2019～2020 年

制御システムセキュリティアセスメント報告書

～アセットオーナーの実態とその後の取り組み～

一般社団法人 JPCERT コーディネーションセンター

2021 年 3 月 23 日

JPCERT CC®

目次

1. はじめに 3
2. JPCERT/CC が実施した制御システムセキュリティアセスメントサービスの概要 4
3. 2019～2020 年における制御システムセキュリティアセスメントサービスの実施概要 6
4. 2019～2020 年における制御システムセキュリティアセスメントサービスの実施結果 7
4.1. 実施した各組織の得点率 7
4.2. 実施結果を踏まえた各組織の対策状況 10
4.2.1. 各組織の対策状況①：リスク管理と統制 10
4.2.2. 各組織の対策状況②：ネットワーク対策と監視 12
4.2.3. 各組織の対策状況③：ホストセキュリティとアクセス制御 13
4.2.4. 各組織の対策状況④：物理セキュリティ 15
4.2.5. 各組織の対策状況⑤：サプライチェーンマネージメント 16
5. 制御システムセキュリティアセスメントサービス実施後のフォローアップ調査 18
5.1. アセスメント実施後の各組織の意識の変化 18
5.2. アセスメント実施後の各組織の取り組み 18
5.3. アセスメント実施後の各組織の課題 20
6. おわりに 21
7. 謝辞 21

1. はじめに

一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）では、日本国内の制御システムにおけるセキュリティ対策状況の把握と今後の支援策検討を目的として、制御システムセキュリティアセスメントサービス（以下、本アセスメント）のトライアルを実施してきた。本報告書は、製造業を中心とする国内 6 組織に実施した本アセスメントをとおしてわかった各組織の対策状況と本アセスメントの実施から半年以上経過した後に実施したフォローアップ調査を通じてわかった各組織の取り組み状況、課題などについてまとめたものである。国内のアセットオーナーを読者として想定して、アセスメント実施の有効性に関する認知度を向上していただくとともに、本報告書の内容を読者の自組織での対策状況や取り組みと比較することで自組織における対策の改善に役立てていただくことを目的としている。

本報告書の構成は、1 章（本章）で本報告書の趣旨と目的を示し、2 章で JPCERT/CC が実施した本アセスメントの概要をまとめている。3 章で本アセスメントの実施概要について説明し、4 章で本アセスメントの実施結果をまとめている。そして、5 章で本アセスメント実施から半年以上経過した後に実施したフォローアップを通じてわかった各組織の取り組み状況や課題についてまとめ、6 章で全体を総括する。

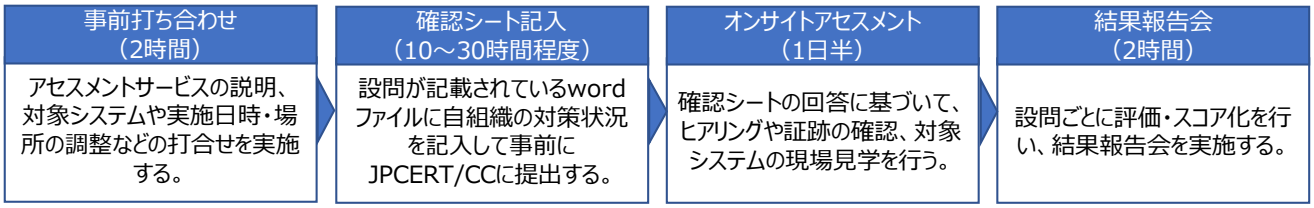
2. JPCERT/CC が実施した制御システムセキュリティアセスメントサービスの概要

本アセスメントは、アセスメントから得られた知見を匿名化した上で公に活用することを了承した組織に対して無料で実施した。本アセスメントはベースラインアプローチの手法を採用しており、英国 CPNI が作成した SSAT（SCADA Self Assessment Tool）をベースに NIST SP800-53、NIST SP800-82 なども参考にして、JPCERT/CC が独自に作成した 22 項目 90 設問のチェック項目で構成されている。設問ごとに配点が決められており、設問で問われていることがすべてできていれば満点が、部分的にできていれば部分点が与えられる。例えば、「1.リスクと脅威の理解」の項目には 6 つの設問が用意されており、それらすべてが完全にできている場合には、合計で 70 点の得点が与えられる。そして、各項目の得点を単純に足しあわせて総合得点が算出される。各項目および設問数、配点を［表 1］に記す。

［表 1：制御システムセキュリティアセスメントの項目、設問数、配点の一覧］

カテゴリー	項目	設問数	配点
リスク管理と統制	1 リスクと脅威の理解	6	70
	2 統制	4	45
	15 変更管理	2	20
	18 意識とスキルの改善	4	30
	19 対応能力の確立	4	20
ネットワーク対策と監視	3 ネットワークアーキテクチャー	6	70
	4 ファイアウォール	10	70
	5 リモートアクセス	6	50
	6 侵入検知	3	40
	7 侵入テスト	2	20
	8 ワイヤレス	1	30
ホストセキュリティとアクセス制御	9 ウイルス対策	3	50
	10 セキュリティパッチ	6	60
	11 システム強化	1	30
	14 接続手順	1	40
	12 パスワードとアカウント	6	30
	13 転入・転出の管理	2	20
	16 バックアップ	2	50
物理セキュリティ	17 物理セキュリティ	6	35
サプライチェーンマネージメント	20 外部委託先管理	10	30
	21 プロジェクト参画	3	20
	22 調達	2	20
	合計	90	850

