経済産業省

資料3

「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」に対する意見募集で頂いたご意見への対応について

経済産業省

サイバーセキュリティ課

産業機械課

パブリックコメントの状況と対応

- 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」について、パブリックコメントを実施し、日本語版・英語版合わせ、216件の御意見を受領。
- 頂いた御意見を踏まえ、ガイドラインの目的や考え方・対策ステップ等記載の充実や、わかりやすさの観点から、ガイドライン案の修正を行った。

パブリックコメントの状況

	「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」	「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」英訳版
期間	2022年4月27日（水）～　2022年6月30日（木）	2022年6月1日（水）～　2022年6月30日（木）
意見数	205件（30者）	11件（2者）

対応の考え方

類型	内容
A	● ガイドラインの目的や考え方、必要性に関するもの ● 対策例の強度や内容に関するもの ● 対策ステップの考え方や内容に関するもの
B	● 表現の見直しや記述の追加など、わかりやすさを高めたもの
C	● 用語の統一や体裁に関わるもの ● セキュリティ政策や工場セキュリティ、国の取組全般に関わるもの ● その他

パブリックコメントで頂いた主な御意見

① ガイドラインの必要性
② 経営層とのコミュニケーション
③ 想定工場におけるインターネット接続やクラウド利用の考慮
④ 想定工場のモデル化
⑤ ゾーンの設定目的／定義
⑥ 各ステップの実施事項
⑦ 脅威と影響
⑧ 残存リスクへの対応
⑨ システム構成面でのセキュリティ対策
⑩ 運用面でのセキュリティ対策
⑪ 情報共有
⑫ チェックリストの記載項目

主な御意見とそれに対する考え方①：ガイドラインの必要性

いただいた御意見

- **ガイドラインの必要性**に関する御意見。
  - インターネットに接続していなければセキュリティ対策は不要との誤認識を与えないような表現にすべき。【No.34】
  - 自社は攻撃を受けないという人に、等しく攻撃を受ける注意喚起をした方がよい。【No.67】
  - 攻撃者の動機を理解したうえでガイドラインを読んだ方がインパクトがある。【No.97】
  - 工場DXが推進されることによるクラウドやサプライチェーンに関するセキュリティ対策が必要になる点を追記してはどうか。【No.184】
  - 生産システムが攻撃し易い点を、ガイドラインの動機付けにすると良いのでは。【No.200】

御意見に対する考え方

- 工場システムは、インターネットに限らず、ネットワークに接続することでセキュリティリスクが高まる点を記載。
- 工場DXの推進によりクラウドやサプライチェーンの接続が進展している点を追記。
- 重要な情報や金銭を目的とした標的型攻撃として特定の工場が狙われる場合もあれば、たまたま攻撃した先が工場である場合もあり、いかなる工場においても、サイバー攻撃を受ける可能性があることを記載。

主な御意見とそれに対する考え方②：経営層とのコミュニケーション

いただいた御意見

- **経営層とのコミュニケーション**に関する御意見。
  - リスクは投資対効果が見えないため、意思決定機関が率先して進めることが前提。【No.73】
  - 経営層及び部門間のコミュニケーションの重要性を強く明記したほうが良い。【No.185】

御意見に対する考え方

- 主な想定読者である実務層が、経営層を始めとした意思決定を行う者と適切なコミュニケーションを行うことが重要である点を本文に記載。

主な御意見とそれに対する考え方③：想定工場におけるインターネット接続やクラウド利用の考慮

いただいた御意見

- **想定工場におけるインターネット接続やクラウド利用の考慮**に関する御意見。
  - 制御ゾーンや生産管理ゾーンから直接インターネットへ接続する経路を記載してはどうか。【No. 17】
  - 制御ゾーンの機器をリモートでメンテナンスしたり、生産性分析業務を外部クラウドで行うことも増えている。外部ネットワークとの接続も想定すべきではないか。【No.35】
  - 想定工場のシステムでクラウドに関する指針を示してほしい。【No.62】
  - 自動倉庫の遠隔保守以外は拠点内に閉じているため、インターネット接続やクラウド技術の使用も想定に加える必要はないか。【No.76】

御意見に対する考え方

- 設備系/生産情報系から直接インターネットに接続し、クラウドを利用する場合でも、本ガイドラインに示したステップに応じて対策を進めることが可能である点を追記。

主な御意見とそれに対する考え方④：想定工場のモデル化

いただいた御意見

- **想定工場のモデル化**に関する御意見。
  - 工場システムの例は、ISA95等のリファレンスに沿った図に変更するのが望ましい。【No.187】
  - 具体的な想定工場の設定と同時に、抽象的な論理モデルとしてPurdue Modelを導入したほうが良いのではないか。【No.201】

