MR-WAFのご紹介

WAFとは

WAFとは

WAF；Web Application Firewallの略です。

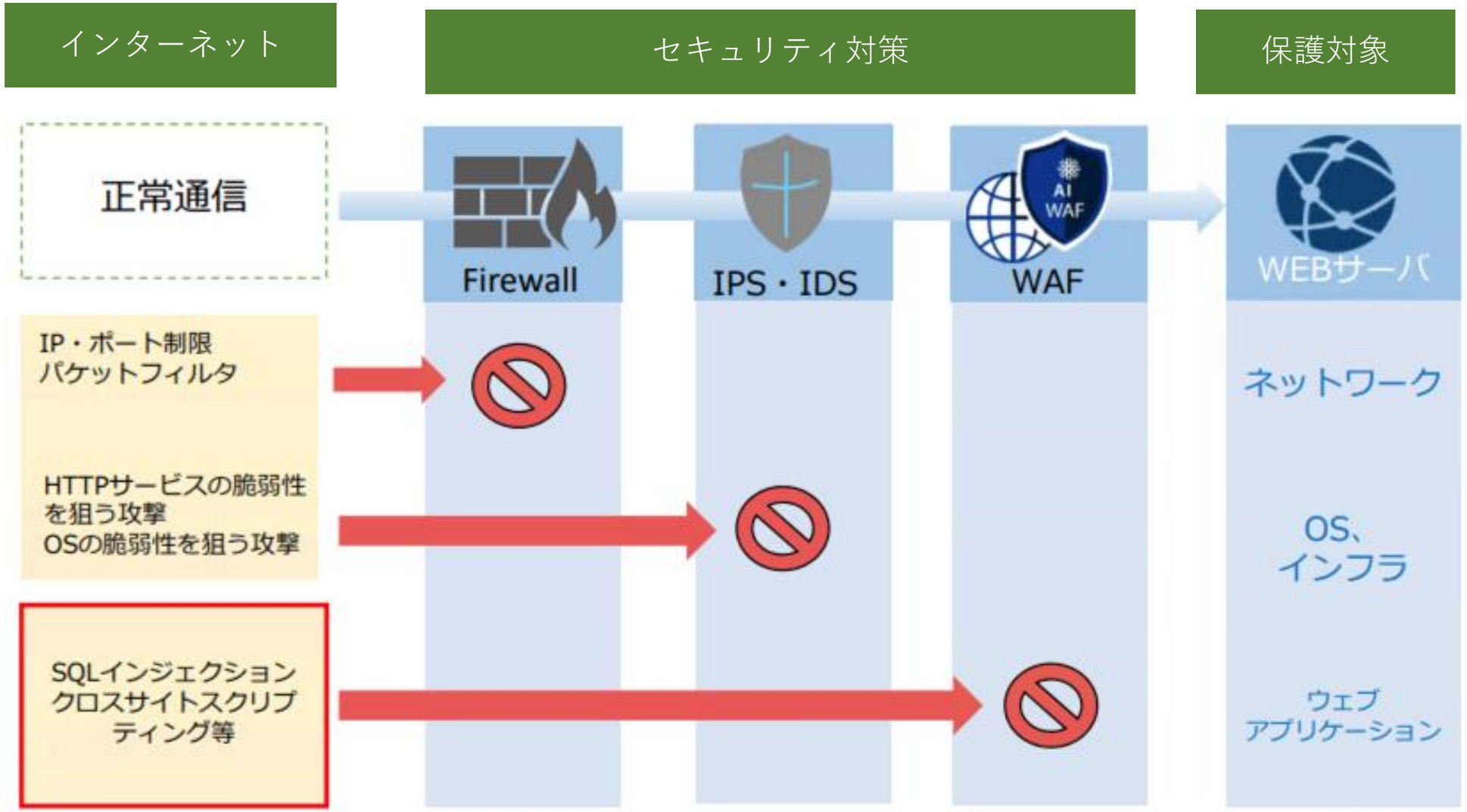
Webサイトを守るための防御ツールです。

FWではだめなの？

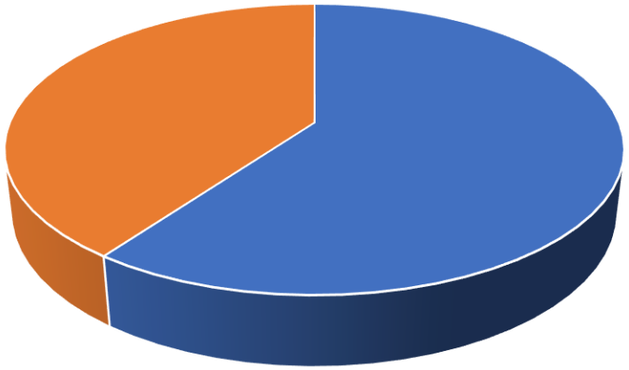
ウイルス対策ソフトで
はだめなの？

守ることができる場所/手法が違います。

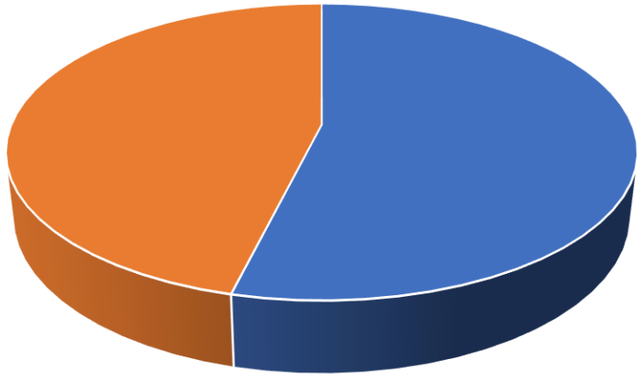
WAFとFW、IDS/IPSの防御範囲



広がるWebサイトへの攻撃



常にサイバー攻撃の脅威にさらされている
ウェブサイトは60%



報告されたWeb脆弱性の中で解決できた
ものは56%だけ

62%のハッキング事例がエクスプロイト
脆弱性を狙った攻撃

196日

新たに発見された脆弱性を解決するまでの
所要時間は196日

データ出典:WhiteHat Security Website Security Statistics Report 2017より

Webサイトへの攻撃事例

Webサイトへのへの代表的なハッキング事例

攻撃手法	対象サイトタイプ	事例
SQLインジェクション	会員サイト	A社のWebサーバーと連携しているデータベース用サーバーにSQLインジェクション攻撃が行われ、保管していた6万３千件の個人情報が不正に持ち出された。