アセスメント結果が報告書として受審組織に提供される。報告書には、設問ごとの評価や項目ごと評価が記載されている。そのため、セキュリティ対策がどこまでできているかの現状を項目ごとに把握し、さらなるセキュリティ対策を実施する上でどのような対策から始めるかといった方向性を検討するための参考として活用できる。本アセスメントの流れを［図 1］に示す。



［図 1：JPCERT/CC が実施した制御システムセキュリティアセスメントサービスの流れ］

3. 2019～2020 年における制御システムセキュリティアセスメントサービスの実施概要

2019～2020 年に、製造業を中心とする国内 6 組織に対して、本アセスメントを実施した。実施したアセスメントの期間や方法および対象組織の概要を［表 2］に示す。

［表 2：アセスメントおよび対象組織の概要］

サービス名	制御システムセキュリティアセスメントサービス(トライアル)	
実施期間	2019 年 3 月～2020 年 3 月	
方法	・組織に事前に確認シートへの回答依頼 ・組織が回答済みの確認シートの内容確認 ・確認シートに基づく対面によるヒアリングおよび現場確認	
組織概要	対象組織	規模
	A 社	30,000 人 ～ 50,000 人未満
	B 社	10,000 人 ～ 30,000 人未満
	C 社	1,000 人 ～ 3,000 人未満
	D 社	50,000 人 ～ 100,000 人未満
	E 社	30,000 人 ～ 50,000 人未満
	F 社	50,000 人 ～ 100,000 人未満

本アセスメントの実施にあたっては、より適切な評価を行えるように、評価対象システムに関係する IT 部門および OT 部門の担当者にご参加いただいた。

いずれの組織も複数の制御システムを運用しているがアセスメント対象は組織が指定した 1 システムのみであり、組織ごとに対象システムの特性や構築時期等の違いがあることに留意されたい。なお、アセスメント対象組織が 6 組織のみであることから、4 および 5 章における「ほとんどの組織」とは 5～6 組織を、「複数組織」とは 3～4 組織を、「一部組織」とは 1～2 組織を表している。

