報道関係者各位

2026 年 3 月 3 日
wolfSSL Japan 合同会社

wolfSSL、EU サイバーレジリエンス法（CRA）への全面対応を発表

コネクテッドデバイスおよび組み込み機器向けの CRA セキュリティ要件に対応

組み込み向け暗号技術およびセキュア通信ソリューションを提供する wolfSSL Inc.（本社：米国ワシントン州エドモンズ）は、同社の全製品において EU サイバーレジリエンス法（Cyber Resilience Act：CRA）に全面対応することを発表しました。

CRA は、EU 市場に投入されるデジタル要素を含む製品に対して、法的拘束力のあるサイバーセキュリティ要件を定める規制です。これには、セキュアな開発プロセス、脆弱性管理、市場投入後の保守責任などが含まれ、市場参入と直接的に結び付けられています。

wolfSSL の CTO である Todd Ouska は、次のように述べています。
「wolfSSL は、製品ライフサイクル全体にわたり、お客様が CRA 要件を満たせるよう支援することをお約束します。当社はその規定を遵守し、EU 市場で機器を販売するメーカーの皆様を、長期的な脆弱性管理や CVE 対応を含めて継続的にサポートしてまいります。」

製品ライフサイクル全体で CRA セキュリティ要件を支援

CRA は、セキュリティを考慮した設計から市場投入後の脆弱性対応に至るまで、継続的なセキュリティを重視しています。wolfSSL は、メーカーが実際にこれらの要件を実装する場合に、それを補助するように設計した組み込み向けセキュリティコンポーネントを提供し、長期サポートにも対応します。

■ セキュア通信およびデータ保護

wolfSSL は、コネクテッドデバイス向けに以下の暗号化通信機能を提供します。

- TLS 1.3 および DTLS 1.3 による通信データの暗号化
- 認証付き暗号および最新の暗号スイートのサポート
- 組み込みシステムやリソース制約が厳しい環境に適した構成オプション

■ **強固な暗号技術とセキュアな鍵管理**

CRA が求める暗号強度および鍵管理要件に対応するため、wolfSSL は以下を提供します。

- AES、RSA、ECC、EdDSA、耐量子暗号アルゴリズムを含む最新の暗号プリミティブ
- ハードウェアベースの鍵保護を行うためのセキュアエレメント、TPM、HSM との統合
- 規制対象市場向けの FIPS 140-3 認証済み暗号モジュール

■ **ファームウェア整合性とセキュアブート**

CRA は、認証されていない不正なファームウェア実行や既知の脆弱性の再混入から保護することを求めています。当社のセキュアブートローダーである wolfBoot は以下をサポートします。

- 起動時におけるファームウェアの暗号学的検証
- OTA（Over-the-Air）を含む認証済みファームウェア更新
- オプションのロールバック保護メカニズム
- 規制対象の組み込みシステムに適した決定論的検証パス(経路)

■ **脆弱性管理および協調的な開示**

市場投入後の保守は CRA の重要な柱です。wolfSSL は継続的義務をサポートするため、以下を整備しています。

- 構造化された脆弱性レポートの受け入れと協調的な開示プロセス
- CVE の追跡および迅速な修正の支援
- 長寿命の製品ライフサイクルに合わせた長期保守オプション

■ **透明性および SBOM 対応**

CRA は、サプライチェーンの透明性と脆弱性の追跡を目的に、メーカーに対しソフトウェア部品表（Software Bill of Materials：SBOM）の維持を求めています。

wolfSSL は以下を通じて SBOM ベースのコンプライアンスを支援します。

- 外部依存を最小限に抑えたソフトウェアコンポーネント
- 明確なコンポーネントトレーサビリティ
- セキュアな構成とライフサイクルでのメンテナンスをサポートするドキュメント
- FIPS 140-3、DO-178C、MISRA-C、IEC 62443 で使用される文書化方法への準拠

なお、CRA は個々のサードパーティのコンポーネントに対しては CRA 認証済みとすることを要求していません。しかしながら、メーカーには採用するすべてのソフトウェアコンポーネントのセキュリティ体制を理解し、維持する責任があります。

CRA と既存セキュリティ規格との整合

多くのメーカーは既に IEC 62443 や ETSI EN 303 645 といった規格に準拠しています。wolfSSL の文書化の実践とライフサイクルサポートは、既存のセキュリティプログラムと、新たに登場する CRA 適合性評価の仕組みとの橋渡しを支援します。

決定論的な組み込み環境における暗号、セキュアブート基盤、構造化された脆弱性対応プロセスを組み合わせることで、wolfSSL は技術的なセキュリティ要件と規制要件の双方を満たす製品設計を可能にします。

CRA 施行に向けた準備

CRA 施行が近づくにつれ、メーカーはセキュアな製品設計だけでなく、継続的な脆弱性管理、文書化されたセキュリティプロセス、そしてライフサイクルサポートの実証が求められています。CRA は、サイバーセキュリティを設計時における考慮事項から、市場参入に直接結びついた継続的なコンプライアンス義務へと移行させます。

wolfSSL の組み込み向けセキュリティポートフォリオは、決定論的暗号、セキュアブート基盤、構造化された脆弱性対応プロセスを統合し、メーカーが CRA に基づく技術的および規制上の要求事項の両方に対応できるよう支援します。

wolfSSL について

wolfSSL Inc.は、速度、サイズ、移植性、機能、標準規格への準拠に重点を置き、高性能で軽量なセキュリティソリューションを提供しています。

当社の TLS 製品と wolfCrypt 暗号ライブラリは、政府機関、自動車、航空電子工学をはじめとする幅広い業界で安全な設計を支えています。wolfBoot セキュアブートローダーは、ファームウェア更新の完全性を確保し、さらなる保護レイヤーを追加します。政府機関向けには FIPS 140-3 認証を複数取得、航空電子工学分野では RTCA DO-178C レベル A 認証をサポートし、自動車分野では MISRA-C 規格に準拠しています。2004 年の創業以来、世界各国で 2,700 社を超えるカスタマーに採用されています。

オープンソース企業として、透明性を保ち、お客様が内部構造を確認できるようにしています。量子脅威から保護するための自社開発の耐量子暗号アルゴリズムは CNSA 2.0 標準に準拠しています。また脆弱性修正への対応時間は平均 36 時間であり、長期間にわたり安定した商用サポートを提供しています。

wolfSSL Inc.は米国ワシントン州シアトルに本社を置き、モンタナ州ボーズマン、オレゴン州ポートランドなどに拠点があります。wolfSSL Japan 合同会社の技術サポートセンターでは、日本人専任スタッフによるサポートサービス、カスタマイズサービスなどを提供しています。

【お問い合わせ先 】
wolfSSL Japan 合同会社　担当: 須賀
Email: info@wolfSSL.jp
TEL: 050-3698-1916
https://www.wolfssl.jp
https://x.com/wolfSSL_Japan