ICSのサイバーセキュリティへの取組み
今，生産制御システム（ICS）が狙われている！

Cybersecurity for Our Industrial Control System, Which is Now a Target for Attack

アズビル株式会社
アドバンスオートメーションカンパニー
木内　誠 Makoto Kiuchi

アズビル株式会社
アドバンスオートメーションカンパニー
田中　良則 Yoshinori Tanaka

アズビル株式会社
アドバンスオートメーションカンパニー
関　英信 Hidenobu Seki

アズビル株式会社
アドバンスオートメーションカンパニー
黒木　亮 Ryo Kuroki

アズビル株式会社
技術開発本部
小森谷　良明 Yoshiaki Komoriya

キーワード
サイバーセキュリティ，ICS，オープン化，コンピュータ・ウイルス，マルウェア，脆弱性，リモートアクセス，PSEC，CSSC，製品セキュリティ認証，ISASecure，EDSA，SSA，SDLA，IEC62443

1996年に初めてオープンなICSとしてアズビル株式会社が開発した協調オートメーションシステム（Harmonas™）にもUSBメモリなどにより，ウイルスなどのマルウェアに感染するケースが散見されるようになった。さらに昨年，リモートアクセス機能を使った情報系からの不正侵入によるサイバー攻撃が発見され，新たな脅威が現実となってきた。azbilグループは，ICSのオープン化とともにサイバーセキュリティに対する活動を開始し，多くの対策を行ってきた。本稿では，それらの取組み内容と製品の高セキュア化開発による製品セキュリティ認証取得の成果について紹介する。

Cases have been reported in which the Harmonized Automation System—Dependable Open (Harmonas-DEO™), originally developed by Azbil Corporation in 1996 as the first open industrial control system (ICS), has been infected by a computer virus or other malware by means such as a USB flash drive. Moreover, last year a remote access cyberattack through the information network was detected. Serious new threats are therefore now a reality. Azbil, in addition to developing the open ICS, has been taking extensive preventive measures for ICS cybersecurity. In this article we discuss our efforts to develop a highly secure product, efforts that resulted in ISASecure Embedded Device Security Assurance Certification.

1．はじめに

1990年代後半から生産制御システム（ICS:Industrial Control System）がオープン化されはじめ，WindowsやEthernetが導入され，情報系と制御系の融合が現実化するようになるとともにICSに対するサイバーセキュリティの問題が起こりはじめた。情報系のサイバーセキュリティは，機密性＞完全性＞可用性の順に国家や企業の機密を守ることが優先されているが，一方制御系のサイバーセキュリティは，24時間365時間止まらないプラントのようにシステムを止めないように守ることが求められている。

当社の協調オートメーションシステム（Harmonas）は，それまでのICSでは専用OSを独自開発・使用してきたのを，業界に先駆けて1996年に初めてWindows NTを採用し，ハイブリッドな協調オートメーションを具体化するものとして商品化された。

しかし，その顧客のシステムで初めてウイルス騒ぎが起きたのは，2001年に発生したNIMDA[*1]であった。それ以来今日に至るまで様々なマルウェアが顧客の現場で発生するようになった。

マルウェアとは，一般に不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称であり，コンピュータ・ウイルス，ワーム，バックドア，キーロガー，トロイの木馬，スパイウェアなどが含まれる。その都度数々の対策を顧客，当社双方で協力して行ってきたが，残念ながらマルウェアの発生がゼロになることはない。

