特集原著論文/Specially issued Original Paper

# 制御系ネットワークのセキュリティ対策立案のアプローチ

孫　晶[*1]・高木 ひとみ[*2]・伊藤 一馬[*1]・越島 一郎[*1]・橋本 芳宏[*1]

# Security Protection for Industrial Automation and Control System Network

**Jing SUN[*1], Hitomi TAKAGI[*2], Kazuma ITO[*1], Ichiro KOSHIJIMA[*1], and Yoshihiro HASHIMOTO[*1]**

**Abstract**– The threat of cyber-attacks to industrial automation and control system network of social infrastructure has risen. In 2010, an epoch making malware Stuxnet was discovered. Stuxnet was developed to attack the controllers in Iran nuclear fuel factory and has succeeded to hinder the operation for a long term. Even if the controllers were not connected to internet, they could be targets. Stuxnet's subspecies were already discovered. The necessity of cyber-security measures for industrial control systems network (ICSN) is now seriously recognized. However, effective cyber-security measures have not been installed to ICSN yet. Based on this background, this paper aims at visualization of tool investment effect and proposes a systematic design approach of protection systems against cyber-attacks for ICSN.

**Keywords**– Cyber security, process safety, ISA 99, incident response, security protection, industrial control systems network

## 1. はじめに

近年, グローバル企業のプラントだけではなく, 原子力発電所や交通システムなど重要なインフラの制御システム（Industrial Control System: ICS）を狙ったサイバー攻撃が増えている．特に, 革新的な仮想化・クラウド技術の利用により, ネットワーク化されている制御システムへのセキュリティ・リスクが一層高まると予想され, 制御系ネットワークシステムのセキュリティ対策は, 企業の事業継続にとどまらず, 社会の秩序を維持するうえでもますます重要な課題となっている [1].

現在, ICS の運用には, 生産計画や実績, 設備管理など様々な情報の工場外部のネットワークとの連携が不可欠になっており, ICS ネットワークは, 企業ネットワーク, ファイアウォールを挟んでインターネットに接続されている（Fig.1）．したがって, 外部からサイバー攻撃される危険性は否定できない状況である．

2010 年にイランの核開発施設のウラン濃縮制御システムが，Stuxnet という標的型マルウェアによりサイバー攻撃の被害を受けた．この事例をはじめとして，制御システムを対象とした標的型サイバー攻撃が急増している．化学プラントの制御システムをはじめとした ICS がサイバー攻撃を受けた場合, 企業の情報の漏洩だけでなく, 爆発や危険物質の流出といったセーフティが破綻する事故が発生する可能性がある．

最近, 制御システムを対象とした APT (Advanced Persistent Threat) 攻撃と呼ばれるサイバー攻撃は, 指向性の強い標的型・ゼロデイを含めた脆弱性を利用し組織的に行われる傾向にあり, 今後さらに高度化すると考えられ, サイバー攻撃からプロセス制御系の安全を守るための研究は常用であり急務である [2-6].

これまで, 24 時間稼働が阻害されるリスクを重要視して, 情報システムでは当然のように適用されているセキュリティパッチやアンチウィルスソフトが制御系では避けられてきた．USB によるアンチウィルスや制御アプリ以外稼働させないホワイトリストなど, 制御系の特

[*1]名古屋工業大学　名古屋市昭和区御器所町
[*2]新生銀行
[*1]Nagoya Institue of Technology, Gokiso-chou, Showa-ku, Nagoya
[*2]Shinsei Bank

Received: 17 July 2016, Revised: 12 September 2016, Accepted: 20 September 2016.

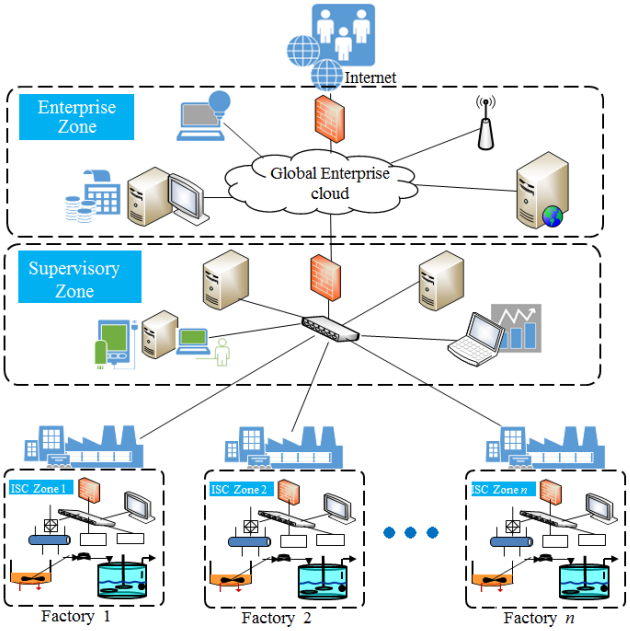


**Fig. 1:** 複数工場を持つ生産ネットワークシステム例

性を考慮した様々なセキュリティツールが, 2014 年ぐらいからようやく各社から登場するようになってきた.

しかしながら, 制御システムへの対策ツールなどの導入はまだまだ進展されていない. サイバーセキュリティ対策は一意に定まるものではなく, 危険性や金銭的な余裕に応じて, 計画的に強化すべきものであると考えられる. 状況に応じた立案とは, どのような観点で, どのような手段を用いて行えばよいのであろうか.

