水と安全は“ただ”と思っていませんか?

狙われる産業制御システム、東芝は安全・安心をどのように確保したのか

東芝は、現実のものとなりつつある産業制御システムへのサイバー攻撃に対応するため、産業用コントローラーで制御システムセキュリティの国際標準である EDSA 認証を取得した。この EDSA 認証の取得に向けてどのような取り組みを行ったのだろうか。

TOSHIBA
Leading Innovation

CSSCで行われた認証書授与式の様子と「ユニファイドコントローラ nvシリーズ“type2”」

徐々に現実のものとなりつつある制御システムを狙う脅威

工場の生産ラインやプラント、あるいは水道や電力といった社会インフラの運用を担う制御システム。従来、インターネットなど外部からのサイバー攻撃とは無縁と考えられてきた領域だが、汎用プラットフォームの採用が広がり、その前提は崩れつつある。幸いにして国内では、制御システムを狙ったサイバー攻撃による大規模なインシデントは今のところ発生していない。しかし万一サイバー攻撃による事故が起これば、自社はもちろん、製品の供給先、ひいては社会全体に影響が及びかねない。こうした危機感を背景に、産官が連携して制御システムのセキュリティの強化に取り組む機運が高まってきた。2012 年に発足し、宮城県多賀城市にテストベッドなどを設置してセキュアな制御システムの研究開発や認証活動に取り組んでいる「制御システムセキュリティセンター（CSSC）」は、その一例だ。

鉄鋼や石油化学プラントに始まり、水道設備や電力など重要インフラ、道路、ビルシステム、放送に至るまで、あらゆる分野向けにコンポーネントを提供している東芝も、設立時から CSSC に参加し、制御システム全般のセキュリティ向上に取り組んでいる。同社は 2017 年 2 月 8 日、産業用コントローラー「ユニファイドコントローラ nv シリーズ “type2”」について、制御システムセキュリティの国際標準に基づく「ISASecure EDSA（Embedded Device Security Assurance）認証」を、CSSC 認証ラボラトリーから取得し、安全なシステム構築のための取り組みをさらに前進させた。認証取得にあたっては、日本シノプシスのファジングテストツール「Defensics」が一役買ったと言う。その狙いと経緯を聞いた。

安心・安全を高める取り組みを証明すべくEDSA認証取得へ

ほぼあらゆる産業向けにコントローラーや産業用コンピュータ、センサーなどを開発、提供してきた東芝は、日本の産業と社会を支える縁の下の力持ちだ。その製品の歴史は 1970 年代半ばにさかのぼり、時代と技術の変化に応じてシステムを提供してきた。この内、さまざまな制御を行うコントローラーは、かつては鉄鋼向け、上下水道向け、電気・機械向け……といった具合に、分野ごとに個別に開発されていた。東芝は徐々にそれらの統合を進め、1999 年にはシーケンス制御（S）と計装制御（L）、コンピュータ処理（C）を統合した「V シリーズ」を、そして 2007 年には共通プラットフォームを採用しさらに統合を進めた「nv シリーズ」をリリースしている。

nv シリーズなどを展開する、東芝 インフラシステムソリューション社 産業システム統括部 計装機器事業統括の岡庭文彦氏は、「nv シリーズは、『統合』『安心・安全』、そして『環境への調和』をコンセプトに、全ての産業分野をカバーするユニファイドコントローラとして提供しています。高速性を実現するため、業界初の高速シリアル I/O システム『TC-net I/O』を採用する他、国際標準言語である IEC 61131-3 の命令をハードウェアで直接実行できます。また、信頼性の確保に向けた監視・制御ネットワークの冗長化も図っています」と語る。

nv シリーズのコンセプトの 1 つに「安心・安全」がある通り、東芝では以前か

らコントローラーのセキュリティを重視してきた。「日本企業は、どうしても水と安全は“ただ”という意識が強く、対策もベンダーがやってくれるものと思いがちです。しかし、適切なセキュリティを実現するには相応の投資が必要です。まずセキュリティの重要性を訴え、そうした意識を変えていく情報を、われわれのような制御機器を扱う事業体から発信していかなければならないと考えました」（岡庭氏）。近年は制御システムを狙ったサイバー攻撃が海外で複数発生し、脅威が現実のものになりつつある。こうした状況を受けて徐々にだが、セキュリティにきちんと投資しようという機運が高まってきたと岡庭氏らは感じている。

こうした追い風を受けて同社は、コントローラーの安心・安全を高める取り組みを進めてきた。岡庭氏は「では、そのセキュリティをどのように担保できるのか。そう考えると、我々自身が宣言するだけでなく、国際標準に則った第三者認証を得ることで示せると考えました」と説明する。

