Protect

zcrWAF

Webアプリケーションファイアウォール

zcrWAFは、タイで開発されたWebアプリケーションファイアウォールです。WebサイトとAPIの通信を本番サーバーへ到達する前に検査し、OWASP Top 10攻撃やボットを遮断します。

対象	タイの組織・公開Webサイト・ECチーム・API運用者・IT・セキュリティチーム
運用上の課題	公開WebサイトやAPIは、OWASP Top 10、ボット、自動スクリプト、異常な通信、フラッド、総当たり試行にさらされます。通常の利用者と攻撃を見分ける仕組みが必要です。
保護対象	Webサイト・Webアプリ・API・オリジンサーバー・ボット / スクリプト・組織
導入形態	クラウド／SaaS・仮想アプライアンス・ICTハードウェアアプライアンスから、ソリューション設計時に選択

主な機能

- OWASP Top 10と一般的なWeb攻撃への対策
- ボット、総当たり攻撃、クレデンシャルスタッフィング、Webスクレイピング、Layer 7 DDoSを抑えるレート制限
- ボットや自動スキャナーからの保護と異常な通信の制御
- 不審なユーザーや高リスクのパスに対するCAPTCHAと認証チャレンジ
- Allow・Block・Challengeのカスタムルール
- リアルタイムダッシュボード、攻撃マップ、セキュリティログ、バックエンドの稼働状況の可視化
- メール、Microsoft Teams、LINE、Webhookによるリアルタイム通知
- RBAC、最小権限、監査証跡を備えたマルチテナントのポリシー・ダッシュボード分離

