Japan Computer Emergency Response Team Coordination Center

2015 年度 制御システムセキュリティに関する アセットオーナ実態調査

一般社団法人 JPCERT コーディネーションセンター
2016 年 11 月 15 日

JPCERT CC®

目次

1. はじめに

本資料は、産業用制御システム（Industrial Control System：以下 ICS）のセキュリティ対策促進のため、ICS を利用しているアセットオーナの ICS セキュリティに対する認識や対策状況を把握することを目的として、次の方法で調査した結果をまとめたものである。

調査方法は、総務省統計局の日本標準産業分類（平成 25 年 10 月改定分）に準拠した各業界（表 1 参照）で従業員 300 人以上を有し、制御システムを所有するアセットオーナ（2,308 組織）に対してアンケートを郵送（必要に応じて直接取材、電話ヒアリングなども実施）する方法を採用し、318 組織から回答を得た。（表 2 参照）
回答を得た業種は 26 業種。従業員規模では 300～1,000 人の組織が回答の 8 割を占め、中小企業基本法に基づくと大企業とされる組織から回答を得られていることとなった。

また、本資料では調査結果を次の構成でまとめる。
「調査結果」は、2015 年度の調査結果をグラフと表で掲載し、その分析を「2.13. ICS セキュリティの認識に関する実態調査結果の分析」に記載する。また、3 章では、主として DCS（Distributed Control System）を利用する業界を PA（Process Automation）、主として PLC（Programmable Logic Controller）を利用する業界を FA（Factory Automation）と定義し、PA/FA 別に集計して比較した考察を記載する。最後に、「4. まとめ」においてこれらの調査結果を概観した国内の ICS セキュリティに対する認識や対策の状況を記載する。

表 1　調査基礎データ

調査対象エリア	日本国内
調査方法	国内事業者へのアンケート（郵送、取材および電話ヒアリング）
調査対象業種	農業・林業 鉱業・採石業・砂利採取業 建設業 食料品製造業 飲料・たばこ・飼料製造業 繊維工業 木材・木製品製造業（家具を除く） 家具・装備品製造業 パルプ・紙・紙加工品製造業 印刷・同関連業 化学工業 石油製品・石炭製品製造業 プラスチック製品製造業 ゴム製品製造業 なめし革・同製品・毛皮 窯業・土石製品製造業 鉄鋼業 非鉄金属製造業 金属製品製造業 はん用機械器具製造業 生産用機械器具製造業 業務用機械器具製造業 電子部品・デバイス・電子回路製造業 電気機械器具製造業 情報通信機械器具製造業 輸送用機械器具製造業 その他の製造業 電気業 ガス業 熱供給業 水道業 運輸業・郵便業
回答組織数	318 組織

表 2　回答業種と全回答における各業種の回答割合（全 32 業種）

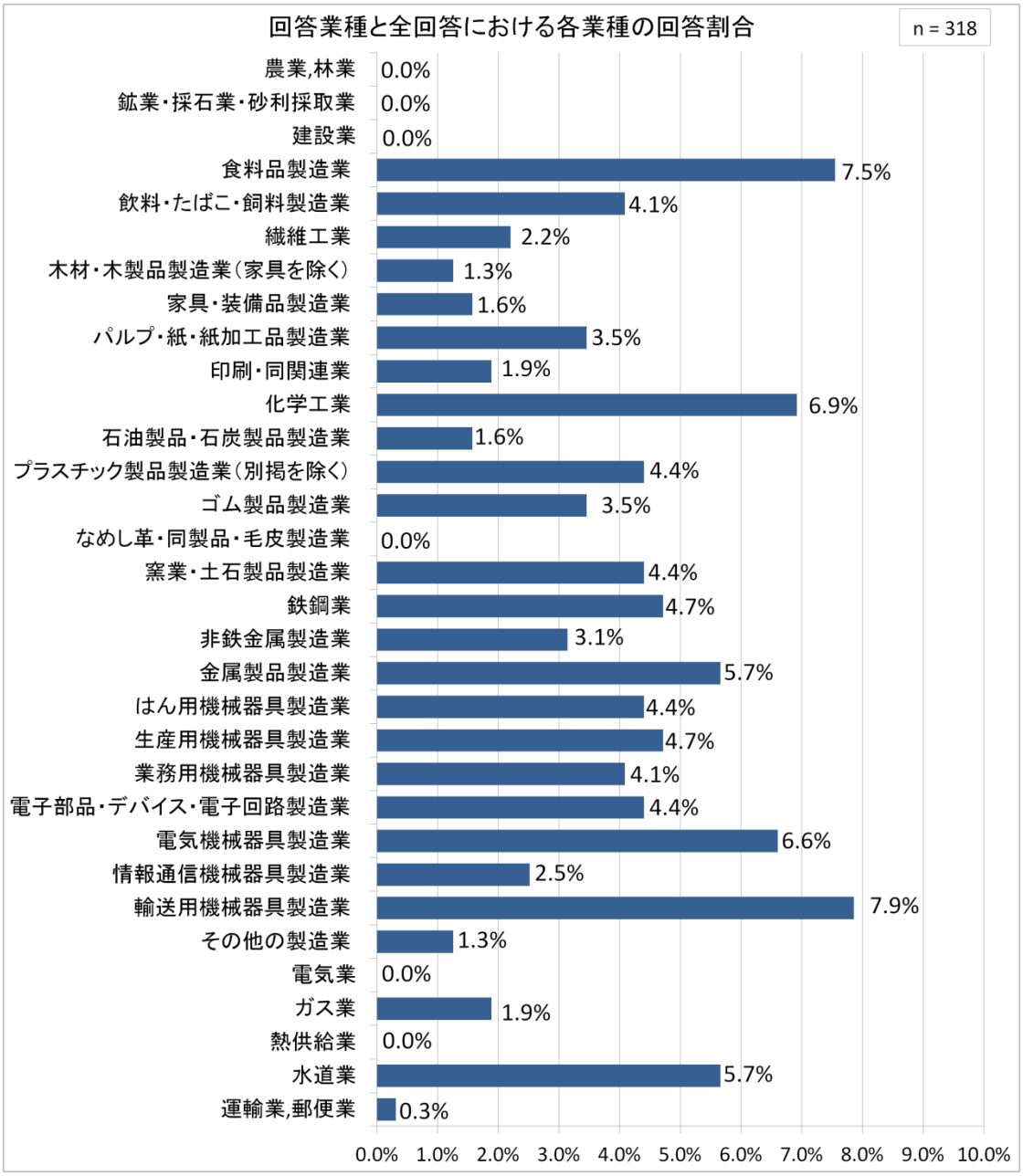
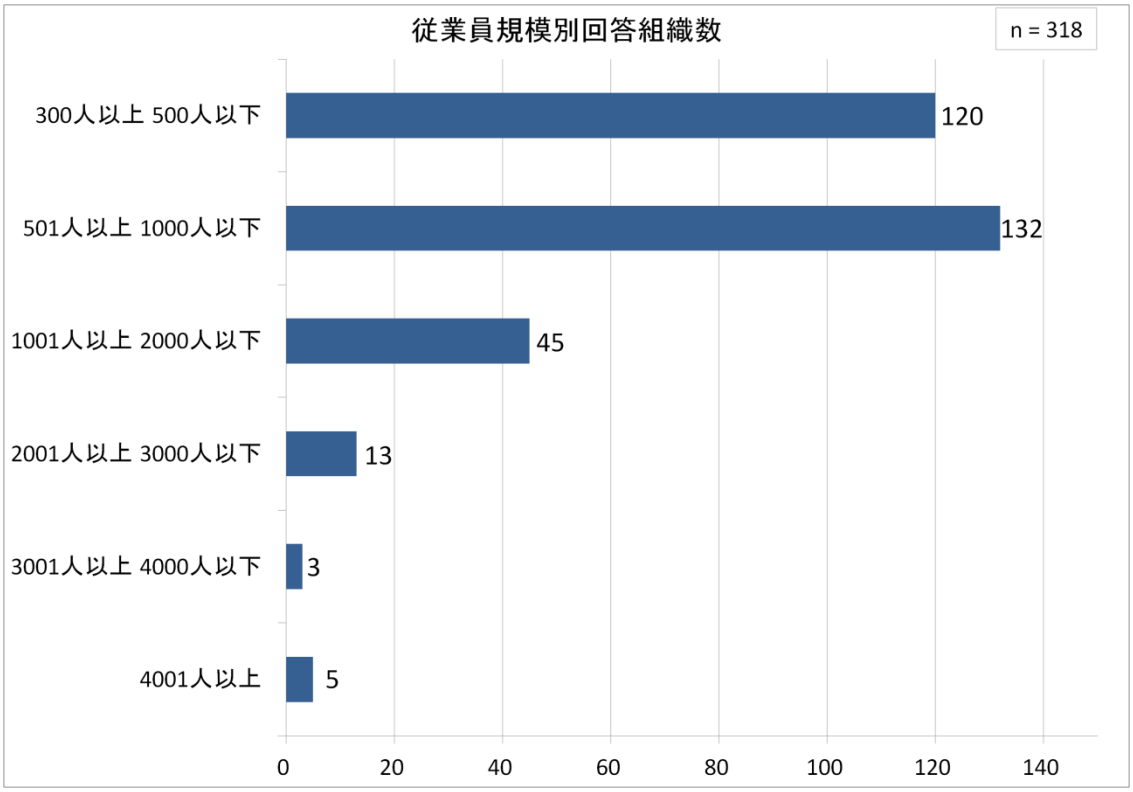