この背景を受け, 私達は, 1 つのプラントの制御システムを対象として, 制御系セキュリティ立案の手順を提案し [7][8], 制御系セキュリティツールの選択と配置について検討を行った [9]. しかしながら, 複数のプラントを持つ制御系ネットワークへのセキュリティ評価, 及び対策立案について論議されていない.

多くの事業所を有し, 各事業所に複数のプラントをもつ重要インフラの企業では, 一部のプラントへサイバーセキュリティ対策を適用したとしても企業としての取り組みとしては不足である. しかし, 一度に大規模な投資を行うことも難しい. 各プラントへのサイバーセキュリティ対策は一意に定まるものではなく, 危険性や金銭的な余裕に応じて, 計画的に強化すべきものであると考えられる. 複数の事業所とプラントの制御系ネットワークに対して, 対策を提案する側にとっても, 対策の提案を受けて, 投資を決定する側にとっても, その投資の妥当性を評価しやすい形で示されることが望まれる [7].

一方, ICS サイバーセキュリティの国際標準 IEC62443 (IEC: International Electrotechnical Commission) と ISA99(ISA: International Society of Automation) では, Zone-Conduit による評価が提唱されている. ISA99 では, ICS セキュリティを評価するための 7 つの基本要件, 及びセキュリティレベルの指標の SAL (Security Assurance Level) が定義されている. しかしながら, 提案者と採択者の双方が理解しやすい形で, セキュリティ対策ツールの導入を検討するには, 上記の国際標準では不足で, セキュリティ対策検討のためのアプローチを整備することが必要であると考えた.

そのため, 本研究では, 複数プラントをもつ制御系ネットワークへのセキュリティツールの投資効果の「見える化」に注目し, 国際標準に則りながら, 各プラントへのリスク要求, セキュリティ性能, 及び経済性のバランスを考慮した検討を可能にするアプローチを提案する.

## 2. ICS セキュリティ対策の現状

### 2.1 これまでのセキュリティ評価

制御システムのサイバーセキュリティ問題に取り組むにあたって, 制御システムを構築しているソフトウェアをはじめ, プラントのハードウェア, システムに携わるエンジニアやオペレーターのリスク, さらに対策を講じる費用など, 様々な要素を考慮しマネジメントする必要がある. しかし, セキュリティ対策を導入する為の明確な指標は十分に議論されていない.

これまで, 情報セキュリティに関しては, セキュリティ評価基準 (CC: Common Criteria) によって, IT プロダクトのセキュリティ機能要件が, また, 情報セキュリティマネジメントシステム (ISMS: Information Security Management System) や, セキュリティ対策評価モデル [2] によって, 組織における情報セキュリティ確保のために取り組まなければならないことが示されているが, その要求に応えるための具体策までは示しておらず, 検討はこの標準を適用する側に任されている状況である. さらにこれらの取り組みは, プロセス系がもつ大量なエネルギーや, 毒劇物によるハザードのリスクを踏まえた, 安全の確保という制御系に重要な観点が全く入っていない. 制御系では何をどう守るべきか, どのような対策をどの程度導入するべきか, 指標が必要であると言える.

### 2.2 評価基準

本研究では, ISA 99[10] で定義されている 7 つの基本要件 FR (Foundational Requirements) と SAL (Security Assurance Level) をそれぞれセキュリティの評価基準とレベル指標として, 対策ツール及び制御系ネットワークシステムに対するセキュリティの評価を行う. 7 つの基本要件 FR 及び SAL は以下のように示される [11].

7 つの基本要件 FR

1. Access control (AC) :
   システムの使用前にユーザー認証・許可を行う.

2. Use control (UC)：
   ユーザーのリクエストを実行する前に権限を求める.
3. Data integrity (DI)：伝達・保持中のデータの不正操作を防ぎ完全性を保つ.
4. Data confidentiality (DC)：
   伝達・保持中のデータの拡散を防止し機密性を保つ.
5. Restrict data flow (RDF)：
   データのやり取りをゾーン内に限定し, システムのセグメント分けを行う.
6. Timely response to an event (TRE)：
   インシデント発生時に侵入を伝え, 証拠を集め, 即座に正しい行動をとる.
7. Resource availability (RA)：
   システムの可用性を確保する.

4段階の SAL のレベル

SA L1：AProtection against casual or coincidental violation
アプリケーション，セキュリティポリシーの甘さから従業員・部外者が簡単に無意識的に脅威になることを防ぐレベル.

SA L2：Protection against intentional violation using simple means
システムやセキュリティについてあまり知識のないハッカーが，インターネット上に公開されている攻撃手法などを用いて，愉快犯的にサイバー攻撃を行うことを防ぐレベル.

SA L3：Protection against intentional violation using sophisticated means
セキュリティやターゲットとなるシステムを熟知し，標的型のあまり知られていない攻撃手法を用いたり，脆弱性を狙ったりするサイバー攻撃を防ぐレベル.

SA L4：Protection against intentional violation using sophisticated means with extended resources
SAL3 よりも更に高度なコンピュータ資源，時間を用いたサイバー攻撃を防ぐレベル.