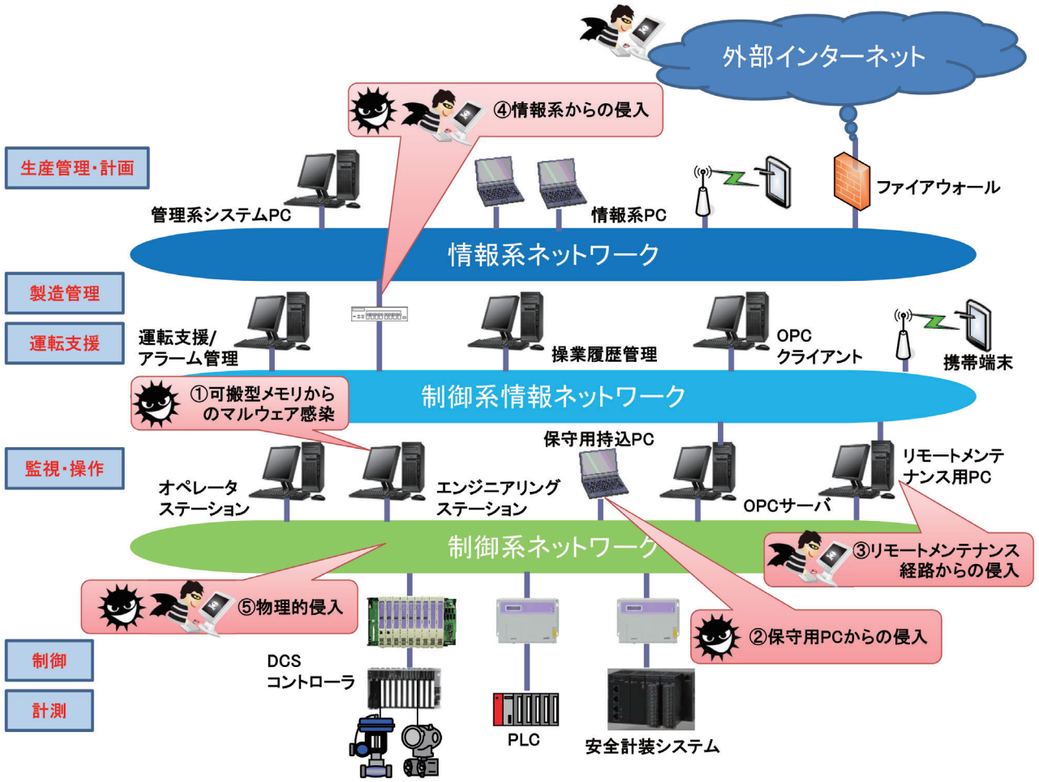

図1　ICS へのサイバー攻撃経路

本稿では，ICSサイバーセキュリティの現状と当社が取り組んできた活動について解説する。ただし，サイバーセキュリティへの最新対策技術の詳細を公開することは，残念ながら攻撃者を利することにもなるため，ここでは概要の解説に留める。

2. ICS のサイバーセキュリティ脅威とリスク

2.1　ICSへのサイバー攻撃経路ごとの問題

一般的にICSのセキュリティリスクとして考えられるサイバー攻撃経路は，図1に示す五つとされている。いずれも技術的な問題だけではなく，人の問題も抱えていることから，なかなか経路を遮断することができない。

(1)可搬型メモリデバイスからの侵入

2001年以来当社の制御システムの顧客で最も多く発生したのは，記憶メディアの一つであるUSBメモリからウイルスに感染するというものであった。ICSの特性上，パフォーマンスや外部ネットワークとの接続上の問題から，ブラックリスト型ウイルス対策ソフトウェアの搭載が難しく，OSのセキュリティパッチを定期的に当てられないことや出処不明もしくは使用履歴の不明なUSBメモリを使用することなどの管理・運用対策が不十分であったケースが多い。

(2)保守用PC経由の侵入

ICSへの機器追加・変更，ソフトウェアの更新やトラブル対応の解析などのための常設や仮設の保守用PCに潜んでいたマルウェアが，ICSに感染したり，攻撃を仕掛けたりすることがある。これも実際に顧客の現場で発生しており，保守用PCのセキュリティ管理が不十分なことが原因とされている。

