報道関係者各位

2024 年 5 月 21 日
wolfSSL Japan 合同会社

# wolfSSL、新製品 wolfHSM を発表
# 車載向け HSM の統合を容易にするフレームワーク。耐量子暗号に対応

組み込み向けネットワークセキュリティ専門ベンダの wolfSSL Inc.（本社：米国ワシントン州エドモンズ）は本日、新製品 wolfHSM を発表しました。HSM(ハードウェアセキュリティモジュール)はセキュリティの核となる署名検証や暗号処理を物理的に独立したプロセッサに隔離し、暗号鍵と暗号処理の安全性を飛躍的に向上させる技術です。HSM は従来、大型のクラウドサーバなどで広く利用されてきた技術ですが、最近は車載デバイス、医療機器、産業オートメーションなど堅牢なセキュリティが求められる分野でも利用が義務化、あるいは強く推奨されるようになってきています。そうした背景から、各社の組み込み向けプロセッサでもマルチコアのコア間の独立性を利用して、物理的にアプリケーションコアから隔離させた高い安全性を持つ HSM 機能をサポートするものが増えてきています。

しかし、そのようなプロセッサ(MCU)が提供する機能単体で従来の機器、デバイスに HSM を導入するにはいくつかの課題もありました。wolfHSM はそうした課題を解決し、HSM による堅牢なシステムを容易に実現するためのハードウェアセキュリティのフレームワークです。wolfHSM を付加することで、 MCU の HSM 基本機能が持つ高い安全性を維持しつつ、暗号アルゴリズムの拡張性、従来型の暗号技術からの移行性、セキュリティ機能との統合性などを強化することができます。

**暗号アルゴリズムの拡張性**

セキュリティにおいては攻撃側の技術も常に進歩していることを考慮し、これを守る側も常に進化させていく必要があります。wolfHSM ではハードウェアが提供する固定的な機能に限定されることなく、ハードウェアレベルの高い安全性を維持しつつソフトウェアによって暗号アルゴリズムや機能を強化、拡張することができます。

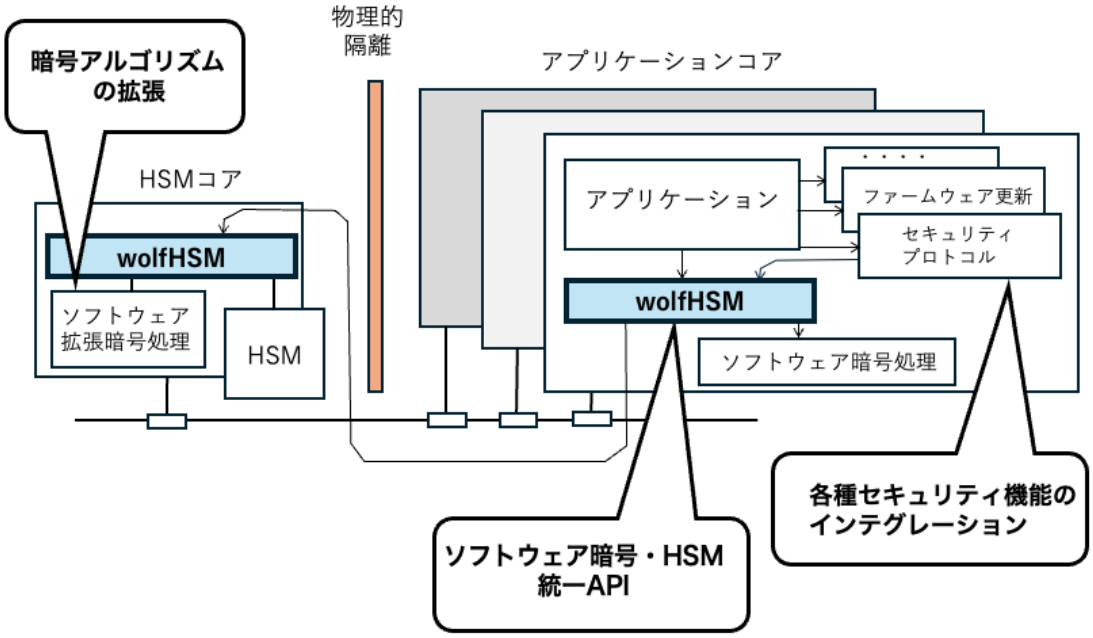
たとえば、現在研究開発が進んでいる量子コンピューティングが実用化されると、今広く使われている公開鍵暗号はほとんど無力化されてしまうことが予測されています。そうした場合にも、ハードウェアを変更することなく、HSM プロセッサ自体に含まれていない Kyber、LMS、XMSS などの耐量子暗号アルゴリズムや、SM2、SM3、SM4 などの特定分野向けアルゴリズムも wolfHSM で新たに拡張することが可能です。