ISA99 では, あるシステムの 7 つ要件のレベル指標の状態が, 以下のようにベクトルを用いて表している．その表現形式はベクトルフォマート (Vector Format) と呼ばれている [6][12].

$$\text{SAL\_X}\ (\text{[FR,]}\ \text{Control system}) = \{\text{AC}, \text{UC}, \text{DI}, \text{DC}, \text{RDF}, \text{TRE}, \text{RA}\}$$

また，ISA99 では，セキュリティレベルのタイプとして，Target SAL，Achieved SAL と Capabilities SAL の３種類が以下のように定義されている.

$$\text{SAL\_X} = \text{(Required) The SAL type.}$$

ここで,

$$\text{SAL\_T} = \text{Target SAL.}$$
$$\text{SAL\_A} = \text{Achieved SAL.}$$
$$\text{SAL\_C} = \text{Capabilities SAL.}$$

である.
例えば：

$$\text{SAL\_T(Control system)} = \{2, 2, 0, 1, 3, 1, 3\}.$$

は Control system の 7 つ要件の AC, UC, DI, DC, RDF, TRE, RA の Target SAL は, それぞれ 2, 2, 0, 1, 3, 1, 3 であることを意味する.

## 3. 制御系ネットワークのセキュリティ対策の立案手順

本研究では，制御系ネットワークのセキュリティ対策立案のアプローチとして，Fig.2 のセキュリティ対策立案のフローチャートを提案する．Step 0～Step 17（略 S0～S17）はフローの実行順である.

ここで，Fig.3 の制御ネットワークを用いて，提案した対策立案の手順を説明する．この例は，DM (DeMilitarized) ゾーン，生産管理ゾーンと n 個の ICS ゾーン (工場) により構成される．本論文では，DM ゾーンに設置されている Web サイトやメールなど外部に向けたサービスサーバーのようなマシン群を Enterprise Machines と呼び，OPC Server (OPC: Object Linking and Embedding for Process Control)，Scheduling，Asset Management などのようなマシン群を Management Machines と呼ぶことにする．ICS ゾーンにおいては，Data Server，Operation Support Systems などのサーバー群を Control Servers と呼び，SCADA (Supervisory Control and Data Acquisition System) や現場の PC などを HMIs (Human Machine Interfaces) と呼ぶことにする．さらに，DCS (Distributed Control System）や PLC (Programmable Logic Controller) などのコントローラを Controllers と呼ぶことにする.

本章では，理解しやすいため，３つの工場を持つ制御系ネットワークシステムを例として，Fig.2 の手順を説明する.

**Step 0： 対策ツール効能と基本要件の関係整理**

Table 1 は，対策ツール効能と基本要件の関係の整理例を示している．横軸は 7 つの基本要件, SAL とコストで, 縦軸は対策ツールである．読み方としては, 例えば, ①の User Control は AC,UC,DI と DC の要件が満たされ, SAL の 1, 2 と 3 の 3 種類があり，コストは数万円程度

