2025 年 11 月 11 日
株式会社ユビキタス AI

PRESS RELEASE

ユビキタス AI、IoT 製品のセキュリティを高める
耐量子暗号への対応を低価格マイコンで実現

― セキュリティ 2030 年問題に備えた堅ろうなソフトウェアソリューション提供を加速 ―

株式会社ユビキタス AI（本社：東京都新宿区、代表取締役社長 CEO：大吉 裕太、以下「ユビキタス AI」）は、世界的に深刻化するサイバーセキュリティ攻撃に対抗する重要技術「耐量子暗号（PQC = Post-Quantum Cryptography）」の研究開発を 2023 年より進めており、このたび、低価格 IoT 製品への搭載を可能にする Arm® Cortex®-M ベースの 32bit マイコンでの実装に目途を得ました。
ユビキタス AI では、NIST（米国国立標準技術研究所）によって標準化された FIPS 203、FIPS 204、FIPS 205 について実装・検証を完了しています。さらに、標準化作業中の FALCON および HQC についても暫定仕様に基づく実装・検証を完了しており、NIST の最終標準化を待つ段階にあります。

標準 / 標準名	標準化段階	アルゴリズム名	用途
FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard	発行済	ML-KEM	鍵交換
FIPS 204 Module-Lattice-Based Digital Signature Standard	発行済	ML-DSA	デジタル署名
FIPS 205 Stateless Hash-Based Digital Signature Standard	発行済	SLH-DSA	デジタル署名
FALCON	策定中	FN-DSA（予定）	デジタル署名
HQC	策定中	未公表	鍵交換

NIST標準化済もしくは標準化作業中の耐量子暗号アルゴリズム

耐量子暗号への対応は、量子コンピューターの実用化を待たずに世界中で進められており、NIST は「2035 年までの移行完了」を推奨しています。特に、現在広く用いられている公開鍵暗号アルゴリズムの RSA 2048 bit については「2030 年 12 月 31 日まで」が安全利用期限とされており、データの保存期間に応じて耐量子暗号などの新しい暗号方式への移行が急務となっています。こうした流れは公共システムにも及んでおり、例えば日本のマイナンバーカードでも、RSA 2048 bit が使われているため、将来のマイナンバーカードに向けた耐量子暗号対応を含む強固な暗号技術への移行が検討されています。

ユビキタス AI は今後も、既存のセキュリティ基盤の多くが耐量子暗号に対応していくことを想定し、将来の IoT 製品のニーズに備えたソリューションを提供していくための取り組みを継続してまいります。

■株式会社ユビキタス AI（証券コード：3858）について

ユビキタス AI は、製造業のお客様を支えるテクノロジーとサービスを提供する企業です。長年にわたる組込みソフトウェアビジネスの実績をベースに、自社開発製品および世界中のソフトウェア製品の販売・サービスにおいて成功を収めています。強みである先進かつ優れたテクノロジーと強固で幅広い顧客基盤を活かしながら、ベンチャー・スタートアップや学術機関との連携による新しいビジネスプラットフォームを構築し、製造業のお客様を支えるテクノロジー・サービスを世界に展開し続けることによって「お客様」「ビジネスパートナー」「社会」の発展に貢献します。

本社所在地 ： 東京都新宿区西新宿 1-23-7 新宿ファーストウエスト 17F

URL ： https://www.ubiquitous-ai.com/

■投資家の皆さまへ

本ニュースリリースは、ユビキタス AI の定性的な業務進捗をお知らせするためのものであり、投資勧誘を目的としたものではありません。当社業績・経営指標の進捗・予想に関しては、取引所開示情報である、決算短信などをご参照ください。

■本ニュースリリースに関するお問い合わせ先

株式会社ユビキタス AI マーケティング＆コミュニケーション部 （担当：麻生）

TEL ： 03-5908-3451

Web からのお問い合わせ ： https://www.ubiquitous-ai.com/contact/others/