(3)リモートメンテナンス経路からの侵入

ICSのユーザーの中には，24時間365日継続した運転を必要とするため，夜中でもトラブル発生時にベンダが提供するリモートメンテナンスサービスを利用しているケースがある。リモートメンテナンスからの侵入事例はまだ報告されていないが，専用線とはいっても，実際には公衆ネットワーク網の一部を利用した回線であるのが一般的で，より高度な攻撃を行える攻撃者であれば，この経路からの侵入も技術的には不可能ではないとされる。また，サービスを提供するベンダ側のシステム構成やセキュリティ対策が重要なことは言うまでもない。

(4)情報系ネットワークからの侵入

今後最もリスクが増大していくと言われるのが，情報系ネットワークからのICSへの侵入である。今や多くの先端的なICSは，制御系と情報系の融合というより一体として成り立っているものである。

市況の変化やエネルギー事情の変化をリアルタイムにICSに活かして最適生産を常に目指すためには，制御系を情報系から分離するわけにはいかない。

もちろん情報系にも，様々なセキュリティ対策を施しているのが実態であるが，今日の最新脅威は，その裏をかき不十分な対策をついてサイバー攻撃を仕掛けてきている。

最近では，正規の文書やメールに添付して特定の相手のネットワークに侵入したり，フィッシングサイトにアクセス時にマルウェアをダウンロードさせたりするような標的型攻撃により，機密情報を盗む例が増えてきているが，もはや情報系には，何らかのマルウェアが潜んでいることを前提にシステム構成全体を考えたリスク管理をしなければならない時代になっている。最新のサイバー攻撃者は，侵入に成功してもそこでは悪事を働かせず，黙って次の標的を探しているのである。その標的の一つがICSであると考えられるのも当然のことになりつつある。

(5)物理的侵入

ICSを構成する機器の設置環境を考えると一般的には考えにくいと言われる物理的侵入であるが，実際にはコントロールルームへの自由な出入りや，鍵がかからない機器・制御盤などの存在により，この攻撃も現実味を帯びてくる。パスワードで管理しているからといって安全であるとは限らない。最近情報系のインシデントで話題のように，内部犯行者が関わってくるとさらに脅威が現実的になってくる。

2.2　ICSでの具体的な被害

ある顧客のシステムは，サイバー攻撃によって，被害を受けたプラントの操業を止め，復旧までに数日を要したこともあった。また，2003年に発生したMS Blaster[*2]は，Windowsの脆弱性を狙った攻撃であったため，セキュリティパッチをタイムリーに当てられない多くのICSが被害にあった。また最近では，国内のインシデント発生よりも海外での発生数が多くなっており，サイバーセキュリティの問題は，国境がなくなっている。

このような具体的な被害の例では，従来，情報系を狙っていたマルウェアが，たまたま制御系に紛れ込んだものがほとんどであり，直接制御系システムを狙っていたものではなかったと考えている。

ところが2010年に発見されたStuxnetは，イランの核燃料工場で使われていた特定のベンダの制御システムを狙い，そのウラン濃縮製造工程に大きな影響を与えるものであった。しかも，その侵入経路は複数，多段のバックアップを用意し，かつ最終目的に達するまで存在を隠すという手法を駆使し，情報系からの侵入後数カ月かかってICSに侵入するという壮大な計画を持ったものであった。最後にICSのエンジニアリング・ステーションに到達後，PLC（Programmable Logic Controller）に送られた制御ロジックソフトウェアに付随してPLCの制御を不正に操作し遠心分離機の回転数を異常に高め機器の故障に至らしめた。同時に監視用のオペレータ・ステーションの画面を偽装し，異常に気づかせないといった，スパイ映画まがいの攻撃をしたとのことであった。実際のサイバー攻撃の背景には，ウラン濃縮を阻止するといった国家レベルの戦略があったものと言われているが，我々がそれまで考えてきた対策の多くは，もはや役に立たなくなったとさえ認識させられるに至った。

