LMS に最適な負荷分散装置
ーTLS/SSL 管理を容易にー

HTTPS 化 -盗聴・改ざん・なりすましの危険-

昨今、**LMS(学習管理システム)**の多くはインターネット上に公開されており、攻撃者からの盗聴・改ざん・なりすましといった脅威に対する対策として、**HTTPS** で提供されています。

HTTPS の課題

HTTPS 通信であれば必ず安全が保障される訳ではありません。暗号スイート(Cipher Suite)[1]と呼ばれる複雑な要素の組み合わせのうち**脆弱性**が指摘されている暗号化アルゴリズムを設定してしまった場合、結局は盗聴などの危険に晒される可能性があります。クライアント-サーバ間の鍵交換で使用される暗号化アルゴリズムや、アプリケーションデータ保護用の共通鍵(もしくはそのブロックモード)で使用されるアルゴリズムなどに脆弱性が報告されており、管理者は暗号スイートに注意を払う必要があります。

容易なオペレーションで脆弱性を排除

ADC(ロードバランサ)ベンダーである **Kemp Technologies** 社の **LoadMaster** を導入することでこれらの課題が解決できます。

SSL/TLS のチューニングに関し、**LoadMaster** では環境に応じて適切な暗号スイートをいくつかまとめた**推奨グループ**(Cipher Set)を簡単に選択できます。特に昨今注目されている暗号化アルゴリズムとして、**暗号鍵漏洩時の対策**がなされた**楕円曲線暗号**の **DHE と ECDHE**、署名アルゴリズムとして既存のものよりも**処理性能が高い**とされる **ECSDA** があります。これらを含む暗号スイートのみで構成された ECSDA_BestPractices のようなグループを選択することにより **LMS・HTTPS 環境での脆弱性を容易に排除することができます。**他にも、上記と合わせて 10 以上の推奨グループの中から選択することができます。もちろん管理者が自由に暗号スイートを選択することも可能です。

選択可能な推奨グループ一例

Cipher Set 例	Best Practices	ECSDA_BestPractices
説明	高いセキュリティを担保しつつ、署名アルゴリズムは多くのクライアントが使用できる RSA を許容	Best Practices から RSA 証明書を使用する Cipher Suite を除外

TLS1.3

Kempは最新のTLSプロトコルバージョンである**TLS1.3**を他ベンダーと比較してもいち早く実装しています(ハードウェア版、仮想マシン版両方に対応)。TLS1.3 を導入することにより TLS プロトコルレベルにて、**脆弱なハッシュ関数・ブロック暗号モードを排除**します。また以前のプロトコルバージョンと比較しても RTT(ラウンドトリップタイム)が改善し、体感的な速度の向上が期待できる等のメリットもあります。

1 SSL/TLS 通信で使用される鍵交換方式、署名、アプリケーションデータ暗号化の共通鍵、メッセージ認証コードの組み合わせ。クライアント側使用のスイートと同一のものが双方で最終的に使用される。

データシート

LMS に最適な負荷分散装置
ーTLS/SSL 管理を容易にー

管理ポイントを一か所に統合

LoadMaster 導入により、複雑な SSL/TLS の設定を一か所に統合します。管理が容易になることに加え、CPU タイムを多く消費する暗号化処理からリアルサーバ(実サーバ)のオーバーヘッドを開放します。

TLS1.3 対応サイトとして提供

実サーバ側が TLS1.3 などのプロトコルに未対応であっても、LoadMaster がクライアント-サーバの間に入ることでサービス利用者に最新のプロトコルでのサービス提供が可能なります。

主な性能

TLS1.3 や HTTP/2 にも対応

<ハードウェア版ラインナップ>	LM-X1	LM-X3	LM-X15	LM-X25	LM-X40
スループット	1Gbps	3.4Gbps	15Gbps	25Gbps	40Gbps
SSL トランザクション処理（TPS）	1,000	1,700	12,000	20,000	35,000
バルク暗号化	1 Gbps	2Gbps	8Gbps	20Gbps	20Gbps
同時接続数（L4）	4,000,000	8,600,000	35,000,000	75,800,000	75,800,000

※別途保守契約を結ぶ必要がございます、詳細な内容に関しては別途お問い合わせください。

<仮想マシン版ラインナップ>	VLM-500	VLM-3000	VLM-MAX
スループット	500Mbps	3Gbps	無制限
SSL トランザクション処理（TPS）	500	4,000	無制限
同時接続数（L4）	3,000,000	3,000,000	無制限

SSL/TLS 通信に関しハイパフォーマンス

※アプライアンスモデル(永続ライセンス)にて購入する場合は別途保守契約を結ぶ必要がございます。詳細な内容に関しては別途お問い合わせください。
※サブスクリプションモデルの購入体系もございます。
※性能は仮想マシンのリソース割り当てなどに左右されます。サイジングの目安に関しては別途お問い合わせください。

FXC 株式会社は日本総代理店として Kemp LoadMaster シリーズを販売しております。
お見積り、評価版仮想マシン、その他お問い合わせは以下までお願いいたします。

sales_dep@fxc.jp
kempmarket@fxc.jp

FXC 株式会社
〒111-0053 東京都台東区浅草橋 3-20-15 浅草橋ミハマビル
tel. 03-6823-6185