2011 年 2 月 15 日
株式会社 パイオリンク

SSL 公開鍵長の 2048 ビット移行と SSL パフォーマンス問題

暗号アルゴリズムの 2010 年問題に、ＳＳＬ ＴＰＳパフォーマンス低下率0％
ロードバランサ「PAS 3716-SSL3000」実証結果を発表

1．暗号アルゴリズムの 2010 年問題

インターネット上でのショッピング、個人情報送信や機密文書のやりとり等においては、盗聴や内容の不正改ざんを防ぐために認証やデータの暗号化して通信を行うのが基本となっています。近年、コンピュータ性能の向上と暗号解読技術の進展により従来の暗号技術が破られる危険が高まっています。このような状況の中で米国国立標準技術研究所（NIST）が弱い暗号アルゴリズムを 2010 年末までにより安全な強い暗号アルゴリズムに移行させる方針を打ち出しており、世界的により高い暗号技術への対応が急がれています。
今後、高い暗号技術に移行した場合にインターネット上の暗号技術を支える各種機器においては高い暗号技術への対応は勿論のこと、さらに高い暗号処理能力の実装が求められています。

2．SSL 公開鍵長の 2048 ビット移行に伴う問題

インターネットショッピングや個人情報を入力するなど、インターネット上のセキュリティを確保するために SSL 技術が標準的に使用されています。 SSL 処理には高い処理能力を必要とすることから、サーバの前に位置する負荷分散装置（ロードバランサ）で SSL アクセラレーション処理を行うのが一般的です。
SSL 処理において要求される高い暗号技術として、SSL 公開鍵長を今まで標準的に使用してきた 1024 ビットからはるかに堅牢な 2048 ビットの鍵長に移行することが求められています。
しかし、1024 ビットから 2048 ビットへの移行により、負荷分散装置には高い SSL 処理能力が必要となります。SSL 処理能力としては、SSL TPS と SSL スループットがありますが、鍵長が 2048 ビットに移行することにより大きく影響するのは SSL TPS になります。SSL TPS が影響するのは、新しい接続で SSL 処理を始めるための初期ハンドシェイク、再ネゴシエーション、及び SSL セッション ID 再利用のみです。

負荷分散装置（ロードバランサ）として SSL 公開鍵長の 2048 ビット化による SSL 処理能力の低下は致命的です。特に、既に SSL を使用しているお客様でこれから「暗号アルゴリズムの 2010 年問題」の対応として SSL 公開鍵を 2048 ビットに移行しなければならない場合、SSL TPS 処理能力の大幅な低下により今まで運用してきたシステムを見直さなければなりません。または、これからシステム導入を進めるお客様にとっては高い処理能力のロードバランサを必要とするのでコストが膨らみます。