コマンドインジェクション	会員サイト	B社が利用しているソフトウェアが不正アクセスによる攻撃を受け、Webサイトで、OSに対して操作できるような命令文を入れ込んでサーバを乗っ取り、最大43万件の個人情報（氏名、住所、電話番号等）が外部に流出された。
脆弱性を利用した不正アクセス	EC、会員サイト	C社が運営しているオンラインショップにてウェブサイト内に内在するシステム脆弱性を利用した不正アクセスによりお客様のクレジットカード情報１千７百件が流出した。
DoS攻撃	会員サイト	オンラインゲームサービスを提供しているD社に「被害を受けたくなければ、100 万円を支払え」という脅迫メールが届き、支払を拒否する旨を回答したら本格的なDoS攻撃が始まり、１週間同社サービスを提供出来ない状態となった。
CMS脆弱性を利用したWebページ改ざん	CMSサイト	サイバー攻撃に強いと言われていた人気なCMSの脆弱性を突いた攻撃により、155万以上のWebサイトが改ざんの被害に遭った。その中には企業も多かったため、かなり大きい規模の被害が出た。Webサイトに身に覚えのない画像や文章が挿入されたり、勝手に広告が表示されたりするなどの改ざんが行われた。

Webサイトのセキュリティ対策を実施しなかった結果と影響範囲は、企業の経済的損失にとどまらず、信頼やブランドイメージ損失まで及びます。
アプリケーションレベルで行われる攻撃がメインである昨今、Webサイトのセキュリティ対策にWAFが必須です。

