強力なアプリケーション セキュリティを
実現にするための手法とソリューション

ロードバランサとWAFのコンビが性能を最大化

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

Contents

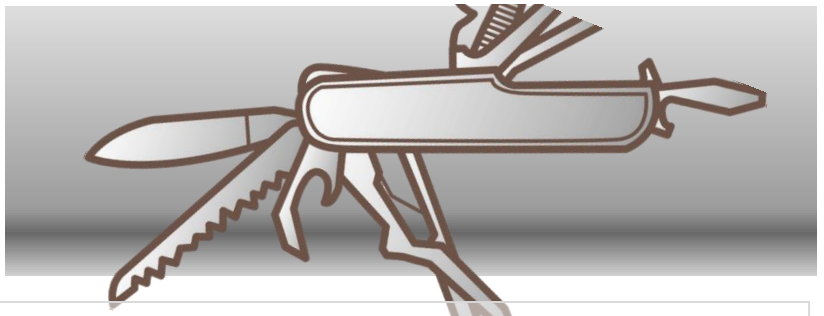
New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

ADCとロードバランサ

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

ADCの条件



ADC(アプリケーションデリバリ コントローラ)は、SSLオフロードに加え、サービスやアプリケーション別のリクエストをコントロールして、サーバとアプリケーションの負荷分散を効率よく行う装置です。サーバクラスタリングだけを目的とするものではありません。

SSLアクセラレーション

- SSLオフロード、コンテンツキャッシュ、コンテンツ圧縮で、サーバ負荷を軽減し、スループットを最大化する。
- マネージドPKIではOCSPと連携でリアルタイムな失効管理。ADFSやRadius認証によるエッジセキュリティを実現する。

L7コンテンツスイッチ

- 複合したサービスを効率よく分散し、アプリケーションの負荷を軽減することでサーバ負荷も軽減できる。
- 1つのIPアドレスエントリで、リクエストを複数のサービスやに配信し、IP資源を有効に活アプリケーションサーバ用する。

GSLB

- 広域展開するアプリケーションへのリクエストは、アクセスユーザのもっとも近い地域にあるサーバに配信する。
- DR対策ではホットスタンバイでシームレスな復旧を可能にする。DDoS対策でも有効な機能となる。*1

セキュリティ

- WAF機能を装備し、高度なアプリケーションセキュリティを実現する。
- IPS(侵入検知と防御)やエッジセキュリティなど、システムとアプリケーションの安全運用のための防御機能を実装している。

*1: GSLBは追加ライセンスが必要です

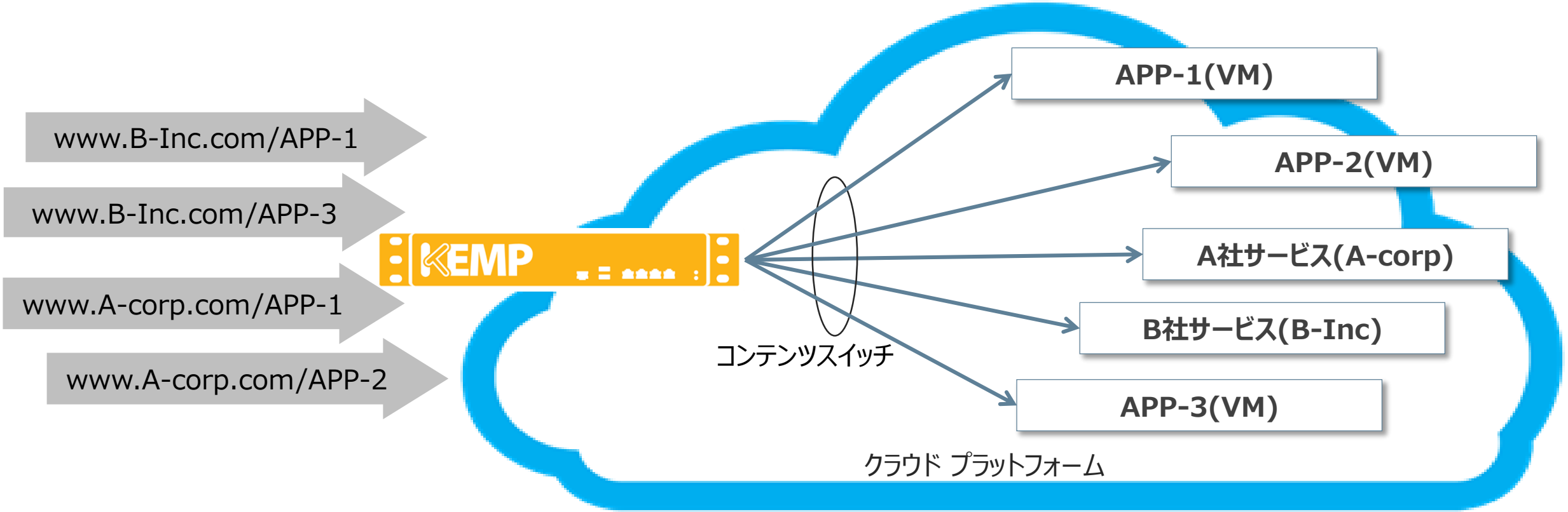
ADCとロードバランサ

ロードバランサは一般的にサーバ ロードバランサを指し、サーバのアクセス負荷を分散し、サーバクラスタリングによるフォールトトレーラントを実現します。ADCはさらに、リクエストをアプリケーションごとに分散して、アプリケーションの負荷を軽減します。

New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

クラウドへの応用

クラウドやハイパーバイザ環境でのシステム構築では、デプロイしたアプリケーションやサービスは1つの仮想マシンとして機能します。
ADCは、クラウド内に分散したアプリケーションをシームレスに統合して、IPと仮想マシンの資源を有効に活用します。



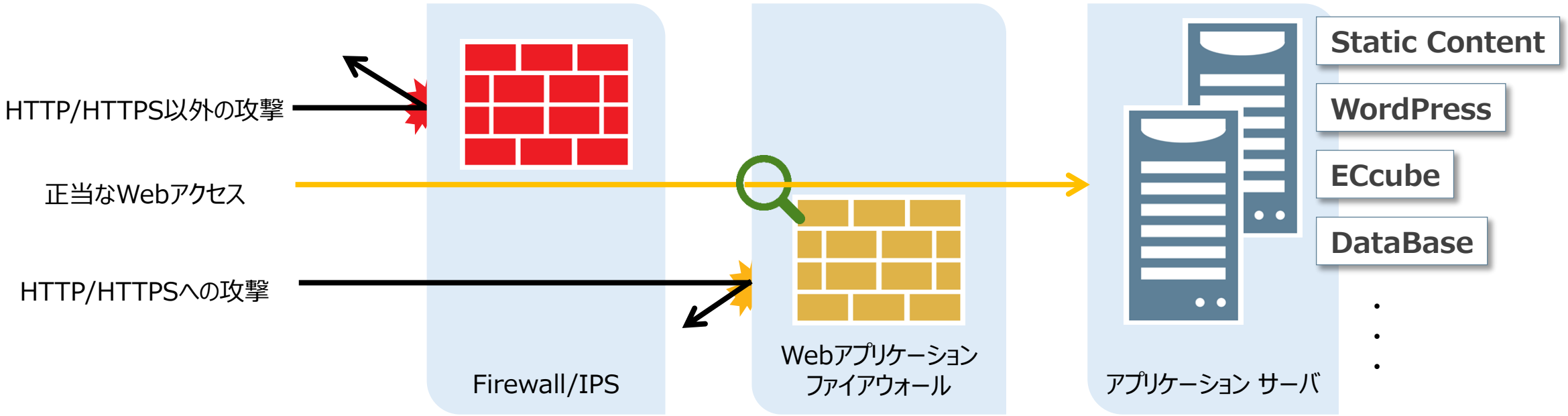
New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