表 3　従業員規模別回答組織数



2. 調査結果

本章では、項目ごとに、設問と回答の集計結果を示す。

2.1. PLC、SCADA ソフトウエア、DCS の使用状況

（複数回答）

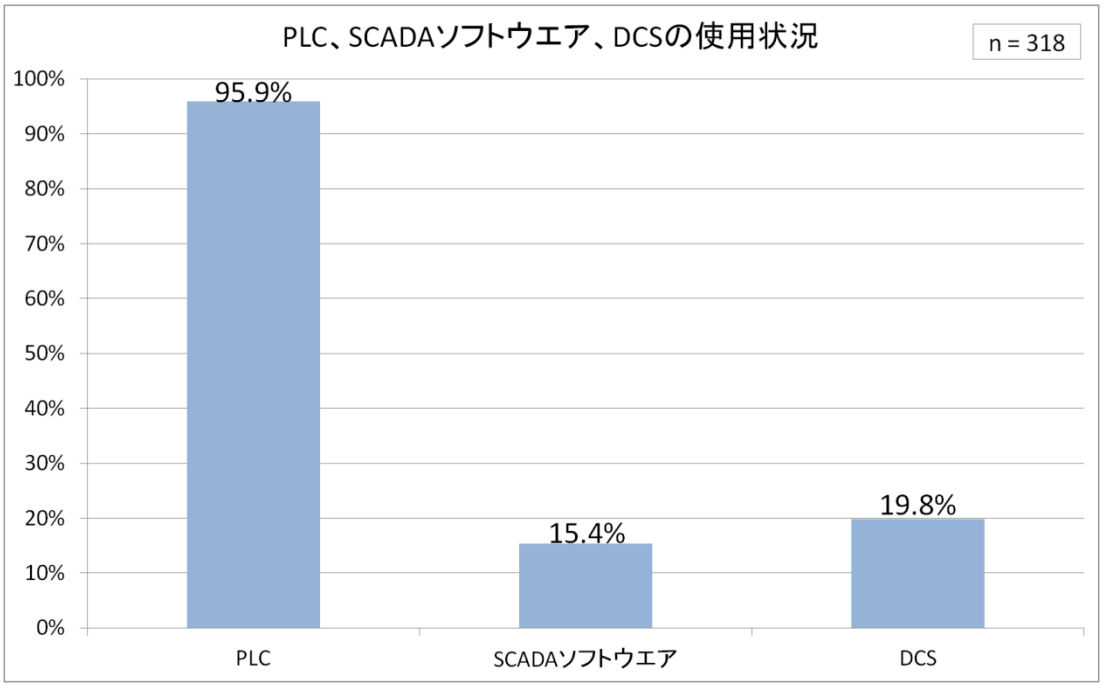


図 1　PLC、SCADA ソフトウエア、DCS の使用状況

Q.1 現在、貴組織の生産システムにおいて以下のコントローラーやシステム、ソフトウエアの採用はございますか

選択肢	回答割合
PLC[1]	95.9%
SCADA ソフトウエア	15.4%
DCS	19.8%

[1] 本回答にはハードウエア PLC のみでなく、ソフトウエア PLC も含んでいる

2.2. 拠点間接続方法

（複数回答）

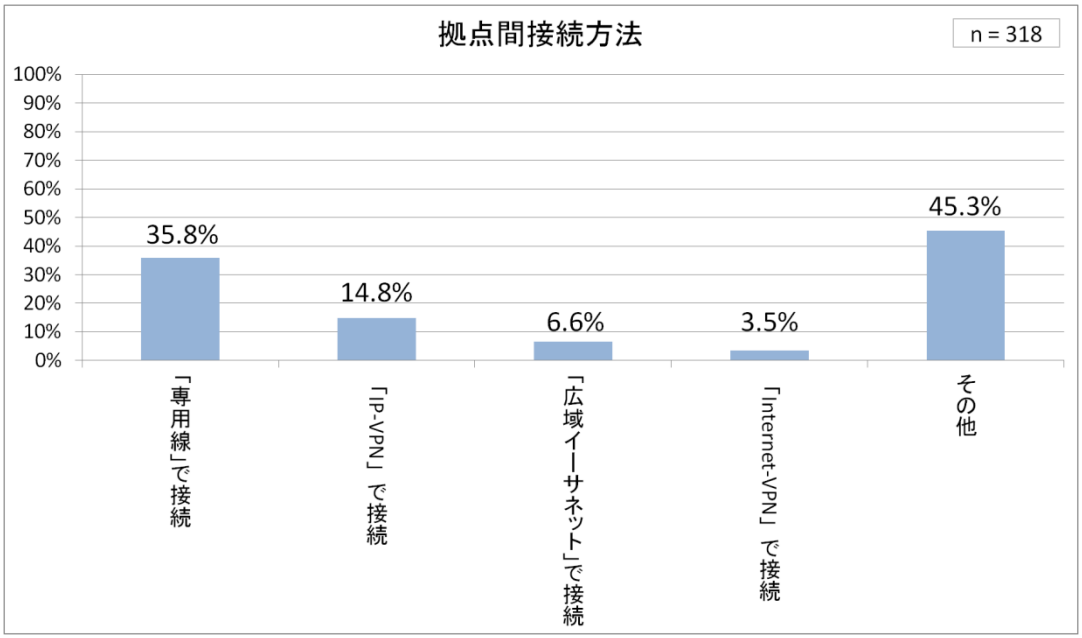


図 2 拠点間接続方法[1]