4. 2019～2020 年における制御システムセキュリティアセスメントサービスの実施結果

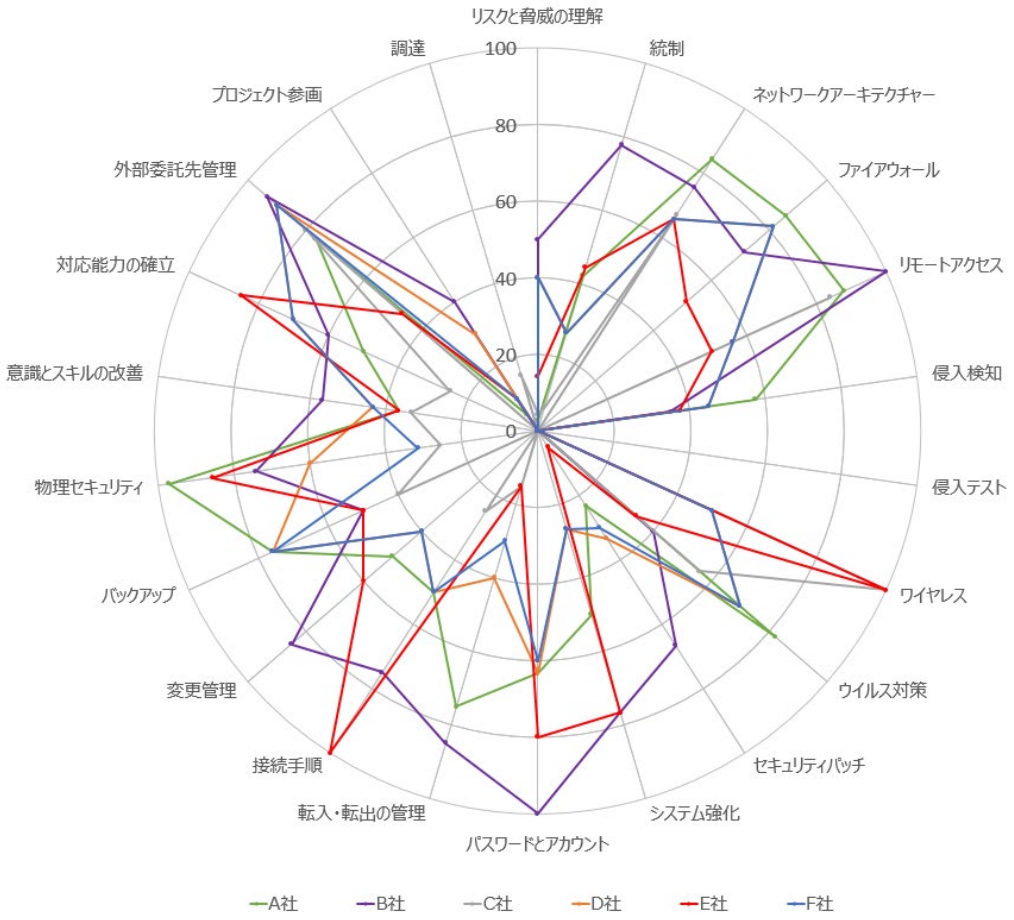
4.1. 実施した各組織の得点率

本アセスメントでは、［表 1］に示したような 22 の項目にカテゴライズされた 90 の設問の一つ一つについて、各組織の対策状況を点数で評価する。そして、関連する設問に対する点数を合計して項目ごとの得点としている。項目ごとに満点が異なるので、項目間を比較して論じる本節では、得点を満点に対する百分率で表現したものを導入し、それを得点率と呼ぶことにする。本アセスメントを実施した 6 組織の項目ごとの得点率と 6 組織の得点率の平均値を［表 3］に示す。［表 3］では、項目ごとの得点率が 100%ならば青、0%ならば赤で表示し、中間値については得点率に応じて濃淡をつけている。

［表 3：本アセスメントを実施した組織の項目ごとの得点率］

カテゴリー	項目	A 社	B 社	C 社	D 社	E 社	F 社	平均値
リスク管理と統制	1 リスクと脅威の理解	3%	50%	4%	40%	14%	40%	**25%**
	2 統制	42%	78%	7%	27%	44%	27%	**37%**
	15 変更管理	50%	85%	0%	40%	60%	40%	**46%**
	18 意識とスキルの改善	37%	57%	33%	43%	37%	43%	**42%**
	19 対応能力の確立	50%	60%	25%	70%	85%	70%	**60%**
ネットワーク対策と監視	3 ネットワークアーキテクチャー	84%	76%	67%	66%	66%	66%	**71%**
	4 ファイアウォール	86%	71%	0%	81%	51%	81%	**62%**
	5 リモートアクセス	88%	100%	84%	56%	50%	56%	**72%**
	6 侵入検知	58%	35%	0%	45%	38%	45%	**37%**
	7 侵入テスト	0%	0%	0%	0%	0%	0%	**0%**
	8 ワイヤレス	0%	0%	100%	50%	100%	50%	**50%**
ホストセキュリティとアクセス制御	9 ウイルス対策	82%	40%	56%	70%	34%	70%	**59%**
	10 セキュリティパッチ	23%	67%	0%	33%	5%	30%	**26%**
	11 システム強化	50%	77%	0%	27%	77%	27%	**43%**
	14 接続手順	50%	75%	25%	50%	100%	50%	**58%**
	12 パスワードとアカウント	63%	100%	0%	63%	80%	60%	**61%**
	13 転入・転出の管理	75%	85%	15%	40%	15%	30%	**43%**
	16 バックアップ	76%	50%	40%	76%	50%	76%	**61%**
物理セキュリティ	17 物理セキュリティ	97%	74%	26%	60%	86%	31%	**62%**
サプライチェーンマネージメント	20 外部委託先管理	77%	93%	80%	90%	47%	90%	**79%**
	21 プロジェクト参画	5%	40%	0%	30%	10%	10%	**16%**
	22 調達	0%	0%	15%	0%	0%	0%	**3%**
	全項目の平均値	**54%**	**62%**	**28%**	**52%**	**47%**	**50%**	**49%**

あわせて、［表 3］の各組織の項目ごとの得点率を［図 2］のレーダーチャートに示す。



［図 2：各組織の項目ごとの得点率のレーダーチャート］

本アセスメント結果によれば、「1 リスクと脅威の理解」「2 統制」「6 侵入検知」「7 侵入テスト」「10 セキュリティパッチ」「21 プロジェクト参画」「22 調達」の 7 項目で 6 組織の平均値が低かった（40%以下）。ちなみに、全項目について平均した得点率では、多くの組織が 50%前後の水準にある。また、「8 ワイヤレス」については、ワイヤレス技術を使っていない場合には対策が不要なので無条件に満点としている。

4.2. 実施結果を踏まえた各組織の対策状況

本アセスメントを実施した組織の項目ごとの得点率（表 3）を踏まえ、カテゴリーごとの各組織のセキュリティ対策状況について特筆すべき事項を次に述べる。

4.2.1. 各組織の対策状況①：リスク管理と統制

4.2.1.1. 制御システムの棚卸管理がなされてはいたが、セキュリティ対策に必要な情報が欠けていた

ほとんどの組織において制御システムを構成する資産を一覧できるように管理されていたが、管理の粒度は組織ごとにばらつきがあり、資産の減価償却の算定ができるように設備単位では把握していても設備に組み込まれている PLC やフィールド機器（センサーやアクチュエーター）まで把握できていない組織があった。また、設備に組み込まれているコンポーネント機器も含めて一覧化していても機器の OS やソフトウェアの種類・バージョンまでは把握していない組織などが見受けられた。さらに、ほとんどの組織において定期的な棚卸ができていない状況であった。対象システムの現場確認では、セキュリティ担当者だけでなく現場の運用者も把握していないテストサーバー等の機器が、ネットワークから切り離されているものの廃棄されずに工場内に放置されていた事例もあった。

棚卸管理において情報不足となっている背景として、情報システムと異なりネットワーク負荷などによる制御システムの可用性への影響が懸念されるため資産管理ツールの導入が難しいこと、設備単位で調達しコンポーネント機器の詳細情報を入手していないこと、セキュリティ管理に棚卸管理の情報を利用するという認識が不足していることなどが挙げられる。

