ユニファイドコントローラnvシリーズtype2のセキュリティー認証への対応

Security Certification Obtained for Unified Controller nv series type2

伊東　雄 ITO Yu　立野　元気 TATENO Genki　梅田　裕二 UMEDA Yuji

社会インフラシステムでは，セキュリティー機能の確立や向上の重要性が高まっており，計測・制御システムにおいても，制御システムセキュリティーへの対応が求められている。

東芝インフラシステムズ（株）は，“ユニファイドコントローラnvシリーズtype2”で，組み込み機器のセキュリティー認証であるISASecure® EDSA（Embedded Device Security Assurance）認証を取得した。認証されたtype2を基幹コントローラーとすることで，サイバー攻撃などの脅威に対し，セキュアな制御システムを提供できる。

The importance of system security continues to increase in the field of measurement and control systems for infrastructure facilities. This is particularly true in the case of social infrastructure systems.

Toshiba Infrastructure Systems & Solutions Corporation has obtained ISASecure® Embedded Device Security Assurance (EDSA) certification for its Unified Controller nv series type2. The use of the type2 controller as a core controller provides control systems with robust security against the threat of cyberattacks.

1. まえがき

重要な社会インフラを標的としたサイバー攻撃の報告が増加し，制御システムのセキュリティー対策や管理の重要性が高まっている。従来の制御システムは，外部ネットワークから隔離された構成や，独自の通信プロトコルを用いて構築されたクローズドなシステムであったため，比較的安全であると信じられてきた。しかし，ネットワークを介さずに，USBメモリーなどの外部メディアを経由して感染することで，特定の制御システムを攻撃するマルウェア Stuxnetの出現は，制御システムにおけるセキュリティー対策を見直すきっかけとなった。また，近年はIoT（Internet of Things）技術の普及やネットワークのオープン化により，制御システムの構成が大きく変化しつつある。外部ネットワークと接続した制御システム，汎用機器や一般的な通信プロトコルを用いて構築された制御システムなどが増加しており，制御システムにおいても多様な脅威を想定する必要が生じている。IoT機器を狙うマルウェアの中には，感染した機器を利用してほかのシステムへの攻撃を行うMiraiなどもあり，制御システムが，標的となるだけでなく更に他者への攻撃に利用されるリスクが高まっている。

こうした背景から，東芝インフラシステムズ（株）は，制御システムにおけるセキュリティーへの対応を進めている。当社が提供する産業用コントローラーの“ユニファイドコントローラnvシリーズtype2”（以下，type2と略記）（**図1**）は，国際的に認められた第三者認証機関である技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）の認証ラボラトリーによる審査に合格し，2017年2月にISASecure® EDSA認証を，東芝グループで初めて取得した。ここでは，認証取得した製品と審査の内容について述べる。

図1. EDSA認証を取得したユニファイドコントローラnvシリーズtype2

高い信頼性と大規模システムの高速制御に加え，EDSA認証に対応したセキュリティー機能を備えている。

EDSA-certified Unified Controller nv series type2

2. ユニファイドコントローラnvシリーズ

当社は，制御コンポーネントとして使用されるPLC（Programmable Logic Controller）及びDCS（Distributed Control System）として，“ユニファイドコントローラnvシリーズtype1”（電気制御用）及びtype2（計装制御用）を提供している。“ユニファイドコントローラnvシリーズ”は，高い信頼性と大規模システムの高速制御を特長とし，これまでに，様々な分野で多くの実績を積み重ねてきた。その上，安全PLCや中小型PLCなどのラインアップにより，システムに応じた柔軟な対応を可能にしたほか，SOE（Sequence of Event）表示や，診断機能，アラーム管理パッケージ，プロセス制御最適化ツールなどを製品化し，各種のアプリケーションに対応できるようにすることで適用範囲を広げている。また，各種フィールドバス，プログラム言語の国際標準規格などに対応しているほか，欧州RoHS（Restriction on Hazardous Substances）指令（電気・電子機器における特定有害物質の使用制限に関する指令）などに対応し，環境にも配慮している。更に，IoT対応の要求に応えた“ユニファイドコントローラnv-packシリーズtypeFR”もリリースした[1), 2)]。

3. type2のセキュリティー機能の特長

type2は，制御システムの資産（制御データやパラメーターなど）を守るため，セキュリティー機能を備えている。主な機能としては，アクセス制御があり，この構成を**図2**に示す。type2はサーバー／クライアント機能を備えており，コントローラーと通信するためには，接続するデバイスがコントローラーに認証される必要がある。コントローラーは，認証されていないデバイスからの要求には応答しないため，外部から不正に操作されるのを防ぐことができる。また，認証履歴を記録しているので，不正アクセスの有無を確認でき，システムのセキュリティーをより向上させることが可能である。