Q.2 貴組織の拠点間（本社と工場、工場と工場など）ネットワーク接続は、どのような方法で行っておられますか

選択肢	回答割合
「専用線」で接続	35.8%
「IP-VPN」で接続	14.8%
「広域イーサネット」で接続	6.6%
「Internet-VPN」で接続	3.5%
その他	45.3%

[1] 拠点間には「本社・工場間」、「工場・工場間」を含む。

2.3. ICS 製品におけるマルウエア感染経験

（単一回答）

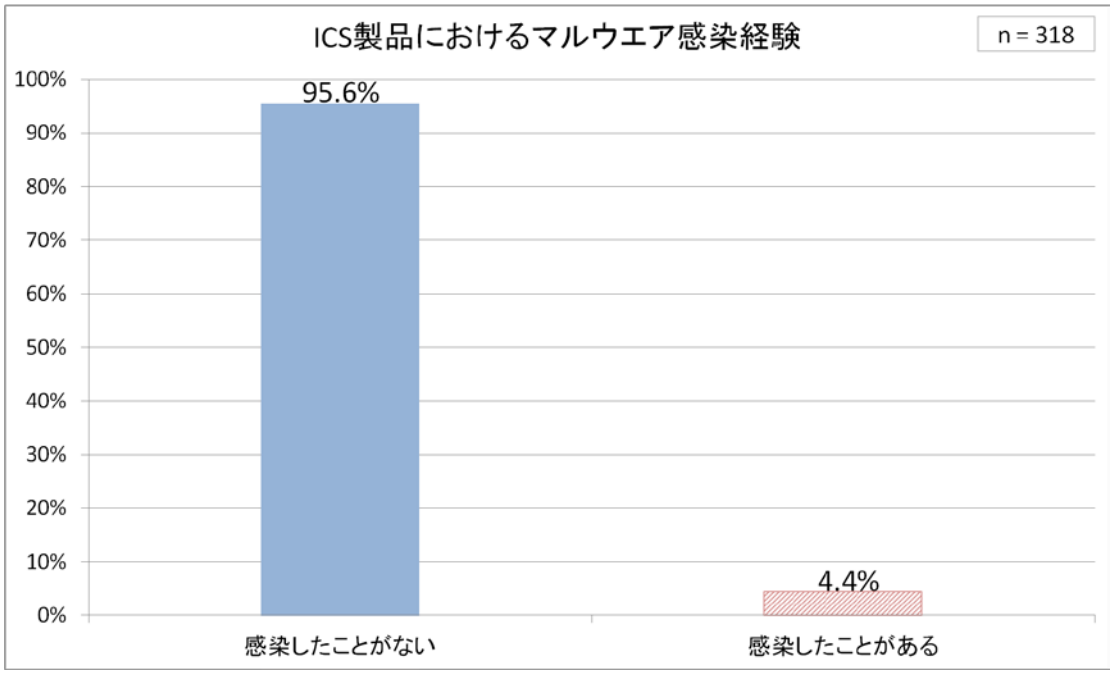


図 3　ICS 製品におけるマルウエア感染経験

Q.3 ICS 製品におけるマルウエア（ウィルス、ワーム、スパイウエア、トロイ）などへの感染例はございますか。

選択肢	回答割合
感染したことがない	95.6%
感染したことがある	4.4%

2.4. ICS 製品ベンダへのセキュリティに関する対応や助言の要求

（単一回答）

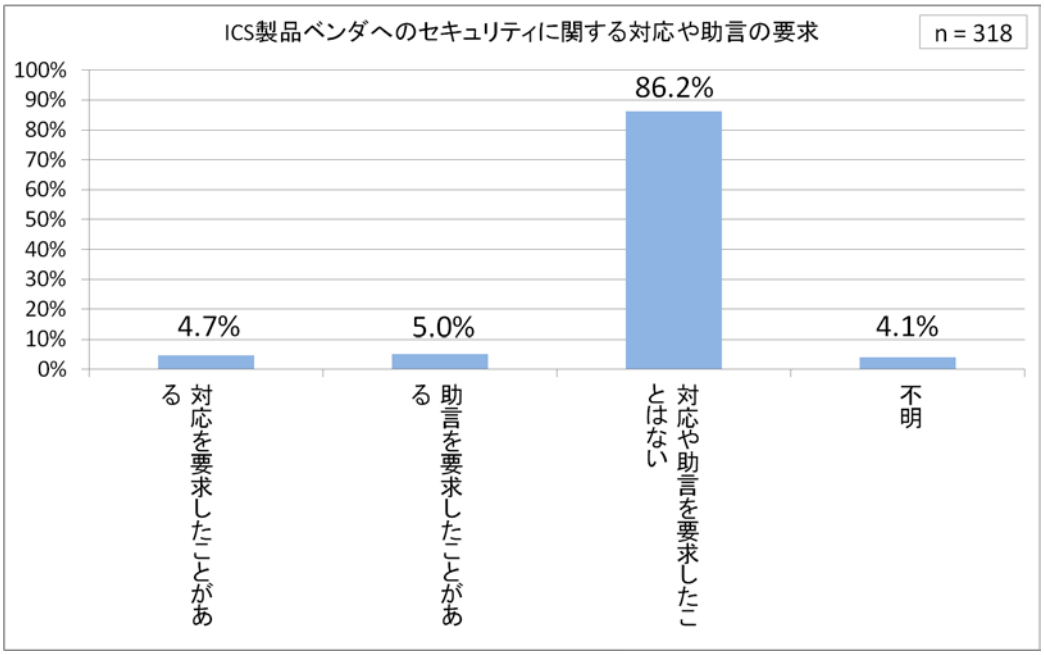


図 4　ICS 製品ベンダへのセキュリティに関する対応や助言の要求

Q.4 ICS 製品メーカーに対してセキュリティに関する対応や助言を要求されたことがございますか

選択肢	回答割合
対応を要求したことがある	4.7%
助言を要求したことがある	5.0%
対応や助言を要求したことはない	86.2%
