組込みセキュリティのしくみ（実践篇）

古城 隆、wolfSSL, Inc.

松原 豊、名古屋大学

概要

- 組み込みシステムにおける、現実のネットワークセキュリティ・プロトコル（SSL/TLS）における暗号アルゴリズムやプロトコルの実際について解説します。
  - wolfSSL社のSSL/TLSライブラリーのオープンンソースを使って、C言語ソースコードを覗いたり
  - TOPPERS ASPカーネル上のwolfSSLライブラリーをデモ動作させたり
  - 組み込みSSL/TLSの実際のプロトコルをWireSharkを使ってモニターしてみたり。

そんなことを通じて組み込みの開発の要点について触れていきます。

- 最近ちらほら耳にする新しいTLS標準TLS1.3は、単なる1.2のマイナーバジョンアップじゃないぞ、みたいな話にも踏み込んでみたいと思っています。

後編セッションだけの参加もOKです