FIDO アライアンスがモノのインターネット（*IoT*）を保護するための新たなオンボーディング（初期設定）標準を策定

安全なプラグアンドプレイ機能により産業用 *IoT* の可能性を解放

（国際版の日本語訳）

2021 年 4 月 20 日、カリフォルニア州マウンテンビュー - FIDO アライアンスは、デバイスをクラウドやオンプレミスの管理プラットフォームに簡単かつ安全にオンボード（初期設定）を可能にする新しいオープンな IoT 標準「FIDO Device Onboard（FDO）、ファイド・デバイス・オンボード（エフ・ディ・オー）と読む」プロトコルを発表しました。FIDO アライアンスは、この標準規格を通じて、IoT デバイスを大規模に展開する際に生じるセキュリティ、コスト、複雑さといった課題に取り組みます。FIDO デバイスオンボードは、データ漏洩を防ぎ、安全なオンライン体験を実現するために、世界中から最も影響力のある革新的な企業や政府機関 250 社以上を集め、サイバーセキュリティに取り組んできたアライアンスの基本的なビジョンをさらに発展させるものです。

IDC は、IoT 市場が 2 桁の年間成長率を維持し、2022 年には 1 兆ドルの大台を突破すると予想しています。このような成長予測にもかかわらず、プロバイダーと企業ユーザーの両方を対象とした最近の調査では、大多数の企業が自社のインフラに対する侵害について深刻な懸念を抱いていることがわかりました。今回の調査では、170 名の IoT リーダーのうち、85%がセキュリティに関する懸念が IoT 導入の大きな障壁になっていると回答しています。また、回答者の約 3 分の 2（64%）が、エンドツーエンドの IoT セキュリティが短期的な最優先事項であると回答しており、エッジコンピューティング（55%）、人工知能（AI）／機械学習（50%）、5G の導入（28%）を上回っています。

FIDO アライアンスの IoT 向け FDO 仕様は、オンボーディング（初期設定）における IoT セキュリティの問題を解決するために共同で策定されました。これは、FIDO 認証標準で世界的なデータ漏洩問題の解決に貢献したのと同様です。この FDO 仕様は標準仕様のステータスに達しており、オープンで自由に実装することができ

ます。当面、この仕様は産業用および商業用アプリケーションを対象としています。開発者の皆様は、次のURL より仕様書を閲覧、ダウンロードすることができます。

https://fidoalliance.org/specifications/download-iot-specifications/

FIDO アライアンスのエグゼクティブ・ディレクター兼 CMO であるアンドリュー・シキアは、「本日発表された FIDO デバイスオンボード標準は、現在ウェブ上に存在するセキュリティギャップを解消するためのアライアンスの継続的な取り組みをベースに、この取り組みを IoT アプリケーションに拡大したものです。企業は、IoT の大きな可能性を認識しており、製造、小売、医療、輸送、物流などに多大な利益をもたらすことができます。パラダイムの転換を早急に行い、産業・商業環境での重要な用途において、より安全で堅牢でセキュアな認証手段を用いて IoT 技術を推進する必要があります」と述べています。

高速で安全な IoT デバイスオンボーディングの標準規格

FDO は、IoT デバイスの自動オンボーディング（初期設定）プロトコルであり、非対称な公開鍵暗号方式を活用して、あらゆるデバイスをあらゆるデバイス管理システムにオンボーディング（初期設定）するための高速かつ安全な方法を産業用 IoT 業界に提供します。

FIDO デバイスオンボード標準によるビジネス上のメリットは以下の通りです。

- **シンプルさ** – 企業はもはや、デバイス自体にかかる費用よりも、長くて高度な技術を要するインストールプロセスにかかる費用を多く支払う必要はありません。高度に自動化された FDO プロセスは、どのようなレベルの経験者でも迅速かつ効率的に実施することができます。
- **柔軟性** – 企業は、（製造ではなく）インストールの時点で、どのクラウドプラットフォームにデバイスをオンボードするかを決定することができます。1 つのデバイス SKU をどのプラットフォームにも搭載することができ、デバイスのサプライチェーンを大幅に簡素化することができます。
- **セキュリティ** – FDO は「信頼されていないインストーラー」というアプローチを採用しているため、インストーラーはネットワークにデバイスを追加する際に、機密性の高いインフラやアクセスコントロール情報を必要とせず、またアクセスすることもできないようになっています。