御意見に対する考え方

- 本ガイドラインでは、工場システムをモデル化して現場の業務や保護対象に当てはめリスク分析・対策を行うというアプローチではなく、現場の業務や保護対象の重要性からゾーンを設定しリスク分析・対策を行うというアプローチを提示している旨を記載。

主な御意見とそれに対する考え方⑤：ゾーンの設定目的／定義

いただいた御意見

- **ゾーンの設定目的／定義**に関する御意見。
  - ゾーンを設定する意図目的を補足したほうが良い。個社・業界の性質を踏まえ、作業の粒度を調節すればよいことが伝わることが望ましい。【No.1】
  - ゾーンは論理的な区画だけなのか、物理的な区画も含まれるのか説明すべき。【No.125】

御意見に対する考え方

- ゾーンを設定することにより、工場の機器やシステムを俯瞰的に見ることが可能となるなどの考え方を追記。
- ゾーンの定義を明確化し、同じゾーンの保護資産に対しては、同等の水準のセキュリティ対策が求められる点を記載。

主な御意見とそれに対する考え方⑥：各ステップの実施事項

いただいた御意見

- **各ステップの実施事項**に関する御意見。
  - 「計画・対策・運用体制の不断の見直し」は、「ステップ2：セキュリティ対策の立案」で実施すべき。【No.15】
  - 「ステップ3：セキュリティ対策の実行」ではステップ2の中で決められたことを実施することを記載し、実施内容をいかに従業員等に周知徹底させるか記載しては。【No.15】
  - 「ステップ4：セキュリティ対策実施の監査と評価」を追加してはどうか。【No.16】
  - 「3.2.2　体制や運用面での対策」では「（１）システム構成面での対策」、「（２）物理面での対策」しかないが、「体制面での対策」「運用面での対策」「教育面での対策」等もあるのでは。【No.14】

御意見に対する考え方

- ステップ3では、周知徹底も含め運用や不断の見直しについて求めていることから、ステップ3の名称を「（PDCAサイクルの実施）」に修正し、実施・運用状況の確認と評価について明示。
- 体制面、運用面、教育面での対策は、ステップ1-1 (1)経営目標等の整理や(3)内部要件／状況の整理において自社の状況を確認する際に、内部要件として体制や運用面等で対策が十分でない点があれば、この段階で実施することを明記。

主な御意見とそれに対する考え方⑦：脅威と影響

いただいた御意見

- **脅威と影響**に関する御意見。
  - 工場の脅威をグルーピングして記述した方がよい。（1. 管理上の脅威（ISO27001）、2. 設備への脅威（IEC62443）、3. サイバー攻撃の脅威、4. 誤検知、誤動作による動作停止の脅威、5. 災害の脅威。）【No.60】
  - 自然環境の脅威とシステム／機器の障害・故障と、セキュリティとの関連性、意図を示した方が良い。【No.93】
  - 「自然環境の脅威」に「火災」がない。その他「施設や作業環境の脅威」をまとめてはどうか。【No.13】
  - 従業員の過失に加え、保守要員（設備ベンダ）のリスクも記載するのが望ましい。【No.189】
  - 「ゾーン外からのネットワークを介した不正アクセス」については、外→内に限らず、内→外を想定した記述にすることが望ましい。【No.190】

御意見に対する考え方

- 脅威の種別を再整理。
- セキュリティ脅威への対策としてパッチの適用等を行うことにより、システム・機器の障害という別の脅威につながる場合もある点について記載。

主な御意見とそれに対する考え方⑧：残存リスクへの対応

いただいた御意見

- **残存リスクへの対応**に関する御意見。
  - ステップ 2-3 に、対策後の残存リスクに対する対策方針の策定（サイバー保険への加入等）を追加しては。【No.81】

御意見に対する考え方

- システム構成面や物理面でのセキュリティ対策後、残存するリスクに対しては、対策方針の策定（例：サイバー保険への加入、事業継続計画におけるセキュリティリスク対応の考慮　等）を行うことを記載。

主な御意見とそれに対する考え方⑨：システム構成面でのセキュリティ対策

いただいた御意見

- **システム構成面でのセキュリティ対策**に関する御意見。
  - 出口対策（インターネット出口のURLフィルタリングや通信ログ監視）に関しても記述すべき。【No.30】
  - 境界防御だけでは、ゾーン内の拡散を防げないのではないか。NDRなどの対策を例示すべき。【No.64】
  - 脆弱性対策の高「＋ソフトウェア更新」は、OSは古いままでも良いとの誤解を生むため、最低限又は中であるべき。【No.40】
  - 「パスワード(定期)変更」に加えて「複雑なパスワードの設定」を追記した方が良い。【No.6】