制御システムの構成の現状を正確に掌握するとともに構成内容の変更の都度、構成情報を更新することがセキュリティ対策の第一歩である。資産を把握できていない場合、新たに公表された脆弱性への対応に漏れが生じたり、インシデント発生時に迅速に状況が把握できなかったりする恐れがある。

4.2.1.2. 自組織のインシデントで過去に顕在化した脅威のみについてリスク分析に終始していた

制御システムによって実現されている自組織の事業へのサイバー脅威に関するリスク分析を網羅的に行っている組織は無かった。リスク分析をする上で前提となる脅威の特定が、USB メモリ経由でのマルウェア感染や不正アクセスによるネットワーク機器の侵害など、実際に自組織のインシデントで過去に顕在化した脅威に基づいたリスク分析に終始していて網羅性が不十分であった。また、社内ネットワークに対する完全な信頼を置いて、社内ネットワーク経由の通信についてサイバー脅威を考慮せず、物理的な脅威しか想定していないといった組織が見受けられた。

脅威の特定が網羅的になされていない背景として、リスク分析の手法が組織内で確立されていないことが挙げられる。

自組織の事業へのサイバー脅威に関するリスク分析が網羅的でない場合、本来実施すべき対策に漏れが生じる恐れがある。また、対策の優先度付けが適切になされず、過剰な対策が行われたり、つぎはぎに対策が行われたりすることにより、対策コストが積みあがる恐れがある。さらには、自組織で経験していない新たなインシデントが発生した場合に対処が遅れる恐れがある。

4.2.1.3. 事業法による規制の有無によって制御システムの変更管理に差が生じていた

一部組織において、制御システムを構成する機器の変更管理を行う際の手順が定められておらず属人的に変更管理が行われていた。また、複数組織においては簡単な作業手順書のみで済ませていた。例外的に一部組織では厳格な変更管理が行われており、対策レベルの二極化が見られた。

対策レベルの二極化が見られる背景として、関連する規定を含む事業法の存在がある。一部の業界では、製品の安全性や品質の維持に関する規制を含む事業法が適用されており、機器の構成変更や、機器の OS・ソフトウェアのバージョンや設定の変更について厳格な管理が要求されている。一方、変更管理が不十分であった組織においては、設備の稼働率や製品の品質の改善の一環として機器の構成を頻繁に変更していて変更管理を行う工数が割けない、機器の構成をほとんど変更することがないため手順書を設けていない等の実状が見られた。

厳格な変更管理が行われていないと、制御システムを構成する機器やソフトウェア、ネットワーク構成を変更したことが原因で問題が生じても、変更がなされていたことが共有された認識とならず、原因特定が困難になる恐れがある。また、変更にあたってセキュリティへの影響が考慮されず、変更によって発生するセキュリティ上の脅威への対応に漏れが生じる恐れがある。

4.2.1.4. IT 部門と OT 部門との連携は進んでいたが、制御システムのセキュリティに関する責任の所在が定められていなかった

連携の度合いは組織ごとに異なるものの、ほとんどの組織において IT 部門と OT 部門とが連携できる状況になっていた。具体的には、オフィスネットワークに繋がっている製造現場の一部機器（ネットワーク機器等）を IT 部門が管轄している関係で OT 部門が保有する機器の利用に関して OT 部門が IT 部門に相談できる状況にある組織や、生産データの活用に向けて社内システムと生産システムの連携の検討を行うために協力している組織があった。また、工場も含め組織全体として統制を取るために現場の実態に沿った工場セキュリティガイドラインを連携して策定している組織などがあった。このように IT 部門と OT 部門の連携が進んでいるものの、複数組織において制御システムのセキュリティを受け持つ責任者を配置していない、または明確にしていないケースがほとんどだった。

制御システムセキュリティに対する責任者が明確になっていない場合、対策に不備が生じたり、インシデント対応遅れにつながったりする恐れがある。

4.2.2. 各組織の対策状況②：ネットワーク対策と監視

4.2.2.1. 制御システムのネットワーク構成が変わってもネットワーク構成図が更新されていなかった

ほとんどの組織において、構築した当初にベンダーからアセスメントの対象システムのネットワーク構成図を入手していたが、その後にネットワーク構成が変わってもネットワーク構成図を更新している組織は一部に留まっていた。

ネットワーク構成図が更新されていない背景としては、制御システムのネットワーク構成図を更新するための工数が不足していることなどが挙げられる。

制御システムを構成する資産の管理と同様に、制御システムのネットワーク構成や他システムとの接続状況の把握はセキュリティ対策の基礎となる。ネットワーク構成図が最新の状態になっていない場合、インシデント発生時にタイムリーな影響範囲の把握に手間取る恐れがある。