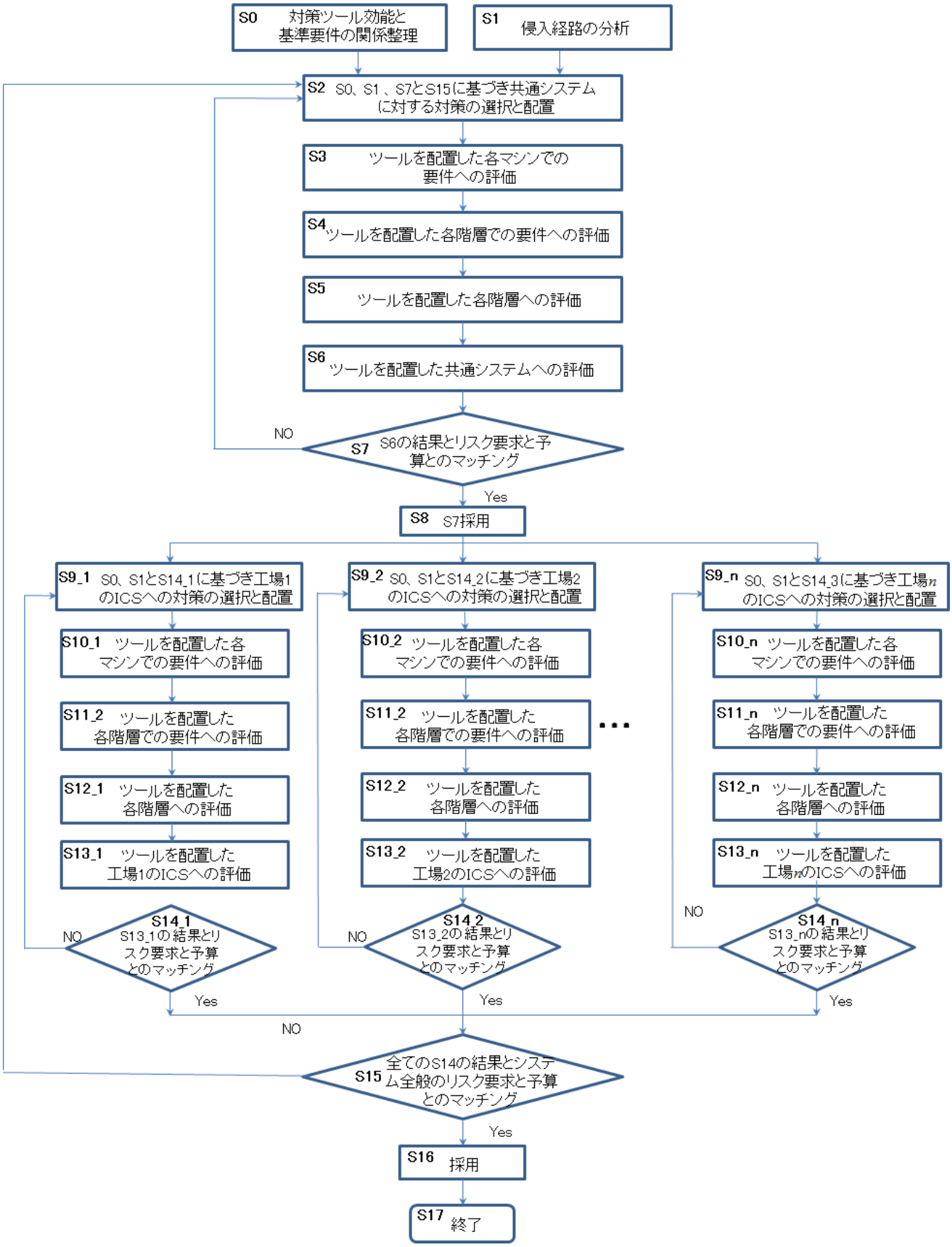


**Fig. 2:** 制御系ネットワークのセキュリティ対策立案のフローチャート

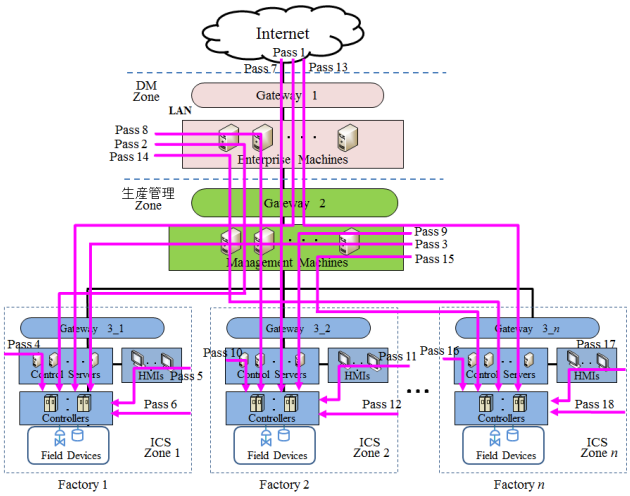


**Fig. 3:** Fig.1 の具体例における侵入経路の分析例

**Table 1:** 対策ツール効能と基本要件の関係の整理例

| ツール | FR (Foundational requirements) | | | | | | | SAL | コスト (JAP) |
|---|---|---|---|---|---|---|---|---|---|
| | AC | UC | DI | DC | RDF | TRE | RA | | |
| ①User Control | ○ | ○ | ○ | ○ | | | | 1, 2, 3 | 数万 |
| ②Firewall | | | ○ | | ○ | | ○ | 1, 3 | 数万 |
| ③Anti-Virus | | | | | | ○ | ○ | 1, 2 | 数千 |
| ④USB port Block | | | | | | | ○ | 2 | 0 |
| ⑤Backup Server | | | | | | | ○ | 1, 2, 3 | 数万～数十万 |
| ⑥Com. Shut (Communication Shutdown) | | | | | ○ | ○ | ○ | 1, 2 | 0 |
| ⑦White list | | | ○ | | | | ○ | 1, 2 | 数千～十数万 |

であることを意味する．ここで示しているツールのコストは [12] を参照して定めた概算値である．

**Step 1**： 侵入経路の分析

Fig.3 中の矢印は侵入経路の分析例を示している．ここでは, 各 Factory の Controllers への侵入経路は，Internet から, Enterprise Machines から, Management Machines から, Control Servers から，HMIs から，Controllers からの 6 種類と考えられる．ここで，n=3 の場合は例としているので，全部 18 Pass となり,Factory1～3 の Controllers への侵入経路は, それぞれ,Pass1～6,Pass7～12 と Pass13～18 である．ここは, 侵入の入り口として, インターネット, 外部機器との臨時接続（USB, 保守用 PC），及び無線計装など挙げられる．

各ゾーンにはマシンが複数存在する．本研究には, Controller 以外のマシンは, 全部 PC とする． ICS のセーフティを守るためには, すべての経路のセキュリティを確保しなければならないので，各階層において，1 本の矢印で表現しているが，各階層のすべてのマシンを対象としている．どこ, 何の目的で, どのツールを配置すればよいのかが本研究の重要な着眼点である．

**Step 2**： **S0**，**S1**，**S7** と **S15** に基づき共通システムに対する対策の選択と配置

本研究では，侵入経路の分析結果 (リスク要求)，予算及びセキュリティ性能のバランスを考慮した上，ツールの選択と配置を行う．Fig.4 の上部の共通部分 (DM ゾーンと生産管理ゾーン) には，Step 0, 1, 7 と 15 の分析結果に基づいた対策ツールの配置例を示した．

下記の Step 3～6 において, ツールを配置した共通システムに対してセキュリティ評価を行う．

**Step 3**： ツールを配置した各マシンでの要件への評価

各マシンにおける各要件の SAL レベル (FR level）を式 (1) により求める．

$$\begin{aligned}&\mathrm{SAL\_Machine}(i,j)[\mathrm{FR}(n)]\\&=\mathrm{Max}\{\mathrm{SAL\_Machine}(i,j)[\mathrm{FR}(n)\_①],\\&\qquad\cdots,\mathrm{SAL\_Machine}(i,j)[\mathrm{FR}(n)\_ⓜ]\}\end{aligned}\quad(1)$$

ここで，$i$ は階層の識別番号，$j$ はある階層におけるマシンの識別番号，$\mathrm{FR}(n)$ は要件の識別番号，ⓚはツールの識別番号を示す．

**Step 4**： ツールを配置した各階層での要件への評価

各階層における各要件の SAL レベルを式 (2) により求める．

$$\begin{aligned}&\mathrm{SAL\_Zone}(i)[\mathrm{FR}(n)]\\&=\mathrm{Min}\{\mathrm{SAL\_Machine}(i,1)[\mathrm{FR}(n)],\\&\qquad\cdots,\mathrm{SAL\_Machine}(i,j)[\mathrm{FR}(n)]\}\end{aligned}\quad(2)$$