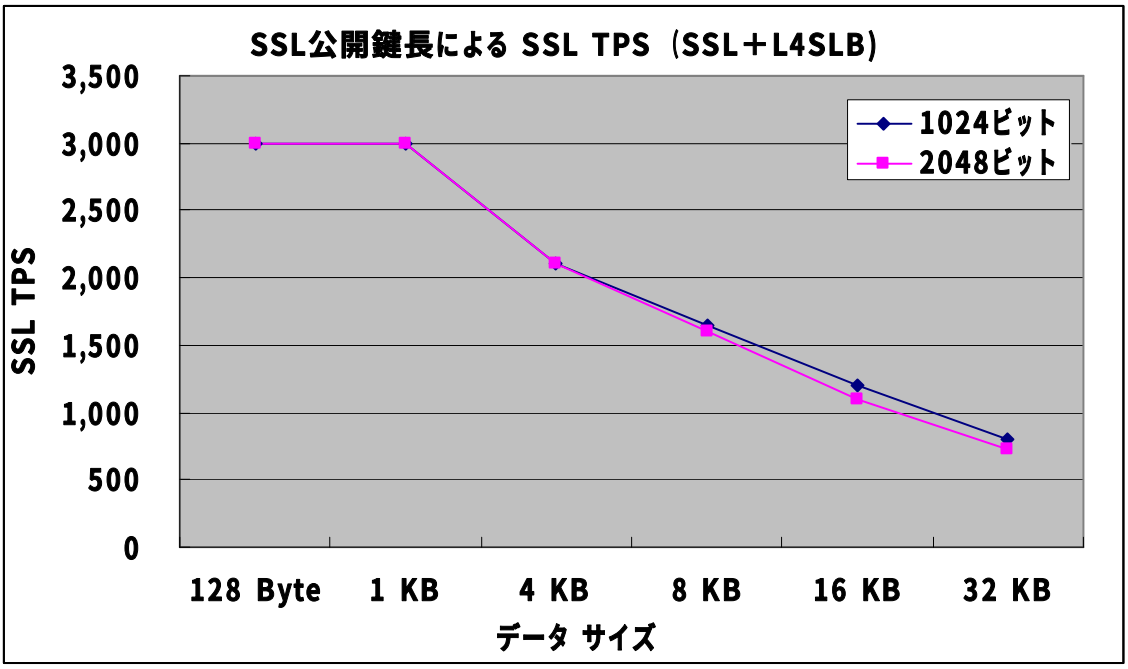
3．PAS における SSL パフォーマンス検証の結果

お客様の「暗号アルゴリズムの 2010 年問題」の対応に役に立てるために、弊社のロードバランサである PAS において SSL 公開鍵長の 2048 ビットへの移行による SSL パフォーマンスについて計測機器を用いて検証しました。検証対象の PAS としては、お客様に一番多く導入されているローエンドのエントリーモデルである「PAS 3716-SSL3000」を用いて実施しました。

■ 測定結果 1 ：「SSL＋L4SLB」機能における SSL TPS

測定対象機器の PAS には、SSL 設定と L4 のサーバ負荷分散機能を定義し一番シンプルなデフォルト設定を行いました。測定時のトラフィックは一番負荷の掛かるシナリオとして、1 SSL トランザクションとして「TCP 接続・SSL セッション接続・HTTP リクエスト・HTTP 応答・SSL 終了・TCP 終了」で定義しました。詳細設定環境及び用語については、本レポートの＜参考 1＞ SSL パフォーマンス検証時の動作環境と＜参考 2＞ 用語の説明を参照してください。

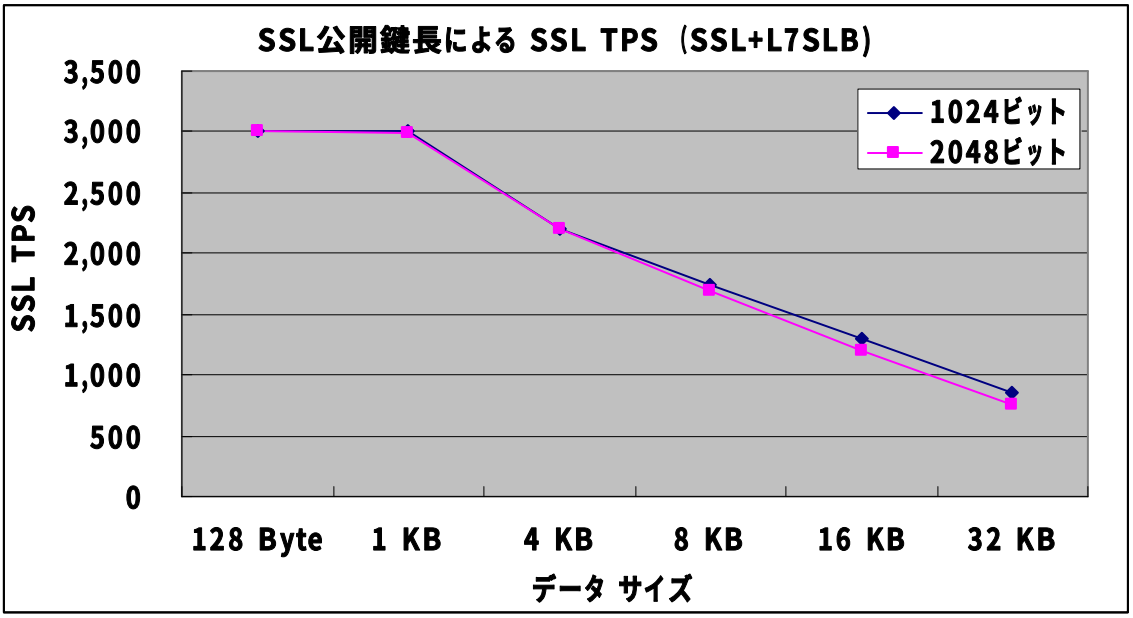
測定結果としては、データサイズが1KB までには鍵長 1024 ビットでも 2048 ビットでも 3,000TPS を維持しています。



■ 測定結果 2 ：「SSL＋L7SLB」機能における SSL TPS

測定対象機器の PAS には、SSL 設定と L7 のサーバ負荷分散機能を定義し一番シンプルなデフォルト設定を行いました。その他の条件は「SSL+L4SLB」と同じです。