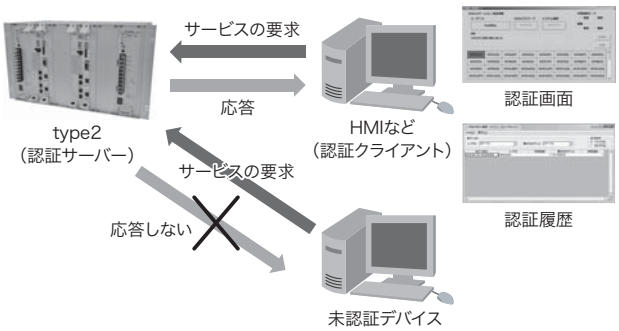


図2. type2におけるアクセス制御
認証サーバーであるtype2は，ユーザー認証で認証済みのデバイスに対してだけ応答を行う。
Access control of type2 controller

更に，通信堅牢（けんろう）性を向上させることで，不正パケットや多量の通信による影響をより小さくしている。例えば，不正パケットなどを受信したとき，type2ではこれを破棄し，動作を継続させる。これにより，DoS（Denial of Service）攻撃やDDoS（Distributed Denial of Service）攻撃などを受けた場合でも，システムの停止を防ぎ，安全に稼働できる。

4. EDSA認証

EDSA認証は，制御機器（組み込み機器）のセキュリティー保証に関する認証制度である。国際計測制御学会（ISA：International Society of Automation）のISCI（ISA Security Compliance Institute）がスキームオーナーであり，特に海外では，EDSA認証を取得していることが，石油化学を中心とした事業者の調達要件として盛り込まれる傾向にある。また，EDSA認証はIEC 62443（国際電気標準会議規格62443）シリーズに統合される見込みであるため，様々な業界から注目されている。EDSA認証の評価は，CRT（Communication Robustness Testing：通信の堅牢性テスト），FSA（Functional Security Assessment：セキュリティー機能の実装評価），SDSA（Software Development Security Assessment：ソフトウェア開発におけるセキュリティー評価）の三つの項目で構成されており，以下では，type2のセキュリティー耐性を，これらの認証項目ごとに述べる[3)]。

4.1 CRT

type2には，上向きサービスと下向きサービスの二つの通信機能がある。下向きサービスは制御プログラム演算及び入出力機能，上向きサービスはHMI（Human Machine Interface）などのためのプロセスのビュー，コマンド，アラームなどの機能である。また，通信プロトコルとしては，IEEE 802.3（電気電子技術者協会規格 802.3）（Ethernet），ARP（Address Resolution Protocol），IPv4（Internet Protocol version 4），ICMPv4（Internet Control Message Protocol version 4），UDP（User Datagram Protocol），TCP（Transmission Control Protocol）の6種類のほか，アプリケーションレイヤーのプロトコルやサービスなどを有している。

CRTにおいては，ISCI認定の試験機器を使い，試験（攻

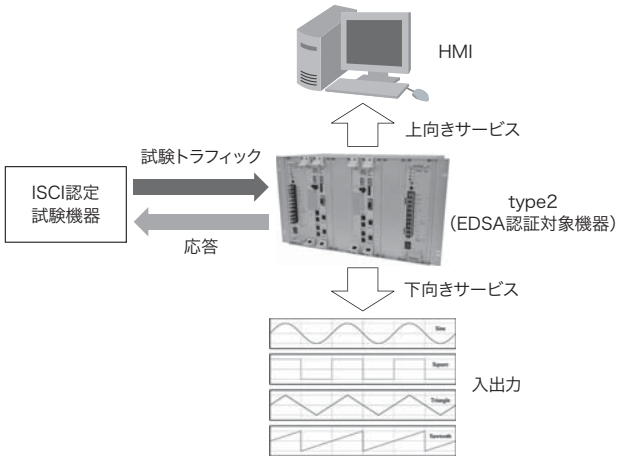


図3. CRTの概要
CRTでは，試験（攻撃）中でのサービス維持が求められる。
Overview of communication robustness testing (CRT)

撃）中のtype2で，下向きサービスと上向きサービスが維持されることが確認されている。CRTの概要を**図3**に示す。

4.2 FSA

type2のセキュリティー機能には，ユーザー認証，認証履歴の保管などのアクセス制御のほか，データの完全性・機密性の確保，通信の暗号／復号などがある。

FSAでは，設計仕様書やユーザーマニュアルなどのドキュメント及び動作試験により，EDSAが要求するセキュリティー機能要件をtype2が満たしていることが確認されている。

4.3 SDSA

type2のセキュリティー機能開発のプロセスでは，設計部門のソフトウェア開発プロセス（一般的なV字モデル）に，セキュリティーに関する追加要件を加え，各工程で設計部門外のセキュリティー専門家を交えて設計妥当性の確認を行っている。セキュリティーに関する追加要件を**表1**に示す。