分散WAFコンセプト

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

WAFとファイアウォール

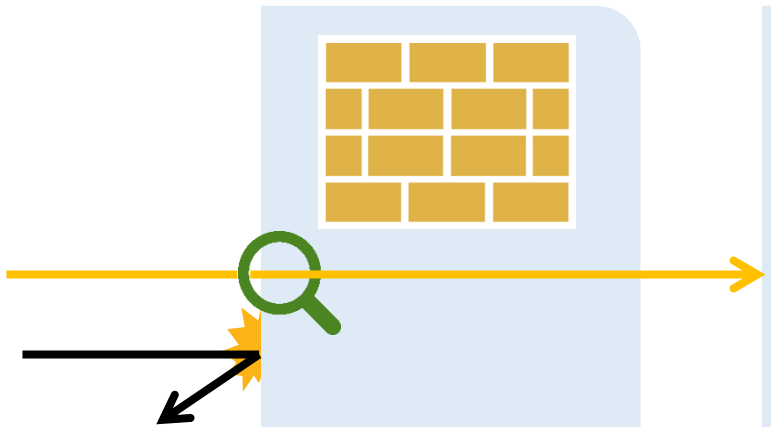
Webアプリケーションのセキュリティ対策ではWAF(Webアプリケーション ファイアウォール)の導入が強力なソリューションです。一般的なWAFのデプロイは、L3/L4の攻撃をファイアウォールで、HTTP/HTTPSの攻撃を最新のルールセットを備えたWAFが防御します。



New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

WAFデプロイの弊害

WAFは、さまざまな攻撃を防御するためルールセット(シグネチャ)をアプリケーションの特性に応じてインストールします。このため、一般的なWAFのデプロイでは、インストールしたルールですべてのリクエストを検査することになり、応答性の劣化を招きます。



- **Static Content** ← 基本的にルールは不要
- **WordPress** ← phpコードが置かれたパスアクセスをチェック。sqli、xss等
- **ECcube** ← phpコードが置かれたパスアクセスをチェック。sqli、xss等
- **DataBase** ← 他のアプリケーションで対策済みなら不要。sqliルールで対策

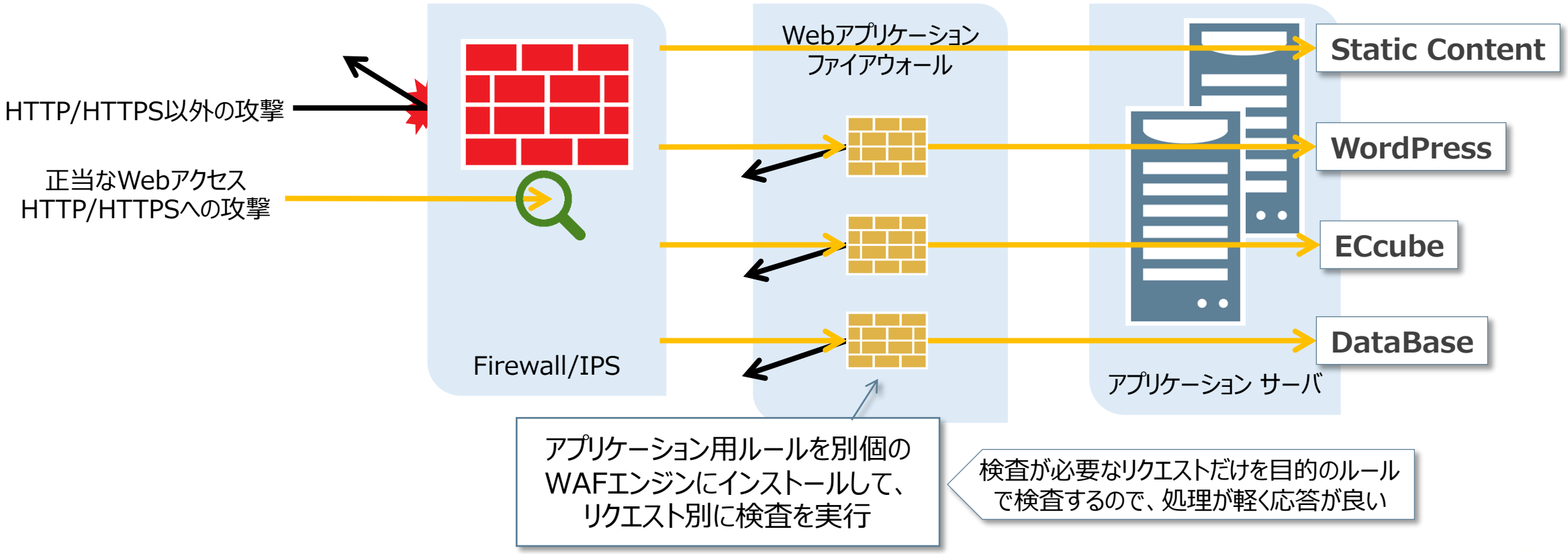
WordPress用ルール
ECcube用ルール
SQLインジェクション用ルール

すべてのリクエストパケットを
インストールしたルールで検査

**アプリケーション特性に適合したルールセットの選択で最大のプロテクション効率を実現できます。
不要なルールセットのインストールはCPUパワーとメモリを過剰に消費します。**

WAFの理想的なデプロイ

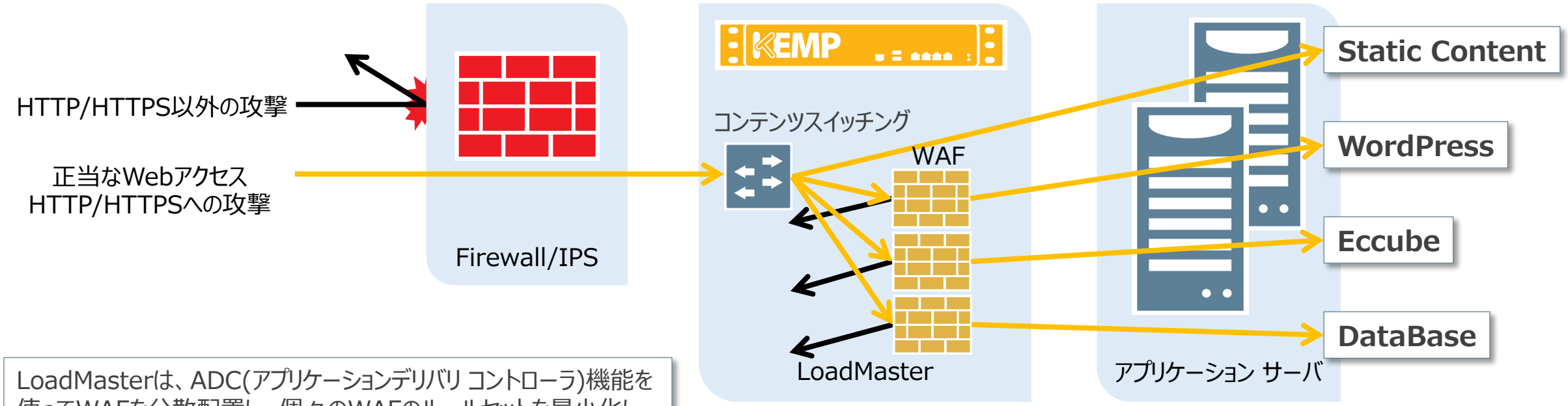
WAFはファイアウォールという名称を含みますが、ファイアウォールと同じ概念でデプロイする装置ではありません。本来、アプリケーションが対応すべき脆弱性を肩代わりするものであり、アプリケーションを密接に関係したデプロイが効果を発揮します。



