター

北海道の冷涼な外気を冷房に活用し、空調にかかる消費電力の大幅削減を実現しています。1・2号棟では直接外気を取り込む「直接外気冷房方式」を、3号棟では室外機と空調機の間を循環する冷媒を外気で冷やしてサーバールームを冷却する「間接外気冷房方式」を導入しています。実際にそれぞれの設備を見学することができました。「間接外気冷房方式」は外気を室内に取り込まないため湿度変動が少なく、除湿器・加湿器、加湿のための給水などにかかるランニングコストをさらに削減するとのこと。

石狩データセンターでは、高電圧直流(HVDC)給電システムが一部の環境で稼働していて、交流・直流交換の回数を減らすことができ、設備投資の削減と給電効率の改善を同時に実現しています。

この直流給電をより活用するため、「石狩太陽光発電所」を建設していて、データセンターの敷地内に大量の太陽光パネルが設置されているのを見ることができました。発電から給電、消費までの一連の流れを自社でまかなっているとのことです。



※外気モデルの図(提供元: さくらインターネット株式会社)

北国ならではの意外な工夫

冷涼な外気を空調に使えるほどの石狩データセンターですが、逆に冬場の対策として面白い工夫があったので紹介したいと思います。冬場はトラックで搬入したサーバーにそのまま電源を入れると結露して故障してしまうため、サーバーを一旦室内で温めるための、通称「サーバー解凍部屋」が用意されています。サーバーを冷やすことはよく聞きますが、「サーバーを温める」というのはこの業界に入って初めて聞いたので、とても驚きました！

さくらインターネットさんが石狩を選んだ理由

地震・津波・液状化リスクが低い安全なロケーション

① 地震リスク

データセンター所在地の配下に活断層は無く、大規模地震による影響を受けにくい地域

② 津波リスク

津波予測結果は海岸線および港湾の一部に限定され、陸上での最高到達点4.7mという数値に対し建設地の地盤高は5.5m以上となっているため、リスクはほとんどない

③ 液状化リスク

地盤の簡易検査による液状化リスクは低く、仮に発生した場合も、石狩データセンターは低層構造で、建物重量も比較的軽いいため、深刻な沈下は回避できる。

寒冷地立地による消費電力の低減

全国的に比較しても石狩は年間の平均気温が低いため、空調にかかる消費電力を削減することに成功しています。

石狩：平均気温



※年間平均気温グラフ（提供元：さくらインターネット株式会社）

交通アクセス

石狩は新千歳空港や札幌市街からもアクセスが良く、札幌駅からは車で30～40分程度



セキュリティ対策

監視カメラによる24時間365日の監視だけでなく、建物ゲート、有人チェック、ICカード、生体認証による4重のセキュリティで、サーバールームへの入退室管理を行っているとのこと。実際にサーバーに触れるためには7つ以上のセキュリティチェックが必要です。



提供元：さくらインターネット株式会社

オフィス内も様々な工夫



さくらインターネットの皆様 ありがとうございました！

なかなか見ることができないデータセンターを紹介いただき、大変勉強になりました！新しい技術を取り入れながら拡大していく石狩データセンターに今後も注目していきたいです。



おまけ

データセンター見学後は、
さくらインターネットさんと札幌の夜を満喫！



WAFサービス「攻撃遮断くん サーバセキュリティタイプ」 便利な機能を追加してリニューアルされました！

ネットアシストでは、サーバー監視・運用管理代行サービス「MSPアシスト」だけでなく、各種セキュリティサービスの取扱いがあり、WAF(Web Application Firewall)は多くのお客様にご利用いただいております。中でも「攻撃遮断くん」は、弊社がサイバーセキュリティクラウド社の販売代理店として、お客様へご提案・ご提供をしております。今回は、「攻撃遮断くん」の「サーバセキュリティタイプ」がリニューアルされるという事で、その内容についてご紹介していきます。ぜひ導入をご検討される際の参考にしていただければと思います！

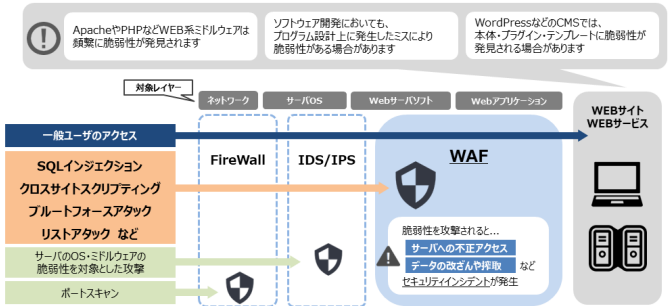
攻撃遮断くんとは？

[サービス詳細はこちら](#)

