

# 制御システムセキュリティ

## 第三者認証が裏打ちする安全と安心

技術研究組合制御システムセキュリティセンター 理事長  
電気通信大学 情報理工学研究科 教授

### 新 誠一

21世紀の生活はネットワーク化されたIT機器で支えられている。それは重要インフラも同様である。このサイバーセキュリティ対策を行うために産学官の連携で設置されたのがCSSC（技術研究組合制御システムセキュリティセンター）である。ここでは、CSSCが今年度始めたEDSAと呼ばれる認証事業について報告する。

#### 1 はじめに

現在の社会はスマートフォン、スマート家電に自動改札、自動販売機などのコンピュータ製品に支えられている。そして、これらのバックボーンが電気、ガス、水道、交通、通信などの重要インフラである。

この重要インフラが2010年夏にサイバー攻撃された。ターゲットはイランのナタンツにあるウラン濃縮工場であった。そして、2011年3月11日に起こった東日本大震災では重要インフラが停止した。国内では当たり前とされていた安全、安心が剥ぎ落された。それは被災地だけでなく、電力不足という形で日本全国に現在でも影響を及ぼしている。

この二つの出来事を合わせて考えるとサイバー攻撃に対する重要インフラの防護が急務である。そこで、2012年3月にCSSC（技術研究組合制御システムセキュリティセンター）が設置された[1]。2013年5月には被災地である宮城県多賀城市に構築した模擬プラント7基をお披露目した。実は稼働中の重要インフラを用いて、サイバー攻撃の演習や防御手法の開発を行うことはできない。そのため、発電、ガス、上下水、化学プラント、組立工場、ビル、スマートグリッドなどの実在のシステムと同等な模擬プラントが必要である。この設備を使って、電気、ガス、ビル、化学プラントなどのサイバー演習を行うと共に対策の技術研究を行っている[2]。

昨年度は経済産業省の支援を受けて国際標準に基づくEDSA（Embedded Device Security Assurance）の予備認証を行った。2014年7月には、横河電機と日立製作所の二社の製品に対し正式認証を発行した[3]。これは、国内外に安全、安心を届けるといふ本組合の設置方針に沿った活動である。以下、これらの経緯を少し詳しく紹介する。

#### 2 日本

我が国自体は高度成長を経て人口減少に向かっている。これを日本の衰退ととらえる向きもある。私自身は日本の良さが世界に広がりつつあると認識している。最近、和食がユネスコの無形文化遺産に登録された[4]。素材の味を活かし、健康に留意し、見た目の美しさにも配慮した日本食は世界の誇りである。しかし、日本で生まれ、日本で育ち、日本で生活している人々にとって和食は当たり前のものである。そのため、和食以外の食べ物を求める傾向もある。この結果、東京がパリやニューヨークを押さえて世界一星が多い都市にミシュランガイドでは認定されている。和食が海外に広まると共に、国内で世界中の食べ物が味わえる。これこそが、真のグローバリゼーションだと認識している。

その素晴らしさは食べ物だけではない。ほとんど停電をしない電力網、安全なガス事業、蛇口から直接飲める水を供給する水道、そして、汚水を処理し、雨水を適切にコントロールする下水網。加えて、LTEを始めとする高速無線通信網とそれを支える光通信によるバックボーン。全国に張り巡らされた空路に鉄道網、道路網。銀行ネットワークにコンビニ。これら当たり前の光景が日本人以外には信じられない贅沢だろう。

この贅沢は現在、マイコンと通信網で支えられている。1972年に開発されたマイコンが重要インフラ、家電、自動車に搭載されていったのが20世紀末の日本。2000年からは、それがネットワーク化されていった。お陰で、スマートフォン一つで経路探索、自動改札、自動販売機、銀行決済など主要な作業ができる国が誕生した。それがIT立国日本である。

### 3 グローバル化

日本の良さは世界に伝搬している。とくに、21 世紀になって技術を持つベンダが人口減少による国内市場の限界を認識し始めてからは伝搬が加速している。当初はコストの安さから海外展開していくが、進出先の成長に連れて人件費は高騰していく。この高騰は、二つの変化を誘発する。一つは IT を用いた工場の自動化である。これは日本が経験済みの進歩の過程である。もう一つは給与の高騰による展開先に生まれる新たな市場である。これは現地工場の自立化につながる。つまり、海外展開先の消費者が望む製品を現地の工場で企画、設計して素早く生産するということがある。調達や購買、販売までも連携できなければいけない。そして、この対応には世界で一番厳しい消費者をお客様としている日本にノウハウがある [5]。

この二つの変化を 4 年目となる一般社団法人 日本能率協会主催の GOOD FACTORY 賞 [6] 審査委員長として痛切に感じている。書類審査をパスした国内外の工場を審査委員が手分けして現地審査に赴いているが、日本の物作りのノウハウを吸収し、自立化していく状況には毎年目を見張らされている。昨年訪れたインドネシアでは Black Berry の携帯電話を持つことがステータスであった。審査委員間で、ここにスマホが普及すると社会が変わると話し合っていた。それが、今年には iPhone や Andoroid が急速に普及し始めている。

