

Microchip、PolarFire® FPGA のシングルチップ暗号化設計フローが 英国 NCSC (National Cyber Security Centre)の審査に合格した事を発表

PolarFire FPGA のセキュリティ ソリューションの堅牢性を実証

2023 年 8 月 31 日[NASDAQ: MCHP] – 全ての垂直市場において、セキュリティはあらゆる設計の必須事項となっています。本日、システム設計開発の現場は、通信、産業、航空宇宙、防衛、原子力、その他のシステムで Microchip Technology Incorporated(日本法人: 東京都港区浜松町、代表: 樺晴彦 以下 Microchip 社)の PolarFire FPGA を採用する際のセキュリティの確保に関して、大きな安心を手に入れました。英国政府の NCSC (National Cyber Security Centre)が、厳しいデバイスレベル サービス回復力要件に対して、シングルチップ暗号化設計フローで使った場合の本デバイスの審査を完了したのです。

「NCSC は非常に厳密な解析を行います。Microchip 社の協力の下で行われた、PolarFire FPGA での設計分離手法に関する審査に合格した事で、本デバイス内でのサービス回復力向上と機能的絶縁の利用が可能になりました。これは、セキュリティに対する包括的なアプローチへの Microchip 社の取り組みを強化するものです」と Microchip 社 FPGA 部門技術フェローの Tim Morin は述べています。「この解析により、IP の保護、データの保護、物理的改ざんに対する保護のために本デバイスが既に備えている機能に加えて、シングルチップ暗号化手法の有効性が確認されました。物理的改ざんは見落とされがちですが、全ての電子システム、特にインテリジェント エッジの電子システムにおいては非常に大きな脅威です。」

Microchip 社の PolarFire FPGA は、IP(知的財産)、データ、サプライチェーンを保護するため、業界トップレベルのセキュリティアーキテクチャを実装しています。

- PolarFire FPGA の IP 保護には以下が含まれます。
 - AES 256 暗号設定ファイル(SHA 256 に基づく HMAC 認証済み)
 - CRI 社(Cryptography Research Incorporated)からライセンス提供された技術を使って、DPA (Differential Power Analysis)に対してプロセスを保護
 - 公開鍵暗号コア:鍵のセキュアな配布のための ECC (Elliptic Curve Cryptography: 楕円曲線暗号)
 - 真性乱数生成器
- PolarFire FPGA のデータ セキュリティ機能には以下が含まれます。
 - 最終アプリケーション向けの強化型暗号処理アクセラレータ
 - CRI 社の特許技術を使ったロイヤリティ フリーの DPA 保護アルゴリズム開発を可能にする CRI パススルー ライセンス

Microchip、PolarFire FPGA のシングルチップ暗号化設計フローが英国 NCSC の審査に合格した事を発表

2-2-2-2

- 偽造、再マーキング、過剰生産/過剰在庫のリスクを下げ、以下の機能を備えた PolarFire FPGA サプライチェーン セキュリティ機能
 - シリコン バイオメトリクス機能。PUF (Physically Unclonable Function: 物理的複製防止機能)を含みます。これにより、各デバイスを一意的に識別し、暗号的に検証ができます。

本デバイスは、Microchip 社のオンラインストア(www.microchipdirect.com)でライセンス提供している Libero® SoC 設計スイート(無償版を含む)でサポートされています。PolarFire FPGA および SoC 開発キットおよびハードウェアもこのオンラインストアで提供しています。

PolarFire ファミリーについて

Microchip 社の [PolarFire](#) デバイスは、他社比 2 倍の電力効率、軍用グレードのセキュリティ、業界最高の信頼性の実現において競合製品をリードしています。Microchip 社は、さらに小型化かつ低コスト化した産業用 IoT およびその他エッジ コンピューティング製品において計算能力をさらに強化し続ける事を目指しており、PolarFire 2 FPGA のロードマップに従って同製品カテゴリの拡充を計画しています。リアルタイム性に優れた Linux®対応 RISC-V ベース マイクロプロセッサ サブシステムを備える [PolarFire SoC](#) デバイスは、高速 FPGA ファブリック内の強化 RISC-V コア コンプレックスを利用して、構成可能な処理機能を新たに開発できる、市場で唯一の SoC です。カスタマイズされた計算機能を FPGA ファブリック内に構築するのに理想的なこの FPGA および SoC ファミリーは、省電力インテリジェント エッジがコンピュータの作業負荷を担うシステムの市場が急成長する上で主要な役割を果たしてきました。これらの[ソフトウェア ツール](#)を利用すると、PolarFire ファミリーを使った設計を今すぐ始められます。これらのツールは Microchip 社のウェブサイト提供しています。第 1 世代 PolarFire デバイスは全て量産中です。

リソース

高画質の写真は報道関係専用窓口までお問い合わせ頂くか、Flickr でご覧ください。掲載に許可は不要です。

- アプリケーション画像: www.flickr.com/photos/microchiptechnology/53137375615/sizes//

Microchip Technology 社について:

Microchip 社はスマート、コネクテッド、セキュアな組み込み制御ソリューションのトッププロバイダです。使いやすい開発ツールと包括的な製品ポートフォリオにより、リスクを低減する最適な設計を作成し、総システムコストの削減、迅速な商品化を実現できます。Microchip 社は産業、車載、民生、航空宇宙と防衛、通信、コンピューティングの市場で 125,000 社を超えるお客様にソリューションを提供しています。Microchip 社は本社をアリゾナ州

Microchip、PolarFire FPGA のシングルチップ暗号化設計フローが英国 NCSC の審査に合格した事を発表

3 – 3 – 3 – 3

チャンドラーに構え、優れた技術サポート、確かな納期、高い品質を提供しています。詳細は Microchip 社ウェブサイト(www.microchip.com)をご覧ください。

###

Note: Microchip 社の名称とロゴ、Microchip ロゴ、PolarFire は米国およびその他の国における Microchip Technology Incorporated の登録商標です。Libero は米国における Microchip Technology Incorporated の登録商標です。その他の商標は各社に帰属します。

詳細については、以下にお問い合わせください。

Daphne Yuen (Microchip 社): (852) 2943 5115

(メール: daphne.yuen@microchip.com)

松田、仙場 (共同 PR): (03) 6260 4863

(メール: mchp-pr@kyodo-pr.co.jp)

報道関係者の方へ: このニュースリリースのメールによる配信については、共同 PR 株式会社 松田もしくは仙場まで電話(03) 6260 4863 またはメール mchp-pr@kyodo-pr.co.jp でお問い合わせください。