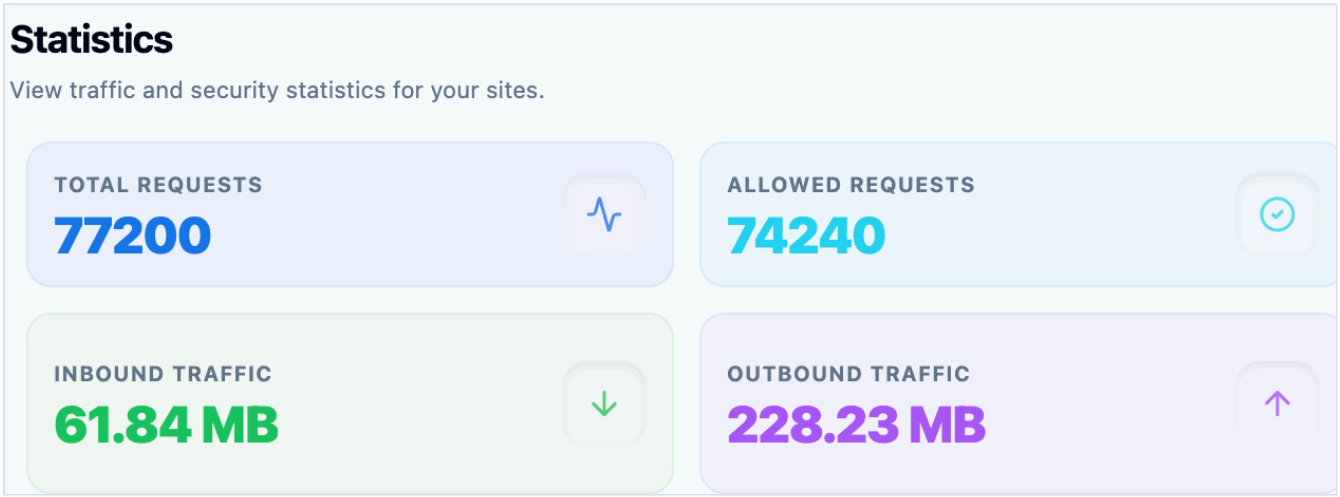
zcrWAFの仕組み

本番環境の手前で通信を検査し、チャレンジで確認する

zcrWAFは通信を検査し、レート制限やCAPTCHA・認証チャレンジを適用し、攻撃をリアルタイムに監視します。

zcrWAFで得られる効果

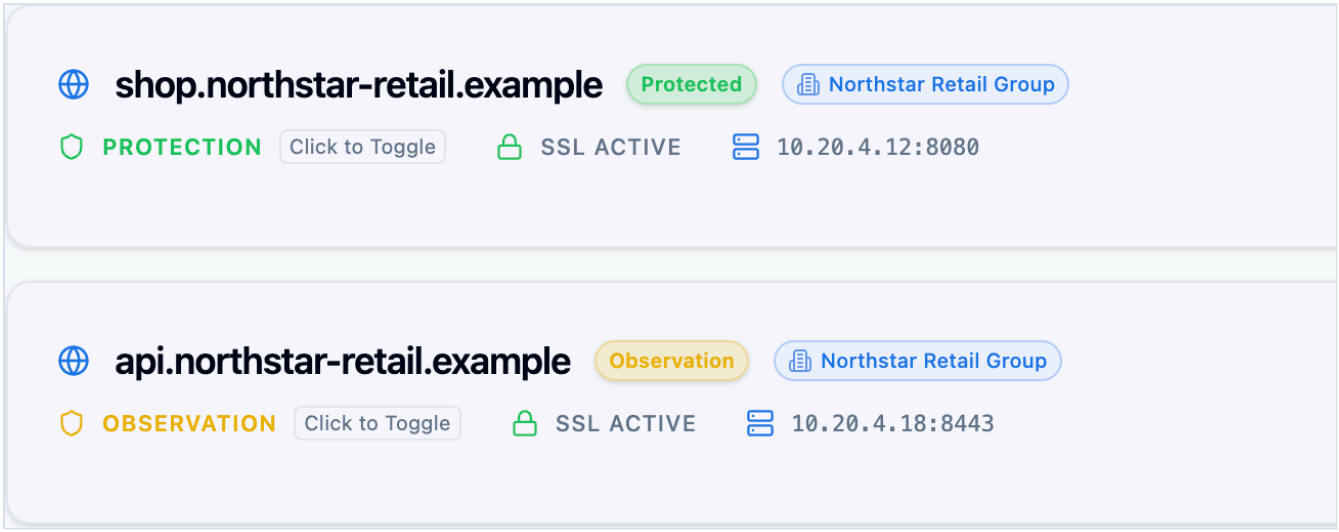
- **アプリケーション層の保護** — 一般的なWeb攻撃とOWASP Top 10の攻撃パターンを本番システムの手前で遮断します。
- **通信量の制御** — 異常通信、フラッド、総当たり試行を抑えながら、正規利用者への影響を減らします。
- **ユーザー確認** — リスクの高いページや不審なセッションにCAPTCHAや認証チャレンジを適用します。
- **運用の可視化** — セキュリティログ、攻撃状況、ダッシュボード、ルール動作をリアルタイムで確認できます。



デモ環境のリクエスト数と通信量を示す一部のウィジェットです。処理性能、攻撃防止の保証、顧客実績を示しません。 元の画面を開く ↗

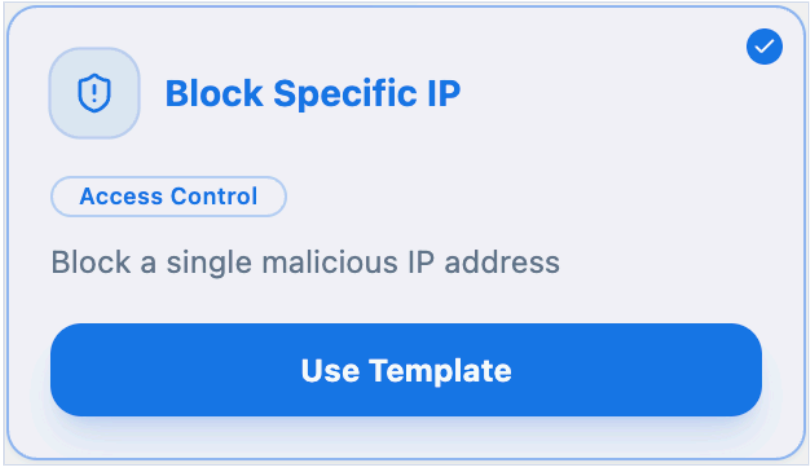
> 説明用のデモデータです。顧客実績、処理容量、性能の証拠ではありません。元の英語UIを保持しています。

01・サイトの実際の保護状態を確認する



2つのサイト行にProtectedとObservation、SSL状態、originが表示されています。Observationは保護有効と同じ意味ではありません。サンプル名は顧客実績を示しません。 元の画面を開く ↗

02・具体的なルールテンプレートを確認する



Block Specific IPのカード全体にAccess Control分類、説明、Use Template操作があります。選択は本番ルールの有効化を証明しません。 ライブラリには管理ページのアクセス制限と機密ファイルの遮断用テンプレートもあります。元画面全体で確認できます。 元の画面を開く ↗

> 説明用のデモデータです。顧客実績、処理容量、性能の証拠ではありません。元の英語UIを保持しています。

zcrWAF FAQ

どの導入形態がありますか？

zcrWAFは、クラウド／SaaS、仮想アプライアンス、オンプレミス向けのICTハードウェアアプライアンスの3つの導入形態から選べます。

zcrWAFの価格はどのように決まりますか？

zcrWAFの価格は規模、契約期間、サポート内容によって異なります。見積もりについてはzcr.ai のチャネルパートナーにお問い合わせください。

どのような保護が含まれますか？

OWASP Top 10対策、レート制限、ボットと自動通信の保護、CAPTCHAまたは認証チャレンジ、リアルタイム監視、ログが含まれます。

導入・運用と商用範囲

クラウド／SaaS	1年契約のクラウド型WAF。最大3ドメインを保護。
仮想アプライアンス	オンプレミス仮想アプライアンス。保護ドメインは無制限、初年度保守（MA）込み。
ICTハードウェアアプライアンス	オンプレミス専用機。保護ドメイン無制限、スループット1 Gbps（GbE）、初年度保守（MA）込み。

柔軟な導入とWAF運用

zcrWAFは、柔軟な導入形態、リアルタイムのセキュリティログ、保守、セキュリティポリシーのチューニングを必要とする、タイで事業を行う組織向けのWAFです。

サポート：一次サポートはチャネルパートナーが提供し、zcrはパートナーに製品サポートを提供します。

承認済みパートナーと評価する

保護対象ドメイン／API、origin、導入形態、期間、支援要件を用意してください。パートナーが規模、保守範囲、ポリシー調整の責任を提案で確認します。

承認済みパートナーが提案範囲、見積もり、契約、導入を担当します。

パートナーに相談 ↗　現行プラン ↗　製品資料 ↗