MR-WAFの詳細

MR-WAFとは

モニタラップ社　＋　Technol

＝　MR-WAF

特徴
・柔軟な料金プラン
・直感的な操作感
・知識のあまりない方からより詳細管理をしたい方まで広く対応

※MR-WAFとは、モニタラップ社のAIONCLOUDを使ったWAFサービスです。

こんなお客様に最適です

・Wordpress等のオープンソースCMSを使ったWebサイトをお持ちのお客様

・問い合わせフォームや掲示板機能があるWebサイトをお持ちの方

・EC、通販サイトなどお客様の支払情報を取り扱うWebサイトをお持ちの方

・動的コンテンツが多いWebサイトをお持ちの方

・SSL化されていないサイトをお持ちの方

・Webを使って他社へサービスを提供されている方

MR-WAFの特徴

シンプルかつ詳細な管理機能

直感的なWebUIで、
初心者向けの簡単設定から
プロ向けの詳細設定にも対応

世界レベルの脅威情報共有基盤

世界15カ国40箇所のIDCにサービスインフラを保有し、脅威情報を収集するインテリジェントプラットフォームを活用し世界レベルの攻撃遮断能力を提供

柔軟な課金体系

圧倒的な低コストの容量課金体系を用意

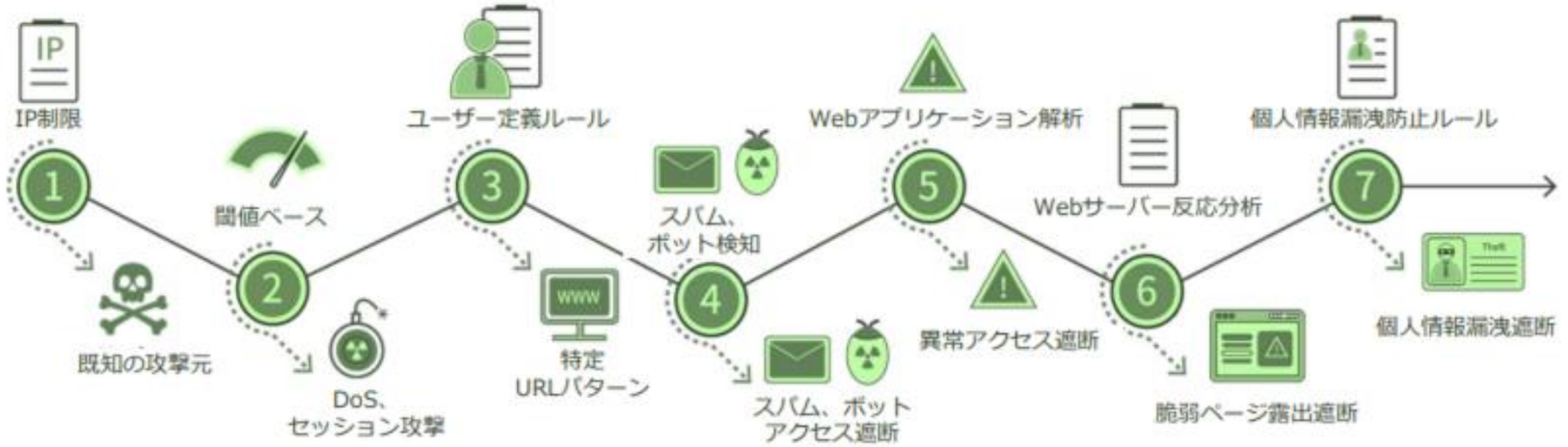
かんたん無料のSSLサイト化機能

HTTPサイトでも、WAFを通すだけでSSLサイト化できます。

テクノルによるサポート

平日9:00から17:00、お客様専用サポートダイヤルを準備

MR-WAFの防御概要



MR-WAFは、日々高度化するWEBサーバーへサーバー攻撃を検出しブロックします。

-SQLインジェクション

-ウェブサーバー脆弱性攻撃

-悪意のあるファイルアップロード

-システムファイルへのアクセス

-クロスサイトスクリプティング

-アプリケーション脆弱性攻撃

-ディレクトリリスティング攻撃

-ディレクトリトラバーサル

-スキャナー、ボットによるアクセス

-CSRF

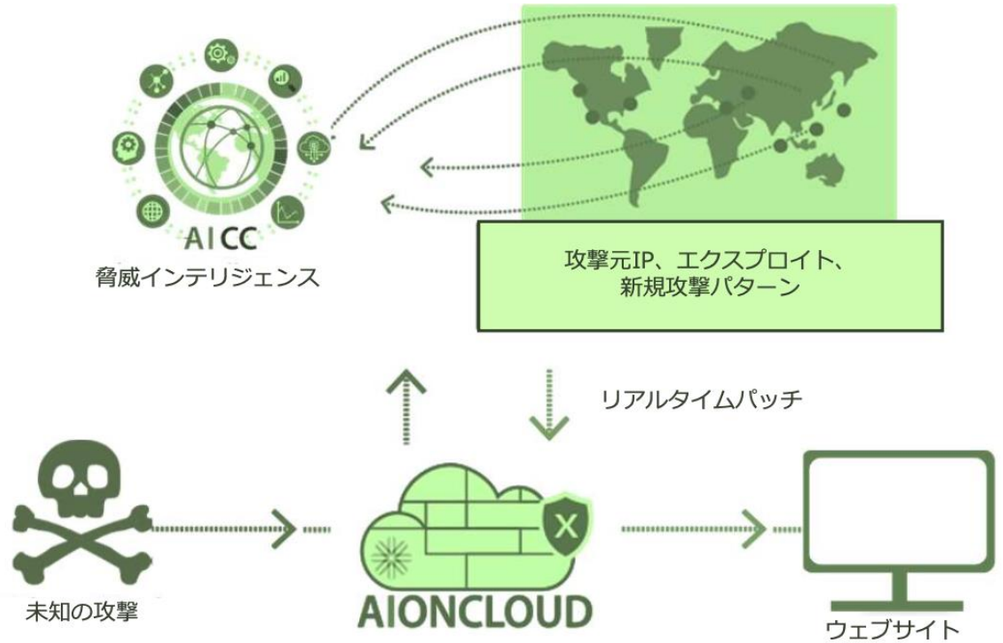
-DoS攻撃

世界レベルの脅威情報共有基盤

・世界各地で発生している脅威やインシデントを収集し、パターン化して配布する仕組みのプラットフォームと連携し、事後対応ではなく事前対応を実現
・攻撃の類似性を分析し、新たな攻撃に直ちに対応可能

