

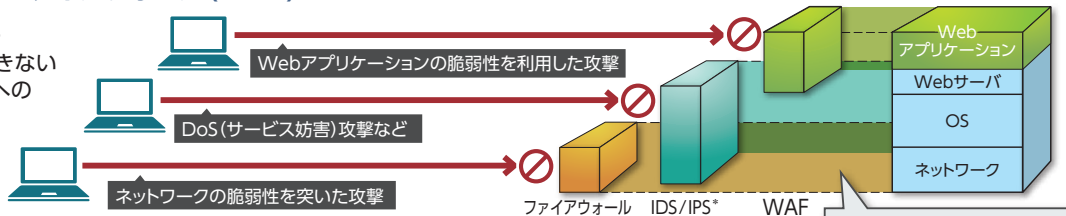
Webアプリケーションファイアウォール

InfoCage SiteShell/ActSecureクラウドWAFサービス

外部からの不正アクセスを検知/防御し、機密情報の流出を防止。
安全なWebサイトの運営を実現。

Webアプリケーションファイアウォール(WAF)

従来のファイアウォールやIDS/IPSでは防ぐことができないWebアプリケーション層への攻撃を防御。



Webアプリケーションへの攻撃は、従来のファイアウォールやIDS/IPS*では防ぎきれません。

*IDS/IPS:不正侵入検知/防御システム

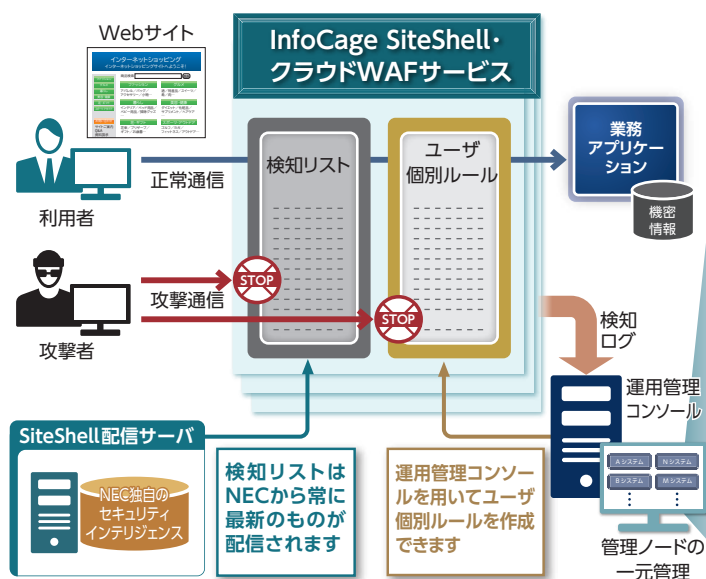
特長

NECから最新の検知リストを配信

NECから配信される検知リストは再起動なしで適用可能。検知リストの世代管理機能により、最新の検知リストのみ評価することができるため、WAF運用でありがたいな過剰検知リスクを低減。