3. 最新の ICS セキュリティ脅威

昨年Stuxnet以来と言われるICSを狙った新たなマルウェアが発見された。このマルウェアは，Havexまたは Dragon Fly作戦と呼ばれるもので，当初は欧米を中心としてエネルギー産業をターゲットにして登場したようである。ICSでは，異機種間でのデータ交換を効率化させるため，Microsoft社のDCOM（Distributed Component Object Model）と呼ばれるネットワーク上に分散設置されたコンピュータ上のソフトウェアコンポーネント間通信の規約を使い，1996年に登場したOPC（OLE for Process Control：当初名）というプロセス制御の標準規格を多用している。しかし，このDCOMの脆弱性を突いたサイバー攻撃がいまだに後を絶たない。Havexは，まず情報系ネットワークに複数の経路から侵入を試み，その系に繋がっているOPCクライアントを探し出し，それに繋がるOPCサーバの情報を攻撃者のサイトに外部漏洩させてしまうものである。既に多くのアンチウイルス対策ソフトウェアに定義ファイルが用意され，現時点では，情報系に侵入しても駆除されているはずである。しかし，このマルウェアにより，ICSのベンダの種類を問わない広範な脅威が存在しており，真のターゲットはファインケミカルや医薬品製造におけるレシピデータとも言われ，今後亜種の登場が危惧されている。

4. ICS サイバーセキュリティへの取組み

4.1　大規模プラント・ネットワーク・セキュリティ対策委員会

我が国でICSのサイバーセキュリティに対し，官民一体となって研究，対策を初めて行ったのは，1997年の通商産業省（当時）の「大規模プラント・ネットワーク・セキュリティ対策委員会（以下PSECと略す）」であった。当時はまだ実際のICSではウイルス発生やマルウェアによるサイバー攻撃は発生していなかったが，情報系システムではそれらが日常的になりつつあり，制御システムにおける来たるべき脅威に対し，プラントの運転，制御，管理を対象にして，調査・研究を行った。委員会は図2のような構成をとっており，当社も多くの分科会・ワーキンググループに参画した。

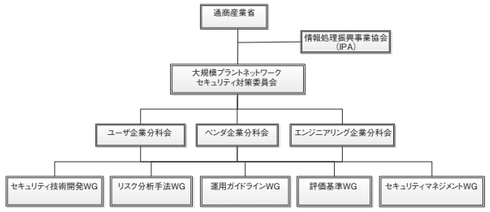

図2　PSEC の組織図

本委員会では，クラッキングおよびサイバーテロリズムに関して以下の定義を用いて活動した。

・クラッキングとは，正規の認証を経ずにコンピュータ・ネットワーク・システムに悪意を持ってアクセスを試みること

・サイバーテロリズムとは，ネットワークを通じて政府や産業に対して行われる敵対的な行動であり，大規模で組織的な不正アクセスを試みること

また，コンピュータ・セキュリティに関する意図的な脅威の目的として

・国家転覆や社会攪乱目的
・脅迫，恐喝などの営利目的
・産業スパイなどのビジネス目的
・怨恨による復讐目的
・趣味（達成感，優越感）目的

これらが，今日のICSにおいて正に現実の脅威になりつつあることを改めて認識させられる。

三つの分科会では，それぞれ下記のような活動を実施した。

(1) ユーザー企業分科会

・全委員が共通基盤の下で議論を進めるための，国内各ユーザー企業のシステム構成に即したモデル・システムの構築
・委員相互の理解を深めるための用語の統一
・内外からの脅威に対して「防御すべき項目」のリストアップ
・ユーザーの立場からの運用管理要件の検討
・ベンダやエンジニアリング企業への要求事項の検討

(2) エンジニアリング企業分科会

・HAZOP，FTA，JRAMなどのプラント・リスク分析手法のネットワーク・セキュリティリスクへの応用
・ネットワーク・セキュリティのリスク分析を「プロセス・セキュリティ・エンジニアリング」としての作業フロー化