**Step 5**： ツールを配置した各階層への評価

各階層の SAL レベルを式 (3) により求める．

$$\begin{aligned}&\mathrm{SAL\_X}(\mathrm{Zone}(i))\\&=\mathrm{Min}\{\mathrm{SAL\_X}([\mathrm{FR}(1)]\ \mathrm{Zone}(i)),\\&\qquad\cdots,\mathrm{SAL\_X}([\mathrm{FR}(7)]\ \mathrm{Zone}(i))\}\end{aligned}\quad(3)$$

**Step 6**： ツールを配置した共通システムへの評価

システムの SAL レベルを式 (4) により求められる．

$$\begin{aligned}&\mathrm{SAL\_X}([\mathrm{FR},]\ \mathrm{System})\\&=\mathrm{Max}\{\mathrm{SAL\_X}([\mathrm{FR},]\ \mathrm{Zone}(1)),\\&\qquad\cdots,\mathrm{SAL\_X}([\mathrm{FR},]\ \mathrm{Zone}(i))\}\end{aligned}\quad(4)$$

式 (4) は，複数の障壁を超えるとき，その経路を攻略する難しさは，最も困難な障壁で定まることを示す．

式 (1)～(4) を用いて，Fig.4 でのセキュリティツールを配置した共通システムへの評価結果を Table 2 の上部に示している．Table 2 の各階層のマシンの台数は 3 で，大学に所有の実験装置を想定して小さな値としている

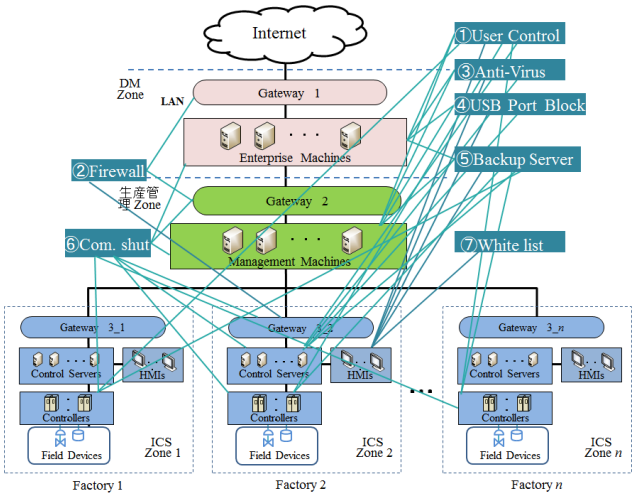


**Fig. 4:** セキュリティ対策ツールの配置例

が，検討対象のネットワークの構成での数値とする．コストは，ゾーン内のすべてのマシンに適用するのに必要な価格となり，マシンによっては価格が異なることも考慮した値にすべきである．

**Step 7**： **S6 の結果とリスク要求と予算とのマッチング**

S6 の結果，リスク要求と予算を満たせば，対策案を採用し，そうではなければ，S2 に戻って再検討する．

**Step 8**： **S7 の結果を採用する．**

Step 0〜Step 8 は，共通システムへの対策立案の手順である．下記の Step 9$n$〜Step 16$n$ においては，各工場の制御システムへの対策立案を行う．ここでの $n$ は工場の識別番号である．

**Step 9**$\_n$： **S0，S1，S14**$\_n$ **に基づき各工場** $(1,2,\cdots,n)$ **の ICS への対策の選択と配置**

Fig.4 の下の部分には，Step 0, 1 と 14$_n$ の分析結果に基づいて Factory 1〜3 への対策ツールの配置例を示した．下記の Step 10$_n$〜13$_n$ において，ツールを配置した各 Factory の制御システムに対してセキュリティ評価を行う．ここで，Factory 2 を例（Table 2 の下の部分を参照）として，具体的評価方法を説明する．

**Step 10**$\_n$： **各工場において，ツールを配置した各マシンでの要件への評価**

ここでの評価方法は Step 3 の内容と同様である．

例えば，Factory 2 の階層 6 (HMIs) の M(6, 1) の FR(7) の場合は，配置されたツール③④⑤⑦の SAL はそれぞれ 1, 2, 2, 1 のため，式 (1) により

$$\begin{aligned}&\text{SAL\_Machine}(6,1)[\text{FR}(7)]\\&=\text{Max}\{\text{SAL\_Machine}(6,1)[\text{FR}(7)\_③④⑤⑦]\}\\&=\text{Max}\{1,2,2,1\}\ =\ 2\end{aligned}$$

である．

**Step 11**$\_n$： **各工場において，ツールを配置した各階層での要件への評価**

ここでの評価方法は Step 4 の内容と同様である．

例えば，Factory 2 の階層 6 (HMIs) の FR(7) の場合は，式 (2) により，

$$\begin{aligned}&\text{SAL\_Zone}(6)[\text{FR}(7)]\\&=\text{Min}\{\text{SAL\_Machine}(6,1)[\text{FR}(7)],\\&\qquad\cdots,\text{SAL\_Machine}(6,3)[\text{FR}(7)]\}\\&=\text{Min}\{2,2,3\}\ =\ 2\end{aligned}$$