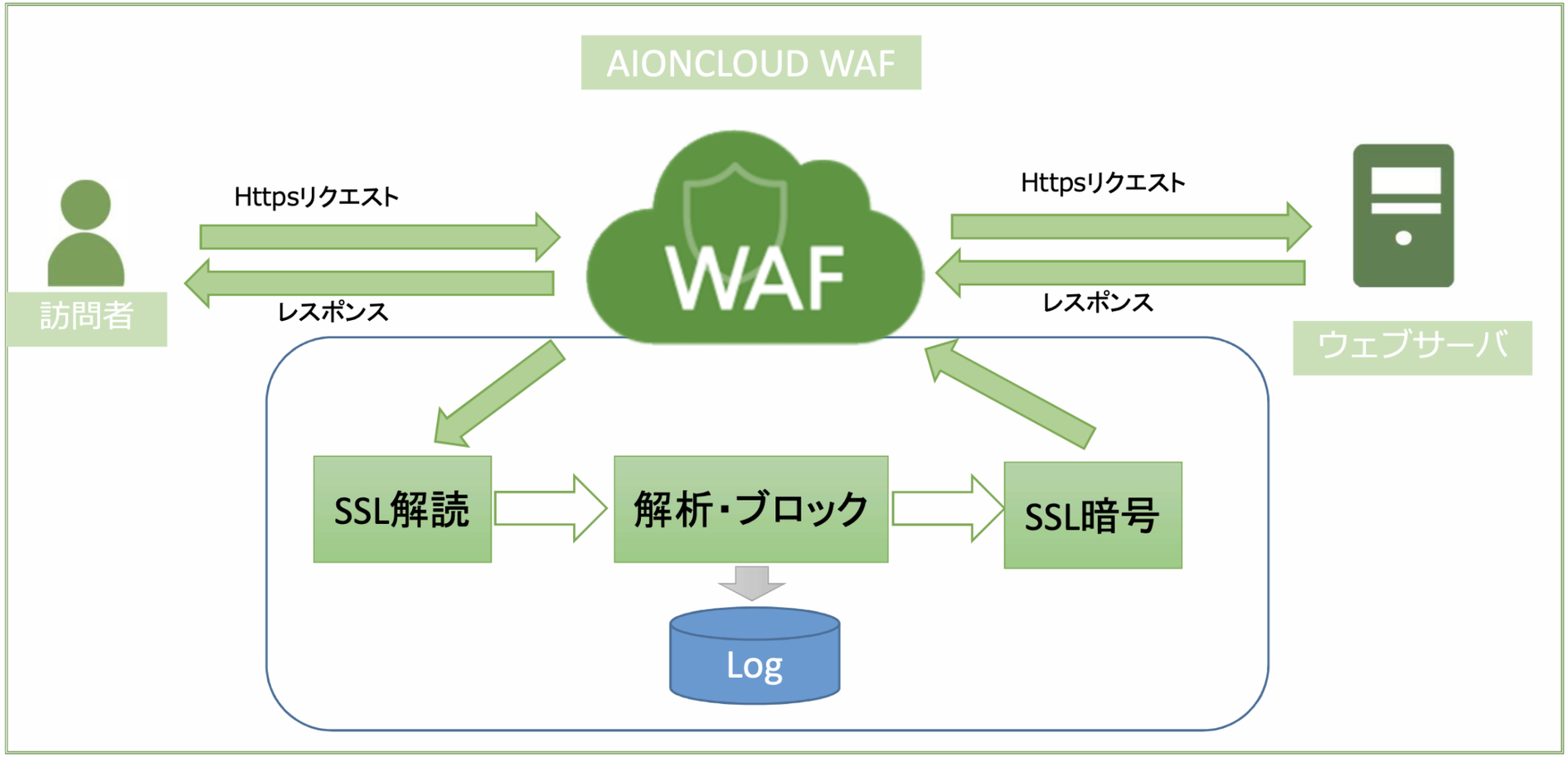
◯バーチャルパッチ
-分析・加工済みの脅威はリアルタイムでWAFに適用されます
-お客様のアップデート作業は一切不要です