(3) ベンダ企業分科会

・外部からの侵入方法とセキュリティ侵犯事象との関連の分析
・侵入経路別のFTA脅威分析
・侵入経路別セキュリティ対策の提案
・新規セキュリティ技術開発の提言

当社が参加した活動の中には，ICS設計時におけるセキュリティ要件を明らかにするというセキュリティ・マネジメントワーキンググループがある。ここでは，情報セキュリティの評価認証の分野で国際的な相互認証を行う動きのあったコモン・クライテリア（ISO/IEC15408）の枠組みを参考に，これをICS分野に適用しようという試みであった。当時欧米各国では，主に軍事調達や政府調達を対象として，各国固有のセキュリティ評価基準を国際統一基準にしようという動きがあったが，それをICSの分野に適用拡大するという考えは，PSECが初めて試みたのではないかと考える。

さらに当社が参加・貢献できた活動の中には，世界で初めて実施されたICSへのサイバーアタック実験がある。当時はまだICSへのサイバー攻撃の実例はなかったので，情報系への攻撃例を真似てユーザー企業分科会がまとめた「防御すべき項目」が守られるのか，いろいろな観点で実験を行った。その結果，大きな脆弱性と攻撃の可能性のある領域が判明し，報告書（非公開）を作成した。これらを元に，その後ベンダー各社は，ICSの対策開発に乗り出す契機となった。

PSECは継続的な組織ではなかったので，国や関係団体への提言を中心とした報告書をまとめた後，解散された。最終報告書の今後の課題には，以下の四つを掲げた。

・セキュリティに対する理解を啓発する活動
・セキュリティ問題を継続的に取り扱う機関の設置
・実証的な横展開の活動
・その他の研究課題（分析手法などの研究課題セキュリティ評価の定量化などの理論研究課題，プラント運用におけるセキュリティレベル向上のための必要な改善策の研究課題など）

しかし誠に残念ながら，日本では官民一体となった活動はその後しばらく行われなかった。そしてその後，欧米でICSに関するセキュリティ対策のための規格化・標準化を行う団体が組織化され，それ以後我が国がICSのサイバーセキュリティで世界をリードするチャンスは失われてしまった。

当社は最終報告書で提案された情報系と制御系の間に設置するファイアウォールやOSの不要なサービスを停止するなどの開発を行った。さらに一時USBメモリを制御システムで使った際にDOWNAD[*3]といったウイルスに感染するというインシデントが多く発生した時期があったので，物理的な対策，ウイルス対策ソフトウェアの適用や適切な使用・運用管理により，顧客でのインシデント発生はかなり抑えられるようになった。

4.2　制御システムセキュリティセンター（CSSC）

(1) CSSC設立に参画

2.2で述べたように2010年になってそれまでのウイルス騒ぎとは異なるICSを直接狙うサイバー攻撃が初めて現実の脅威となったことから，我が国では経済産業省が2010年12月に「サイバーセキュリティと経済研究会」，2011年10月に「制御システムセキュリティ検討タスクフォース」を立ち上げ，社会の重要インフラを守るために制御システムのセキュリティ確保が必須であるとの提言をまとめた。さらに2012年3月には，「技術研究組合制御システムセキュリティセンター」（以下CSSCと略す）を設立し，恒常的な組織として研究開発，普及啓発，人材開発，評価認証，標準化などを行うこととし，東日本大震災への復興を支援するために，減災・復興を目指されている宮城県多賀城市に東北多賀城本部を設置した。多賀城市は，奈良時代から外敵から守る要害として設置された国府があったところで「守りの都市」でもある。

写真1　CSSC の玄関

当社ではこの組織化を契機に「安全と安心を提供する」企業理念に沿った活動・貢献ができることから，発起人会から参画し，積極的に活動することとし，理事会，運営委員会と四つのすべての委員会および研究開発部に参加している。

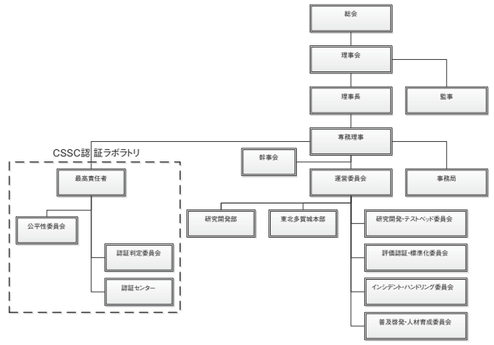

図3　CSSC 組織図

(2) テストベッドを納入

CSSCでは上記の活動を行うため，制御システムと模擬プラントから構成されるテストベッド（名称:CSS-Base6）を構築した。現時点では，9種類のテストベッドが用意され，電力，ガス，化学，組立加工，ビルなどの各業界に対応した様々な研究開発や普及啓発に利用されている。