不明	4.1%

2.5. ICS 製品に関するセキュリティ情報の入手

（複数回答）

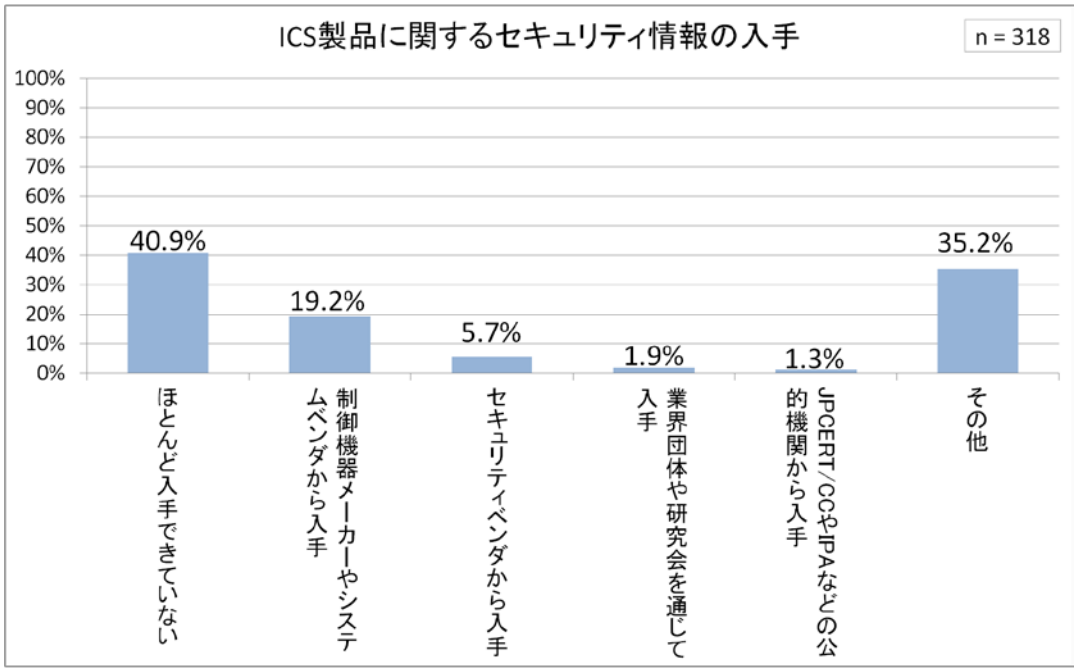


図 5　ICS 製品に関するセキュリティ情報の入手

Q.5 対象制御システムのセキュリティ情報の入手はどのようにされておられますか

選択肢	回答割合
ほとんど入手できていない	40.9%
制御機器メーカーやシステムベンダから入手	19.2%
セキュリティベンダから入手	5.7%
業界団体や研究会を通じて入手	1.9%
JPCERT/CC や IPA などの公的機関から入手	1.3%
その他	35.2%

2.6. ICS 製品のセキュリティリスク評価

（単一回答）

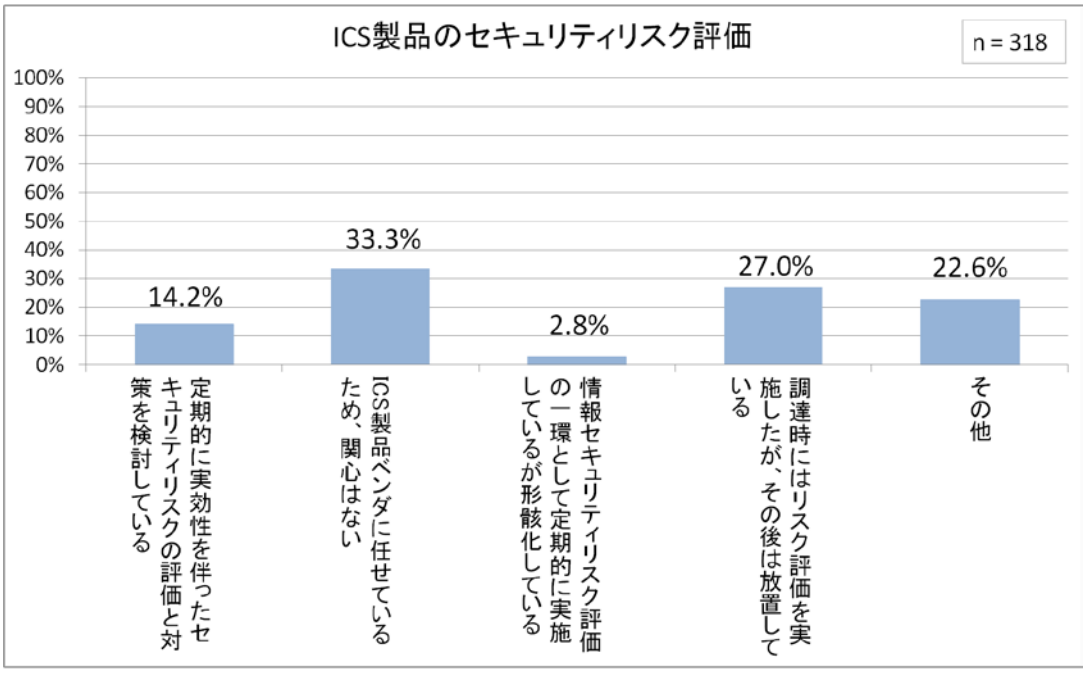


図 6　ICS 製品のセキュリティリスク評価

Q.6 ICS 製品のセキュリティリスク評価の取組みはどのような状況ですか

選択肢	回答割合
定期的に実効性を伴ったセキュリティリスクの評価と対策を検討している	14.2%
ICS 製品ベンダに任せているため、関心はない	33.3%
情報セキュリティリスク評価の一環として定期的に実施しているが形骸化している	2.8%
調達時にはリスク評価を実施したが、その後は放置している	27.0%
その他	22.6%