測定結果としては、データサイズが 128Byte までには鍵長 1024 ビットでも 2048 ビットでも 3,000TPS を維持しています。



4．SSL パフォーマンスにおける PAS の優位性

PAS における SSL パフォーマンス検証の結果は下記の通りです。

「PAS 3716-SSL3000」は、SSL 公開鍵長が 2048 ビットになっても SSL パフォーマンスの低下はありません。

コストパフォーマンスを提唱する私達パイオリンクにとって、この 2010 年問題及び検証結果はエンドユーザー様の影響範囲が大きいものと捉えました。そこで PAS 製品の特徴である基本に忠実なサーバ負荷分散機能と SSL アクセラレーション機能でシンプルなロードバランサ性能を利用した SSL TPS パフォーマンスは、SSL 公開鍵長が 2048 ビットになっても低下しないことを確認しました。低下率 0％の理由は、CPU のリソース、ハードディスク等のシステムリソースを多く使用する機能が無く、余分なファンクションが現れない事が性能低下を回避し、全てのお客様に PAS 3716-SSL3000 をスペック通り 3000TPS でご提供できる環境を整えました。

なお、今回の SSL パフォーマンス検証においては、エントリーモデルである PAS 3716-SSL3000 を採用しました。他のアプリケーション・スイッチ・ベンダーは上位機種でのパフォーマンステストレポートを公開しているのに対して、弊社はお客様が一番多く導入して頂いているモデルでのパフォーマンステストレポート先に提供することによりお客様の「暗号アルゴリズムの 2010 年問題」対応に役に立つロードバランサベンダーであることに心がけております。

＜参考1＞ SSL パフォーマンス検証時の動作環境

区分	項目	設定内容
Avalanche	S/W バージョン	Avalanche 3.30
	HTTP	HTTP 1.1
	SSL 暗号化アルゴリズム	RC4-MD5
	データサイズ	128Byte, 1KB, 4KB, 8KB, 16KB, 32KB
	HTTP Cookie	使用しない
	SSL バージョン	SSL v3 / TLS v1
	SSL セッション ID 再利用	使用しない
	Client IP 個数	200個
PAS	製品モデル名	PAS 3716-SSL3000
	SSL ライセンス	3000 TPS
	公開鍵長 (SSL key)	RSA 1024 ビット、2048 ビット
	SSL セッション再利用	使用しない
	L4SLB 対象のサーバ数	7個
	L7SLB 対象のサーバ数	7個

Avalanche と Steady state が 5 分間持続できるように設定して TPS を測定します。Zero Loss 率を 0.001%とし、3 回測定した後、その平均値を最終 TPS として算定しました。

＜参考2＞ 用語の説明

用語	意味
L4SLB	OSI 参照モデルの第4層（Layer 4)であるトランスポート層での情報を基に負荷分散処理を行うことを意味する。TCP/IPで説明するとIPアドレスとTCP、UDPのポート番号を用いて負荷分散を行うことを意味する。L4サーバ負荷分散とも言う。
L7SLB	OSI 参照モデルの第7層（Layer 7)であるアプリケーション層での情報を基に負荷分散処理を行うことを意味する。TCP/IPで説明するとHTTP、FTP、SIP、DNSなどのアプリケーション レイヤにおける情報に基づいて負荷分散を行う。例えば、HTTPヘッダーの詳細内容に基づいて処理すべきサーバを割り当てたり、セッションを維持するなどの処理を行うことを意味する。L7サーバ負荷分散とも言う。
SSL TPS	1秒あたりのSSLトランザクション数を意味する。1 SSL トランザクションは、TCP接続、SSLセッション接続、HTTPリクエスト、HTTP応答、SSLセッション終了、TCP終了と定義する。
SSLスループット	SSLトランザクション処理でSSLセッション確立の後はバルク暗号化したスループットとして測定する。最大SSLスループットを測定する場合は大きいデータのバルク暗号化スループットとして測定する。

「PAS 3716-SSL3000」は、実際に検証が可能な評価機の無料貸し出しサービスを実施しております。
貸し出しのご希望は、お問い合わせ欄よりご依頼下さい。

お問い合わせ先
株式会社パイオリンク 営業部
住所：160-0022 東京都新宿区新宿 1-34-14 第 2 貝塚ビル 3F
TEL：03-5367-2547 FAX：03-5367-2546
E-mail：sales@piolink.co.jp URL： http://www.piolink.co.jp