当社は，化学分野のプロセスオートメーションシステムにIndustrial-DEO™を納入し，またガス分野にSCADA+PLCシステムを納入した。

(3) 研究開発に参加

情報系セキュリティの分野では，大量導入によってコスト的にペイできるツールや機器が比較的豊富に市場にあるが，ICSの分野で使われているOSや通信プロトコルは固有なものが多く，なかなかセキュリティベンダに開発してもらえない悩みがある。そこでCSSCでは，研究開発予算を使ってそういったICS固有の対策に適用可能なツールや機器を独自に開発している。またCSSCでは，世界中のいろいろなセキュリティ対策製品が，実際のICS分野に有効であるかどうかの検証もCSS-Base6のテストベッドを使って行っている。これも海外の他の組織にないユニークな特徴である。


写真2　CSSC 納入の Industrial-DEO システムと化学模擬プラント

当社は独自に委託研究開発に参加するとともに，他社が研究開発の検証する際にテストベッドのノウハウを提供し貢献するという二つの方法で参加している。CSSCの独自開発の中にはユニークな製品があり，実用化に近づいているものもあって大いに期待している。

(4) 普及啓発・人材育成に参加

経済産業省では，重要インフラとして定めた分野のうち，電力，ガス，化学，ビルの4分野でサイバーセキュリティ演習を実施している。2013年5月のCSS-Base6開所と同時にそれらの実施運営をCSSC東北多賀城本部に集中し，効果的な演習となるようCSSCが運営協力している。当社も化学，ガスの分野で参画し，Stuxnetの摸擬，最新の脅威への対策の提案などを演習の場で体験できるようシナリオ構築などを提供してきた。この演習は，重要インフラ各分野の事業者を対象に実施されており，脅威と対策を体験・演習できるものであり，CSSCが実施した事業の成果である。2014年度のサイバー演習は，12月から2015年2月にかけて実施され，3章の「最新のICSセキュリティ脅威」で説明したマルウェア攻撃を取り込んだタイムリーな演習を実施した。

4.3　アズビル セキュリティフライデー

当社がICSに対するサイバーセキュリティの分野で他社にない特徴は，アズビル セキュリティフライデー株式会社というグループ会社を有することである。この会社の詳細紹介は，本書の別稿に譲るが，社内ベンチャー起業提案制度から生まれたこの会社は，ICSやITの世界で独特なサイバーセキュリティ対策製品を開発・販売している。現在，前述のCSSCのCSS-Base6のテストベッドのいくつかにアズビ

ル セキュリティフライデーのサイバーセキュリティ対策製品が採用され，サイバーセキュリティ演習に寄与すると同時に研究開発の検証にも貢献している。

5．製品セキュリティ認証への取組み

今や制御システムの安全運用には，サイバーセキュリティへの対策なしには考えられない時代が到来した。そのためには制御システムをどのように設計･構成し，どのように運用･保守するか，そのライフサイクルを通じて対策を講じていかなければならない。

その拠り所となるよう考えられたのが，セキュリティ認証制度である。現時点ではカナダのWurldtech社のような私企業が認証するものと業界団体であるISA（International Society of Automation）が規定する規格に基づくISA Secureセキュリティ認証が存在しているが，ゆくゆくはIEC62443の認証制度に移行していくことが考えられる。CSSCでは，評価認証･標準化委員会による，