New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

ADCとWAF

アプリケーションの特性に適したルールセットでリクエストパケットを検査すること。WAFを利用する上では、CPUやメモリ資源の消費を最小限に抑えて検査効率を最大化することが、サイトの応答性とユーザエクスペリエンスに大きく貢献します。

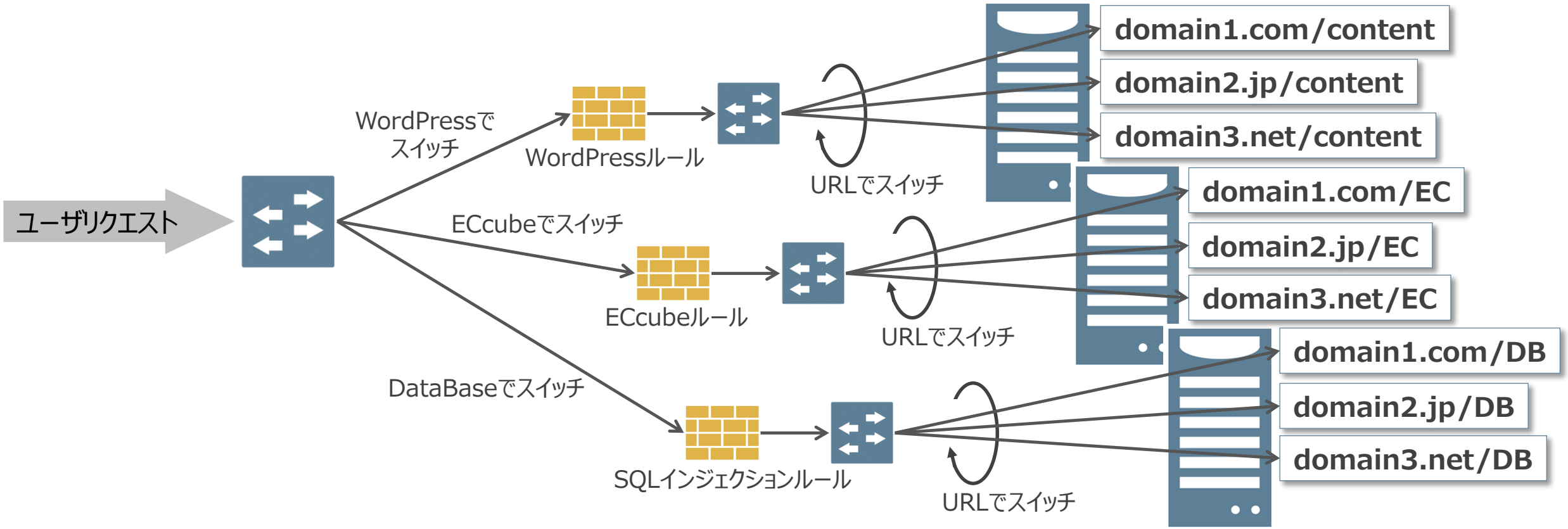


LoadMasterは、ADC(アプリケーションデリバリ コントローラ)機能を使ってWAFを分散配置し、個々のWAFのルールセットを最小化し、検査に振向けるCPUとメモリの消費量を削減します。

New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

LoadMasterの構造

分散型WAFを実現するLoadMasterの構造はどうなっているのでしょうか。L7コンテンツスイッチを実現するための構造は、WAFを分散化し、ユーザリクエストに必要な対策を行った上で、安全なリクエストのみを目的のアプリケーションにを届けます。



New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

WAFルール

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

ルール型とシグネチャ型

一般的なWAFは、シグネチャと呼ばれる攻撃パターンをデータベース化しパターンマッチで攻撃を特定します。一方、ルール型は攻撃パターンの解析アルゴリズムを用意し、リクエスト パケットを解析します。KEMP LoadMasterはルール型を採用しています。

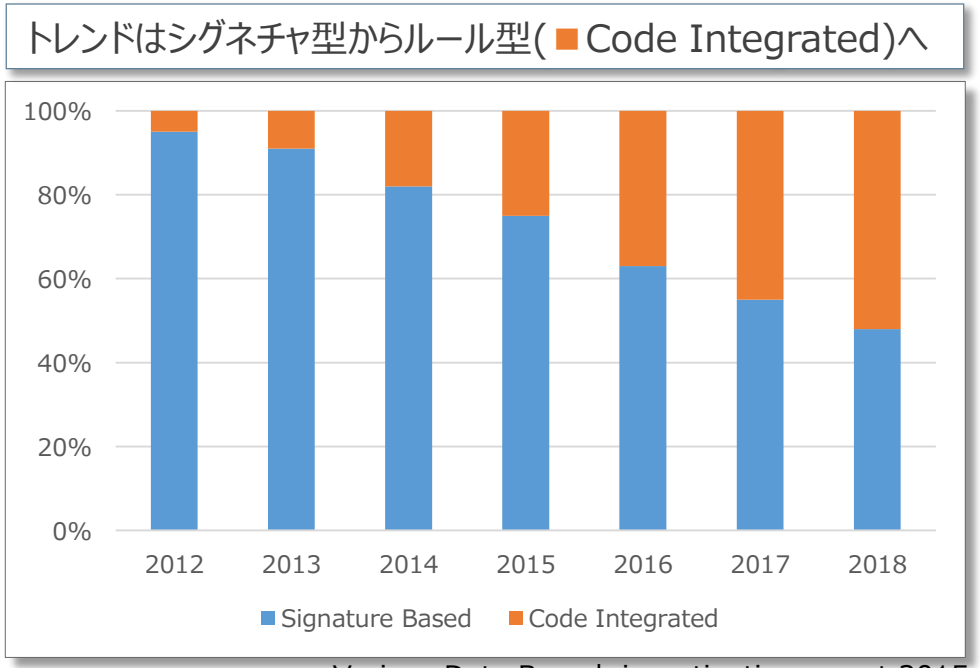
ルール型

- 攻撃パターンを保持せず、アルゴリズムでのパターンを解析し、攻撃を特定します。
- 膨大な攻撃パターン データベースが不要で、処理の軽さとパターン アップデートの頻度の少なさが特長です。
- OWASP ModsecurityのCRS(コアルール セット)はフリー版で提供されています。

シグネチャ型

- 多くのWAFが採用する従来型の攻撃検知方式です。
- 攻撃パターンをデータベース化し、パターンマッチにより攻撃を検知します。
- 運用を重ねるとパターン データベースが増えていくので、レスポンスビリティに影響を与えます。