◯マシンラーニング
-怪しいアクセスに対して既存の攻撃手法との類似性を分析します。
-新型SQLインジェクションの98.99％が防御可能なことが検証されました。



基本構成

-リバースプロキシ型のWAFです
-Webサーバーへのインストールは不要
-DNSに、弊社発行のCNAMEを登録いただくことで、WAFを経由の通信となります。

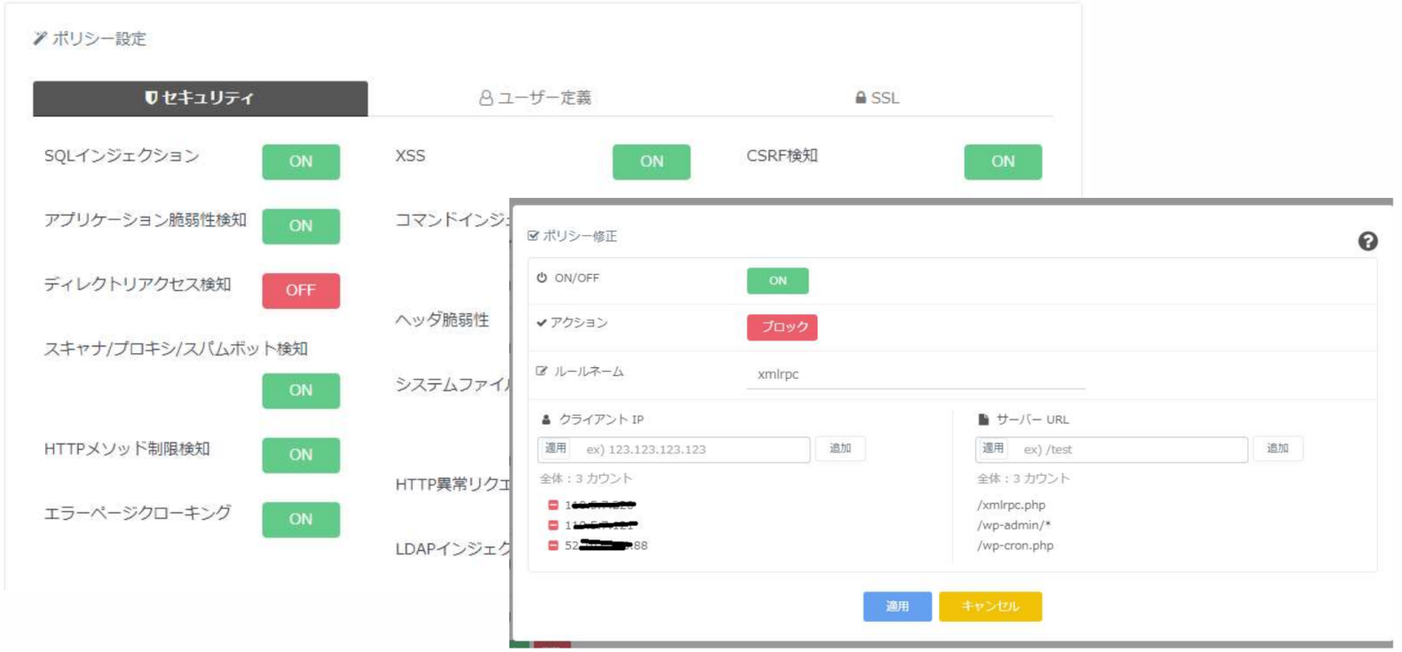


シンプルかつ詳細な管理機能

○直感的なUI
-リアルタイム検知ログ
　検知時間、攻撃社IP及び国情報、検知理由、リクエスト本文データ情報提供
-ドメイン別ダッシュボード
-期間指定レポート（PDFとWord形式いずれか）
-GUIは、日本語、英語、韓国語をサポート

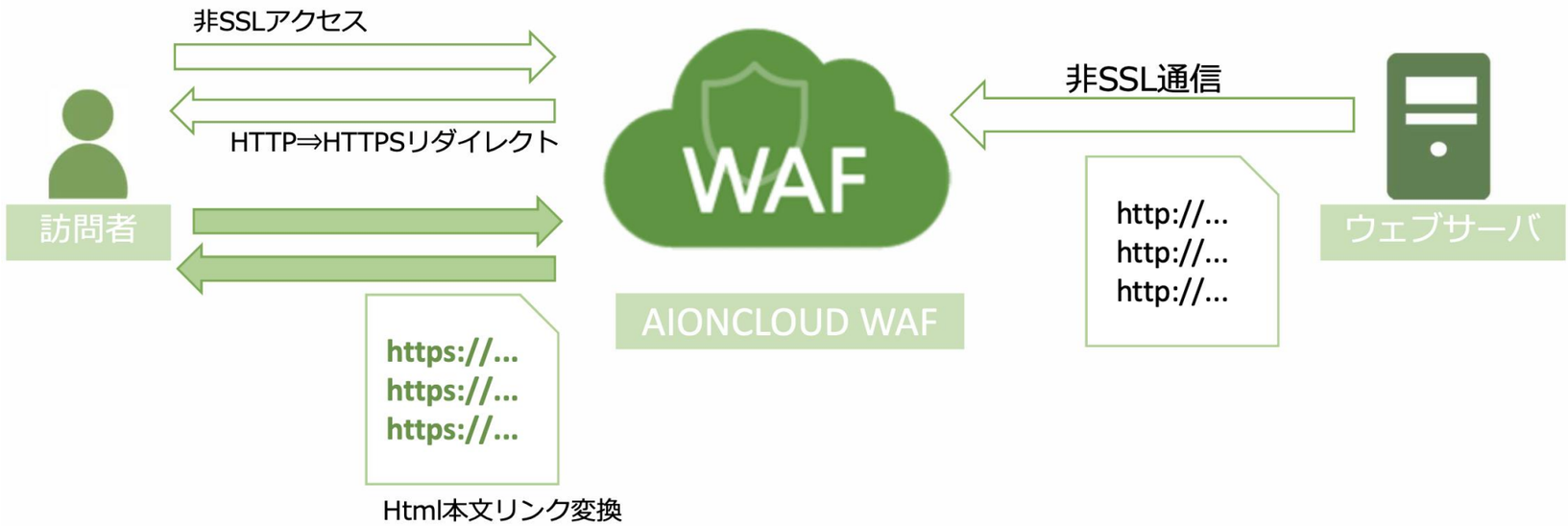
詳細なポリシー設定

○他のクラウドWAFにはない、ユーザーに依る詳細なポリシー調整機能
-ルールごとに、適用URL＆IP設定による対象外設定が可能
-ポリシーごとのON/OFF設定
-特定の国からのIPをまとめて接続拒否が可能