4.2.2.2. 制御ネットワークとオフィスネットワークの間にファイアウォール等が設置されていたが、その間の通信制限が十分でない

ほとんどの組織において、制御ネットワークとオフィスネットワークの間に、ファイアウォールや UTM、ファイアウォール機能を有するルーターを設置していた。これらを用いて、一部組織では社内ポリシーに基づいて業務上で必要最低限の通信に制限されていた。一方、ほとんどの組織においては、 IP アドレスまたはポートのいずれかしか特定していないなど、通過させる通信の絞り込みが甘かった。また、複数組織においては、ファイアウォール等の設定が機器の設置当初のままの状態になっており、ネットワーク構成の変更時などに設定の見直しを行っていなかった。中には、制御ネットワークとオフィスネットワークの分離がされておらず、重要なシステムとその他システムとのセグメントの分離もできていない組織があった。なお、本アセスメントでは制御ネットワークとオフィスネットワーク間の分離の一手段として DMZ 構築を確認しているが、アセスメント対象組織では制御ネットワークとオフィスネットワーク間に DMZ を構築している組織はなかった。

制御ネットワークと他ネットワークを分離が不十分な場合、他ネットワークで発生したセキュリティインシデントが波及して制御ネットワークにまで影響を受ける恐れがある。

4.2.2.3. 外からのリモート接続を許可している組織においてセキュリティ対策が不十分なケースが見られた

一部組織において、社外から外部委託業者による制御システムへの直接のリモート接続を許可していた。また、一部組織ではオフィスネットワーク経由でのリモートアクセスを許可していた。外部委託業者からのリモートアクセスを許可している組織では、事前に業務上の必要性を確認して承認する手続きや二要素認証を取り入れるなど一定のセキュリティ対策を講じていたが、リモートアクセスに関する手順の文書化

がされていなかった。また、リモートアクセス端末環境のセキュリティ対策は、外部委託先が行う対策に依存しており把握ができていなかった。

リモートアクセス端末環境のセキュリティ対策を把握していなかった背景としては、リモートアクセスに使用するシステムの導入やそのセキュリティ対策を含めて SIer に任せていたことが挙げられる。

リモートアクセスの対策が不十分な場合、リモートアクセスの経路が攻撃の入口となる恐れがあり、セキュリティ対策が不十分な端末へのリモートアクセスを経由してマルウェアに感染する恐れがある。今後、新型コロナウイルス感染症（COVID-19）の影響等で、リモートアクセスをせざるを得ない環境も想定されるため、外部委託業者と契約する段階からリモートアクセスに関するセキュリティ要件を明示し、対策を講じる必要がある。

なお、本アセスメントは、新型コロナウイルス感染症（COVID-19）流行前に実施しており、その後に導入された可能性がある同感染症への対策に伴う制御システムセキュリティへの影響を含んではいない。

4.2.2.4. 導入した侵入検知が有効に活用されておらず、検知時の対応手順が整備されていなかった

ほとんどの組織において、侵入検知の仕組みを導入していなかった。一方、侵入検知の仕組みを導入している一部組織においては、IDS の機能でログを記録していたものの、ログを確認しておらず異常を検知できない状況で、せっかく導入した侵入検知の仕組みが有効に活用されていなかった。また、制御システムにおけるセキュリティの異常検知時の対応手順がほとんどの組織で整備されておらず、制御システムではセキュリティインシデントが発生したことがないため、インシデント対応フローを定義していない、安全と環境に関する手順はあり毎年見直しも訓練も行っているがセキュリティに特化したものがない、経験則だけに頼って文書化されていないため対応手順が属人化しているなど、各組織の状況が伺えた。

侵入検知の仕組みが導入されていない場合、インシデントの兆候を見逃し、異常に気付かないまま重大な事態に繋がる恐れがある。また、対応手順がないことで、誤った対応や措置によって二次的な被害や事故に繋がる恐れがある。

4.2.3. 各組織の対策状況③：ホストセキュリティとアクセス制御

4.2.3.1. 制御システムへのウイルス対策ソフトの導入およびパッチ適用が困難なため代替策を講じていた

ほとんどの組織において、オフィスネットワークに接続されている機器に関してはウイルス対策ソフトの導入およびパッチ適用が実施されていた。一方で、オフィスネットワークに接続されていない制御ネットワーク上の機器に対しては実施されていなかった。

ウイルス対策ソフトの導入やパッチ適用が実施されていない背景として、ウイルス対策ソフトの導入が機

器の動作に影響を及ぼす等の可能性があるため容易に導入できないといった声があった。ウイルス対策ソフトの導入やパッチ適用をしないことでウイルス感染のリスクが高まるが、代替策として、ネットワーク機器上でのウイルスチェックや通信制限を行うなど、制御ネットワークと接する境界防御を実施している組織が見受けられた。

制御システムへのパッチ適用をしていない場合、パッチ未適用のシステムの脆弱性を突かれて被害を受ける可能性がある。上述の境界防御の代替策を講じていたとしても、USB 等を経由してマルウェア感染させられるなど、代替策では対応できない攻撃を受ける可能性がある。また、パッチの適用が適切な手順で行われない場合、作業時にマルウェアに感染したり、異常を引き起こしたりする恐れがある。

4.2.3.2. 未使用のサービス、ポート番号の無効化や物理的なポートの閉塞は一部の機器に留まっていた

ほとんどの組織において、未使用のサービスやポート番号の無効化は一部の機器に留まっていた。各組織の実施状況にはばらつきが見られ、サーバーなどの制御システムに関わる情報システムについては業務上必要のないサービスやポート番号をすべて無効化している、重要と捉えているシステムのみ業務上必要のないサービスやポート番号を無効化している、初期導入時から未使用のサービスやポート番号を把握していないとさまざまだった。また、ほとんどの組織において、USB ポートや LAN ポートなどの物理的なポートの閉塞は一部の機器に留まっていた。