OWASPは国際的な組織として、OWASP財団という非営利団体の支援を受けて活動しています。組織はWebアプリケーションの開発から運用までの信頼性を高めるためのコミュニティであり、ツールやドキュメントはフリーで公開しています。アプリケーションセキュリティの改善に対し、人、プロセス、技術的問題の面からアプローチし、効果的な改善手法を提唱しています。



Verizon Data Breach investigation report 2015

ルールの種類

LoadMasteのWAFではKEMPが提供するルールの他に、OWASP ModsecurityのCRS(コアルール セット)が利用できます。
WAFの運用にあたっては、利用するルールに応じて、運用性やアプリケーションの適合性などでいくつかの方法を選択できます。

KEMPコマーシャルルール

- KEMPが供給するルールセットです。年間サブスクリプション契約で、最新のルールセットを毎日アップデートします。
- OWASP Top10に対応することはもちろんのこと、アプリケーション別にルールを選択できるので、比較的簡単に設定ができます。
- 運用面においては、もっとも使いやすいルールセットです。

OWASP Modsecurity CRS

- OWASP Modsecurityが供給するCRSです。フリーでダウンロードでき、そのままでWAFの運用が可能です。
- CRSは多くのルールを含んでおり、アプリケーションの特性に応じて選択する必要があり、インストール時にノウハウが必要です。
- サイトの脆弱性によってチューニングを加えると、最適なパフォーマンスを発揮します。

カスタムルール

- カスタムアプリケーションの脆弱性に応じて、独自にルールを記述することが可能です。
- ルール記述ガイドは、KEMPで提供していますが、Githubでもマニュアルを入手することができます。サンプルルールも多数用意されています。
- ルールの記述は独自のノウハウが必要ですので、導入前にご相談ください。

OWASP コア ルールセット	https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
ルール記述ガイド (KEMP)	https://support.kemptechnologies.com/hc/en-us/articles/204301909-AFP-Rule-Writing-Guide
ルールコマンド マニュアル	https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual

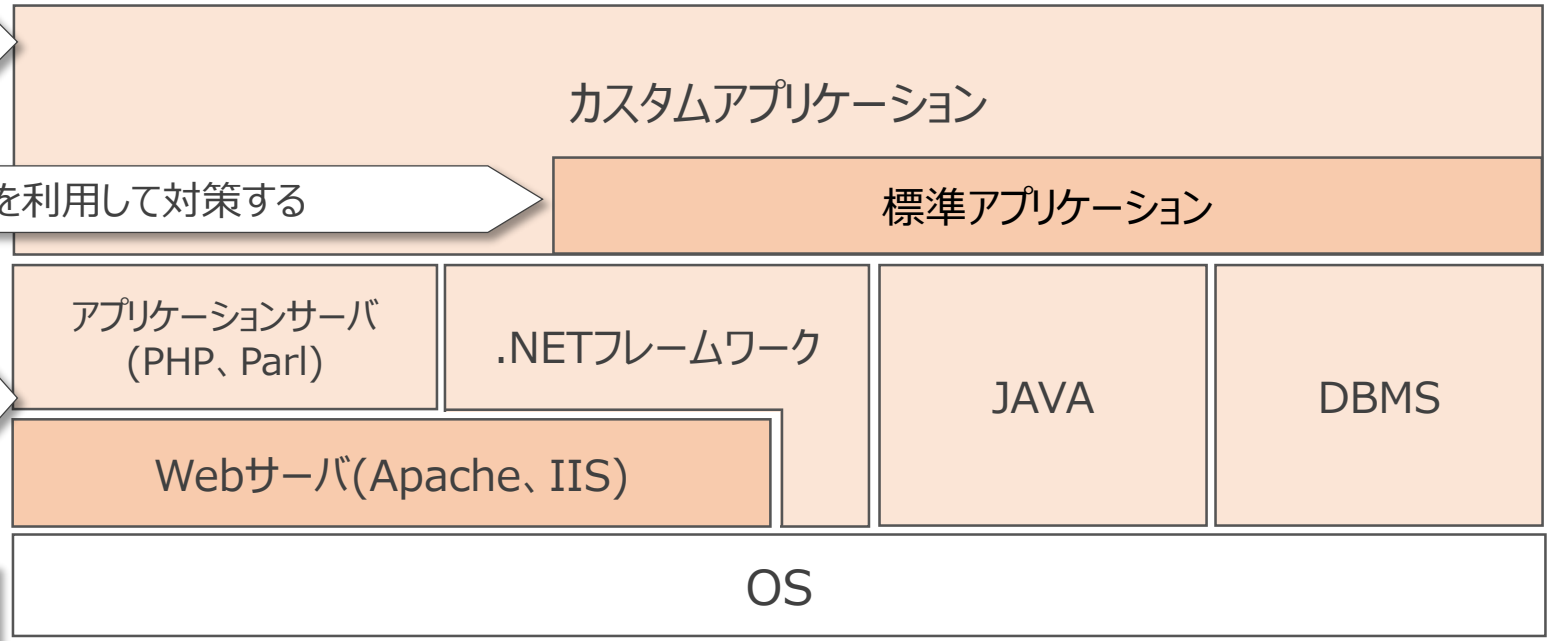
WAFの適応ポイント

アプリケーションの脆弱性を補うのがWAFの役割です。正しいアプリケーション記述と環境設定の下では、本当にWAFが必要でしょうか。WAFの適応は、JAVA、.NETで開発したアプリケーションでなく、プラットフォームそのものの脆弱性に対して行われるべきものです。もちろん、開発規模の大きなアプリケーションでは、WAFの適応はセキュリティ面で大きなアドバンテージになります。

開発者が脆弱性を改版することが可能。アプリケーション規模に応じてWAF利用の検討が必要

アプリケーションの最新バージョンを導入するか、WAFを利用して対策する

各プラットフォームの最新パッチを導入するか、
WAFを利用して対策する
※WAFの活用効果が高いソフトウェア レイヤ



が対策の必要なサービスやアプリケーションです。
OWASPとKEMPのコマーシャルルールには、標準アプリケーション向けルールセットが豊富に用意されています。また、IIS向けには、KEMPコマーシャルルールで対応可能です。

