

PRESS RELEASE

ユビキタス AI、IoT 製品向け耐量子暗号技術をセキュリティソリューション「Ubiquitous Securus」へ統合、2027 年度の製品化に向け開発を加速

— 次世代暗号技術と量産実績を持つセキュリティ基盤を融合し、
組込み製品への PQC 実装を支援 —

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、サイバーセキュリティの重要技術である耐量子暗号（PQC = Post-Quantum Cryptography）について、組込みデバイス向け耐タンパセキュリティソリューション「Ubiquitous Securus」へ統合し、フィジカル AI 時代に必要とされるセキュリティソリューションの提供を 2027 年度から開始することを発表いたします。

量子コンピュータの実用化を見据え、現在広く利用されている公開鍵暗号を、量子コンピュータによる解読にも耐え得る PQC へ移行する取り組みが世界的に進んでいます。

ユビキタス AI では、約 25 年にわたり培ってきた「小さく、軽く、速い」組込みソフトウェア技術を次世代暗号にも応用し、2023 年より PQC の研究開発を進めてきました。2025 年秋にはリソース制約の大きい低価格 IoT 製品向けの Arm® Cortex®-M ベースの 32bit マイコンでの実装にめどをつけました。このたび、この PQC 技術を、IVI や家電機器向けに多数の採用実績を持つ自社のセキュリティ基盤「Ubiquitous Securus」へ統合します。

これにより、PQC 対応の暗号ライブラリを提供するだけでなく、暗号鍵の安全管理・運用、暗復号処理の保護、異なる SoC への移植性など、実際の組込み製品への導入に必要な機能を組み合わせたセキュリティソリューションとして提供することで、お客様の PQC への段階的な移行と実装を支援します。

■Ubiquitous Securus について

Ubiquitous Securus は、暗号鍵や証明書、ユーザーデータなどの秘匿情報を安全に管理し、暗復号処理を保護するための組込みデバイス向け耐タンパセキュリティソリューションです。

ユビキタス AI の著作権保護製品「Ubiquitous DTCP」、「Ubiquitous HDCP」との組み合わせで、IVI や家電機器向けを中心に多数の採用実績があり、2026 年 9 月 1 日時点で、約 840 万本の出荷実績があり

ます。

DTCPやHDCPなどの著作権保護規格では、暗号鍵の漏洩を防ぐための厳格な鍵管理が求められます。Ubiquitous Securusは、こうした要求に対応するため、ソフトウェアによる暗号ライブラリに加え、SoCが備えるハードウェアの暗復号機能の活用や、Arm TrustZone®などのセキュアなメモリ空間で暗号鍵・証明書・ユーザーデータなどの秘匿データを安全に管理・運用する「Secure Storage 機能」を提供しています。

また、SoC メーカーや型番が異なるとハードウェアの暗復号機能の API や Arm TrustZone で動作する Secure OS が異なるため、派生機種や後継機の開発時に既存の開発資産の改修が必要となる場合があります。Ubiquitous Securus では、こうした SoC や実行環境の違いを吸収する Wrapper 層を設けています。SoC ごとの API の違いを意識することなく、派生機種や後継機への移植に伴う開発負荷を軽減できます。

暗復号処理についても、Ubiquitous Securus が提供するソフトウェアライブラリと、SoC が備えるハードウェア暗復号機能を環境に応じて選択できる構成としています。

■PQCをUbiquitous Securusへ統合するメリット

今回の統合では、PQCによる次世代の暗号アルゴリズムに、Ubiquitous Securusがこれまで量産製品への実装を通じて培ってきた暗号鍵管理やハードウェア差異の吸収といった機能を組み合わせます。

これにより、以下の特徴を備えたPQC対応セキュリティソリューションの実現を目指します。

- ・ 暗号鍵のセキュアな管理・運用
- ・ 暗復号プロセスの隠蔽によるハッキング防止
- ・ 異なる SoC 間でも同一 API を利用でき、ハードウェア機能の活用が容易
- ・ 将来的に SoC 側が PQC に対応した際、ソフトウェアからハードウェア処理への切り替えをスムーズに実現
- ・ 従来暗号と PQC のハイブリッド暗号に対応し、段階的な PQC 移行を支援

■ 研究開発から製品化へ、「エッジセキュリティ 3.0」の実装を加速

PQCへの移行は、暗号アルゴリズムを一度実装して完了するものではありません。特に製品寿命の長いIoT・組み込み機器においては、将来の標準化動向や脅威の変化、ハードウェア環境の進化に応じて、利用する暗号方式を継続的に更新できる仕組みが不可欠です。

ユビキタス AI は、中期経営計画においてセキュリティ領域を成長領域の一つと位置付け、PQCをはじめとする次世代セキュリティ技術の研究開発と、IoT・組み込み機器への実装に向けた取り組みを進めています。（※1）

2026年6月に発表した「エッジセキュリティ 3.0（※2）」構想では、セキュリティを規制対応やリスク

対策のための「義務」ととどめず、製品・サービスの価値や新たなビジネスモデルを支える基盤へ進化させる考え方を掲げています。

今回の Ubiquitous Securus への PQC 統合は、これまで個別に開発・展開してきた次世代暗号技術である PQC と、量産製品への導入実績を持つデバイスセキュリティ技術を組み合わせ、「エッジセキュリティ 3.0」を具体的な製品へ実装していく取り組みの一つです。

今後もユビキタス AI は、次世代の製品セキュリティとお客様の製品競争力向上に貢献してまいります。

■Ubiquitous Securus 製品ページ

URL : <https://www.ubiquitous-ai.com/products/securus/>

※1) 当社の PQC への取り組みについての詳細はこちらをご覧ください。

URL : <https://www.ubiquitous-ai.com/news/2026/005587.html#appendix>

※2) 「ユビキタス AI、『エッジセキュリティ 3.0』構想を提唱し、組込み機器の価値創出を支える次世代セキュリティ設計を推進ーセキュリティを「義務」から「価値創造」へ転換ー」

URL : <https://www.ubiquitous-ai.com/news/2026/005507.html>

■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、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/>

※ 本ニュースリリースに記載されている会社名、製品名は各社の登録商標または商標です。

※ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。