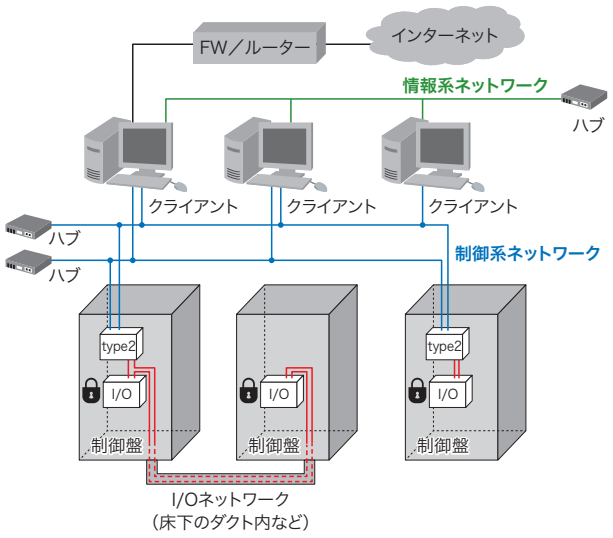
セキュリティー開発プロセスは一般の開発プロセスと大きな相違点があり，制御システムの守るべき資産とそれを脅かすリスク（脅威モデル）をあらかじめ定義し，許容されるレベルまでリスクを低減する施策を仕様として盛り込んでいる。この仕様については，システム部門やセキュリティー専門家の知見を生かし，コンポーネントのセキュリティー機能を強化するほか，システムの使用条件や，ユーザーの前提・制限事項として反映している。その一つに物理的破壊攻撃への対策がある。例えば，悪意ある第三者が物理的に制御盤を破壊できるようなユーザー環境では，コンポーネントの機能だけでは防御できないリスクが存在するので，制御システムのセキュリティーをより高めるために，推奨するシステム構成（**図4**）や使用環境をユーザーマニュアルなどで周知している。

また，製品リリース後の継続的なサポートのため，“東芝PSIRT（Product Security Incident Response Team）”活動に従い，脆弱（ぜいじゃく）性報告の受領段階から，製品影響分析や，パッチリリース，顧客連絡などの対応プ

表1. ソフトウェア開発プロセスにおけるセキュリティーの追加要件
Security requirements for software development processes

項　目	活動フェーズ
PH1	セキュリティ管理プロセス
PH2	セキュリティ要求事項仕様
PH3	ソフトウェアアーキテクチャ設計
PH4	セキュリティリスクアセスメントと脅威のモデル化
PH5	詳細ソフトウェア設計
PH6	セキュリティ指針文書
PH7	モジュールの実装と検証
PH8	セキュリティ結合テスト
PH9	セキュリティプロセス検証
PH10	セキュリティ対応計画
PH11	セキュリティ検証テスト
PH12	セキュリティ対応実行

PH：フェーズ　出典：CSSC認証ラボラトリー Webサイト[3]



FW：ファイアウォール
I/O：信号の入力／出力を行う機器

図4. 制御システムの構成例
制御盤やダクトを用いて，コンポーネントの機能だけでは防御不能な物理的破壊などへのリスク対策を推奨している。
Example of system configuration of type2 controller

ロセスを定義し，運用している。

SDSAでは，type2の開発ドキュメント（計画や成果物）とレビュー記録（PDCA（Plan-Do-Check-Act）プロセスの妥当性と記録確認）により，必要要件を満足していることが確認されている。

5. あとがき

当社は，type2において，セキュリティー機能の開発を行い，EDSA認証を取得した。これにより，当社の産業用コントローラーでセキュアな制御システムを構築することが可能になった。

今後，セキュリティー開発で得られたノウハウを他機種の開発にも生かし，セキュリティー機能を高めた製品の拡充を図るとともに，セキュリティー技術を更に強化することで，よりセキュアな制御システムコンポーネントを提供していく。

文　献

⑴ 岡部基彦，ほか．設備機器のIoT化に柔軟かつセキュアに対応可能な産業用システム機器．東芝レビュー．2017，72，5，p.42–45．<http://www.toshiba.co.jp/tech/review/2017/05/72_05pdf/b04.pdf>，（参照 2018-05-22）．

⑵ 阿南和弘，ほか．計測・制御システムの動向と取り組み．東芝レビュー．2017，72，5，p.32–36．<http://www.toshiba.co.jp/tech/review/2017/05/72_05pdf/b02.pdf>，（参照 2018-05-22）．

⑶ CSSC認証ラボラトリー．“ISASecure® EDSA認証とは”．CSSC認証ラボラトリー．<http://www.cssc-cl.org/jp/about_edsa/index.html>，（参照 2017-05-21）．

・ISASecureは，ISA Security Compliance Instituteの商標。

伊東　雄　ITO Yu
東芝インフラシステムズ（株）
府中事業所
パワーエレクトロニクス・計測制御機器部
Toshiba Infrastructure Systems & Solutions Corp.

立野　元気　TATENO Genki
東芝インフラシステムズ（株）
府中事業所
パワーエレクトロニクス・計測制御機器部
Toshiba Infrastructure Systems & Solutions Corp.

梅田　裕二　UMEDA Yuji
東芝インフラシステムズ（株）
府中事業所
パワーエレクトロニクス・計測制御機器部
Toshiba Infrastructure Systems & Solutions Corp.