攻撃遮断くんは、サイバー攻撃による情報漏えいやWebサイト改ざんなどからWebサイトを守る国産型クラウドWAFです。

日本国内シェアNo.1を誇り、導入サイト数は15,000サイト以上の信頼の導入実績があります。

サイバーセキュリティクラウド社が、開発・運用・サポートを一貫して日本国内の自社で対応しているところも安心なポイントです。

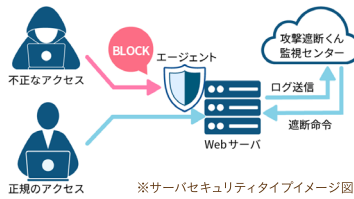


サービスラインアップ

リニューアル

サーバセキュリティタイプ

お客様のサーバーに攻撃遮断くんのエージェントをインストールするタイプです。アクセス情報を監視センターに送信、内容を判断し、必要な場合は遮断命令を返します。



Webセキュリティタイプ

DNSを切り替えるタイプです。お客様のサーバーの前にWAFセンターを設置し、アクセス内容を判定します。不正なアクセスをWAFセンターで遮断します。

DDoSセキュリティタイプ

Webセキュリティタイプの防御性能に加えて、DDoS攻撃もWAFセンターで遮断します。

あんな機能やこんな機能も! ?リニューアル内容

※2022年11月現在までのリニューアル内容となります。

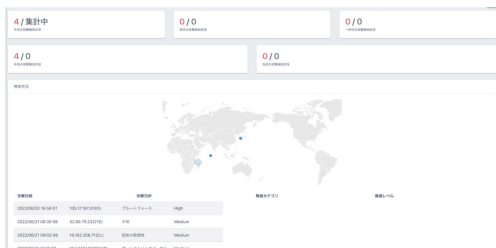
サーバセキュリティタイプのリニューアル内容をまとめてご紹介します。ポイントは「より見やすく、より詳細に、よりカスタマイズの効く」サービスを実現！

設定反映

Before ダッシュボードで攻撃状況が可視化されています。

After 攻撃状況の把握・解説がより明瞭になります！画面に取まりやすいダッシュボードに改修され、攻撃状況を簡易的に可視化できるようになります。さらに攻撃状況を多角的に把握し、詳細について確認できる分析ボードが新たに登場します。

ダッシュボード



分析ボード



攻撃ログ

Before 攻撃対象・攻撃元・攻撃種別から攻撃状況を確認することができ、検知履歴をCSVでダウンロードすることが可能です。

After 多彩な追跡機能が追加され、より詳細なログ確認ができるようになります！攻撃対象のログデータ・ファイルパス、攻撃内容の説明が表示され、検知理由の詳細確認が可能になります。

Beforeの検知履歴に加えて、日時・アクション・ルールなどから攻撃状況を確認・条件検索をすることも可能になります。引き続き、検知履歴をCSVでダウンロードすることができ、カラムに国情報が追加されます。



設定反映

Before これまでも管理画面から設定変更は可能でしたが、設定の反映は定時システム処理（翌営業日の10:00）で、緊急の設定反映が必要な場合は、サポートへの問合せが必要です。

After ユーザーによる設定反映コントロールが出来るようになります！ユーザー操作で設定だけでなく、反映（適用）ができるため、ユーザーのタイミングでの設定反映（適用）が可能になります。



ルールアクション

Before アクションはエージェント単位で「検知」「遮断」の2種類から選択が可能です。

After 多彩なルールアクションを管理画面でコントロールできるように改修されました！管理画面からルール単位でアクションを変更できるようになり、アクションが「検知」「遮断」に加えて「OFF」が選択できるようになります。



ルールカスタマイズ

Before ルールのカスタマイズや攻撃の詳細確認はサポートへの問合せが必要です。

After ユーザー完結型のカスタマイズ機能が実装されます！管理画面でルールカスタマイズが可能になります。攻撃の脅威レベルが3段階「破壊行為（High）」「情報窃取（Middle）」「調査行為（Low）」に分類され、カスタマイズの内容を判断できるようになります。

攻撃の目的	攻撃の例	ランク(小)	攻撃の例	
破壊行為	Injection code excution XXE	12	code excution	High
		11	Injection, XXE	
情報窃取	Injection XSS Traversal	10	Injection, XSS	Middle
		9	Traversal	
調査行為	scan BadUserAgent	8	scan, BadUserAgent	Low
		7	BadUserAgent (SEO tool)	

ルール説明

Before ルール説明は検知後に英語で簡易説明があり、攻撃分類は7種類です。

After より分かりやすい説明と攻撃への対策を補助してくれる機能が追加されました！ルールの詳細説明を事前に日本語で確認できるようになり、攻撃種別14種類以上に細分化できるようになります。