・評価･認証で利用できる国産ツールの開発
・制御システム機器のパイロット認証の実施
・評価･認証基準の策定
・評価･認証要員の育成

を経て，CSSC認証ラボラトリ（CSSCの独立下部組織）が，ISASecureのEDSA（Embedded Device Security Assurance）認証作業を日本で実施できる組織として認定され，2014年4月から認証が正式に開始された。

さらに続いて，ISASecureに規格化されたシステムレベルの認証であるSSA（System Security Assurance）とSDLA（Security Development Lifecycle Assurance）のパイロット認証が2015年4月から募集を始め，夏頃から認証が開始される見込みとなっている。

(1) EDSA認証とは

EDSA認証は，

・通信ロバストネス試験:
　Communication Robustness Testing（CRT）
・機能セキュリティ評価:
　Functional Security Assessment（FSA）
・ソフトウェア開発セキュリティ評価:
　Software Development Security Assessment（SDSA）

の三つの試験･評価項目から構成され，EDSA認証を取得するためには，この三つすべてに合格する必要がある。

・CRTは，デバイスの堅牢性を評価する試験であって，具体的には，組込み機器（DCSコントローラやPLC）へのネットワーク･プロトコル実装が，ネットワークから受信した異常または意図的な悪意のあるトラフィックに対して，自分自身および他のデバイス機能を防御する程度をツール使って測定する。不適切なメッセージ応答，またはデバイスが重要サービスを適切に実行できないと，デバイス内部の潜在的なセキュリティ脆弱性の存在を示す。

現在はまだTCP/IPやUDPなど六つの汎用プロトコルのみが試験対象であるが，今後業界標準やベンダ標準のプロトコルも試験対象として拡張が計画されている。

・FSAは，対象機器のセキュリティ機能が十分であるかアセスメントするもので，実機テストと開発ドキュメントの審査で行われる。要件には，七つのカテゴリと83個の要求事項があり，取得するISASecureレベルに応じて満たすべき要求事項が異なる。

・SDSAは，対象製品の開発プロセスがセキュアに行われているか監査するもので，主にしくみの文書化と成果物の審査で行われる。要件には，12の活動フェーズと各フェーズに対する合計169個の要求事項があり，取得するISASecureレベルに応じて満たすべき要求事項が異なる。

CSSC認証ラボラトリが認証機関となる以前は，米国の認証機関しか存在せず，すべての開発ドキュメントを英文で用意し，英語で説明する必要があったため，日本企業の製品認証はなかなか困難であった。しかし，これからは日本語での対応が可能となったため，認証促進されることが期待される。なお，ここで認証された製品は，ISA Secure認証製品として相互認証され，世界で通用する認証になる。

(2) DOPCⅣの認証取得

現在当社のICS分野での基幹システムであるHarmonasやIndustrial-DEOの主力コントローラはDOPC™Ⅳといい，これはCPUを三重化し，通信ネットワークを二重化した高信頼なプロセスコントローラである。

写真３　DOPC Ⅳの外観

当社は，日本でもCSSC認証ラボラトリでEDSA認証の取得が可能となったことから，「安全と安心」を顧客にお届けするため，ICS分野での基幹システムであるHarmonasやIndustrial-DEOで使われるプロセスコントローラDOPCⅣの認証を取得することとした。そのため，社内に認証取得推進タスクと開発プロジェクトの二つを発足させ，認証取得の準備を開始した。認証取得推進タスクは，まず規格や評価方法の理解と評価ツールの準備から行った。約1年かけて認証取得ガイドラインを作成し，どんな製品でもこのガイドラインに基づいて開発プロセスを構築すれば，認証取得申請の準備ができるようにした。2014年1月にはCSSCによるEDSA認証の公開説明会が開催され，4月のCSSCの正式認証受付開始と同時に申請を行い，各種開発ドキュメントの整備を始めた。また，認証推進タスクの活動の結果，従来のISO9001ベースの業務標準やマニュアルの多くの改訂が必要なことがわかり，高セキュアな対策が求められる製品の企画，開発，評価，保守，品証といったすべてのライフサイクルにわたって対応できるようにした。