インテル Internet of Things グループ、バイスプレジデント兼インダストリアル・ソリューションズ部門のジェネラル・マネージャーであるクリスティン・ボールズは、「これは、IoT システムを展開する上で、今日の重要な課題の一つを解決することを目的とした大きなマイルストーンです。新しい FDO 規格は、コストの削減、時間の短縮、セキュリティの向上に役立ち、IoT 産業の急速な拡大に貢献します。FDO 規格の実装により、現在の手動によるオンボーディング・プロセスを、自動化された安全性の高い業界のソリューションに置き換えることで、企業は IoT の機会を完全に活用することができるようになります」と述べています。

これは、パスワードへの依存度を低減し、スケーラブルな攻撃やアカウントの乗っ取りを防ぐ、よりシンプルで堅牢な認証を実現することを目的とした、FIDO アライアンスの最新の取り組みです。FIDO デバイスオンボードは、FIDO アライアンスの IoT 技術作業部会（IoT TWG）の作業を通じて策定されたもので、共同座長を務めるリチャード・カースレイク（Intel）、ギリダール・マンディアム（Qualcomm）、副座長ジェフ・クーパー（Intel）がその任に当たっています。また、Arm、Amazon Web Services（AWS）、Google、Microsoft などの企業が仕様書のエディターとして貢献参加しています。

FIDO アライアンスと IoT TWG は、5 月 7 日（米国時間）にウェビナーを開催し、「FIDO デバイスオンボード」規格、ユースケース、今後の認定プロセスについて解説を予定してしいます。詳細および登録は以下のリンクを参照ください。https://fidoalliance.org/event/securing-iot-with-fido-authentication/2021-05-07

FIDO デバイスオンボードの紹介は、下記リンクのホワイトペーパーを参照ください。
https://fidoalliance.org/intro-to-fido-device-onboard.

IoT 業界のステークホルダー各社からの FDO に関するコメント（各社コメントは原文のまま掲載）

“As the IoT rapidly expands, the security of devices cannot be optional and a strong foundational root of trust is essential. Arm is dedicated to driving standards in security through initiatives such as PSA Certified, and welcomes further ecosystem collaboration for the advancement of secure, robust solutions that enable innovation. The FDO specification will enable device makers to deploy, onboard and manage secure IoT devices faster at a lower cost, helping scale IoT across both industrial and consumer use cases.” — Mohamed Awad, vice president, IoT Business at Arm

"FDO is a revolutionary standard, leveraged by BT's Zero Touch Onboarding (ZTO), which can address a critical need for the IoT, Edge Compute and 5G industries and help them to scale up securely and fully automated, from the manufacturer to the consumer, from the device to edge, and from edge to the cloud." — Dr Mohammad Zoualfaghari, Research Manager and IoT Architect at BT

"We are delighted to be part of the IoT TWG and will be supporting the FIDO device onboarding (FDO) specification. Originally, we worked closely with Intel SDO and adopted this approach to our IoT security platform, KeyScaler. Now that FIDO has developed a new enhanced standard, we will also be supporting FDO in our KeyScaler platform. Current and future customers will be able to leverage FDO in their IoT projects." — Darron Antill, CEO of Device Authority

"The work the FIDO Alliance is doing to address phishing by closing security gaps on the web would not be possible without industry collaboration and standardization. It's a natural fit for the FIDO Alliance to use these same tools to address the threats against IoT infrastructure. As a board member of the FIDO Alliance since its earliest days, Google is proud to have contributed to this new standardization effort to better secure IoT." — Dave Kleidermacher, VP, Android Security & Privacy, Google

“The Open Horizon project wanted a simple solution to zero-touch provisioning that would have wide support from hardware manufacturers, maximum flexibility, and a staged approach. The FDO specification from the FIDO Alliance certainly meets those requirements. After implementing and shipping support in Open Horizon*, we're pleased with the results and with the feedback we've received from those using it in the field. We're looking forward to implementing FDO in our* Smart Agriculture SIG*'s use cases, and in the* Open Retail Reference Architecture*.” — Joe Pearson, Technology Strategist, IBM Cloud and Technical Steering Committee Chair, Open Horizon project*