Apache Struts2の対策

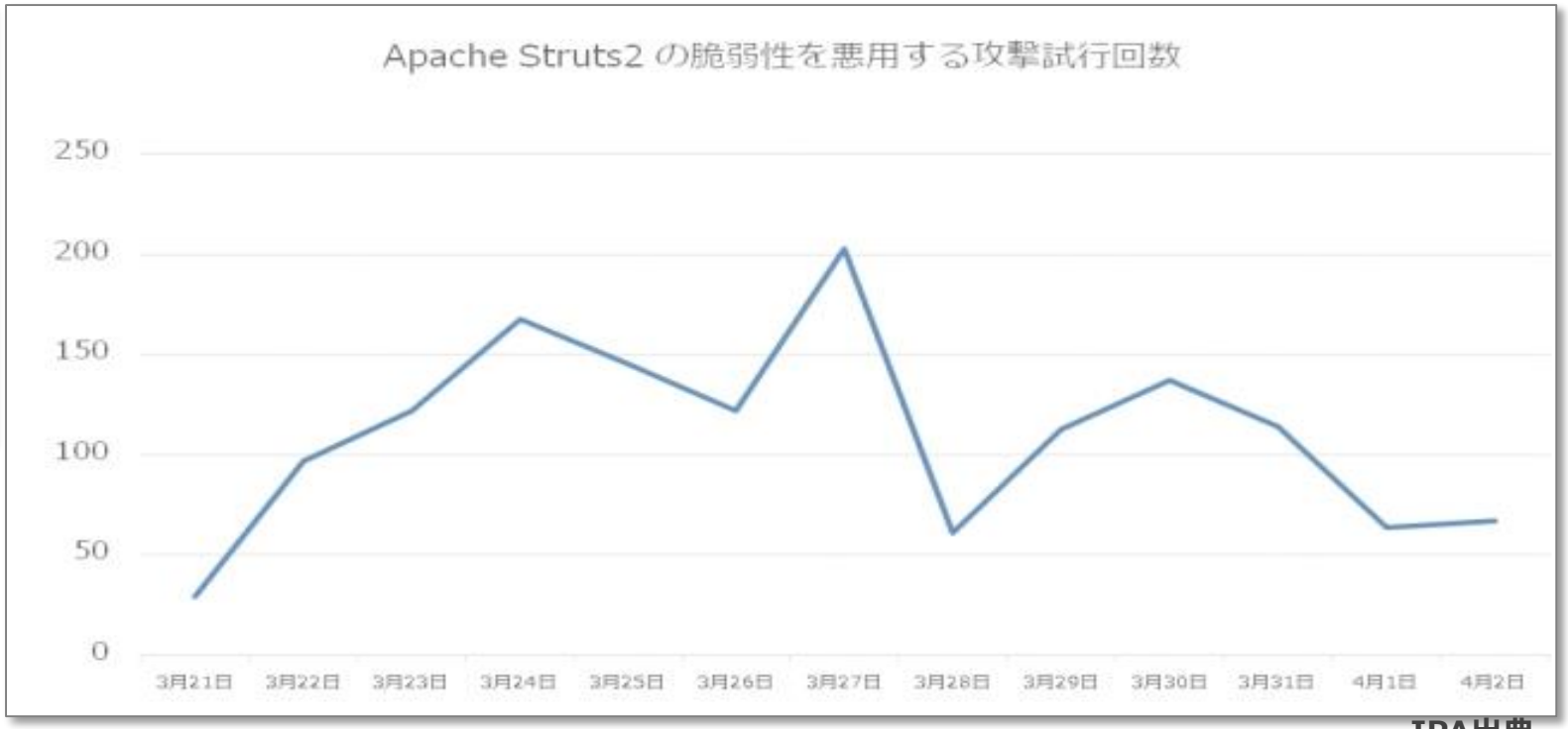
Apache Struts2は、システム プラットフォームの脆弱性を狙われ、多くのサイトで被害報告がありました。脆弱性の発見と発表、被害の発生状況の時間の流れが、発表された脆弱性をどのように対応すべきかを明快に示しています。

▲ 脆弱性の発見　▲ 脆弱性を修正する　▲ パッチファイルのリリース　▲ 脆弱性情報を公開　▲ 脆弱性を狙った攻撃数が急増する

Apache Struts2の脆弱性は、日本ではIPAが3月10日頃に発表しました。この時点で、脆弱性に対応したパッチは存在していますので、ユーザは発表直後に直ちにパッチ対応ができます。

一方で、右のグラフはIPAがまとめたApache Struts2の攻撃状況です。3月21日頃から攻撃数が急激に増加しています。

■この表は脆弱性が発表された後には、いかに素早く対応が必要化を物語っています。



IPA出典

New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

Apache Struts2の対策

Apache Struts2の脆弱性は、JAVA用フレームワークに存在しており、プログラミングで対応できる性格のものではありません。こういった脆弱性は、フレームワークのバージョンアップかWAFの利用でのみで解決が可能です。

短期間の対応と柔軟性

- WAFによる脆弱性対応は、プログラムコードの追加・変更を伴いません。攻撃パターンを示すシグネチャやルールの追加で対応可能です。
- ルール型では、パターンの完全一致を必要としないので、柔軟性の高い防御を行うことができます。

導入時の評価期間

- フレームワークのバージョンアップやパッチは、プログラムコードの変更を伴っていますので、導入時の評価は避けて通れない課題です。
- KEMPのWAFルールは、日々の追加と修正でタイムリーな対応を可能にします。

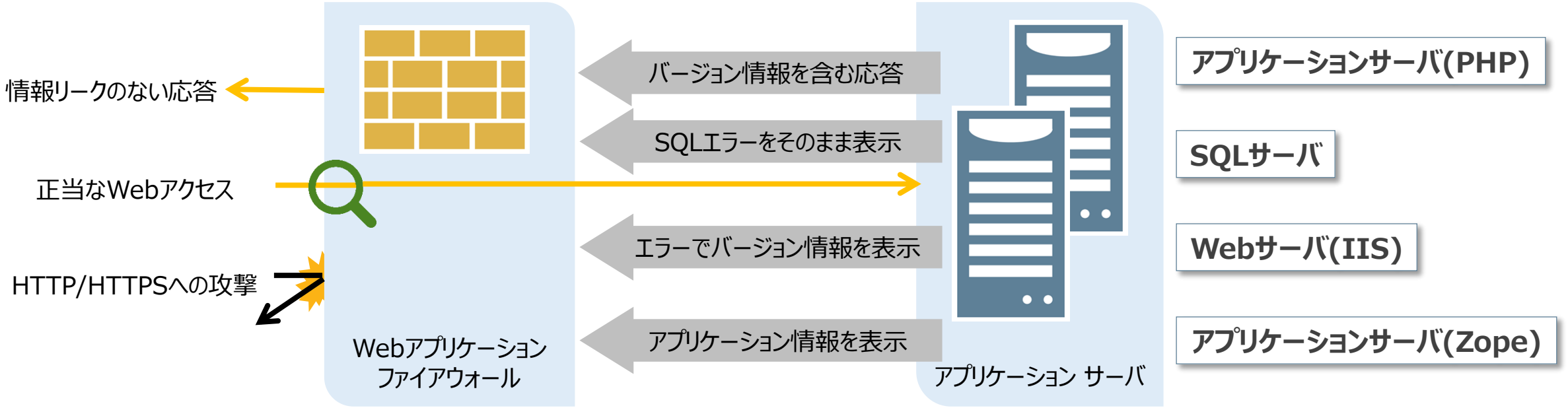
OWASPがベース

- KEMPが提供するWAFルールは、Webセキュリティの研究機関であるOWASPのルールがベースです。
- OWASPは、アプリケーションセキュリティの改善に対し、人、プロセス、技術的問題の面からアプローチし、効果的な改善手法を提唱しています。

脆弱性対策の手順	
1. 脆弱性公開で緊急の対応	WAFルールの改版で、短期間に脆弱性対応を実施し、情報公開後の急激な攻撃の増加に対応します。
2. パッチ/バージョンアップによる対応	フレームワーク ベンダーが提供するパッチや新バージョンを導入し、時間を掛けて動作検証を実施します。

