プレスリリース
Website: www.nordicsemi.com
2016 年 9 月 5 日【参考日本語訳】

新製品：ソフトウェア開発キット（SDK）

Nordic Semiconductor、最新版 nRF5 SDK を発表、署名付きのセキュアな OTA ファームウェア・アップデートを導入し、デバイスのセキュリティ向上を支援

Nordic の最新版 nRF5 SDK v12.0 では、セキュアな署名付きの OTA ファームウェア・アップデートが実現されており、検証済みの信頼できるソースからのアップデートを保証。さらに、本 SDK は今回、Nordic nRF52832 SoC ベースの Arduino Primo ベースボードで使用される Arduino 開発キットをサポート、Keil でグラフィカルな設定を可能にする CMSIS configuration Wizard を有し、Bluetooth low energy 対応持続血糖測定器（CGM）プロファイルをサポート、最適化された浮動小数点演算を提供

2016 年 9 月 5 日、ノルウェー・オスロ発- 超低消費電力無線接続のリーディング・プロバイダーである Nordic Semiconductor（OSE：NOD、以下 Nordic）は本日、検証済みの信頼できるソースからのみ所定デバイスへのアップデートを適用し、損害をもたらす可能性のある、悪意あるデバイス・アップグレードの攻撃からアプリケーションアップデートを強固するためのセキュアな署名付きの OTA-DFU(over-the-air device firmware updates)をサポートする最新の nRF5 SDK v12.0 を発表しました。

Nordic の製品マーケティング担当マネージャーである John Leonard は、次のように述べています。
「モノのインターネット（IoT）に関わる企業にとって、最も重要なのがセキュリティであり、製品のファームウェア・アップグレードでは、それがどんな役割を持ち、信頼できるソースを発信源としているかも、重要かつ基本的な要素として理解する必要があります」

「多くのメーカーにとって、ソフトウェア開発は複数のチームを要する複雑で締め切りの厳しい作業であり、その困難さゆえ、バグが残ったままの製品が出荷されてしまうケースも残念ながらあります。同時にメーカー各社は、最新・最高の製品機能を導入することで、自社製品で最高のパフォーマンスを発揮し、顧客エンゲージメントを維持していきたいと考えています」

「すなわち、ソフトウェアとファームウェアのアップデートの実行能力が絶対的に必要であり、Bluetooth low energy 製品でこれを最も簡単・安全に実行する方法とは、当社の最新版 nRF5 SDK v12.0 の真骨頂である、署名付きのセキュアな OTA-DFU アップデートにほかなりません」

オペレーションでは、公開鍵が配布され、秘密鍵は送信側のみが保有することで、1 対 1 のセキュリティが保証されるという、従来型の公開鍵/秘密鍵のセキュリティ構造が採用されます。Nordic nRF5 SDK v12.0 での暗号による鍵の作成は、さまざまな方法で行うことが可能であり、開発者がどの方法を希望した場合でも、暗号を柔軟に作成できるよう、Nordic は多大な労力を投じてきました。これには、P256 曲線を使用し、*Bluetooth*® low energy でセキュアな接続を確立する ECDH など、Nordic が作成したサンプルが含まれます（署名付き・署名なしのファームウェアで使用するため、Nordic は 2 つの専用 16 ビット UUID も Bluetooth SIG でリザーブしています）。

Nordic は、クロスプラットフォームの PC ツールのスイートに加え、Android と iOS 向けのモバイルツールにより、DFU アプリケーションのセキュアな開発もサポートしています。

さらに、セキュアな OTA-DFU が中断された場合、「resume-from-failure （障害から再開）」機能により、アップグレード・プロセス全体を最初から再スタートするのではなく、最新の既知の良好なポイントからアップデートを再開・完了できるようになっています。

Nordic nRF5 SDK v12.0 の追加機能には、Nordic nRF52832 システム・オン・チップ（SoC）ベースの Arduino Primo ベースボードで使用され、Nordic nRF5 SDK のモジュール、機能、アプリケーション・サンプルのすべてを Arduino プラットフォームに提供する Arduino 開発キットのサポート、プロジェクトモジュールと設定のより明確な表示で開発を簡素化するための Kiel でグラフィカルな設定を可能にする CMSIS configuration Wizard、

Bluetooth low energy 対応持続血糖測定器（CGM）プロファイルのサポート、Nordic の最新 SoC である nRF52832 で使用される ARM® Cortex™ M4F の FPU 命令セット機能を活用する、最適化された浮動小数点ユニット（FPU）実行機能があります。最新の製品やアプリケーション・ソフトウェアのアルゴリズムの多くで、浮動小数点への対応が一般化し、必要性が高まる中、FPU の実行機能は、処理時間とソフトウェアの複雑性を大幅に解消できると考えられます。

Nordic Semiconductor について
http://tinyurl.com/NordicSemi-jp

nRF52832 について（英語サイト）
tinyurl.com/nRF52832

【本リリースに関する報道関係からのお問い合わせは下記にお願いいたします】

Nordic Semiconductor PR エージェンシー（日本国内）
株式会社ブラッド・スウェット アンド ビアーズ
早田 真由美（ハヤタ マユミ）
TEL: 03-6809-2301
E-mail: hayata@bsbeers.com

お問い合わせ
Marketing contact: Domenica Wong
Marketing Communications - APAC
TEL: +852 3462 6283
E-mail: domenica.wong@nordicsemi.no
Website: www.nordicsemi.com