“We are delighted that the FDO protocol is built with security in mind as it enables FDO based systems to store the private key secrets and device credentials in a Trusted Platform Module. TPM is a widely accepted and used technology that creates trust in manufacturing and supply chain. It is a major contribution towards the acceleration of IoT device deployment.” — Jürgen Rebel, Senior Vice President and General Manager Embedded Security at Infineon Technologies

"Today's announcement is a significant leap forward in enabling secure device deployments at scale. By creating the standard and open source reference implementation in parallel, the FIDO Alliance has delivered an IoT standard which is proven to be secure, significantly lowers the cost of onboarding and speeds time to market.” — Francois Ozog, Director of Linaro's Edge and Fog Computing Group

"LoginID continues to support the FIDO standard and its emergence as the de facto global method for authentication. As part of our API strategy of providing the easiest way to integrate FIDO, LoginID will be deploying FDO as a part of our platform in 2021. We look forward to collaborating further with other enterprises on this initiative." — Simon Law, CEO, LoginID

“We are thrilled to see the FIDO Alliance address such a critical piece of the IoT device lifecycle. Device onboarding through a standardized protocol like FDO simplifies device set-up by abstracting the underlying complexities of the hardware, which will accelerate the adoption of IoT in industry.” — Sam George, VP of IoT, Microsoft Azure

“The demand for automatic onboarding, traceability and updating of assets is growing, and manufacturers are challenged to rapidly identify and replace defective devices before they disrupt operations. Integrating FDO into our IAS4.0 platform will prove invaluable in informing our roadmap for the future of industrial automation and Molex’s broad portfolio of industry-leading connectivity solutions.” — Riky Comini, Senior Director of Industrial Automation, Molex

"The FIDO Alliance has set the standards for secure user to device authentication which has gained broad acceptance and adoption worldwide. With their release of these new standards for IoT we now have equally robust standards to support the challenges associated with secure device onboarding." — Phil Dunkelberger, CEO, Nok Nok

“FIDO is simply the most effective way to eliminate both ID theft and unessential password reuse. The Rakuten security team is fully committed to transitioning from traditional authentication methods to a world where passwords aren’t required. This mission is critical if we wish to achieve a truly secure internet for society. This is another important milestone on the way to Internet World Peace.” — Yoshinari Fukumoto, General Manager of Cyber Security Defense Department, Rakuten Group, Inc.

"By promoting the FIDO Device Onboard (FDO) Specification to Proposed Standard, FIDO Alliance is demonstrating its active commitment in deploying its authentication standards to new fields. The FDO specification will pave the way for secure interactions between devices and IoT platforms. As a board member of the FIDO Alliance, RaonSecure is delighted to support the FIDO Alliance in this important progress, enhancing security in IoT environments.” — Soonhyung Lee, CEO, RaonSecure

“SecurID, an RSA business, congratulates FIDO and the identity community for completing the FDO spec, a critical milestone towards securing the IoT supply chain and ecosystem. As a FIDO Board Member and contributor to the FDO technical working group, we are actively exploring ways to incorporate FDO into our market-leading identity and access management and IoT security offerings.” — Salah Machani, Director, Engineering Technologist, RSA

FIDO アライアンスについて

「高速なオンライン ID 認証」を意味する FIDO（Fast IDentity Online）アライアンス www.fidoalliance.org は、セキュリティと利便性の両立をめざすため、2012 年 7 月に設立されたグローバルな非営利団体です。堅牢な認証技術に相互運用性が確保されていない状況を改善し、ユーザーが多くの IDとパスワードを覚えなければならないという煩わしさを解消することを目的としています。FIDO アライアンスは、認証におけるパスワード依存を軽減するために、オープンで拡張性と相互運用性のあるシンプルで堅牢な「FIDO 認証」を標準化することで、オンラインサービスの本質に変革をもたらします。FIDO 認証はオンラインサービスの利用時に、堅牢でプライバシーが確保された便利な認証を提供します。

【本プレスリリースに関するお問い合わせ先】

FIDO アライアンス　アジアパシフィック・マーケット開発マネジャー
土屋 敦裕
pr@fidoalliance.org