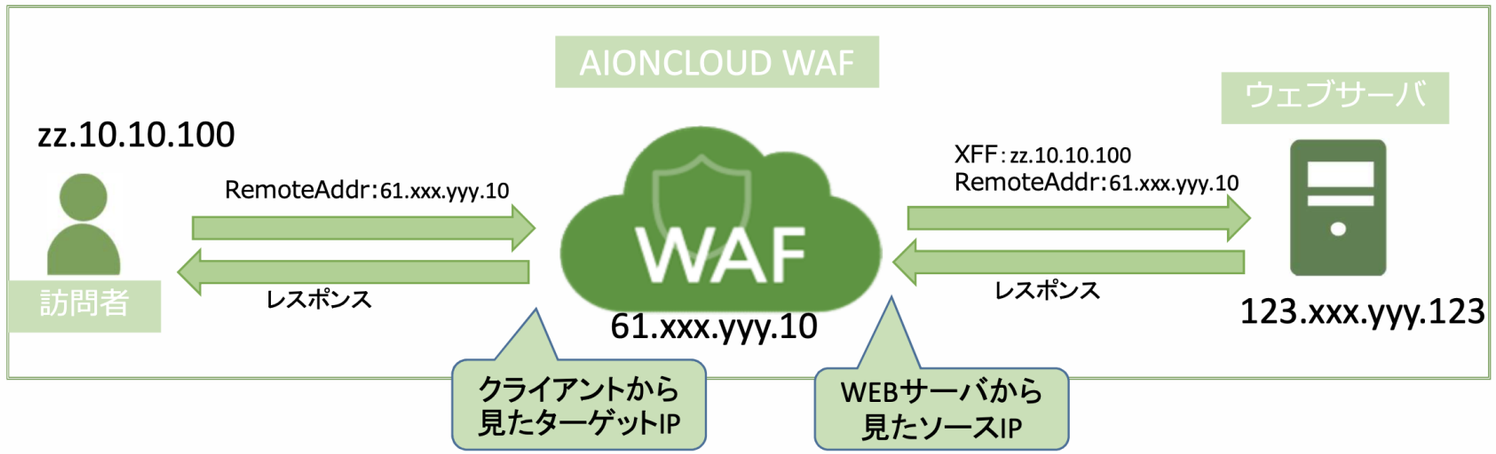
かんたん無料のSSLサイト課機能

-まだSSL化されていないWebサイトのために「無料SSL証明書発行サービス」を提供します。
-「HTTP->HTTPSリダイレクト機能」で暗号化通信を矯正し、「html本文リンク変換機能」で非SSL化サイトの完全SSL化を実現します。



