3Z-7

SSL/TLS 処理のパフォーマンス解析について

小川梨恵† 天野桂輔‡ 齋藤孝道†
明治大学† 明治大学大学院‡

1. はじめに

近年，WAN/LAN 間の通信や遠隔地からのリモートアクセスが容易に実現できるようになった．その一方で，その機能を実現するための主な基本技術である TCP/IP の特性によって，インターネット上を流れる情報の盗聴や改ざん，利用者の成りすましなどの脅威も増えている．それらの脅威への対策としてセキュリティプロトコル SSL(Secure Socket Layer)/TLS(Transport Layer Security)が利用されるようになった．しかし，これらを利用した通信には，暗号化/復号といった高負荷な演算処理を伴うため，システム全体のスループットの低下を招く．

そのため本論文では，暗号処理が SSL/TLS 処理に与える影響について調査するため，UltraSPARC T2 上に Web サーバを構築し，Dtrace を用いて SSL/TLS を用いた通信のパフォーマンスを測定した．そして SSL ハンドシェイクにおいて暗号処理がどれ程の割合を占めるのかを算出した．

2. 計測環境

2.1 UltraSPARC T2

UltraSPARC T2 プロセッサは Oracle 社のチップ・マルチスレッディング・テクノロジー（CMT：Chip Multithreading Technology）に基づくマルチコアプロセッサであり，1 つのプロセッサに 8 つのコアが搭載されている．それぞれのコアは，論理的に 8 つの CPU として動作するため，最大 64 個のスレッドを同時に実行可能である．また，各コアに浮動小数演算ユニットである FPU（Floating point / Graphics Unit）と暗号処理ユニットである SPU（Stream Processing Unit）を搭載している．これらはメインメモリを共有しており，各コア，SPU 及び FPU は並列に動作できる．図 1 に UltraSPARC T2 のアーキテクチャを示す．

また，マルチコア環境での利用を前提とした OS(Operating System)である Solaris は，SPARC に対応しており，様々な用途で，利用者はマルチコアを意識せずに，相応のパフォーマンスを得ることができる．

暗号処理ユニット SPU は主に MAU（Modular Arithmetic Unit）と暗号 / ハッシュ・ユニットから構成される．MAU は FPU を利用し，公開鍵暗号方式 RSA，及び楕円曲線暗号を処理する．暗号 / ハッシュ・ユニットは共通鍵暗号方式やハッシュ関数に対応しており，DES，3DES，AES，RC4，SHA1，SHA256 と MD5 を利用できる．

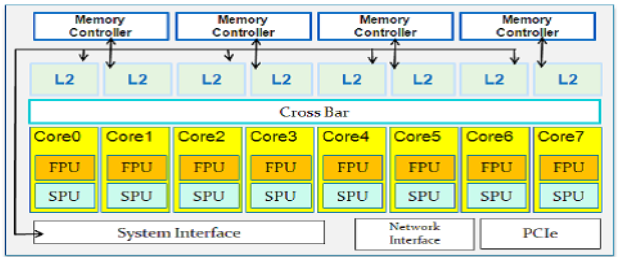

図 1: UltraSPARC T2 プロセッサ

2.2 Dtrace

DTrace は Solaris10 から Solaris に導入された，システム情報をトレースする機能である．DTrace を利用すると，稼働中のシステム上で動作する OS，ユーザアプリケーション，リソースに関する情報をリアルタイムで収集し，解析することができる．

DTrace を利用する方法として，DTrace コンシューマと呼ばれるコマンド群を利用する方法がある．DTrace コンシューマには，割り込みの発生を検出する intrstat コマンド，ロックの発生を検出する lockstat コマンド，DTrace が提供するすべてのサービスにアクセスできる dtrace コマンドなどがある．また，DTrace 用のスクリプト言語である D スクリプト言語を用いて，情報収集を行うための独自のスクリプトを記述することもできる．

2.3 OpenSSL

OpenSSL は，SSL や TLS だけでなく，証明書の発行といった PKI（Public Key Infrastructure）関連の処理や公開鍵暗号方式や共通鍵暗号方式などを容易なインタフェースで利用可能とした API ライブラリを含むツールキットである．

OpenSSL が提供するライブラリは libssl と libcrypto があり，前者は SSL / TLS 通信を，後者は暗号技術を提供するライブラリである．共

Performance Analysis of SSL/TLS Processing
† Rie Ogawa, Takamichi Saito ‡ Keisuke Amano
Meiji University (†), Graduate School of Meiji University (‡)
1 -1-1 Higashimita, Tama-ku, Kawasaki-shi, Kanagawa, 214-83571, Japan (†) (‡)
{ee97121, ce16002}@meiji.ac.jp, saito@cs.meiji.ac.jp

通鍵暗号方式として DES，3DES や AES など，公開鍵暗号方式として RSA や DH (Deffie-Hellman) など，ハッシュ関数として SHA-1 や MD5 など，主要なアルゴリズムが利用可能である．