未使用のサービスやポート番号の無効化を行っていない場合、デフォルトで有効になっているサービス（FTP、Telnet など）やポート番号を使用した攻撃を受ける恐れがある。また、USB ポートや LAN ポートなどの物理的なポートの閉塞が不十分な場合、空いている物理的なポート対して組織で管理されていない機器を接続される恐れがある。

4.2.3.3. デフォルトパスワードから変更されていたが、アカウント管理が不十分となっていた

ほとんどの組織において、制御システムを工場出荷時の設定されているデフォルトパスワードから変更していたが、一部組織ではシステムの納入業者にパスワード設定を任せているため、変更されているかを把握していなかった。また、アカウント管理について、一部組織においては操作端末のアカウントの ID と権限が適切に付与されていたが、ほとんどの組織においてはアカウントに付与されている権限の更新がされていないなど管理が不十分だった。

第三者にアカウント情報やパスワードを取得されると制御システムに不正にアクセスされ、操業データなどの重要な情報を奪取されたり、制御装置のプログラムコードやパラメーターを変更されたりするなどの恐れがある。

4.2.3.4. バックアップは取得しているものの、復元テストが実施されていなかった

ほとんどの組織において、システムおよびデータのバックアップは取られているが、復元テストはされているか不明なものもあった。なお、一部組織では、トラブル対応のためにバックアップから復元しているとのことだった。

復元テストが不十分となっていた背景としては、復元テストの実施にあたって安易に停止ができない制御システムを停止させる必要があること、復元テスト実施後に制御システムが正常稼働するどうかが定かでないこと、自組織の制御システムに合わせた個別の検証環境の構築が難しいことなどが挙げられる。

昨今、ランサムウェアの被害が国内外で散見されておりバックアップの重要性が高まっているが、オンラインバックアップの場合はバックアップも暗号化されてしまい、バックアップからの復元ができなくなる恐れがある。

4.2.4. 各組織の対策状況④：物理セキュリティ

4.2.4.1. 入退室管理を実施していたものの、一部組織では関係者のみに制限していなかった

ほとんどの組織において、敷地の正門にセキュリティゲートの設置や警備員の配置を行っており、対象システムの建屋やフロアの入場の際にセキュリティカードによる制限を行っていた。また、外部の作業者等が生産エリアに入場する場合、申請が必要な仕組みになっており、外部の作業者は帽子やゲストカード等で識別可能になっていた。制御システムの操作・監視端末などの重要な機器の施錠管理については、制御盤に収納され厳格に施錠管理されている組織と、施錠管理されておらず入退室が可能な要員であれば操作が可能な状態になっている組織が見受けられた。このように入退室管理は実施している一方で、重要エリアとそうでないエリアの区分けや制限が不十分となっており、関係者以外の者に侵入される余地が残っていた。

4.2.4.2. 生産エリア入口に監視カメラを設置していたものの、生産エリア内での設置はほとんどされていなかった

ほとんどの組織において、不正侵入や盗難防止を目的に、生産エリアの入口や倉庫などに監視カメラが設置されていたが、制御システムの不正操作や入退室管理などを目的に生産エリア内に監視カメラを設置している組織は一部に留まっていた。

一定数の監視カメラは導入しているが、生産エリア内への監視カメラの設置が一部に留まっている背景として、先に予算付けや実施しないといけない対策があり優先度が下がっていることが挙げられる。

4.2.4.3. 入退室のログの取得はできていたが、ログの確認は十分でなかった

ほとんどの組織において、監視カメラやセキュリティカード等による入退室管理は行っているが、その入退室のログを確認していなかった。一部組織においては、入退室管理システムと監視カメラの両方を設置していたが、入退室管理システムと監視カメラの時刻を手動で管理しているため時刻が同期されているかは不明確なケースもあった。

入退室のログを確認していない背景として、これらのログについては何かしらの事案が発生した際の確認に使用する運用になっており、平時に確認する運用にはなっていないことが挙げられる。

入退室や監視カメラのログの確認を行っていない場合、不正侵入等を見逃してしまう可能性がある。また、時刻同期がされていない場合時刻同期のための余計な作業が必要になるなど、インシデント発生時の原因の究明や分析作業の遅れや困難に至る。なお、監視カメラのログについては、ディスクの使用量に応じて古いものから上書きされてしまう点を留意する必要がある。

4.2.5. 各組織の対策状況⑤：サプライチェーンマネージメント

4.2.5.1. 外部委託先との契約において秘密保持義務は含まれていたがセキュリティ関わる要件が十分でなかった

外部委託業者に運用やメンテナンス等を委託している場合、ほとんどの組織において秘密保持契約は締結しているが、セキュリティ要件（例えば、機密情報やアカウントの取り扱い、システムのインシデント発生時の対応連絡先、新たな脆弱性等が顕在化した場合の情報共有や対応など）については契約を取り交わしていなかった。また、外部委託業者との契約の中で、インシデント発生時の責任範囲が明確になっていなかった。