ソースIPをWebサーバーやロードバランサーに連携

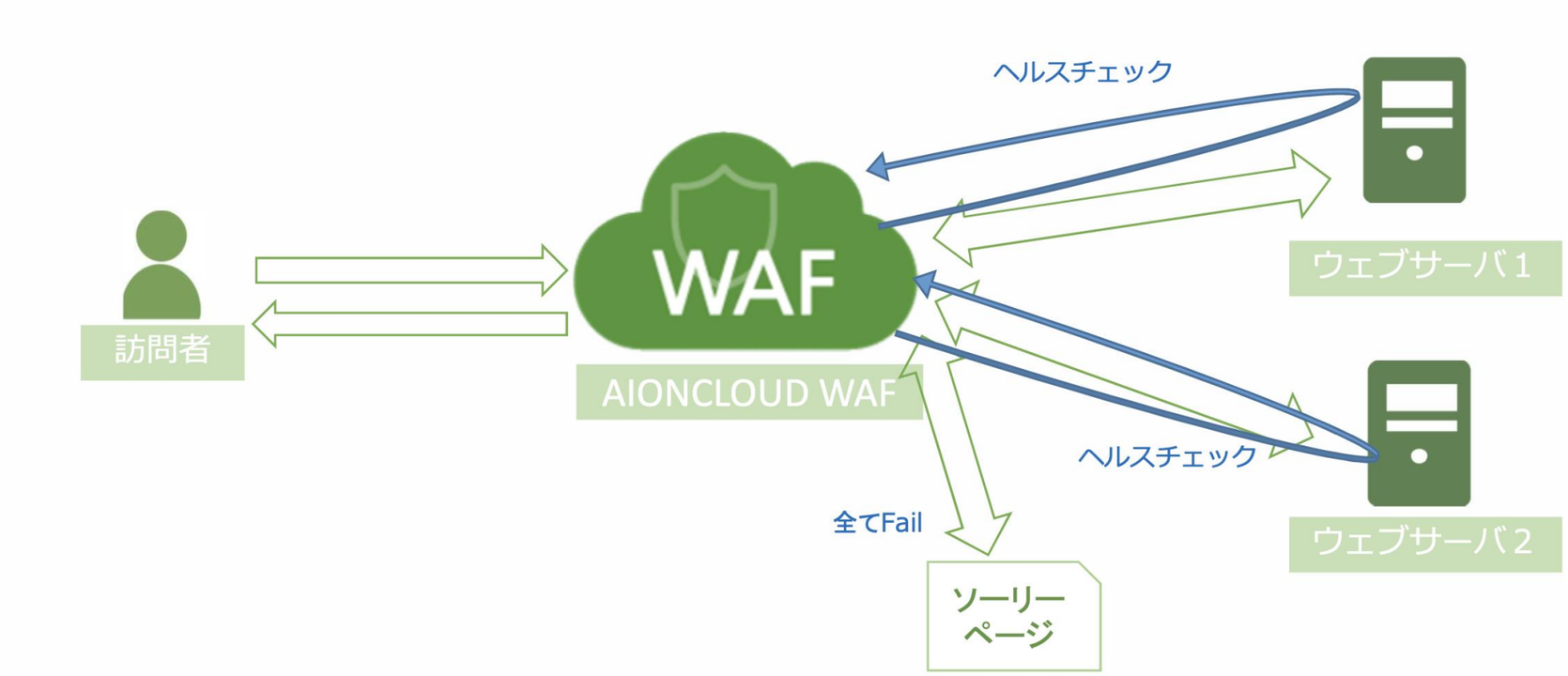
-WEBサーバーへのhttps通信は、すべてWAFのIPヘッダとなります。
-ソースIPは、X-Fowarded-For（以下XFF）ヘッダにて連携します。
-WEBサーバーの設定で、XFFを参照してソースIPを取得してください。



X-Forwarded-Forとは、HTTPヘッダフィールドの1つであり、ロードバランサーなどの機器を経由してWebサーバーに接続するクライアントの送信元IPアドレスを特定する際の標準的な手法です。
クライアントの送信元IPアドレスの特定は、ロードバランサー等でクライアントの送信元IPアドレスが変換された場合でも、HTTPヘッダに元のクライアントIPアドレスの情報を付加することで実現します。
Proxy型段になっている場合は、一番右側がWAFの手前のソースIPとなります。