インバウンドとアウトバウンド

WAFは、インバウンドトラフィックだけを対策するものではありません。レスポンスパケットに対しても情報漏洩の対策が必要です。
Webサーバが表示するエラーメッセージにはバージョン情報が含まれるケースが多くあり、対策が必要になります。



New York: 631-345-5292 • Limerick: +353-61-260-101 • Hannover: +49-511-367393-0 • Singapore: +65-62222429 • Tokyo: +813-6820-0302

レスポンスヘッダの活用

最新のブラウザソフトウェアでは、XSS(クロス サイト スクリプティング)などを対策するための機能が備わっています。この機能はレスポンス ヘッダの設定で有効にできますので、アクセスユーザのセキュリティのために積極的に活用することが望まれます。

主なレスポンスヘッダ リスト		
X-Frame-Options	DENY/SAMEORIGIN	フレーム内にページ表示を制御するヘッダです。悪意のあるページの隠蔽を防ぎます。
X-Content-Type-Options	nosniff	コンテンツタイプと一致しない動作を制限して、意図しない動きを回避します。スクリプト、スタイルシートに適応されます。
X-XSS-Protection	1 (フィルタ有効)	ブラウザのXSSフィルタ機能を有効にします。

ブラウザ別レスポンスヘッダ対策リスト(出展 IPA)				
	Firefox 4	Safari 5	Chrome 4	IE 8
X-XSS-Protection		✓	✓	✓
X-Frame-Options	✓	✓	✓	✓
X-Content-Type-Options			✓	✓

レスポンスヘッダの加工は、本来アプリケーションでおこないますが、運用中であったり、コード量が多い場合などでは、加工を設定することが有効です。レスポンスヘッダは、LoadMasterのコンテンツルールの機能で加工できます。
ヘッダの加工では、HTTPヘッダ インジェクションというハッキング手法がありますので、これを排除するためのヘッダ加工も有効です。

PCI DSS

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

PCI DSSへの対応

2018年3月末までに、クレジットカード会社や決済代行会社、加盟店に対してPCI DSS(Payment Card Industry Data Security Standard)の準拠が求められています。これは、会員カードデータの取り扱いを主眼に、システム構成、データの取扱と運用を規定した基準です。システム面での準拠では、WAFの導入や暗号化方式が重要なポイントに成ります。

安全なネットワーク構築

要件1、要件2

- ファイアウォールによるインターネット、イントラネット、 DMZの安全な配置が求められます。
- 不正ネットワークからのアクセスを排除する必要があります。

会員データの保護

要件3、要件4

- 会員データの安全な保管と暗号化、鍵の管理などの機密性が求められます。
- 通信の暗号化と共にPANの非表示なども必要になります。

脆弱性を管理

要件5、要件6

- アプリケーションのウィルス対策やOSの脆弱性対策が求められます。
- OWASP top10への対応もポイントで、暗にWAFの導入を求めています。

強力なアクセス制御

要件7、要件8、要件9

- アカウント/パスワードの認証とその方式について求めています。
- 2要素認証などのより強固な認証方式が必要になります。

ネットワークの監視

要件10、要件11

- 不正アクセスを発見するためのログ監視など、運用面での要件です。
- 定期的な脆弱性診断で、常に最新の強固な運用を求めています。

ポリシーの整備

要件12

- セキュリティポリシーを明らかにし、インシデント発生時の対応など、アクションプランを明確にする必要があります。

アプリケーション脆弱性対策

アプリケーションの脆弱性は、ソフトウェア開発時におけるコーディング技法や開発者の安全性に対する意識づけなどを提起しています。しかし、具体的な手法については OWASP top10 などの指針を要件としています。KEMPのWAFは、OWASP ModsecurityのCRSを活用できるので、LoadMasterを導入することで脆弱性の対策を実現できます。

PCI DSS要件6.5

※開発者に安全なコーディング技法のトレーニングをする

※一般的なコーディングの脆弱性を避け、機密データをメモリで扱う方法を理解することを含め、安全なコーディングガイドラインに基づいてアプリケーションを開発する

- 開発者のスキルとセキュリティへの意識の高さを求めた要件であり、ハードルが高いと考えられます。

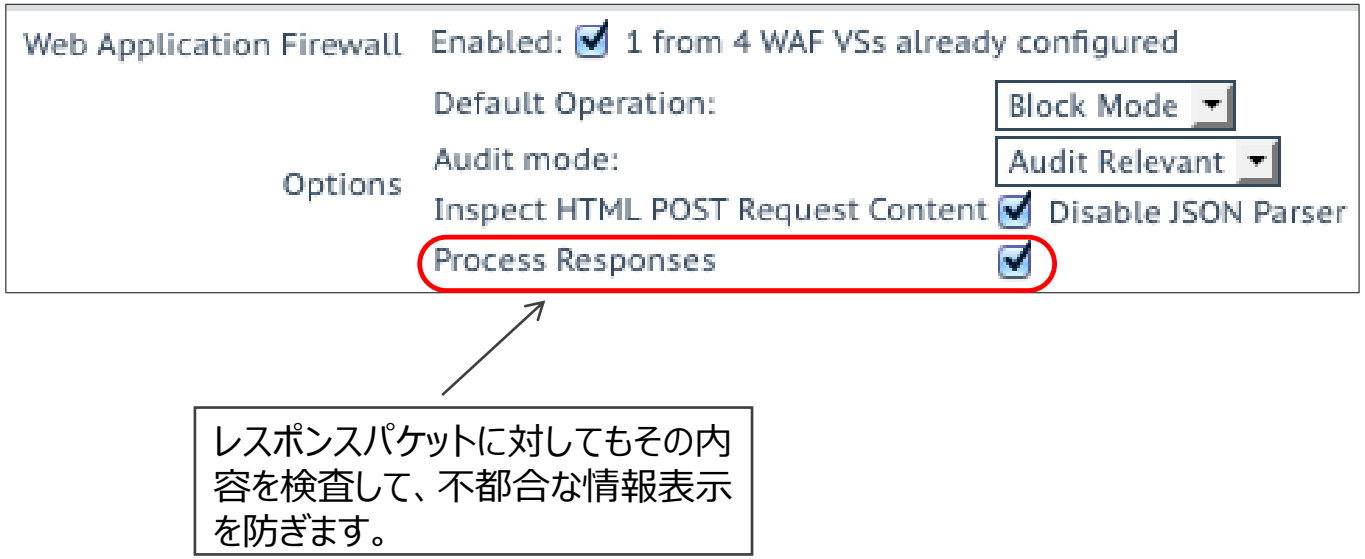
要件6.5.1～6.5.10

- 具体的な攻撃やソフトウェア、データ管理の危険性を定義しています。
- 攻撃手法(6.5.1、6.5.2、6.5.5、6.5.7、6.5.8、6.5.9など)については、OWASP top10に定義されている内容と同等のものです。

OWASP top10	
A1	インジェクション
A2	認証とセッション管理の破壊
A3	クロスサイト スクリプティング
A4	不確かなオブジェクトの参照
A5	セキュリティのミス設定
A6	機密データの露出
A7	機能レベルのアクセス制御ミス
A8	クロスサイトリクエスト フォージェリ
A9	既知脆弱性コンポーネントの利用
A10	無効なリダイレクションと転送