外部委託先へ要求するセキュリティ要件が不十分となっている背景として、契約関連文書のひな型にセキュリティ要件や責任範囲に関する事項が含まれていないこと、外部委託業者のセキュリティに関する専門知識やスキルの不足により調整に時間がかかることなどが考えられる。

外部委託先に対してセキュリティ要件の要求が不十分である場合、そこが抜け穴となってしまい、外部委託先による過失によってインシデントが発生する恐れがある。また、責任範囲を明確にしていないことにより、アセットオーナー側が社会的責任を問われる恐れがある。

4.2.5.2. 自組織が所有する機器の脆弱性情報をベンダーから入手していない

自組織が所有する機器に関する脆弱性情報等のセキュリティ情報を得るには、ベンダーからの情報提供が効率的だと思われるが、ほとんどの組織においてベンダーから脆弱性情報等を入手していなかった。

脆弱性情報等をベンダーから入手していない背景として、設備機器の調達時に締結する保守契約に脆弱性情報の提供に関する要件が含まれていないことなどが挙げられる。

仮に設備構築時に最新のパッチをあてていたとしても、時間の経過とともに新たな脆弱性が追加的に発見されることがあるため、それらの脆弱性を突いた攻撃を受ける恐れがある。

4.2.5.3. 外部委託先によって持ち込まれた USB メモリの取り扱いルールが存在していた

ほとんどの組織において、外部委託先によって持ち込まれた USB メモリの取り扱いに関するルールが存在しており、USB メモリの使用を禁止している組織や、制御ネットワーク内の機器に USB メモリを接続する場合は事前に専用 PC でウイルスチェックを行っている組織などが見受けられた。一方、外部委託先によって持ち込まれた PC を生産設備に接続している一部組織においては、生産設備への接続にあたって最新パッチをあてているかどうかをベンダーに口頭で確認する程度に留まっていた。

USB メモリの取り扱いに関するルールが存在している背景として、自組織において USB メモリ経由でのマルウェア感染の経験があること、他組織において USB メモリ経由でのマルウェア感染により生産ラインの停止に至った事例を他人事にしなかったことが挙げられる。また、持ち込まれた PC の安全性の確認が口頭での確認に留まっている背景として、ベンダーを信頼していることが挙げられる。

外部委託先によって持ち込まれた USB メモリや PC について、安全性のチェックを行わずに制御システムに接続してしまうと、それらを経由して制御システムがマルウェアに感染し、設備の動作遅延による不良製品の製造や生産ラインの停止に至る恐れがある。

5. 制御システムセキュリティアセスメントサービス実施後のフォローアップ調査

本章では、本アセスメントの実施から半年以上経過した後に実施したフォローアップ調査を通じてわかった各組織の取り組み状況、課題などを述べる。

5.1. アセスメント実施後の各組織の意識の変化

アセスメントの受審後に各組織で見られた意識の変化は次のとおりである。

5.1.1. 経営陣における制御システムセキュリティの重要性の認識が向上した

工場のセキュリティについて OT 部門が担うべきか、IT 部門が担うべきか曖昧な状態であったが、本アセスメントの個社ごとの報告書に記載されている自組織の対策状況やリスクを経営層に説明したことで体制の整備が進んだといった回答や、従来から情報セキュリティへの関心は高かったが制御システムのセキュリティ対策の必要性の理解につながった、今後も制御システムのセキュリティ対策を推進していくことになったといった回答がフォローアップで得られ、制御システムに対するセキュリティの重要性が経営層をはじめ社内でより認識されるようになったことが複数組織で確認された。

5.1.2. 認識の差異の発見や問題点が可視化され、IT 部門と OT 部門の情報連携が向上した

本アセスメントを受審したことで、制御システムに必要とされるセキュリティ要件を網羅的・俯瞰的に知ることができ、他のアセスメント対象組織と自組織の対策状況を比べて対策レベルが認識できたといった声があった。また、本アセスメントの設問への回答等に取り組むため、評価対象の制御システムのセキュリティに関連する IT 部門と生 OT 部門が頻繁に連絡しあうこととなり、結果的に制御システムセキュリティに関して協力体制ができたと回答した組織もあった。また、本アセスメントに参加していた関係部門で制御システムセキュリティの意識向上に役立ったといった声や、OT 部門もセキュリティ対策に協力的になっているといった声があった。

5.2. アセスメント実施後の各組織の取り組み

本アセスメント実施後のフォローアップを通じてわかった各組織の取り組みついては次のとおりである。

5.2.1. JPCERT/CC のアセスメントをきっかけとして別拠点の対策状況やリスクの把握に取り組んでいる

本アセスメントの評価対象は 1 システムであったものの、その対策状況が可視化されたことをきっかけに、さらに別拠点のシステムに対してセキュリティベンダーが提供するアセスメントサービスを活用して重要なシステムの対策状況やリスクの把握につとめた組織があった。同組織では、IEC 62443 シリーズや

IPA の制御システムセキュリティリスク分析ガイドをベースに、ネットワークの構成や機器の設定などについて詳細な評価を行っていた。また、他の組織では、本アセスメントの評価項目や評価結果、ならびに業界のガイドライン等を参考にセルフアセスメントの策定を行っていた。同セルフアセスメントの実施においては、海外の工場も含めた全社横断的な実施を計画しているとの話を伺うことができた。