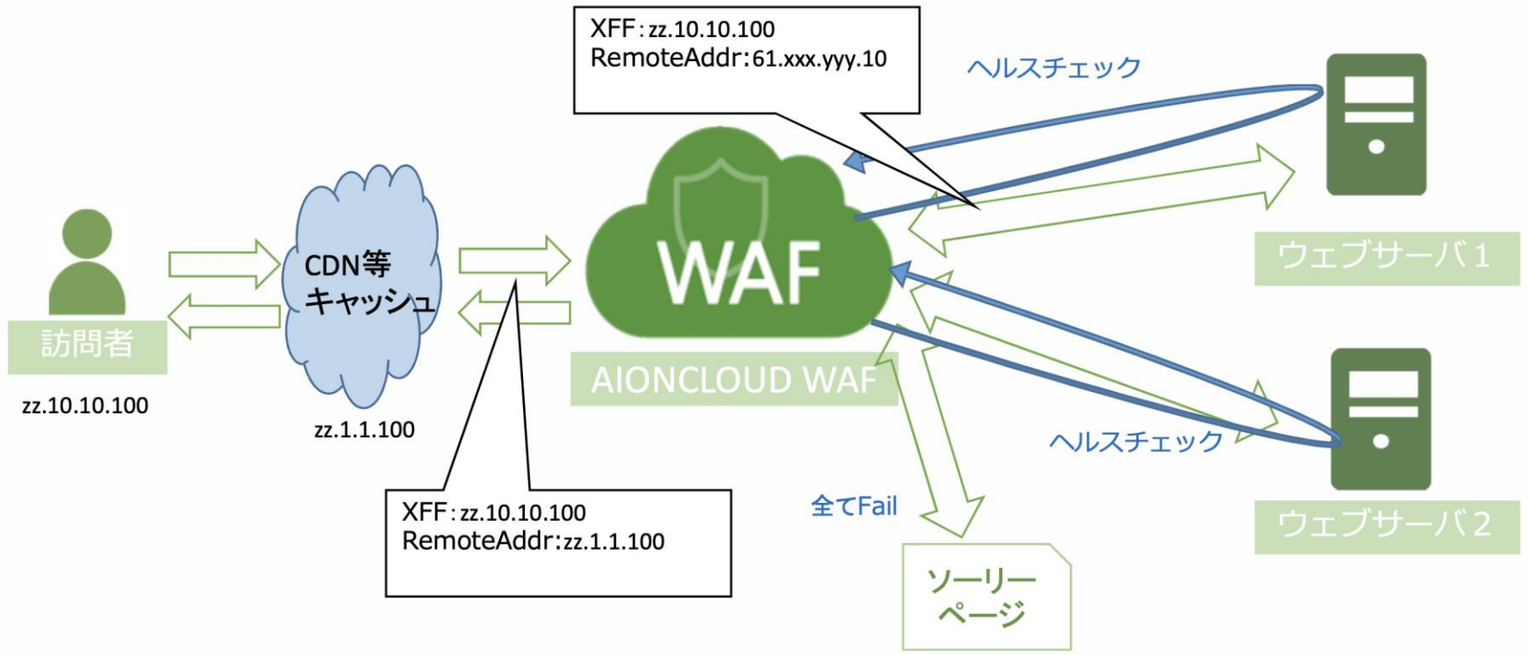
ロードバランサー機能

ロードバランスアリゴリズム：ソースIP+Macアドレス
-ソーリーページのカスタマイズ、リダイレクト表示
-既設のロードバランサーがNLBの場合や、XFFのに対応していない場合、WAF搭載のロードバランサーを利用すると、ソースIPによるセッション維持が可能になります。



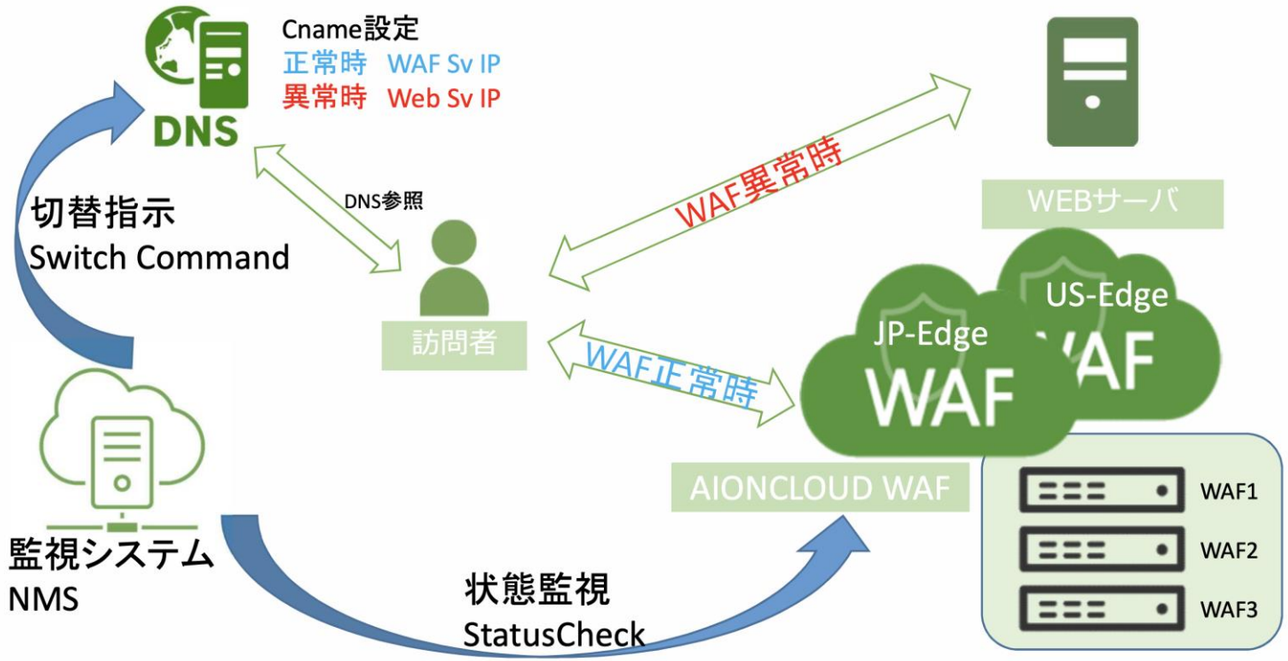
CDNを介してもサーバーロードバランサー機能が有効

WAF搭載のロードバランサーを利用すると、ソースIPまたはXFFによるセッション維持が可能になります。



WAF自体のフェイルオーバー機能

WAFサーバー自体が冗長化されています。
-日本サーバーがデータセンターや回線の都合でメンテナンスをする場合は、一時的にUSサイトのサーバーに切り替わります。
-WAFが障害で機能しなくなった場合には、CNAMEの宛先IPは書き換えによりWEBサーバーへバイパスします。
※バイパス時にWAFを経由しないようにしたい場合は、WEBサーバー側でIP制限を掛ける必要があります。



マルチアカウントを想定した機能

ISO2700、ISMS、プライバシーマークなどのセキュリティ認証を意識した運用機能が充実しています。
-メンバー追加とアクセス制限機能
-サブ管理ユーザーとしてメンバーを追加し、担当するドメインを制御できます。

※複数ドメインを登録する場合は、プランの追加をお願いします。

Technol

Smile&Honesty. 一人ひとりが未来のために。