現在	リニューアル
Webスキャン	<ul style="list-style-type: none"> Webスキャン Blacklisted User Agent
Webアタック	<ul style="list-style-type: none"> 固有の脆弱性 サードパーティドメインロードインジェクション (SSI) LDAPインジェクション HTTPヘッディングジェクション XMLエクスターナルエンティティ (XXE) サードパーティドメインクロスサイトフォージェリ (SSRF) デジリライゼーション攻撃
クロスサイトスクリプティング (XSS)	<ul style="list-style-type: none"> クロスサイトスクリプティング (XSS)
SQLインジェクション	<ul style="list-style-type: none"> SQLインジェクション NoSQLインジェクション
OSコマンドインジェクション	<ul style="list-style-type: none"> OSコマンドインジェクション
トラバーサル	<ul style="list-style-type: none"> トラバーサル
ブルートフォースアタック	<ul style="list-style-type: none"> なし
その他	<ul style="list-style-type: none"> その他、ossecオリジナルのssh認証/メール系認証など

※ブルートフォースアタックへのルールは今後準備が整い次第提供されます

以上が今回のリニューアルでポイントとなる項目です。リリース後のアップデートで順次提供される予定の機能もありますので、順次提供されましたらまたご紹介いたします！

リニューアル版のご提供とスケジュール

リニューアル版につきましては、11月1日にリリースされております。今回は先行して、そのリニューアルの内容をまとめました。今後お客様にご提供するにあたって、弊社でも検証を進めていく予定で、順次リニューアル版のご提供を開始して参ります。

弊社からの具体的なご提供開始時期につきましては、改めてご連絡させていただければと思います。現行版とリニューアル版で約1年間の並行稼働期間が設けられる予定です。

現行版からリニューアル版への移行

すでに現行版をご利用いただいているお客様は、今後リニューアル版への移行が必要になります。具体的なスケジュールや移行の方法に関しましては、サイバーセキュリティクラウド社にて現在調整中です。

弊社でも確認が出来次第追ってご連絡いたしますので、お手数ですが、今しばらくお待ちくださいませ。

現行版のEOLは約1年後を予定しているとの事で、左記の並行稼働期間内のご案内になる見込みです。

まとめ

今回は、WAFサービス「攻撃遮断くん サーバセキュリティタイプ」のリニューアルについてご紹介いたしました。前述しました通り、攻撃遮断くんは弊社で取扱いのあるサービスです。ライセンス提供のみも可能ですが、導入からサポートオプション（※1）までご用意しておりますので、安心してお任せください！

「MSPアシスト×攻撃遮断くん」で、サーバー・Webサイトを安定的かつ安全に運用をしましょう。お客様の環境に合わせてご提案が可能ですので、お気軽にご相談ください！

（※1）：お問合せ代行・遮断内容の調査と緩和・動作モード（検知/遮断）切替え・ホワイトリスト登録

Web負荷テストに関するセミナーを開催！

この度、WEBサイトやECサイト、システムなどを運用されている企業様を対象に『【実演 解説付き】Web負荷テストでサーバーのキャパシティを探る』と題してセミナーを開催いたします。過不足のない最適なインフラ設計を行うためには、Webコンテンツやアプリケーションのパフォーマンスを測定し、システム負荷に起因する不具合を発見するWeb負荷テストの実施が重要です。

今回はセミナー前半でWeb負荷テストの基本部分を解説し、後半にはネットアシストの開発エンジニアがシナリオの設定からテストの実行などデモ画面を交えて解説いたします。質問タイムも設けておりますので、ご興味のある方はぜひご参加ください！

【オンラインセミナー】株式会社ネットアシスト

インフラ担当者必見！

【実演 解説付き】 Web負荷テストでサーバーの キャパシティを探る

2022年12月14日水 14:00～

参加費：無料 開催場所：zoom

セミナー内容

- 負荷テストとは？概要とその目的 負荷テストの種類、ツール
- 負荷テストの実演、解説 ネットアシスト負荷テストサービスのご紹介
- 質問タイム

日程

2022 12月14日水

14:00~15:00

セミナー内容

- Web負荷テストとは？概要とその目的
- Web負荷テストの種類、ネットアシスト使用ツールのご紹介
- Web負荷テストの実演、解説
- ネットアシストWeb負荷テストサービスのご紹介
- 質問タイム

費用

無料

開催場所

Zoom

詳細の確認・お申込みはこちら！ >

※セミナーの内容は一部変更になる場合がございます。

お問い合わせはこちらまで！

 **NET ASSIST** 株式会社ネットアシスト
24/7 Guardian Deity

TEL 03-3985-6780 Mail sales@netassist.ne.jp

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