ユーザデータの非表示

一般的に、PAN(Primary Account Number)と呼ばれるカード会員番号を非表示にすることが重要な対策です。Webアプリケーションでは、レスポンスパケットのボディに含まれる情報で、WAFによる対策が難しいとされています。OWASP Modsecurity CRSとKEMPコマーシャル ルールには、カード番号をマスクするアルゴリズムを用意しています。



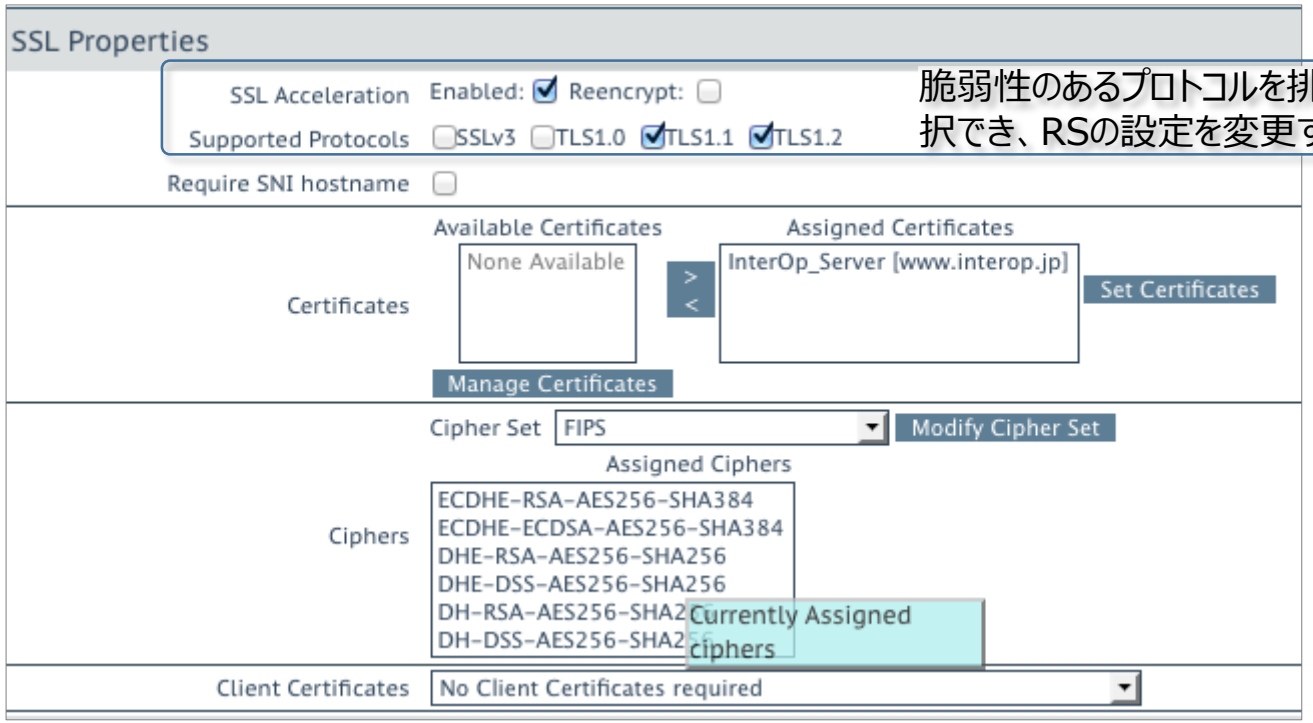
レスポンスパケットに対してもその内容を検査して、不都合な情報表示を防ぎます。

PANの非表示

- OWASP Modsecurity CRSとKEMPのコマーシャル ルールには、PANを読み取るルールが用意されています。
- カード会員番号は、カード会社により規格が異なっており、標準で以下のカード会社に対応しています。
- Master Card、Visa、American Express、
- Diners Club、enRoute、JCB、Discover

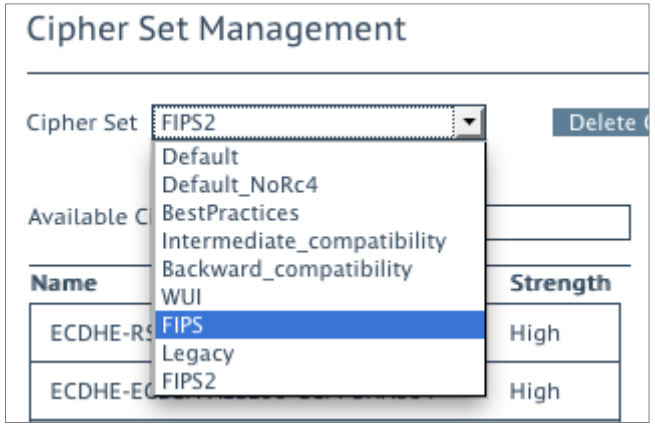
強固な暗号化方式

インターネット経由のアクセスはSSL/TLSを用いて暗号化することを求めています。しかし昨今、SSL 1.2やTLS 1.0などの脆弱性が明らかになり、一部の暗号化アルゴリズムについても脆弱性を指摘されています。LoadMasterはアプリケーションフロントとして、脆弱性のあるプロトコルやアルゴリズムを排除し、安全なプロトコルと暗号化アルゴリズムで運用を可能にします。



脆弱性のあるプロトコルを排除した設定が可能です。サービスシステムに対応して任意にプロトコルを選択でき、RSの設定を変更することなく集中した設定管理が可能になります。

脆弱性を指摘されたCipherを排除し、使用目的に適合したCipherの選択が可能で、セキュリティ強度を任意に設定できます。



あらかじめ、Cipher Setの選択肢が用意されているので、複雑なCipher Suiteのリスト選択の必要がありません。セキュリティ強度に応じた絞り込みが可能です。

PCI DSS対策

WAF機能を実装したLoadMasterの導入で、PCI DSSの要件の多くの部分をクリアすることが可能になります。OWASP Modsecurity CRSにより、ハードルの高いプログラミング要件の多くをクリアし、既存資源を有効に活用することができます。

安全なネットワーク構築

要件1、要件2

- IPレピュテーションに対応したルールセットが供給可能で、不正ネットワークからのアクセスを排除できます。
- アクセスポートが限定されますので、抜けの無い経路構築が可能です。

会員データの保護

要件3、要件4

- 簡単に脆弱性のあるCipher Suiteを排除でき、強固な暗号化を可能にします。
- WAF機能によりPANの非表示にも対応します。

脆弱性を管理

要件5、要件6

- OWASP Modsecurity のCRSが使用可能で、容易にOWASP top10対応が可能です。
- プログラミングもWAFの導入で多くの対策が可能です。

強力なアクセス制御

要件7、要件8、要件9

- LoadMasterのエッジセキュリティ機能は、複数の認証方式に対応します。
- 2要素認証などのより強固な認証方式もサポート可能です。

ネットワークの監視

要件10、要件11

- 不正アクセスを発見するためのログ監視など、運用面での要件です。

ポリシー整備

要件12

- セキュリティポリシーを明らかにし、アクションプランを明確にします。

LoadMasterの選択

url https://kemptechnologies.com/
mailto: japan@kemptechnologies.com

WAFはスモールスタートで

WAF導入ではセキュリティ対策やパフォーマンスなど、多くの問題をクリアする必要があります。また、高度化するハッキング手法に常時対処しなければなりません。WAFは、日々の運用の積み重ねでその性能を向上し、強力な防御システムになります。