御意見に対する考え方

- ネットワークにおけるシステム構成面でのセキュリティ対策、機器におけるシステム構成面でのセキュリティ対策について、工場の実態を踏まえて見直し。

主な御意見とそれに対する考え方⑩：運用面でのセキュリティ対策

いただいた御意見

- **運用面でのセキュリティ対策**に関する御意見。
  - ステップ2-2に、ヒューマンエラーに関する対策を追記しては。【No.E-1】
  - パッチ管理とBCPは多層防御の重要な部分であるため、実用的な方法を追加する必要がある。【No.E-8】
  - 社員教育への注力について記載があっても良い。【No.53】

御意見に対する考え方

- 運用面でのセキュリティ対策として、ヒューマンエラー対策、パッチ管理について追記。
- 人材育成については、工場システムに関わる従業員、セキュリティ確保を職務とする従業員、機器やサービスの提供者、それぞれの立場に応じたセキュリティスキルの向上が必要である点を記載。

主な御意見とそれに対する考え方⑪：情報共有

いただいた御意見

- **情報共有**に関する御意見。
  - OT環境に適した情報収集は困難であり、業種により差がある等の課題を明記しては。【No.196】

御意見に対する考え方

- 産業機械等に関する脅威情報は、業種や対象によって入手可能な情報に差がある点を記載。
- 業界やコミュニティ等を通じて情報共有を行うことが望ましい点を記載。

主な御意見とそれに対する考え方⑫：チェックリストの記載項目

いただいた御意見

- **チェックリストの記載項目**に関する御意見。
  - 3.1節～3.2節の項目がチェックリストにあると良い。【No.173】
  - [2-8] 攻撃方法や脆弱性を特定するだけでなく、脆弱性へ対応している、緩和策を講じている等、特定後の対処を明文化すべき。【No.46】
  - [2-9] 「工場内に外部記録媒体やポータルメディアの利用・持ち込みを制限している。」は困難なので、利用可能な条件を示してはどうか。【No.176】
  - [2-10] 「工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。」について、パスワードの有効期限設定は推奨される内容か。【No.177】
  - [2-11] 「使用していない古いアカウントの削除」は「速やかに」など時間軸を入れるべき。【No.47】
  - [2-13] バックアップしたデータは、可用性の観点からシステム侵害の影響が及ばない保護された場所に格納する。【No.178】
  - [3-6] 外部からのインターネットアクセスが可能な場合、認証(2要素認証等)や接続対象機器の制限、接続可能時間の制限、ネットワーク侵入防護などの保護対策を追記すべき。　他

御意見に対する考え方

- ステップ1～2の内容を、チェックリストに反映。
- チェックリスト記載のセキュリティ対策について、工場の実態を踏まえて見直し。

参考：意見の概要と新旧の対照

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方 旧	新
ガイドラインの必要性	34	インターネットに接続していなければセキュリティ対策は不要との誤認識を与えないような表現にすべき。	・インターネットにはさらされないことを前提に設計されてきた。 ・工場等のネットワークをインターネットにつなぐ必要性や機会が増加することによる、新たなセキュリティ上のリスク源も増加している。	・インターネット等のネットワークにはさらされないことを前提に設計されてきた。 ・工場等のネットワークをインターネット等のネットワークにつなぐ必要性や機会が増加することによる、新たなセキュリティ上のリスク源も増加している。
	200	生産システムが攻撃し易い点を、ガイドラインの動機付けにすると良いのでは。		
	67	自社は攻撃を受けないという人に、等しく攻撃を受ける注意喚起をした方がよい。	＜記載なし＞	・サイバー攻撃は高度化・巧妙化しており、重要な情報や金銭を目的とした標的型攻撃として特定の工場が狙われる場合もあれば、攻撃者の意図性なくたまたま攻撃した先が工場である場合もある。 したがって、いかなる工場においても、サイバー攻撃を受ける可能性があることを認識する必要がある。
	97	攻撃者の動機を理解したうえでガイドラインを読んだ方がインパクトがある。		
	184	工場DXが推進されることによるクラウドやサプライチェーンに関するセキュリティ対策が必要になる点を追記してはどうか。	＜記載なし＞	・工場DX（デジタルトランスフォーメーション）が推進されることにより、クラウドやサプライチェーンにおいて接続された製造現場におけるセキュリティも考慮しなければならない。 一方で、このようにインターネット接続の機会に乏しいと思われる工場であっても不正侵入者等による攻撃を受ける場合もある。
経営層とのコミュニケーション	73	リスクは投資対効果が見えないため、意思決定機関が率先して進めることが前提。	（脚注） ・本ガイドラインは、【略】想定読者が経営層（CTO、CISO等）を始めとした意思決定を行う者と適切なコミュニケーションを行うことを期待する。	（本文） ・本ガイドラインは、【略】想定読者が経営層を始めとした意思決定を行う者と適切なコミュニケーションを行うことを期待する。 セキュリティの推進は経営層等、意思決定を行う者による体制の構築、及び体制を通じた組織に対する適切な指示が重要である。
	185	経営層及び部門間のコミュニケーションの重要性を強く明記したほうが良い。		

