FIPS140-3 を取り巻く環境に対する考察

一般社団法人セキュア IoT プラットフォーム協議会

理事長　辻井 重男

２０２３年６月

1. はじめに

米国では、2021 年 5 月に発生した米国東部の 50%近くの燃料供給を担うコロニアルパイプラインのランサムウェア攻撃による大きな社会的混乱の発生や、2021 年 4 月のワシントン D.C.メトロポリタン警察のハッキングなどのインシデントの発生を背景に、特に重要インフラのセキュリティ強化が進められている。

このような背景を受けて、バイデン政権は 2021 年 5 月 21 日に大統領令を発布し、「国家重要機能を支えるシステムのサイバーセキュリティと回復力に重点を置いて、国家の重要インフラを保護することが、バイデン政権の方針である」と宣言している。

このような状況の中、現在注目される安全基準が、NIST(米国国立標準技術研究所)が定める暗号モジュールのセキュリティ標準規格「FIPS140-3」である。コンピュータおよび電気通信システム（音声システムを含む）において機密情報を保護するための暗号モジュールとして、またセンサーからクラウドサービスにおける安全なデータ伝送を行う上でも FIPS140-3 適応が求められているわけである。

2. FIPS140-3 とは

FIPS140-3 は、2019 年 3 月に認証された米国標準技術研究所(NIST：National Institute of Standards and Technology）が制定した、暗号モジュールに関する標準規格である。暗号モジュールの安全な設計、実装、運用に関連する領域をカバーするものである。2020 年 9 月から、米国とカナダが共同で実施している暗号モジュールのセキュリティ認定プログラム CMVP(Cryptographic Module Validation Program)による認証が開始されている。

現在、市場には旧バージョンである FIPS140-2 と FIPS140-3 準拠のシステム及びクラウドサービスの 2 つが存在し、併用されているが、2022 年 4 月 1 日以降は、FIPS140-2 の CMVP テスト受付が終了しており、それ以前に FIPS140-2 CMVP テスト申し込みを行い、適合検証を受けたシステム及びクラウドサービスも 2026 年 9 月 21 日までに FIPS140-3 への移行が求められている。

3. FIPS140-3 を取り巻く動向

米国サイバーセキュリティ・社会基盤安全保障庁(CISA)の「国家サイバーセキュリティ保護システム（NCPS: National Cybersecurity Protection System)」では、昨今の IT インフラのクラウド移行を受けて、2021 年 5 月 14 日に発行された「クラウドインタフェース リファレンスアーキテクチャ」において、重要インフラに関連するソフトウェアベンダー、サービス提供ベンダー（Web サービス含む)、クラウドサービスプロバイダーに対しても、FIPS140-3 の導入・実装の義務を示している。

またその後も米国政府機関からは、続々とこの流れをサポートする大統領令やサイバーセキュリティに関わるドキュメントがリリースされ、国家安全保障省、国防省購買要件に限定されていたものが、民生品や民間主体で運用されているシステムやクラウドサービスにおいても、製品やサービスが安全に構築され、運用するために同様に対策が求められるようになってきている。それに合わせて Microsoft、AWS、Google、Zoom など個人法人情報や様々な情報コンテンツを扱う、大手クラウドサービスおよび Web サービスを提供する企業も FIPS140 シリーズの認証を受けており、順次最新バージョンである FIPS140-3 への移行が進むと考えられる。

また現在、FIP140-3 への移行期限は 2026 年 9 月 21 日とされているが、国家安全保障上懸念すべき攻撃事案の発生などの国際環境の変化により、FIPS140-3 の適応が前倒しになる可能性もあると考えられる。

4. まとめ

以前よりセキュア IoT プラットフォーム協議会では、国際安全基準に基づくものづくりにおいて、IoT 機器の真正性担保、製造から破棄に至るライフサイクルマネジメント、および IoT 機器に組み込まれるソフトウェアのサプライチェーン管理により、IoT システム全体の安全性担保に対して研究を行ってきた。今回はその基盤となる暗号モジュールの規格である NIST FIPS140-3 に着目し、米国政府の動きや民間の取組みについてまとめてみた。

なお FIPS140-3 は IoT 機器のようなハードウェアだけではなく、システム全体やクラウドサービスにも対応が求められている。先日セキュア IoT プラットフォーム協議会よりリリースさせていただいた「日本デジタルトランスフォーメーション推進協会と連携し、AlmaLinux OS 推進によるオープンソースセキュリティ啓発活動を展開　～安全なソフトウェアサプライチェーンの実現に向けて～」でも取り上げさせていただいた AlmaLinux OS はオープンソースソフトウェアでありながら、いち早く FIPS140-3 に準拠した OS である。

・日本デジタルトランスフォーメーション推進協会と連携し、AlmaLinux OS 推進によるオープンソースセキュリティ啓発活動を展開
～安全なソフトウェアサプライチェーンの実現に向けて～」
(https://www.secureiotplatform.org/news/2023-05-22)

当然この動きは米国に留まらず、待ったなしで、我が国の重要インフラを中心に産業界にも大きな影響を与えることは明らかである。政府機関に関連するシステムの調達要件だけではなく、民生品にも対応が求められるようになるのは間違いないと考える。

そのため早い段階で情報をいち早く取得し、その準備を整えておくことが重要となる。

当協議会では、引き続き会員の皆様の力を結集し、安心安全な IoT 社会の構築に向けて、取り巻く環境変化をいち早く捉え、国際安全基準や日本政府の施策を基に、セキュリティ対策の推進に取り組んでいく予定である。