KEMP | APPLICATION DELIVERY

Solution Catalogue

Web セキュリティ 5 つのポイント

インターネット上でサービスする Web アプリケーションは、常にハッカーの脅威に晒されています。
ハッカーの脅威は、Web アプリケーションの問題を排除しただけでは解決しません。サーバ ソフトウェアとサーバ OS の弱点を取り除き、ユーザが使用するブラウザ ソフトウェアに対しても、適切な働きかけが重要です。サーバのみならず、ユーザの安全も保障することが Web セキュリティの重要な要件です。

LoadMaster
&
Application Firewall Pack

▲ Web セキュリティの対策ポイント

項 目	概 要
汎用アプリケーション対策	• Web サーバや汎用アプリケーションには、既に脆弱性があるものが多々あります。また、オープン系ソフトウェアとアプリケーションでは、新たな発見で周知されるものも多数あります。 • 特にオープン系ソフトウェアの脆弱性は、周知された情報でありため、常に対策済みバージョンの利用が望まれます。
カスタムアプリケーション対策	• オリジナルサービスのために開発したアプリケーションにも、問題は潜んでいます。 • ソフトウェア開発プラットフォームの問題で脆弱性になるケースもあり、日々の問題把握と対策が望まれます。
暗号化の脆弱性対策	• SSL 暗号化でサービスを提供しているサイトでも、暗号化アルゴリズムに問題がある場合は、暗号化そのものが攻撃対象になってしまいます。 • Cipher Suite と呼ばれる暗号化アルゴリズムで、脆弱性のあるものを排除した SSL サービスを提供しなければなりません。
レスポンスヘッダ対策	• 最新の Web ブラウザは、セキュリティ強化のためのオプションを備えており、レスポンス ヘッダでその機能をコントロールできます。 • XXS や悪意のあるページ隠蔽などを防ぐためのヘッダで応答することは、サービスの品質にもつながる重要な行為です。
バージョン情報漏洩対策	• オープン系のソフトウェアでは、バージョン情報を表示する設定になったものがあります。バージョン情報によっては脆弱性が明らかなものがあり、ハッカーに狙われやすくなります。 • ソフトウェアとそのバージョンを表示しないように、Web サーバなどの設定を変更する必要があります。

汎用アプリケーション対策

CMS や EC 等の汎用アプリケーションは、Web サービス構築で重要なツールですが、脆弱性も多く、攻撃対象になり易い問題があります。バージョンアップが難しい場合、LoadMaster + WAF での対策が最適です。

カスタムアプリケーション対策

開発プラットフォームの脆弱性と開発したコードの 2 つの問題が存在する可能性があります。コードの見直しが正しい改善ですが、コストとの兼ね合いで LoadMaster + WAF の導入も検討されてはいかがでしょうか。

暗号化脆弱性対策

SSL 通信で使われる Cipher Suite の脆弱性は見落としがちです。Web サーバで問題のある Cipher Suite を排除するか、KEMP LoadMaster で調整することをお薦めします。

レスポンスヘッダ対策

HTTP ヘッダの設定は Web サーバの役割ですが、LoadMaster でも HTTP ヘッダの任意に加工することができます。WAF 導入と合わせてご利用いただくと、コスト面で有利な対策です。

バージョン情報漏洩対策

バージョン情報の隠蔽は重要なソリューションです。LoadMaster + WAF では、アウトバウンド メッセージのチェックが可能ですので、バージョン情報をマスクすることが可能です。

Cipher Suites: SSL 通信で、実際のコンテンツを交換するための暗号化アルゴリズムです。多くの暗号化技術が使われていますが、一部に脆弱性を持ったものがあり、使用を避けることが望まれています。