2.7. 「ICS 製品ベンダのセキュリティ関連サポート」に対する評価

（単一回答）

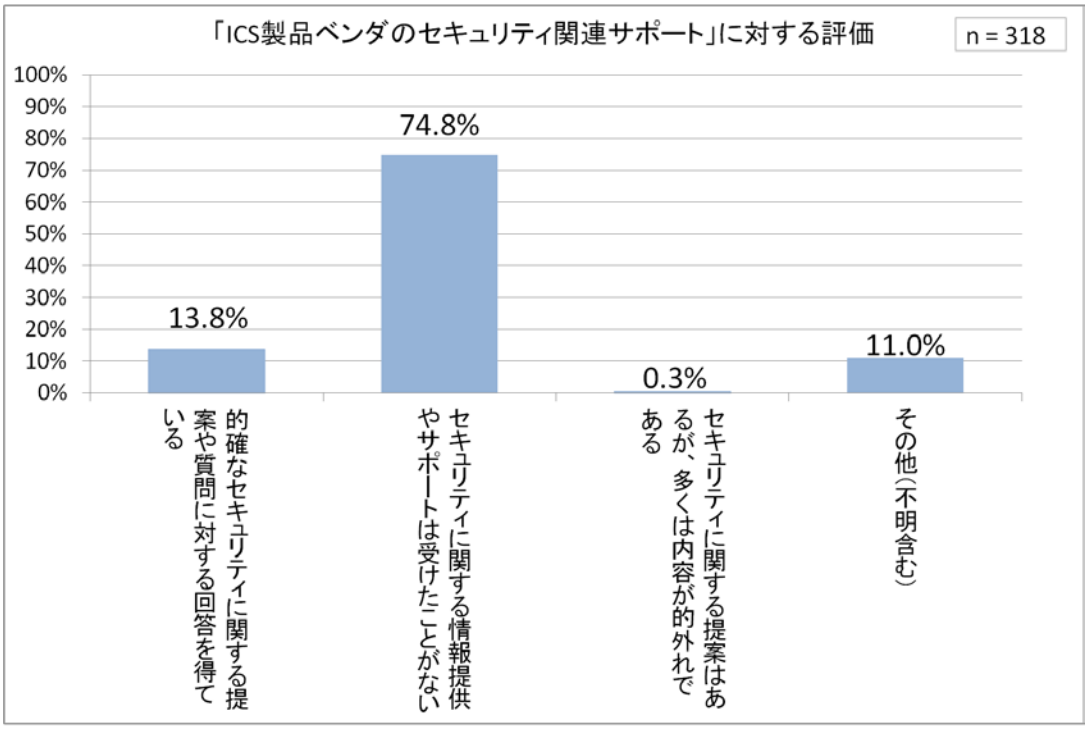


図 7　「ICS 製品ベンダのセキュリティ関連サポート」に対する評価

Q.7 主な調達先となっている ICS 製品ベンダのセキュリティ関連のサポートはどのようなものですか

選択肢	回答割合
的確なセキュリティに関する提案や質問に対する回答を得ている	13.8%
セキュリティに関する情報提供やサポートは受けたことがない	74.8%
セキュリティに関する提案はあるが、多くは内容が的外れである	0.3%
その他（不明含む）	11.0%

2.8. ICS 製品のセキュリティインシデントの可能性に対する認識

（単一回答）

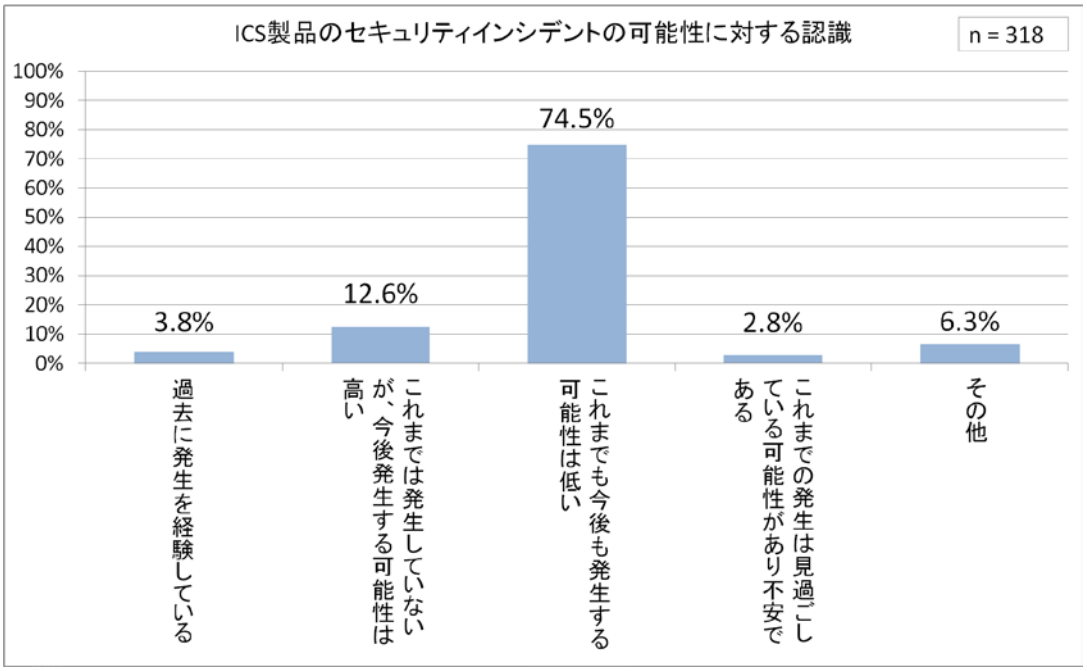


図 8　ICS 製品のセキュリティインシデントの可能性に対する認識

Q.8 ICS 製品のセキュリティインシデント発生の可能性に対する認識はどのようなものですか

選択肢	回答割合
過去に発生を経験している	3. 8%
これまでは発生していないが、今後発生する可能性は高い	12. 6%
これまでも今後も発生する可能性は低い	74. 5%
これまでの発生は見過ごしている可能性があり不安である	2. 8%
その他（不明、非該当、拒否を含む）	6. 3%

2.9. 万一セキュリティ事故が起きた場合のサポート依頼先

（単一回答）

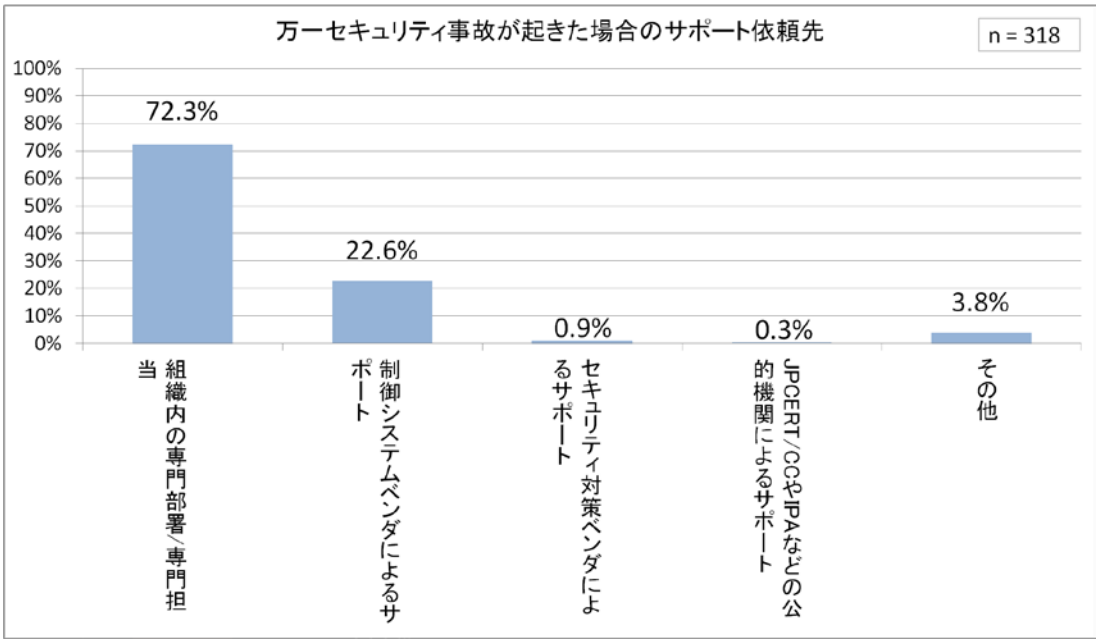


図 9　万一セキュリティ事故が起きた場合のサポート依頼先

Q.9 万一セキュリティ事故が起きた場合に最も頼りになるのはどのようなものですか

選択肢	回答割合
組織内の専門部署/専門担当	72. 3%
制御システムベンダによるサポート	22. 6%
セキュリティ対策ベンダによるサポート	0. 9%
JPCERT/CC や IPA などの公的機関によるサポート	0. 3%
その他	3. 8%