この賞は日本の物作りがグローバル化しているという視点と、その中で国内工場が存続をかけた挑戦を続けているという視点で工場マネジメントを表彰している。どちらも、IT 活用が大きな鍵の一つである。

### 4 IT 機器の停止、暴走

道具を使うことが人間と他の動物を区別する一つの定義である。そして、身の回りの道具にマイコンを搭載していったのが 20 世紀の電子化である。21 世紀は、それをネットワーク化した。両方を含めて IT 化と呼ぶならば、現在の人間の生活を支えている道具の大半は IT 機器である。身近な家電や自動車だけでなく、電気もガスも水道も決済もすべて IT 機器という便利な道具が生活を支えている。

一方、支えられている人間のほうは IT 機器についてどれだけの理解をしているのだろうか。専門用語でブラックボックス化と呼ばれているが、IT 機器の表層を触って知っているつもりの素人、スマホ難民と呼ばれる高齢者。いやいや数千万行に達したスマホの OS、スマホのアプリの作成者もソフトの全容を知らない。ハードや通信方式、コンテンツ

に各種センサ。物知りのふりをしている私もスマホの全容は分からない。そのスマホが中心となって家電や自動車を連携させる。更に、それらは電力やガスなどのエネルギーや証券や外為などの金融取引とも連携を深めている。正に IT 漬けの毎日であり、IT 抜きでは生活が成り立たない。

IT 機器はサイバー攻撃に毎日、毎時間、毎瞬晒されている。どの事業所の情報システム管理者も WEB サーバーへの頻繁な攻撃を認識している。そして、同じく頻繁に出される脆弱性情報に応じてファイアウォールや管理する端末の設定を変える煩わしさに忙殺されている。関係者からは怒られることはあっても、誉められることはない職場である。

今、制御機器もネットワーク化され IT 機器となった。制御機器は重要インフラにも用いられているが、ここも誉められることがない職場である。しかし、重要インフラがサイバー攻撃に襲われると結果は悲惨である。電気の停止をブラックアウトと呼んでいるが、電力だけでなく、ガス、通信、交通なども一斉に攻撃を受け停止する可能性がある。この対策は急務であり、CSSC では研究開発、訓練、啓蒙など各方面で対策を進めている。その中でも最新の成果である認証業務に絞って話をしたい。

### 5 EDSA 認証

サイバー攻撃は日に日に進化している。対策は進化を先回りする必要がある。その意味で完璧な対策は存在しない。そのような状況の中で安全、安心を担保する仕組みが第三者認証である (図 1)。作成者、使用者と利害関係のない組織による国際標準に基づいた認証である。CSSC では、一般コントローラのサイバーセキュリティ国際標準 IEC62243 に基づく認証事業を始めた。図 2 に示すように CRT (Communication Robustness Testing) というブラックボックス検査、FSA (Functional Security Assessment)

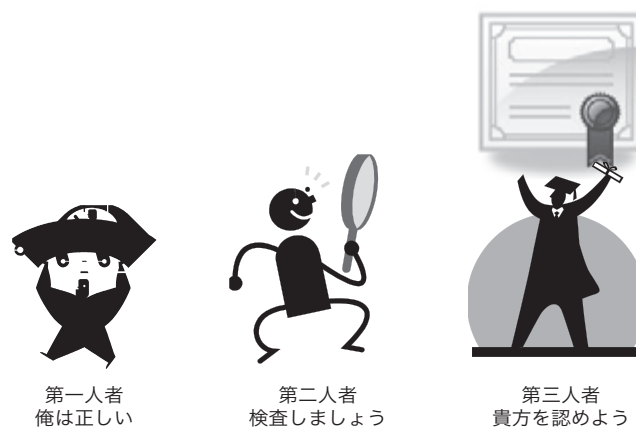
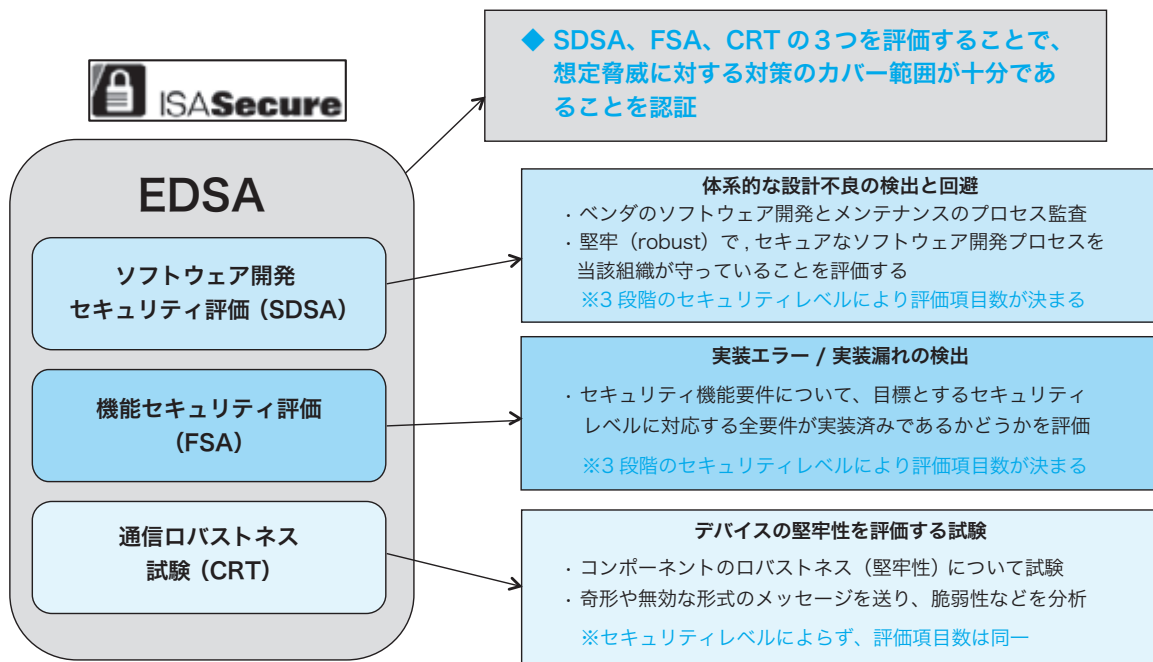