認証要件の中には，製品の脅威分析を行ってそのリスクを評価し，適切な処置が求められているものがある。これらを一つひとつ解決していく地道な開発作業が始まった。一例を挙げると，FSA要件の一つに不要な通信ポートやサービスが閉じられていることというのがある。DOPCⅣでは，一般のユーザーは使用できないものの，製品開発者にのみ使用できる通信ポートが存在していた。これに対する脅威分析の結果，これは閉じるべきとの結論となり，その開発･対策を実施した。

その後約1カ月間におよぶ試験と審査を経てようやく認証取得に至った。2015年初めには，ISASecure（http://www.isasecure.org/End-User-Resources.aspx）とCSSC認証ラボラトリ（http://www.cssc-cl.org/jp/certified_devices/index.html）のホームページでDOPCⅣの認証書を閲覧できるので是非参照されたい。

下記の写真４は，2015年2月に当社本社にて実施されたEDSA認証書授与式の模様である。

写真４　EDSA 認証書授与式の模様

6．おわりに

以前のICSではハードウェアからOS，ソフトウェアまで自社で開発することが当たり前の時代があった。しかし，時代の要請とともにシステムをオープン化して情報系と一体となったICSは，コストダウンや拡張性の拡大に伴い，またたく間に主流となった。しかし，このパンドラの箱を開けたため，サイバー攻撃の対象になってしまった。情報系のセキュリティとは特性が異なるため，同じ対策を講じられないことが多々あり，現在業界を挙げてサイバーセキュリティの対策を進める機運が急速に高まっている。当社は情報セキュリティ大学院大学に聴講生を毎年多数派遣し，セキュリティ専門知識を持った制御エンジニアを育成し，底上げを図るとともにDOPCⅣで取得したEDSA認証のノウハウを活かして他の製品にも高セキュア開発手法を適用していく予定である。そしてシステムレベルのSSA認証取得も考慮しながら，さらに高セキュアな製品を顧客に提供し，「安全と安心」を提供する「人を中心としたオートメーション」の具現化にこれからも注力したい。

＜注記＞

＊1:NIMDAとは，ファイル共有や電子メールを攻撃経由として侵入するワームの一種である。感染するとコンピュータのパフォーマンス低下，ネットワークの混雑を起こすため，HMIのリアルタイム監視に影響した。

＊2:MS Blasterとは，Windowsのファイル共有などで使われるTCP135番ポートにアクセスし，「DCOMのバッファオーバーフロー」と呼ばれる脆弱性を利用してコンピュータに侵入するワームの一種である。Microsoftのセキュリティパッチが当てられていないコンピュータをネットワーク上で検索し，そのコンピュータに侵入する。感染するとOSの一部停止や再起動が発生し，HMIが正常な監視制御を継続できなくなった。

＊3:DOWNAD（別名:Conficker）とは，Windowsの脆弱性「MS08-067」を狙って感染拡大を行うワームの一種である。亜種が多く登場し，未だに感染が後を絶たない。感染すると遠隔操作されたり，機密情報が漏洩したりした。情報系のネットワークに接続しないICSも被害にあった。また，DOWNADは，パスワード解析機能を持ち，安易なパスワードは盗まれてしまう。パスワード変更ができなかったり，変更頻度が低かったりするとICSも被害を受けることとなった。

＜参考文献＞

(1)「大規模プラント･ネットワーク･セキュリティについて」～重要システムのサイバーテロリズム･クラッキング対策のあり方～最終報告書，平成12年3月，大規模プラント･ネットワーク･セキュリティ対策委員会
(2)技術研究組合制御システムセキュリティセンターのWebサイトから引用
http://www.css-center.or.jp/

＜商標＞

＜著者所属＞
木内　誠　　アドバンスオートメーションカンパニー
開発1部
田中　良則　　アドバンスオートメーションカンパニー
開発1部
関　英信　　アドバンスオートメーションカンパニー
開発3部
黒木　亮　　アドバンスオートメーションカンパニー
開発1部
小森谷　良明　　技術開発本部商品開発部