システム増強

■ ルールの増加や高度化でWAFエンジンを増強していきます

安定運用

■ NOC(SOC)との連携が機能し効率よく新ルールの追加ができます

WAF導入

■ ミニマムなWAFエンジンと最小限のルールセットで最大の効果を得る設計で導入します

WAFエンジン実装モデル(仮想)

LoadMasterでWAF機能を利用するには、LoadMasterのライセンスがあれば、ミニマムスタートが可能です。その後、ご予算と運用要件で最適な組合せを選択できます。

モデル	ライセンス	スループット	SSL処理	KEMP コマーシャル ルール	Modsecurity CRS
Free LoadMaster	フリーライセンス	20Mbps	50TPS	–	✓
VLM-200	使用ライセンス	200Mbps	200TPS	✓	✓
VLM-2000	使用ライセンス	2Gbps	1000TPS	✓	✓
VLM-5000	使用ライセンス	5Gbps	10000TPS	✓	✓
VLM-10G	使用ライセンス	10Gbps	12000TPS	✓	✓

※ 使用ライセンスでは保守ライセンスを併せて購入する必要があります。
※ KEMPコマーシャル ルールは、エンタープライズ プラスのサブスクリプション契約が必要です。

WAFエンジン実装モデル(クラウド)

LoadMasterでWAF機能を利用するには、LoadMasterのライセンスがあれば、ミニマムスタートが可能です。その後、ご予算と運用要件で最適な組合せを選択できます。

モデル	ライセンス	スループット	SSL処理	KEMP コマーシャル ルール	Modsecurity CRS
VLM for Azure Free	フリー	20Mbps	50TPS	–	✓
VLM 200 for Azure	BYOL/Hourly	200Mbps	200TPS	✓	✓
VLM 2000 for Azure	BYOL/Hourly	2Gbps	1000TPS	✓	✓
VLM 5000 for Azure	BYOL/Hourly	5Gbps	10000TPS	✓	✓
VLM 10G for Azure	BYOL/Hourly	10Gbps	12000TPS	✓	✓

※ BYOLでは保守ライセンスを併せて購入する必要があります。
※ KEMPコマーシャル ルールは、エンタープライズ プラスのサブスクリプション契約が必要です。

WAFエンジン実装モデル(ベアメタル)

LoadMasterでWAF機能を利用するには、LoadMasterのライセンスがあれば、ミニマムスタートが可能です。その後、ご予算と運用要件で最適な組合せを選択できます。

モデル	ライセンス	スループット	SSL処理	KEMP コマーシャル ルール	Modsecurity CRS
LMB-1G	使用ライセンス	1Gbps	1000TPS	✓	✓
LMB-2G	使用ライセンス	2Gbps	1000TPS	✓	✓
LMB-5G	使用ライセンス	5Gbps	10000TPS	✓	✓
LMB-10G	使用ライセンス	10Gbps	20000TPS	✓	✓

※ H/Wアプライアンスでは保守ライセンスを併せて購入する必要があります。
※ KEMPコマーシャル ルールは、エンタープライズ プラスのサブスクリプション契約が必要です。

LoadMasterトライアル

Azure フリー版LoadMasterのデプロイ

https://azure.microsoft.com/ja-jp/marketplace/partners/kemptech/vlm-azure/からデプロイできます。
AzureのアカウントとKEMP IDが必要です。

フリー版LoadMasterのダウンロード

http://freeloadbalancer.com/download/からダウンロードができます。ダウンロードにはKEMP IDがが必要です。

評価版LoadMasterのダウンロード

https://kemptechnologies.com/ja/vlm-download/からダウンロードができます。
ダウンロードにはKEMP IDが必要です。

KEMP IDの取得

同じページに、新規にKEMP IDを取得するためのダイアログがあります。

KEMPのご紹介

APPLICATION DELIVERY

眠らない街ニューヨークに本社があること。
24時間365日、覚醒し、働き続けるアプリケーションをロードバランサで支えることが私たちの使命だからです。

会社概要

KEMP Technologies社は、アメリカ、ヨーロッパ、アジア、南アメリカで30,000以上の導入実績を持つ、先進的なL2～L7 ADC(アプリケーションデリバリ コントローラ)とアプリケーション ロードバランシングのリーダカンパニです。
KEMPは2000年より、高性能ADC、仮想アプライアンス、アプリケーションセントリックなSDNとNFV構築、リーズナブルな価格のライセンスモデル、企業が求める多様なサイズへの対応、といった多くの分野でリーダとしての揺ぎないポジションを築いてきました。

KEMP アプリケーションセントリック ロードバランサ

- Webとアプリケーション構築の最適化： ハイパフォーマンス、柔軟性、拡張性、安全性を分かり易い管理方式で実現します。
- 仮想システム管理者： システム制御と結果予測を容易にし、アプリケーションの可用性とQoEを高い次元で提供します。
- アプリケーション環境： 最適化と高可用性の実現でTOCを大幅に削減します。

私たちの製品は、フォーチュン50社で分類する企業、リモートオフィス接続、MSP、教育/公共の分野で広く利用されています。
KEMPは、ニューヨーク本社とリメリック(アイルランド)、ミュンヘン(ドイツ)、シンガポールの各地域にサポートサービスの拠点を持っています。

History

KEMP
APPLICATION DELIVERY

2014	■ KEMPは、北米において、テクノロジー分野で最も成長した企業として挙げられました。(デロイト：成長率499.1%) ■ WAF(Webアプリケーション ファイアウォール)機能を持ったパッケージをリリースしました。 ■ SDNに対応した負荷分散方式をリリースしました。HPのSDN Ecosystemに対応します。 ■ HyperFlexアーキテクチャをもつCondor ADCをリリースしました。これは マルチテナントアプリケーションデリバリとNFVサービスチェーンに対応します。
2013	■ マイクロソフトAzure版のフル機能L7 ADCをリリースしました。 ■ フェールオーバ/フェールバックアプリケーション(Exchange) GSLBをリリースしました。
2012	■ Mr. Ray DownesがCEOになりました。 ■ KEMPは本社をニューヨークに、APAC本社をシンガポールにオープンしました。 ■ KEMPは、インサイトでのエンジニアサポートサービスを開始しました。(北米のみ)
2011	■ KEMPは、 120%の売上の伸びを実現しました。. ■ Edison Ventures、Kennet Partners、Orix Venture FinanceがKEMPのバイアウトを締結しました
2010	■ KEMPは、EMEA本社をアイルランドの リメリックにオープンしました。 ■ KEMPは、Hyper-Vの商業的サポートで最初のADCベンダーになりました。
2009	■ KEMPは、VMWare向けのADCを最初にリリースしました。 ■ KEMPは、SPLAの販売モデルを最初にリリースしました。
2008	■ KEMPは、ターミナルサービスのサポートでマイクロソフトとパートナーシップを組みました。 ■ KEMPは、SSLアクセラレーション、IPSエンジン、エッジセキュリティなどによりADCの分野に移行しました。
2007	■ エンタープライズ需要を見据えたLoadMaster 5500をリリースしました。
2005	■ KEMPは、Brainforce Software GmbH (Munich)とのパートナーシップで、最終的に負荷分散ソフトウェアのソースコードを取得しました。