である．

**Step 12**$\_n$： **各工場において，ツールを配置した各階層への評価**

ここでの評価方法は Step 5 の内容と同様である．

例えば，Factory 2 の階層 6 (HMIs) の場合は，式 (3) により，

$$\begin{aligned}&\text{SAL\_A}(\text{Zone}(6))\\&=\text{Min}\{\text{SAL\_A}([\text{FR}(1)]\ \text{Zone}(6)),\\&\qquad\cdots,\text{SAL\_A}([\text{FR}(7)]\ \text{Zone}(6))\}\\&=\text{Min}\{2,2,2,2,0,1,2\}\ =\ 0\end{aligned}$$

である．

**Step 13**$\_n$： **各工場において，ツールを配置した工場** $n$ **のＩＣＳへの評価**

ここでの評価方法は Step 6 の内容と同様である．

例えば，Factory 2 の ICS の場合は，式 (4) により，

$$\begin{aligned}&\text{SAL\_A}([\text{FR},]\text{ICS of Factory 2})\\&=\text{Max}\{\text{SAL\_A}([\text{FR},]\text{Zone}(5\text{ of Factory 2})),\\&\qquad\cdots,\text{SAL\_A}([\text{FR},]\text{Zone}(8\text{ of Factory 2}))\}\\&=\text{Max}\{0,0,2,2\}\ =\ 2\end{aligned}$$

である．

Step 10$_n$〜13$_n$ を用いて，Fig.4 でのセキュリティツールを配置した Factory 2 の制御システムへの評価詳細を Table 2 の下の部分に示している．

また，Factory 1〜3 の制御システムへの評価結果を Table 3 に示している．

**Step 14**$\_n$： **各工場において，S13**$\_n$ **の結果とリスク要求と予算とのマッチング**

ここで，まず，Factory 2 の例を用い考察を行う．

Factory 2 については，Table 2 と 3 に示しているように，上の共通ネットワークと下の ICS には，ツールが配置されているため，守るべき Controller への 6 つの Pass から侵入された場合には，すべての要件が満たされるよ

**Table 2:** Fig.4 の各階層及びシステムへの評価

| 適用可能階層 (i) | | | | Foundational Requirements [FR (n)] | | | | | | | | | | | | | | | | | | | | | 適用可能階層のSal Level | コスト/台（JPY） |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | FR (1)=AC | | | FR (2)=UC | | | FR (3)=DI | | | FR(4)=DC | | | FR(5)=RDF | | | FR(6)=TRE | | | FR(7)=RA | | | | |
| 共通システム | 階層1 | Gatway 1 | Machine (1, j) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | M (1, 1) | M (1, 2) | M (1, 3) | 0 | 数万 |
| | | | Tool_Level | | | | | | | ②_1 | ②_3 | ②_3 | | | | ②_1 | ②_3 | ②_3 | | | | ②_1 | ②_3 | ②_3 | | |
| | | | FR level | | | | | | | 1 | 3 | 3 | | | | 1 | 3 | 3 | | | | 1 | 3 | 3 | | |
| | | | Level | 0 | | | 0 | | | 1 | | | 0 | | | 1 | | | 0 | | | 1 | | | | |
| | 階層2 | Enterprise Machines | Machine (2, j) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | M (2, 1) | M (2, 2) | M (2, 3) | 2 | 数万～数十万 |
| | | | Tool_Level | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ⑥_2 | ⑥_2 | ⑥_2 | ③_1, ⑥_2 | ③_2, ⑥_2 | ③_1, ⑥_2 | ③_1, ④_2, ⑤_2, ⑥_2 | ③_2, ④_2, ⑤_2, ⑥_2 | ③_2, ④_2, ⑤_3, ⑥_2 | | |
| | | | FR level | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | | |
| | | | Level | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | | |
| | 階層3 | Gatway 2 | Machine (3, j) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | M (3, 1) | M (3, 2) | M (3, 3) | 0 | 数万 |
| | | | Tool_Level | | | | | | | ②_1 | ②_3 | ②_3 | | | | ②_1, ⑥_2 | ②_3, ⑥_2 | ②_3, ⑥_2 | ⑥_2 | ⑥_2 | ⑥_2 | ②_1, ⑥_2 | ②_3, ⑥_2 | ②_3, ⑥_2 | | |
| | | | FR level | | | | | | | | | | | | | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | |
| | | | Level | 0 | | | 0 | | | 1 | | | 0 | | | 2 | | | 2 | | | 2 | | | | |
| | 階層4 | Management Machines | Machine (4, j) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | M (4, 1) | M (4, 2) | M (4, 3) | 0 | 数万～数十万 |
| | | | Tool_Level | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | | | | ③_1 | ③_2 | ③_1 | ③_1, ④_2, ⑤_2, ⑥_2 | ③_1, ④_2, ⑤_2, ⑥_2 | ③_1, ④_2, ⑤_3, ⑥_2 | | |
| | | | FR level | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | | | | 1 | 2 | 1 | 2 | 2 | 3 | | |
| | | | Level | 2 | | | 2 | | | 2 | | | 2 | | | 0 | | | 1 | | | 2 | | | | |
| 共通システム | | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | 共通階層のコスト：数万～数十万 |
| | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Factory 2 の制御システム | 階層5 | Gatway 3 | Machine (5, j) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | M (5, 1) | M (5, 2) | M (5, 3) | 0 | 数万 |
| | | | Tool_Level | | | | | | | ②_1 | ②_3 | ②_3 | | | | ②_1, ⑥_2 | ②_3, ⑥_2 | ②_3, ⑥_2 | ⑥_2 | ⑥_2 | ⑥_2 | ②_1, ⑥_2 | ②_3, ⑥_2 | ②_3, ⑥_2 | | |
| | | | FR level | | | | | | | | | | | | | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | |
| | | | Level | 0 | | | 0 | | | 1 | | | 0 | | | 2 | | | 2 | | | 2 | | | | |
| | 階層6 | HMIs | Machine (6, j) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | M (6, 1) | M (6, 2) | M (6, 3) | 0 | 数万～数十万 |
| | | | Tool_Level | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2, ⑦_1 | ①_3, ⑦_1 | ①_2, ⑦_2 | ①_2 | ①_3 | ①_2 | | | | ③_1 | ③_2 | ③_1 | ③_1, ④_2, ⑤_2, ⑦_1 | ③_1, ④_2, ⑤_2, ⑦_1 | ③_1, ④_2, ⑤_3, ⑦_2 | | |
| | | | FR level | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | | | | 1 | 2 | 1 | 2 | 2 | 3 | | |
| | | | Level | 2 | | | 2 | | | 2 | | | 2 | | | 0 | | | 1 | | | 2 | | | | |
| | 階層7 | Control Servers | Machine (7, j) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | M (7, 1) | M (7, 2) | M (7, 3) | 2 | 数万～数十万 |
| | | | Tool_Level | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ⑥_2 | ⑥_2 | ⑥_2 | ③_1, ⑥_2 | ③_2, ⑥_2 | ③_1, ⑥_2 | ③_1, ④_2, ⑤_2, ⑥_2 | ③_1, ④_2, ⑤_2, ⑥_2 | ③_1, ④_2, ⑤_3, ⑥_2 | | |
| | | | FR level | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | | |
| | | | Level | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | | |
| | 階層8 | Controllers | Machine (8, j) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | M (8, 1) | M (8, 2) | M (8, 3) | 2 | 数万～数十万 |
| | | | Tool_Level | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ①_2 | ①_3 | ①_2 | ⑥_2 | ⑥_2 | ⑥_2 | ⑥_2 | ⑥_2 | ⑥_2 | ⑤_2, ⑥_2 | ⑤_2, ⑥_2 | ⑤_2, ⑥_2 | | |
| | | | FR level | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | |
| | | | Level | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | | |
| 共通を含むシステム全体 | | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | | | 2 | 総コスト：数十万～数百万 |