3. 評価

3.1 評価方法

本論文では，UltraSPARC T2 上に構築した SSLWeb サーバに対して，負荷をかけることでパフォーマンスの評価を行う．SSLWeb サーバは Apache を用いて構築し，HTTPS リクエストのアクセスをして負荷を掛ける．HTTPS リクエストを生成する負荷生成器として，Spirent 社の Avalanche2007 モデル B(以下，Avalanche と呼ぶ)を用いた．Avalanche により多数のユーザをエミュレートし，各ユーザが HTTPS リクエストをそれぞれ送信するかのような負荷を生成する．

負荷生成開始から 15 秒間，一定の割合でリクエスト数を増やしていき，最終的に毎秒 500 個のリクエストを生成するようにした ．各リクエストでは，共通鍵暗号方式に DES，その利用モードに CBC，ハッシュアルゴリズムとして SHA-1 を用いた．また，Avalanche からリクエストとして，SSL サーバへ送信するファイルサイズは，平均的な Web ページのサイズである 50Kbytes[2]とした．

また，Apache モジュール内で動作する関数ごとに時間を計測する D スクリプトを記述し，実行した[3]．これによりライブラリやモジュール内の関数の処理時間を特定することが可能になる．計測環境を表 1 に示す．

表 1：計測環境

プロセッサ	CPU	Ultra SPARC T2
	プロセッサ数	1プロセッサ
	コア数	8コア
	スレッド数	8スレッド
メモリ		16Gbytes
ディスク容量		341Gbytes
OS		Solaris Express Developer Edition

3.2 評価結果

SSL サーバが 50Kbytes の Web ページを処理する際のライブラリやモジュールにおける実行時間の内訳を表 2 に示す．

表 2：ライブラリやモジュールにおける実行時間の内訳

ライブラリ/モジュール	概要	時間(ns)	割合
libcrypto.so.0.9.8	すべての暗号化機能を含む暗号化ライブラリ	10922997209	76.34%
libc.so.1	Cの標準ライブラリ	1862433840	13.01%
httpd	Apache Webサーバの関数	1579047857	11.03%
libapr-1.so.0.3.3	アプリケーションライブラリ	577966517	4.03%
a.out	実行ファイル	233278957	1.63%
libssl.so.0.9.8	SSLライブラリ	121561386	0.86%
その他	SSLモジュール，プロキシモジュール	331756352	2.31%
全体		14307935807	100%

表 2 より，暗号化機能を含む暗号化ライブラリ libcrypto.so.0.9.8 の割合が 76.34%あり，全体の処理時間の大部分を占めていることがわかる．

図 2 に SSL ハンドシェイクにおける詳しい内訳を示す．これは libcrypto.so.0.9.8 内の処理にあたる．ハッシュ関数が 1.28%，共通鍵暗号方式が 0.15%にとどまっているのに対し，公開鍵暗号方式で暗号処理している関数は SSL ハンドシェイクの処理時間の 92.48%を占め，非常に高い割合であることがわかる．その他には，乱数を生成する関数や，証明書を管理する X509 についての関数などが含まれている．

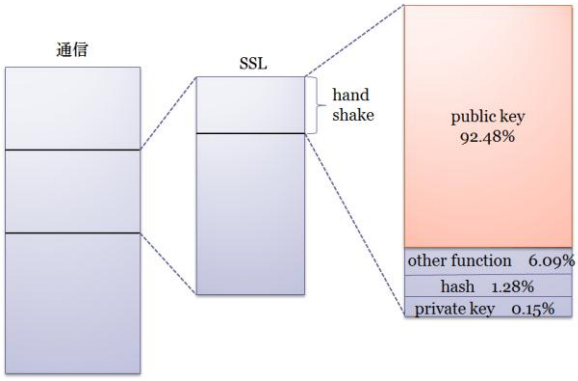

図 2： SSL ハンドシェイクの内訳

4. まとめ

本論文では，SSL/TLS 処理における暗号処理の割合を知るため，そのパフォーマンス解析を行った．

解析の結果から，SSL ハンドシェイクの処理時間において暗号処理の占める割合が非常に高いことがわかる．それによって，暗号処理が SSL/TLS 処理に与える影響が大きいことがわかる．今後の課題としては，暗号処理の高速化を図り，その際に全体に与える影響について調査することが挙げられる．

謝辞 本研究の成果の一部は，科学研究費補助金（課題番号 22700086）の助成を受けたものである．

参考文献

[1] Oracle SPARC Enterprise T5120 サーバ，http://www.oracle.com/jp/products/servers-storage/servers/sparc-enterprise/t-series/035999.pdf

[2] L.Badia, Real World SSL Benchmarking, Rainbow Techologies Whitepaper, Sept. 2001

[3] http://prefetch.net/projects/apache_modtrace/index.html