2.10. 遠隔からのプラントの監視または操作の可否

（単一回答）

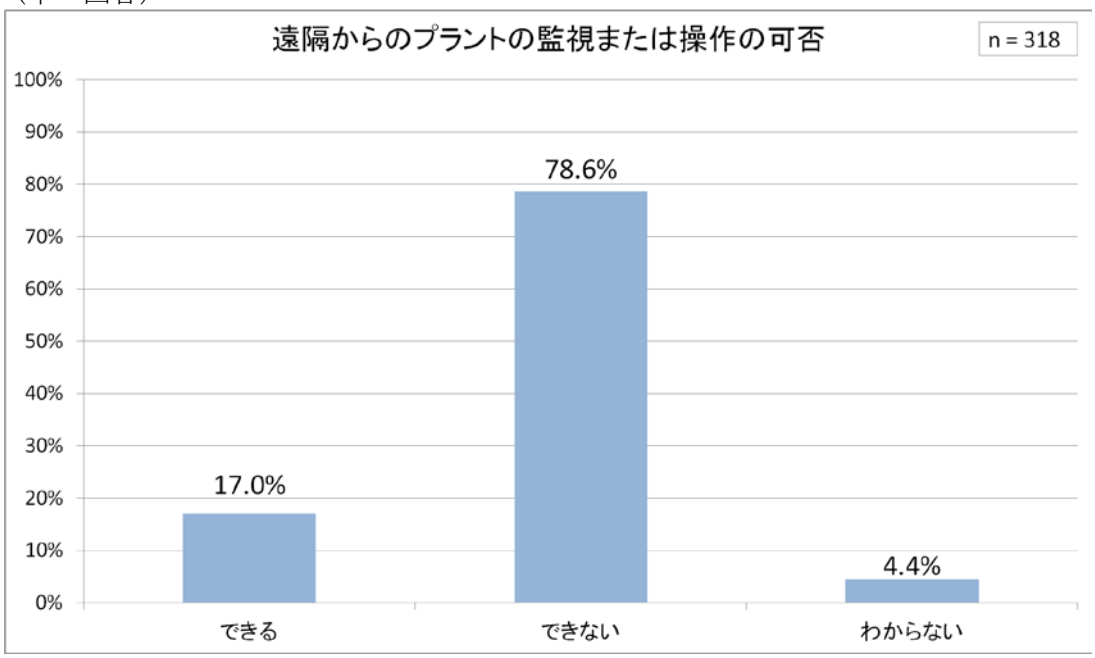


図 10　遠隔からのプラントの監視または操作の可否

Q.10 生産施設内の監視室以外（例えば自宅など）からプラントの監視または操作を行うことができますか

選択肢	回答割合
できる	17. 0%
できない	78. 6%
わからない	4. 4%

2.11. ICS 製品のセキュリティインシデントに備えた体制の整備

（単一回答）

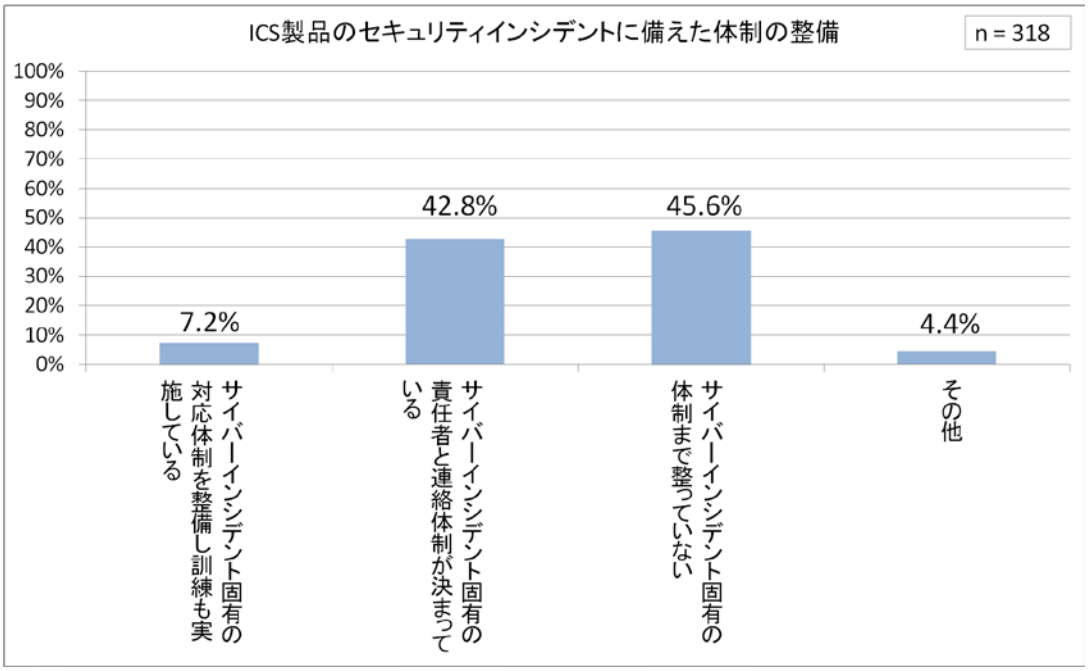


図 11　ICS 製品のセキュリティインシデントに備えた体制の整備

Q.11 ICS 製品のセキュリティインシデントが発生した場合に備えた体制の整備状況について

選択肢	回答割合
サイバーインシデント固有の対応体制を整備し訓練も実施している	7. 2%
サイバーインシデント固有の責任者と連絡体制が決まっている	42. 8%
サイバーインシデント固有の体制まで整っていない	45. 6%
その他	4. 4%