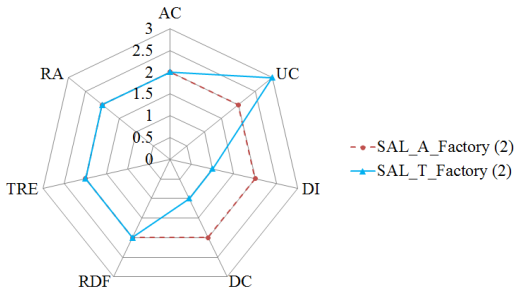


**Fig. 5:** Factory 2 の Achieved SAL と Target SAL

**Table 3:** 各工場の制御システムへの評価

| 各Factoryの制御システム（n=3） | | FR (Foundational Requirements) | | | | | | | Sal Level | コスト/台（JPY） | マシンの台数 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | AC | UC | DI | DC | RDF | TRE | RA | | | |
| Factory (1) の制御システム | Gatway 3_1 | | | | | | | | 0 | 0 | 0 |
| | HMIs | | | | | | | | 0 | 0 | 0 |
| | Control Servers | | | | | | | | 0 | 0 | 0 |
| | Controllers | ① | ① | ① | ① | ⑥ | ⑥ | ⑤⑥ | 1 | 数万 | 3 |
| Factory (2) の制御システム | Gatway 3_2 | | | ② | | ②⑥ | ⑥ | ②⑥ | 0 | 数万 | 3 |
| | HMIs | ① | ① | ①⑦ | ① | | ③ | ③④⑤⑦ | 0 | 数万～数十万 | 3 |
| | Control Servers | ① | ① | ① | ① | ⑥ | ③⑥ | ③④⑤⑥ | 2 | 数万～数十万 | 3 |
| | Controllers | ① | ① | ① | ① | ⑥ | ⑥ | ⑤⑥ | 2 | 数万～数十万 | 3 |
| Factory (3) の制御システム | Gatway 3_3 | | | | | | | | 0 | 0 | 0 |
| | HMIs | | | | | | | | 0 | 0 | 0 |
| | Control Servers | | | | | | | | 0 | 0 | 0 |
| | Controllers | ① | ① | ① | ① | ⑥ | ⑥ | ⑤⑥ | 1 | 数万 | 3 |

うに対策を用意した．

Fig.5 は Factory 2 の Achieved SAL と要求された Target SAL の結果を示している．Fig. 5 により，

$$\text{SAL\_A\_Factory}(2) = \{2,2,2,2,2,2,2\}$$
$$\text{SAL\_T\_Factory}(2) = \{2,3,1,1,1,2,2\}$$

なので，Factory 2 の Achieved SAL{AC, DI, DC, RDF, TRE, RA} は Target SAL に満たしているが，Achieved SAL{UC } は Target SAL に満たしていないため，予算可能であれば，対策ツールの UC のレベルアップが行われることが望ましい．

また，Fig.5 と Table 2 を，Factory 2 の制御システムへの対策の提案者と投資を決める採択者がともにながめて，その投資で妥当と判断するか，さらに対策を追加する，あるいは削除するかを検討する．

次は，Table 3 により，Factory 1 と 3 の考察を行う．ここで，Factory 1 と 3 は，サイバー攻撃からの安全確保（Field Device の不安全な動作の回避）に，最小限の投資で済ませたい場合の検討例になっている．弱点があると，そこをつかれてサイバー攻撃に陥落してしまうと考えられるので，すべてのパスについて検討しなければならない．不安全な状態を発生させるのは Field Device であり，Controllers への対策は，すべてのパスに共通の対策になる．