運用管理の容易性

Webサーバ数十台～数千台規模のシステムでも、運用管理コンソールを用いて管理ノードの一元管理が可能となり、日々の運用負荷を軽減。



攻撃状況を一目で把握可能

攻撃元

攻撃種類

攻撃箇所

防御方法

視覚的にわかりやすい GUI



運用管理コンソールを用いて、防御設定や過剰検知時の除外設定を視覚的に行えます。除外設定は細かい条件設定により、必要最小限の除外範囲に適用できます。

Webアプリケーションファイアウォールの導入形態

お客様の環境・要件に合わせて、様々な形態で導入することが可能です。

<p>ネットワーク型</p> <p>ネットワーク上にWAF専用サーバを設置し、そこにInfoCage SiteShellをインストール。</p>	<p>インターネット ファイアウォール ロードバランサ WAF専用サーバ InfoCage Webサーバ</p> <p><small>※ロードバランサとしてInterSec/LBを利用している場合、ロードバランサにInfoCage SiteShellを導入できます。</small></p>	<p>特徴</p> <p>導入: 導入時にネットワークの設計/構築、および冗長構成の検討が必要</p> <p>運用: 運用管理コンソールにてユーザ個別の細かいカスタマイズが可能</p> <p>性能: WAF専用サーバの性能に依存</p>
<p>スニファ型</p> <p>スイッチのミラーポートを利用し、パケットをキャプチャ。InfoCage SiteShellサーバで攻撃のチェック(検知のみ)を実施。</p>	<p>インターネット ファイアウォール ロードバランサ スイッチ WAF専用サーバ InfoCage Webサーバ</p>	<p>特徴</p> <p>導入: 導入時にネットワークの追加設定が必要 Webサーバに影響を与えずに導入でき、攻撃のチェック(検知のみ)が可能</p> <p>運用: 運用管理コンソールにてユーザ個別の細かいカスタマイズが可能</p> <p>性能: WAF専用サーバの性能に依存</p>
<p>ホスト型</p> <p>Webサーバに直接InfoCage SiteShellをインストール。</p>	<p>インターネット ファイアウォール ロードバランサ Webサーバ InfoCage</p>	<p>特徴</p> <p>導入: Webサーバへの導入に対する影響の考慮が必要</p> <p>運用: 運用管理コンソールにてユーザ個別の細かいカスタマイズが可能</p> <p>性能: Webサーバの性能に依存</p>
<p>クラウド型</p> <p>NECから提供される「ActSecureクラウドWAFサービス」を経由するようにネットワークの経路を変更</p>	<p>インターネット ファイアウォール ロードバランサ ActSecureクラウドWAFサービス Webサーバ</p>	<p>特徴</p> <p>導入: DNSの設定変更のみで導入可能</p> <p>運用: NECにて運用管理を行うため、ユーザでの運用負荷軽減</p> <p>性能: サービスレベルに依存</p>

機能一覧

機能	概要	ホスト型/ ネットワーク型	スニファ型	クラウド型
攻撃対策	SQLインジェクション対策	○	○*	○
	クロスサイトスクリプティング対策	○	○*	○
	セッションハイジャック対策	○	○*	○
	OSコマンドインジェクション対策	○	○*	○
	パストラバーサル対策	○	○*	○
	HTTPプロトコルのメソッド対策	○	○*	○
	バッファオーバーフロー対策	○	○*	○
	クロスサイトリクエストフォージェリ対策	○	○	○
	パラメータ改ざん対策	○	○	○
	強制的ブラウズ対策	○	○	○
	Cookieに関する脆弱性攻撃対策	○	○	○
	パスワードリスト攻撃対策	○	○	○
ユーザ個別の攻撃対策	○	○*	○	
予兆検知	既知の攻撃元IPのリスト	○	○	○
	攻撃予備動作となる文字列のリスト	○	○	○
運用管理	GUIでの攻撃状況確認、設定変更	○	○	○
	攻撃検出時のメール通知	○	○	○
	攻撃検出時のsyslog通知	○	○	○
	攻撃検出時のSNMPトラップ通知	○	○	○
	検知リストの自動更新	○	○	○
	検知リストの手動更新	○	○	○

*: 検知のみ

動作環境

InfoCage SiteShell本体

対応プラットフォーム	ネットワーク型	ホスト型	
	スニファ型	IIS版	Apache版
Windows Server 2012 (x64)	—	○	○
Windows Server 2012 R2 (x64)	—	○	○
Windows Server 2016 (x64)	—	○	○
Windows Server 2019 (x64)	—	○	○
RedHat Enterprise Linux v.6 (x64)	○	—	○
RedHat Enterprise Linux v.7 (x64)	○	—	○
RedHat Enterprise Linux v.8 (x64)	○	—	○
CentOS v.6 (x64)	○	—	○
CentOS v.7 (x64)	○	—	○
CentOS v.8 (x64)	○	—	○
Amazon Linux (x64)	○	—	○

運用管理コンソール

対応プラットフォーム	全導入形態共通
Windows Server 2012 (x64)	○
Windows Server 2012 R2 (x64)	○
Windows Server 2016 (x64)	○
Windows Server 2019 (x64)	○
RedHat Enterprise Linux v.6 (x64)	○
RedHat Enterprise Linux v.7 (x64)	○
RedHat Enterprise Linux v.8 (x64)	○
CentOS v.6 (x64)	○
CentOS v.7 (x64)	○
CentOS v.8 (x64)	○
Amazon Linux (x64)	○

● 導入形態による、動作環境についての詳しい情報及び最新情報についてはお問合せください。

お問い合わせは、下記へ

InfoCage SiteShell ▶ <https://jpn.nec.com/infocage/siteshell/index.html>

ActSecureクラウドWAFサービス ▶ https://jpn.nec.com/act/acts_cloudwaf.html

●本カタログのシステム名、製品名、会社名、及びロゴは各社の商標または登録商標です。
 ●本製品の輸出(非居住者への役員提供等を含む)に際しては、外国為替及び外国貿易法等、関連する輸出管理法等をご確認の上、必要な手続きをお取ください。
 ●ご不明な場合、または輸出許可等申請手続きに当たり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
 ●本カタログの内容は改良のため予告なしに仕様・デザインを変更することがありますのでご了承ください。