**従来型の暗号技術からの移行性**

wolfHSM は、従来のソフトウェアベースの暗号処理と HSM による処理を統一するインターフェース(API)を提供します。既存のシステム構造を大きく変更することなく、アプリケーションコアから隔離された高い安全性を持つ HSM 機能のスムーズな導入を可能にします。

**AUTOSAR HSE などのセキュリティ機能との統合性**

wolfHSM は、AUTOSAR との互換性がある同社の暗号エンジンである wolfCrypt の API を利用するため、AUTOSAR との統合も実現します。また単体の HSM としての利用だけでなく、wolfSSL、wolfSSH ほかのセキュリティプロトコルや、安全なファームウェア更新を実現する wolfBoot などとの統合性を提供します。




【図 1　車載向け HSM の統合を容易にする wolfHSM】

サポートする HSM は以下の通りです。

Infineon AURIX TC3xx

Infineon AURIX TC4x (近日対応予定)

ST SPC58NN

Renesas RH850 (近日対応予定)

このほかサポート対象を拡大中です。詳細は info@wolfssl.jp までお問い合わせください。

wolfSSL Inc.の日本法人、wolfSSL Japan 合同会社は、明日 2024 年 5 月 22 日からパシフィコ横浜で開催される、人とくるまのテクノロジー展 2024 YOKOHAMA に出展いたします。wolfHSM のほか、ポスト量子暗号、FIPS140-3 を含む最新のネットワークセキュリティについて説明いたします。TLS 1.3 ライブラリ wolfSSL のご使用を希望される方には、使用開始の準備も会場でご案内します。
日時： 2024 年 5 月 22 日 (水)～23 日 (木) 10:00 ～ 18:00、24 日 (金) 9:00 ～ 16:00
会場： パシフィコ横浜
wolfSSL ブース番号：展示ホール・ノース　N34

展示会会場での打ち合わせ予約は info@wolfssl.jp で受け付けています。

wolfSSL について
wolfSSL Inc.は、米国ワシントン州エドモンズに本社を持ち、組み込みシステム向けに軽量なセキュリティライブラリを提供しています。スピード、サイズ、移植性、機能、標準への準拠にこだわり、自社の専門エンジニアが開発、サポート、コンサルティングを行っています。米国連邦標準規格 FIPS 140-2 の認証取得では多くの経験があり、最新 FIPS 140-3 認証取得も進めています。航空宇宙では RTCA DO-178C レベル A 認証、車載向けでは MISRA-C をサポートします。

2004 年の創業以来世界各国で 2,000 社を超える OEM カスタマーに採用されています。社名と同名の組込み向け TLS ライブラリである wolfSSL は、世界初の最新のプロトコルバージョン TLS1.3 をサポートする商用版ライブラリです。

wolfSSL Japan 合同会社の技術サポートセンターでは、日本人専任スタッフによるサポートサービス、カスタマイズサービスなどを提供しています。

【お問い合わせ先 】
wolfSSL Japan 合同会社　担当: 須賀
Email: info@wolfSSL.jp
TEL: 050-3698-1916
https://www.wolfssl.jp
https://twitter.com/wolfSSL_Japan