2.12. ICS における今後のセキュリティ対策の必要性

（単一回答）

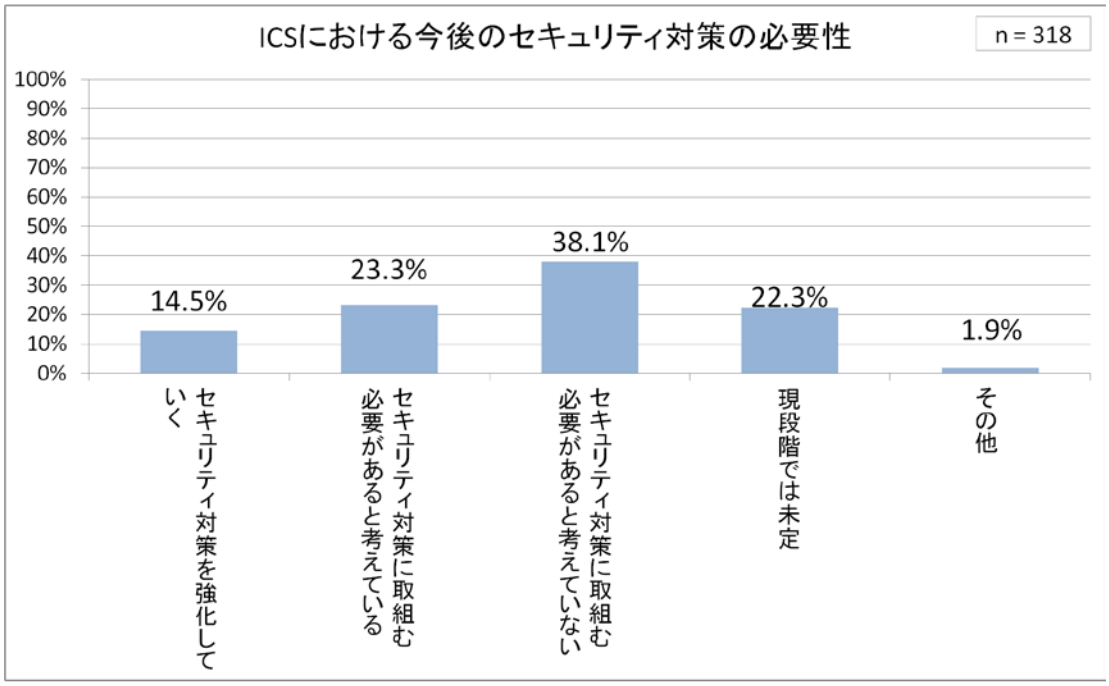


図 12　ICS における今後のセキュリティ対策の必要性

Q.12 今後の貴組織工場内の ICS 製品におけるマルウエアや外部侵入に関する方向性について

選択肢	回答割合
セキュリティ対策を強化していく	14. 5%
セキュリティ対策に取組む必要があると考えている	23. 3%
セキュリティ対策に取組む必要があると考えていない	38. 1%
現段階では未定	22. 3%
その他	1. 9%

2.13. ICS セキュリティの認識に関する実態調査結果の分析

本章では、ICS セキュリティの認識に関する実態調査について分析を行った結果を記載する。

まず、設備やネットワークについて見てみると、設備では「2.1. PLC、SCADA ソフトウエア、DCS の使用状況」に見るように回答組織の約 95%がソフトウエア PLC を含む PLC を採用していることが分かった。また、拠点間接続では、「専用線」が 3 割強を占め、以下「IP-VPN」（14.8%）、「広域イーサネット」（6.6%）、「Internet-VPN」（3.5%）の順で利用されていることが分かった。（「2.2. 拠点間接続方法」参照）

■セキュアなネットワーク構成がマルウエアの感染防止に一定の効果を発揮

上述のように拠点間の接続にはセキュアな回線を使用している上、「2.10. 遠隔からのプラントの監視または操作の可否」では「できない」とした回答が約 8 割に達しており、いわゆる「エアギャップ」によって一定のセキュリティを確保していることが分かった。これらのことから、多くの業界では制御システムネットワークはセキュリティに配慮された運用が行われていることが分かる。このことは「2.3. ICS 製品におけるマルウエア感染経験」で「感染したことがない」とする回答が 95.6%と、制御システムに対するマルウエアの感染件数がほとんどないとした結果の要因になっていると思われ、ネットワークに対するセキュリティ対策が一定の効果を発揮しているものと考えられる。

■サイバー攻撃に備えた対応体制の整備

一方、前項で示したように国内ではマルウエア感染被害事例が少ないためか、「2.8. ICS 製品のセキュリティインシデントの可能性に対する認識」では、7 割以上のアセットオーナが「これまでも今後も（ICS セキュリティインシデントが）発生する可能性は低い」と回答しており、制御システムを利用するアセットオーナがサイバー脅威を差し迫ったものと捉えていないことが分かった。

こうした意識を反映しているものとして、「2.6. ICS 製品のセキュリティリスク評価」では「ICS 製品ベンダに任せているため、関心はない」とした回答と、「調達時にはリスク評価を実施したが、その後は放置している」との回答が合わせて 6 割を超えた。また、「2.11. ICS 製品のセキュリティインシデントに備えた体制の整備」では 5 割弱が「サイバーインシデント固有の体制まで整っていない」と回答し、「2.12. ICS における今後のセキュリティ対策の必要性」では「セキュリティ対策に取組む必要があると考えていない」と回答した組織が 4 割弱あり、これらのことから多くの組織においてセキュリティ対策の必要性が広く浸透していないことが分かった。また、「2.5. ICS 製品に関するセキュリティ情報の入手」の「ほとんど入手できていない」という回答が 40%程度あることも同様の理由によるものと思われる。

■制御システムを取り巻くサイバー脅威の変化

アセットオーナのセキュリティ意識が低い要因として、国内で大規模なインシデントが発生していないことや、自社の周辺を含めてマルウエア感染といったインシデントがあまり発生していないことにより、セキュリティ対策が喫緊の課題として捉えられていないことが考えられる。インシデント事例が少ないことに加え、これまでのマルウエア感染はたまたま制御システムに感染したようなケースが主で、そういったケースの多くが制御システムの動作にまで影響を与えるものではなかったことも一因といえる。

（ただし、昨今情報系システムで大きな被害を引き起こしているランサムウエアについては、制御システムを狙ったものでなくても制御システムに感染した場合は操業などに大きな影響を与えることには注意が必要である。）

その一方で、近年制御システムを標的としたマルウエア（HavexRAT、BlackEnergy2/3 など）が海外で確認され、2015 年 12 月にはウクライナの発電所がサイバー攻撃により停電するといった事態[1]も発生しており、国内でも同様のインシデントが発生してもおかしくない状況にある。

このように制御システムに対するサイバー脅威が徐々に大きくなっているのに加え、Industry4.0 や IIoT（Industrial IoT）といった製造業の変革により、制御システムが外部ネットワークに接続されるケースが増えていくことが予想され、これまでエアギャップによって確保されていた安全性が確保されなくなってしまうことが危惧される。

[1] Analysis of the Cyber Attack on the Ukrainian Power Grid
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

3. PA と FA 別比較による考察

本章では、各業種を表 4 のように PA と FA に分類した視点から調査内容を考察した結果を記載する。

表 4　PA/FA 分類データ

対象エリア	日本国内
PA	鉱業・採石業・砂利採取業 パルプ・紙・紙加工品製造業 化学工業 石油製品・石炭製品製造業 ゴム製品製造業 電気業 ガス業 熱供給業 水道業 運輸業・郵便業
FA	農業・林業 建設業 食料品製造業 飲料・たばこ・飼料製造業 繊維工業 木材・木製品製造業（家具を除く） 家具・装備品製造業 印刷・同関連業 プラスチック製品製造業 なめし革・同製品・毛皮 窯業・土石製品製造業 鉄鋼業 非鉄金属製造業 金属製品製造業 はん用機械器具製造業 生産用機械器具製造業 業務用機械器具製造業 電子部品・デバイス・電子回路製造業 電気機械器具製造業 情報通信機械器具製造業 輸送用機械器具製造業 その他の製造業