5.2.2. 自組織での制御システムに関するポリシーやガイドラインの策定とその社内教育など、予算が無くてもできる対策から取り組んでいる

本アセスメントでの指摘も踏まえて、工場のセキュリティガイドラインの策定を進めている組織が複数で見受けられた。ガイドラインの策定にあたっては、理想的なルールを検討した後に、現場の担当者にヒアリングしながら、工場の可用性に配慮した実施可能なルールの策定に取り組んでいる組織、外部委託業者が持ち込んだ USB メモリや PC などを接続する際の手順の明確化など自組織でリスクが高いと思われるものからルール化に取り組んでいる組織があった。また、OT 部門の担当者向けのセキュリティ教育を実施し、工場ごとにマルウェア検出件数や、数時間生産が止まった事例などを紹介して認識向上に取り組んでいる組織や、朝礼のような場を使って USB メモリ等の外部記憶媒体の取り扱いや、アカウントの共有、パスワードの使いまわしの防止など基礎的なセキュリティ教育をはじめている組織があった。その他にも、対策が進んでいる組織では制御システムのセキュリティ担当者が制御システムのセキュリティ対策を進める上で必要な知識やノウハウを習得するための専門教育を受講し、人材育成に取り組んでいる組織もあった。以前は現場判断でアクセスポイントの追加などがされていたが、現場部門へのセキュリティルールが浸透してきたことで、機器の追加等でも IT 部門へセキュリティの相談がくるようになったといった組織もあった。その他、LAN ポートや USB ポートを塞ぐ物理対策が一気に進んだという組織もあった。

5.2.3. 多層防御に向けた対策に取り組んでいる

本アセスメントにおいて制御ネットワークのセグメント化が不十分と評価された組織では、ネットワークのセグメント化は構築時に行う必要があることに気付いたため、新たにネットワークを構築する際には棟単位や設備単位でセグメント化を行うとのことだった。また、本アセスメント実施後に、他拠点のシステムの対策状況を確認したところ、一部の制御装置や計測機器がオフィスネットワークに繋がっていることが発覚した組織があり、ネットワークの分離に取り組んでいた。本アセスメントをとおして、資産の所在やネットワークの接続状況の把握が不十分であることが明らかになった組織（4.2.1 章参照）においては、ネットワーク上で行われる通信をミラーポートから採取し、その通信内容から接続されている機器およびネットワーク構成を可視化するツールの導入検討を進めていた。その他にも、生産のパフォーマンスに影響しないような実験装置などの端末は EDR の導入の検討を進めている組織や、制御ネットワークとオフィスネットワークの間にある IPS で通信をモニタリングしているといった組織があった。このように多層防御に向けた対策に取り組んでいることがわかった。

5.3. アセスメント実施後の各組織の課題

本アセスメント実施後のフォローアップを通じてわかった各組織の課題ついては次のとおりである。

5.3.1. 新設工場は可能だが、既設工場への後付けのセキュリティ実装に苦慮している

既設工場に対するネットワークのセグメント化やエンドポイント対策などによる補強の実施については、セキュリティ実装をすることで設備のパフォーマンスに影響する可能性があるため容易に実施できないといった声や、制御システムのシステム変更を行う場合は事業法による規制で再検証の必要性があり、膨大な工数が発生するために困難といった声があった。

5.3.2. 工場ごとの運用実態が異なるため、一律なルールの策定が容易ではない

工場ごとにさまざまな生産体制があり、使用している機器や運用の仕組みなどが異なることから、標準的なルール化が困難といった声があった。それを克服するための戦略として、まずは全社的な制御システムセキュリティの方針を決め、実際に現場の方が遵守する個別具体的なルールはその方針に沿って現場単位で決めていくといった進め方に関するアイデアなどがあった。

5.3.3. 人材確保がされていないため、制御システムセキュリティ対策は後回しになっている

本アセスメントを実施したすべての組織では、その結果を踏まえて対策を進めることが重要であると認識しているものの、一部組織では人材不足により制御システムのセキュリティ対策を優先的に実施できない現状があることも分かった。

6. おわりに

JPCERT/CC が 2019～2020 年に実施した制御システムセキュリティアセスメントサービスのトライアルについて、各組織の結果とその後の取り組みや課題を報告書としてまとめた。本アセスメントを実施した結果、多くの組織で対策状況が可視化されて、その後の制御システムのセキュリティ対策への取り組みに繋がっており、アセスメント実施の有効性が認められた。これから制御システムのセキュリティ対策に取り組む組織においては、本報告書に記載されている各組織の対策状況やアセスメント実施後の取り組みを参考に、制御システムのセキュリティ対策を実施いただけると幸いである。また、すでに制御システムのセキュリティ対策に取り組んでいる組織においては、自組織の対策状況と比較して改善の参考とするベンチマーキング資料として活用いただければ幸いである。なお、制御システムのセキュリティ対策に参考となる標準やガイドラインとして ISA/IEC62443 シリーズや NIST SP800-82 がある。また、JPCERT/CC においても制御システムのセキュリティ対策に資する各種ガイドや自己評価ツール、情報発信サービスなどを提供している。これらを自組織の運用に沿った対策に活用いただきたい。

7. 謝辞

最後に、本アセスメントおよびその後の取り組みに関するヒアリングにご協力いただいた組織の皆さまに感謝を申し上げます。