そのため，最小限の投資での対策を指向するとき，Controllers から対策ツールの配置を検討すればよいと考えられる．また，1 つのツールで，セキュリティの 7 要件をすべて満たすものはないので，Table 3 に示すように，Factory 1 と 3 においては，Controllers の脆弱性をなくすために，①⑤⑥を配置する．

**Step 15**： **全ての S14 の結果とシステム全般のリスク要求と予算とのマッチング**

S14_$n$ の結果，リスク要求と予算を満たせば，対策案を採用し，そうではなければ，S9_$n$ に戻って再検討する．

**Step 16**： **S15 の結果を採用する．**

**Step 17**： **対策立案を終了する．**

## 4. まとめ

サイバー攻撃の手口は日々進化しており，制御システムネットワークへのサイバー攻撃の脅威が高まっている．本研究では，セキュリティツールの投資効果を「見える化」することを目指し，リスク要求，セキュリティ性能及び経済性のバランスを考慮した制御系セキュリティ対策のアプローチを提案した．

対象のネットワークシステムの構造からアプローチする本手法により，制御システムにおけるサイバーセキュリティレベルの評価をし，実施すべきセキュリティ対策を選択し，さらにその有効性を検討する，PDCA サイクルによる考察が可能になった．

提案した対策手法は対象の危険性，企業の経営状態などで一意にさだめるものではないが，提案したテーブルを用いて，コストも考慮しながら，ツールの選別，配置箇所の選択を，対策立案者と評価者がともに，可視化された情報をもとに論じることができるようになった．

**謝辞:** 本研究は，科学研究費助成事業（【基盤研究 B：研究代表者 越島一郎，課題番号 24310119】と【基盤研究 B：研究代表者 橋本 芳宏，課題番号 25282101】）により助成を受けて進められる．

## References

[1] 独立行政法人・情報処理機構（IPA）編：「重要インフラの制御システムセキュリティと IT サービス継続に関する調査」(2009).

[2] H. Yoneda, “View point and challenges of OPC UA utilization in FA/PA viewed from user”, Keiso, Vol.57, No.10,

pp.1-6, Oct., 2014.

[3] Y. Hashimoto, et al., “Safety securing approach against cyber-attacks for process control system”, International Journal of Computers and Chemical Engineering, Vol.57, pp. 181-186, 2013.

[4] H. Moritani, et al., “Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security”, Proceedings of 14th International Conference on Control, Automation and Systems, Oct. 22-25, 2014, Korea.

[5] T. Morita, et al., “Detection of Cyber-Attacks with Zone Dividing and PCA”, Proceedings of Procedia Computer Science, Vol.22, pp.727-736, 2013.

[6] M. Kojima, et al., “Development of CAD for Plant-Wide Control Loop Configuration”, Proceedings of ADCONIP 2014, pp.450-454, 2014.

[7] H. Takagi, et al., “Strategic Security Protection for Industrial Control System”, Proc. SICE Annual Conference, pp.1215-1221, 2015, China.

[8] 孫晶, 橋本芳宏, 高木ひとみ, 越島一郎, ICS セキュリティ対策の立案手法, 日本設備管理学会秋季研究発表大会予稿集 (2015)

[9] 孫晶, 高木ひとみ, 伊藤一馬, 越島一郎, 橋本芳宏, 制御系セキュリティツールの選択と配置, 第 6 回横幹連合コンファレンス予稿集, pp.158-162 （2015）.

[10] ISA_99. 03. 03, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels (2013)

[11] G. James, et al., Security Assurance Levels: A Vector Approach to Describing Security Requirements, 2010.

[12] 佐々木弘志 :「制御システムセキュリティソリューション紹介」, 名古屋工業大学 平成 27 年度制御系セキュリティ演習テキスト 2 （2015）.

孫　晶

2007 年電気通信大学大学院電子情報学専攻博士課程修了, 工学博士. 電気通信大学特別研究員と青山学院大学客員研究員を経て, 2010 年より名古屋工業大学大学院工学研究科助教. 総合的品質経営, 生産マネジメント, 製販サビースと SCM, 生産システムのサーバセキュリティなどの研究に従事. 2007 年社団法人日本経営工学会論文奨励賞受賞.

高木 ひとみ

2013 年名古屋工業大学工学部都市社会工学科卒業, 2015 年 名古屋工業大学大学院工学研究科社会工学専攻修了. 2015 年新生銀行, 現在に至る.

伊藤 一馬

2016 年名古屋工業大学工学部都市社会工学科卒業, 2016 年名古屋工業大学大学院工学研究科社会工学専攻に進学, 現在に至る.

越島 一郎

1979 年早稲田大学院工学研究科応用化学専攻修士課程修了, 同年千代田化工建設株式会社入社. 1998 年千葉工業大学プロジェクトマネジメント学科准教授, 教授を経て, 2008 年より名古屋工業大学院工学研究科教授, 現在に至る. エンジニアリング企業での実務経験を踏まえて, プロジェクトマネジメント, セーフティ＆セキュリティマネジメント等の研究に従事.

橋本 芳宏

1985 年京都大学大学院工学研究科博士課程化学工学専攻単位取得 退学. 1985 年名古屋工業大学大学院助手, 2003 年教授, 現在に至る. プロセスシステム工学, プロセス制御などの研究に従事. 工学博士. 計測自動制御学会, 化学工学会などの会員.