以下の設問に関して、PA と FA ごとに集計して比較したグラフを記載する。
なお、回答組織数は PA（74）、FA（244）である。

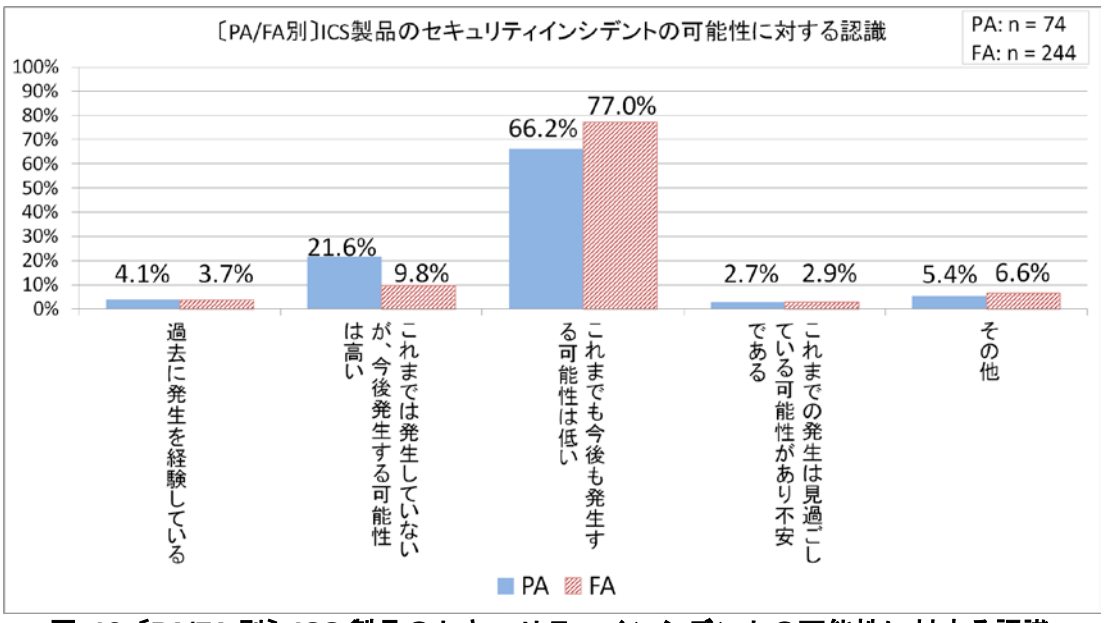


図 13〔PA/FA 別〕ICS 製品のセキュリティインシデントの可能性に対する認識

■PA と FA、それぞれに見るセキュリティ意識

本設問の「〔PA/FA 別〕ICS 製品のセキュリティインシデントの可能性に対する認識」では、「これまでは発生していないが、今後発生する可能性は高い」とした割合が PA の回答では 20%を超え、FA と 10 ポイント以上の差があり、「これまでも今後も（ICS 製品のセキュリティインシデントが）発生する可能性は低い」とした回答でも両者の間に 10 ポイントほどの差があることが分かる。

この結果には、さまざまな要因が考えられるが、PA における回答組織の多くが、内閣サイバーセキュリティセンター（NISC）が定める重要インフラ事業者であり、政府からセキュリティ対策を求められていることから、セキュリティ意識が高まってきた結果と思われる。

4. まとめ

本調査の結果、ICS を利用しているアセットオーナの ICS セキュリティに対する認識や対策状況を把握することができた。
また、「2.13. ICS セキュリティの認識に関する実態調査結果の分析」でも述べたが、総じて制御システムを利用するアセットオーナにセキュリティの重要性が浸透していないことが分かった。しかしながら、PA と FA で見てみると、セキュリティ意識に若干の違いがあり、PA の制御システムを使用する業界の方が、セキュリティ意識が高い結果であった。

■制御システム利用者における今後のセキュリティ対策の進展
2 章で述べたウクライナへのサイバー攻撃の事例のように、海外の制御システムに対するサイバー攻撃は電力を中心とした重要インフラで発生している。こうした海外でのサイバー攻撃事例は概して政治的背景をもち、日本ではこのような事例がこれまで発生してこなかったが、今後は日本でも発生するかもしれない事を念頭に置くべきである。そのため、サイバー攻撃が起きるかもしれないという前提に立ち、さらなるセキュリティ意識の向上と今後のセキュリティ対策の進展が望まれる。

■Industry4.0 や IIoT の導入によるセキュリティリスクの増加
制御システムを使用する業界では、Industry4.0 や IIoT の導入が進んでいくとみられる。経済産業省の「2015 年版ものづくり白書[2]」においても、ドイツの Industry4.0 といった各国の取り組みや、国内の産業界における省力化や新たな価値創造のための IoT の利活用を取り上げ、「IoT 活用によるメリットを享受する積極的な姿勢が重要」であると述べられている。
Industry4.0 や IIoT の導入に合わせて、制御システムにおいてどのようにセキュリティを確保するかが重要になってくる。なぜなら、これまではエアギャップを構築し、それを維持することで一定のセキュリティを確保していたが、あらゆるものがネットワークに“つながる”ことを前提とする Industry4.0 や IIoT では、ネットワークにつながることによりセキュリティリスクが増大することになり、セキュリティ対策の必要に迫られるからである。
先述のものづくり白書でも「今後は「つながる工場」でさらなる付加価値を模索する流れの中、工場（制御系）の外とつながりつつもセキュリティが確保されることをしっかりと担保することが必要」だとしており、産業界における新たなチャレンジを推し進めていくためにも積極的にセキュリティ対策に取り組んでいくことが重要である。

■制御システムのセキュリティ情報の収集と効果的なセキュリティ対策の検討が肝要
2 章で述べたように、海外における制御システムへのサイバー脅威が徐々に高まってきており、日本国内でもセキュリティ対策の重要性が高まってきている。このような中で「2.5. ICS 製品に関するセキュリティ情報の入手」の「ほとんど入手できていない」という回答や「2.12. ICS における今後のセキュリティ対策の必要性」の「セキュリティ対策に取組む必要があると考えていない」とした回答がいずれも 40%程度あることは、今後増加していくと思われるサイバー脅威に対してセキュリティ対策の重要性を広く普及させていく必要があることを示している。

アセットオーナがこのような環境変化に対応していくには、ニュースメディアや JPCERT/CC 等のセキュリティ対策組織から適宜発信されるセキュリティ関連情報を意識

[2] 2015 年版ものづくり白書（ものづくり基盤技術振興基本法第 8 条に基づく年次報告）

的に収集しつつ、サイバー脅威に対する事前対策と事後対応ができる体制を整備していくことが重要である。
当センターにおいてもセキュリティ意識の普及啓発等さらなる支援を行っていく必要があると考えており、今後もこのような調査を実施して、制御システム関係者へのセキュリティ対策に資する情報を提供していく。