柔軟性、拡張性に優れた「Defensics」で認証取得

東芝の nv シリーズには、目的や適用規模に応じて複数のラインアップが用意されている。特に安全性を重視しているのが「nv-safety シリーズ」だ。鉄鋼プラントなどの PLC として用いられている nv シリーズの“type1”について、機能安全に関する国際規格である IEC 61508 の認証取得を 2015 年 2 月に発表している。

nv シリーズとして次に取り組んだのが、DCS である“type2”での EDSA 認証の取得だった。EDSA は、国際認証組織の ISA Security Compliance Institute（ISCI）が運営している、制御機器のセキュリティ保証に関する認証制度だ。IEC62443 標準のフレームワークがベースとなっており、「ソフトウェア開発の各フェーズにおけるセキュリティ評価（SDSA）」「セキュリティ機能の実装評価（FSA）」「通信の堅牢性テスト（CRT）」という 3 つの評価項目がある。

EDSA 認証取得に取り組み始めた東芝では、当初、CSSC が推奨するファジングツールを用いてユニファイドコントローラを検査し、指摘された問題を修正して認証に耐えられる開発に取り組んだ。認証取得作業を担当した東芝 インフラシステムソリューション社 府中インフラシステムソリューション工場 パワーエレクトロニクス・計測制御機器部 制御機器開発担当 主査の梅田裕二氏は「このツールは、TCP/IP をはじめとする標準プロトコルをサポートしており、CRT で求める 6 つの必須サービスの維持についてテストすることはできました。しかし、それら以外の DCS 独自のプロトコルのテストはできませんでした。ここで問題になったのが、評価項目の 1 つである SDSA への対応です。SDSA では、標準プロトコルだけでなく全てのプロトコルについてファジングを行う必要があると定めており、独自プロトコルやアプリケーションレイヤーのプロトコルについてもテストする必要がありました」と、振り返る。

東芝 インフラシステムソリューション社の岡庭文彦氏、梅田裕二氏、同社 研究開発センターの春木洋美氏

そこで採用したのが、200 種類以上のプロトコルや多様なファイルフォーマットをサポートしている日本シノプシスのファジングツール「Defensics」だった。東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 主任研究員の春木洋美氏は、「我々自身が一からスクラッチで作って対応するのは大変な上、品質保証の面でも万全とは言えません。その点 Defensics は、設定さえ記述すれば独自プロトコルについてもテストが実行できます。EDSA 認証の公式な試験ツールとしても認定されています」と述べる。

春木氏が所属する研究開発センターでは、梅田氏らが所属する部署から提供されたプロトコル仕様に基づいて、Defensics でのテスト用に拡張定義を行った。春木氏は「ネットワークアナライザソフトウェアである『Wireshark』のプラグインがあり、それを使って自動的に通信を分析して仕切ってくれるため、開発工数を減らせました。また、ファジング検査は意外と時間がかかるもので、その間ずっと人間が貼りついている訳にはいきません。Defensics ではスクリプトを活用でき、テスト中にエラーが発生したらリセットして復帰させるといった仕組みを自動化できたのもメリットです」と述べる。

今回の認証取得では利用していないが、Defensics では Java を用いた拡張も可能であり、柔軟性があることも特長だ。「今後、さまざまな制御システムのセキュリティを考える上でも、検査ツールの拡張性は意識しています」（春木氏）。

他の部門にもセキュリティの浸透を

こうして東芝は無事、nv シリーズ“type2”の EDSA 認証を取得した。研究開発センターに所属する春木氏は「東芝社内には他にも多くの部門がありますが、そういった所にもセキュリティの意識を徐々に浸透させていきたいと考えています。お客様の意識が高まったタイミングで必要な技術を提供できる体制を用意することが我々の役割です」と意気込む。梅田氏も「一度認証取得を経験したことで、ノウハウを蓄積できました。例えば PLC の“type1”についても、要望があればすぐに対応できるよう準備を進めています」と語る。

岡庭氏は並行して、社内外でセキュリティに関する啓蒙活動も進めていくとした。「その際に Defensics のようなツールをうまく活用できたら、より安心・安全なインフラが実現できるのではないでしょうか」と述べている。

制御システムを狙った脅威は現実のものになりつつあるが、一方で「そう遠くない将来、セキュリティに対応したコンポーネントが標準となるでしょう」（梅田氏）。東芝はもう、その日のための準備ができている。

SYNOPSYS®

www.synopsys.com/japan/software

日本シノプシス合同会社 営業本部 ソフトウェア インテグリティグループ
〒158-0094 東京都世田谷区玉川2-21-1二子玉川ライズオフィス
TEL: 03-6746-3600 Email: sig-japan-sales@synopsys.com

※この冊子は、MONOist（http://monoist.atmarkit.co.jp/）に2017年4月に掲載されたコンテンツを再構成したものです。
http://monoist.atmarkit.co.jp/mn/articles/1704/13/news003.html