XSS: 掲示板など、ユーザの書込みを許可するサイトにスクリプトを入力して、一般ユーザを悪意のあるサイトに誘導する攻撃手法です。

(Corporate HQ) 600 Fifth Ave. New York, NY 10020 |
KEMPTechnologies.com

KEMP | APPLICATION DELIVERY

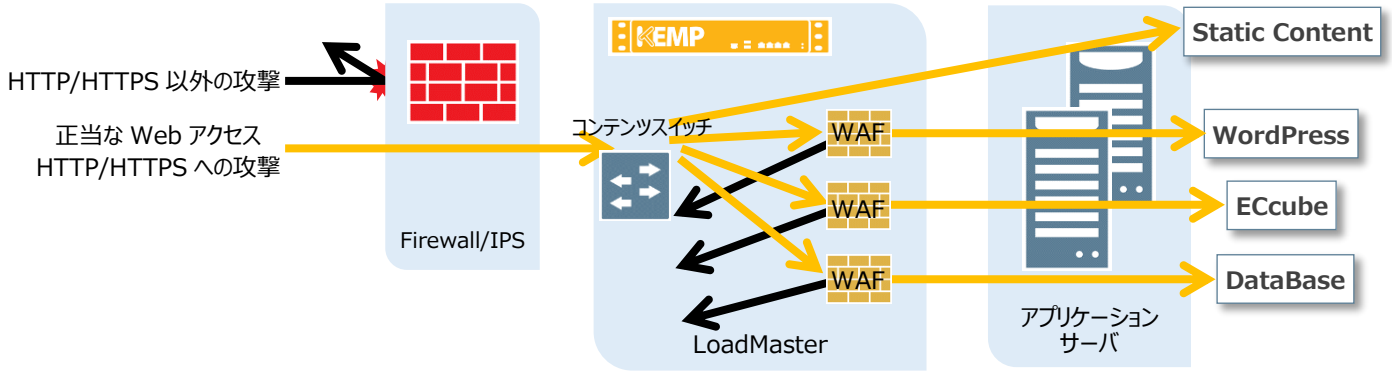
KEMP WAF Solution

Solution Catalogue

WAF 導入のポイント

LoadMaster が標準で実装する WAF(Web アプリケーション ファイアウォール)エンジンは、アプリケーション ソフトウェア単位に複数インスタンスを構築することができます。各インスタンスには、担当するアプリケーションの脆弱性に応じてルールセットを設定できますので、スループットの劣化を最小限にした効率のよいメッセージの問題監査ができます。

WAF のルールには、サブスクリプション契約による KEMP コマーシャル ルールと OWASP が提供する CRS(コア ルール セット)を使用できます。KEMP コマーシャル ルールはアプリケーション別にルール選択が可能で、ルールセットを簡単に導入できます。CSR は OWASP がフリーで提供するルールセットですが、ルール設定などに独特のノウハウが必要ですので導入のための支援プログラムを用意しています。



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。

レスポンスヘッダー対策

最新の Web ブラウザは、セキュリティ強化のためのオプションを備えており、レスポンス ヘッダでコントロールすることができます。WAF によるプロテクションだけでなく、レスポンス ヘッダをチューニングすることで、信頼性の高いサービスサイトが構築できます。

X-XXS-Protection	Web ブラウザの XSS フィルタ機能を強制的に有効にします。
X-Frame-Options	Frame、iframe オプションを無効にして、悪意のあるページの隠蔽を防ぎます。
X-Content-Type	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。

Cipher Suite の対策

SSL 通信で、メッセージ交換のための暗号化方式は多くありますが、脆弱性が指摘されている方式では、利用が推奨されません。このため、Web サーバの設定では、RC4 や CBC などで脆弱性が指摘されている方式を外す必要があります。KEMP LoadMaster を利用すると、推奨する Cipher Suite をリスト化していますので、セキュリティポリシーに合わせてリストを選択し、その後詳細にチューニングすることが可能です。これにより、複雑な Cipher Suite の設定の負荷を大幅に軽減することができます。

オーダリング情報(バーチャル アプライアンス モデル)

Virtual LoadMaster 本体	VLM-200	仮想マシン本体ライセンス。保守ライセンスを同時にご購入ください
スタンダード保守	VLM-200 J-Standard	平日日勤帯の e メールと電話サポート、ソフトウェア保守サービス
エンタープライズ 保守	VLM-200 J-Enterprise	7x24 の e メールと電話サポート (英語)、ソフトウェア保守サービス ESP(エッジセキュリティ)のサブスクリプション ライセンス
エンタープライズ プラス保守	VLM-200 J-Enterprise+	7x24 の e メールと電話サポート (英語)、ソフトウェア保守サービス ESP(エッジセキュリティ)、WAF ルールアップデート、GSLB の各サブスクリプション ライセンス

※サイトのトラフィック量に応じて、複数のスループットモデルをご選択いただけます。

FXC 株式会社
〒111-0043 東京都台東区駒形 1-3-14 駒形 TC ビル
tel. 03-5827-0745

(Corporate HQ) 600 Fifth Ave. New York, NY 10020 |
KEMPTechnologies.com