平成29年度 情報工学コース卒業研究報告要旨

高田・本田 研究室	氏　　名	小 松　大 河
卒業研究題目	組込みシステム向けSSL/TLSライブラリの評価	

近年，IoT機器が急速に普及し，ネットワークに接続される組込みシステムが増加している．それに伴い，脆弱性を持つシステムへの攻撃も増加している．IoT機器は，医療機器や自動車など人命に直接関わることに利用されるものが増えている．このため，IoT機器のセキュリティを確保することが必要不可欠である．IoT機器がセキュアな通信を行うために必要となる主な要件として，通信している情報を秘匿すること（機密性，confidentiality），第三者による通信相手への成りすましを防ぐこと（真正性，authenticity），通信している情報の改ざんを防ぐこと（完全性，integrity）の3つが挙げられる．

複数の要素技術を組み合わせて，これら3つの要件を満たす手段として，SSL/TLS（Secure Socket Layer / Transport Layer Security）がある．SSL/TLSはセキュアでない従来のTCP接続上にセキュリティ層を実現し，HTTPやFTPなど様々なアプリケーションのデータを安全にやり取りする手段として，広く利用されているプロトコルである．しかし，SSL/TLSを用いることにより，単純なTCP接続のみで通信を行う場合よりも通信時間が長くなる．IoT機器にはリアルタイム性が求められる製品も多いため，通信時間が長くなることは望ましくない．そのほかにも，メモリ使用量やコスト面などさまざまな制限が課せられる．このような制限の厳しいIoT機器で，SSL/TLSを省メモリ，低オーバーヘッドで実装することが必要である．

本研究では，組込みシステムに適したSSL/TLSの高速化手法を検討するための第一段階として，SSL/TLSの実装を対象に，処理時間の構成を詳細に分析することを目的とする．そのために，Webサーバと TLS1.2で接続し，HTTP GETリクエストを送信，同サーバのWebページを受信する，というクライアントアプリケーションを使用した．このアプリケーションを組込みボードGR-PEACHに，リアルタイムOS（TOPPERS/ASPカーネル）を使用している環境上に実装した．組込みシステム向けSSL/TLSライブラリとしてwolfSSL，mbed TLSの2つを使用し，SSL/TLSセッションを確立するために必要な，クライアントが行う処理や，アプリケーションデータの暗号化，復号にかかる処理時間を測定し，ボトルネックとなる処理を探った．また，2つのライブラリについてメモリ使用量や機能面の比較を行った．

処理時間の測定の結果，セッション確立に必要な処理で最も負荷が大きいのが，共通鍵の生成を行う処理であり70%以上を占めていることがわかった．次いでサーバ証明書の検証，サーバから送られる共通鍵の生成に必要なパラメータの処理での負荷が大きく，上位3つで処理時間の約99%を占めていることが判明した．また，アプリケーションデータの暗号化，復号処理は，今回のデータ量程度では負荷が比較的小さいことが分かった．これらの結果から，SSL/TLSのセッション確立において，共通鍵の生成と，証明書の検証処理を高速化することが有効だと考えられる．また，セキュリティ強度とのトレードオフにはなるが，セッション確立の頻度を下げることで，このオーバーヘッドの影響を軽減できると考えられる．アプリケーションデータの通信では，共通鍵の暗号化処理を高速化する方法があるが，その効果はセッション確立処理の高速化に比べ小さいと考えられる．

今後の課題としては，今回使用したGR-PEACHと比べ，性能の劣るボードを用いた場合の処理性能の差や，今回使用していない暗号技術を用いた場合の処理コストの変化について調べる必要がある．さらに，実際のIoT機器の使用環境を考慮し，今回判明したボトルネックに対する高速化手法を検討するということなどが挙げられる．