図 1 第三者認証



EDSA : Embedded Device Security Assurance  
 Communication Robustness Testing (CRT), Functional Security Assessment(FSA), Software Development Security Assessment (SDSA)  
 出典 : 「ISA Security Compliance Institute (ISCI) and ISASecure™及び http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

図2 EDSA 認証の各評価項目概要

というホワイトボックス検査、そして、SDSA (Software Development Security Assessment) というプログラム開発と維持管理に関する検査から成り立っている。

この認証を行う機関として CSSC は米国 exida 社に続いて世界で二番目に CL (Chartered Lab.) として認定を受けている (図3)。この認証作業を実行するためのマニュアル作り、検査作業を行うための要員教育、認証のオーナーである ISCI (ISA Security Compliance Institute) との交渉などにあたり、IPA を始めとした CSSC の各組合員には大変お世話になった。この場を借りて御礼を申し上げたい。既に日立製作所と横河電機の二製品を認証している。この認証を後ろ盾にして、国内の皆様だけでなく海外の皆様にも安全、安心を提供していただきたい。このような認証事業を始めたことでヨーロッパや ASEAN 各国からは多数の問い合わせをいただいている。サイバーセキュリティへの関心の高さと認証事業への関心の高さを痛感している。

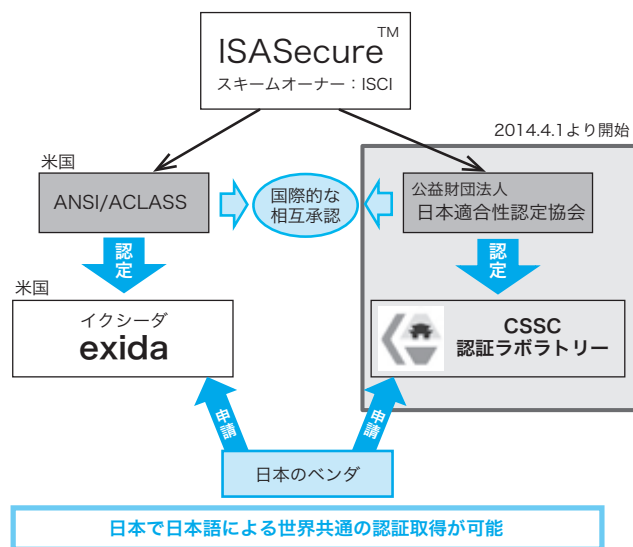


図3 国際的な相互承認により世界に通用する EDSA 認証

## 6 まとめ

安全とは客観、安心とは主観。サイバーセキュリティについては安全を第三者認証で担保し、担保された安全の中で安心して生活してもらう枠組みができつつある。しかし、セキュリティ対策は常にイタチごっこ。すべてがネットワークキングされる時代、サイバーセキュリティが安全、安心の一つの要である。皆様の更なるご支援を賜りたい。

### 【参考文献】

- [1] <http://www.css-center.or.jp/>
- [2] 新誠一：社会インフラへのサイバー攻撃に対する課題と取り組み，情報処理，vol.55, no.7, pp.640-646, 2014
- [3] [http://www.cssc-cl.org/pdf/press/press\\_20140715.pdf](http://www.cssc-cl.org/pdf/press/press_20140715.pdf)
- [4] <http://www.nippon.com/ja/genre/culture/l00052/>
- [5] 「日本のものづくりの未来」編集委員会編：エビローク「日本のものづくりの未来」，日本のものづくりの未来，日本能率協会，pp.213-220，2012.6.20
- [6] <http://www.jma.or.jp/mono/factory/>