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方	
			旧	新
想定工場のモデル化	187	「図2-1 工場システムの例」は、ISA95等のリファレンスに沿った図に変更するのが望ましい。	<記載なし>	（本文） ・1.1で述べたとおり、工場といってもその分類や規模は様々であり、機器やシステムも千差万別であるため、ある抽象的なモデルから立脚し、当該モデルに現場を当てはめて具体的な対策を講じる策を立案しようとしても、現場の実態とモデルが合致しない例外が多数生じ、効果的なセキュリティ対策が立案できない可能性がある。そこで、現場感と矛盾しない効果的な対策が立案できるよう、ある抽象的なモデルから具体的な対策を立案するアプローチではなく、現場の業務から立脚し、工場の機器やシステムを大きな括りの概念として俯瞰的に捉えるためのゾーンを設定し、セキュリティ対策を立案するアプローチを提示している。
	201	具体的な想定工場の設定と同時に、抽象的な論理モデルとしてPurdue Modelを導入したほうが良いのではないか。		
想定工場におけるインターネット接続やクラウド利用の考慮	17	制御ゾーンや生産管理ゾーンから直接インターネットへ接続する経路を記載してはどうか。	<記載なし>	（脚注） ・近年、設備系ネットワークや生産情報系ネットワークから情報系ネットワークを経由することなく、直接インターネットに接続できる経路も増えている。そのような場合でも、本ガイドラインに示したステップや対策は活用可能であるため、本ガイドラインの記載に沿って対策を進めていただきたい。なお、クラウド固有のセキュリティについてはコラム4も参考に、ベンダ等と相談の上実施していただきたい。
	35	制御ゾーンの機器をリモートでメンテナンスしたり、生産性分析業務を外部クラウドで行うことも増えている。外部ネットワークとの接続も想定すべきではないか。		
	62	想定工場のシステムでクラウドに関する指針を示してほしい。		
	76	自動倉庫の遠隔保守以外は拠点内に閉じているため、インターネット接続やクラウド技術の使用も想定に加える必要はないか。		

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方	
			旧	新
各ステップの実施事項整理	15	「計画・対策・運用体制の不断の見直し」は、「ステップ2：セキュリティ対策の立案」の中で一緒に実施すべき。 「ステップ3：セキュリティ対策の実行」ではステップ2の中で決められたことを実施することを記載し、実施内容をいかに従業員等に周知徹底させるか記載しては。	・ステップ3：セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの構築 ）【3.3】 ・ステップ2で導入した物理面／システム構成面での対策に加え、ライフサイクルでの対策や、サプライチェーンを考慮した対策を実施する。	ステップ3：セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施 ） 【3.3】 ・ステップ2で導入した物理面／システム構成面での対策に加え、ライフサイクルでの対策や、サプライチェーンを考慮した対策を実施する。実施・運用状況とその効果の確認、及び評価・見直しを行う。
	16	「ステップ4：セキュリティ対策実施の監査と評価」を追加してはどうか。		
	14	「3.2.2　体制や運用面での対策」では「（１）システム構成面での対策」、「（２）物理面での対策」しかないが、「体制面での対策」「運用面での対策」「教育面での対策」等もあるのでは。	(1) 経営目標等の整理 【略】 (3) 内部要件／状況の整理 【略】 この段階で考え方を整理する。	(1) 経営目標等の整理 【略】 特に、事業継続の観点では、事業継続計画（BCP）が策定されているかが重要であるため、その内容を確認する。BCPが整備されていなければ、必要に応じて担当部署とともに策定の検討を実施する 。 (3) 内部要件／状況の整理 【略】 この段階で考え方を整理し、セキュリティ対策を推進するための体制やルール・手順等を整備し実施計画を立案するとともに、周知・教育等を実施する 。

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方 旧	新
ゾーンの設定目的／定義	1	ゾーンを設定する意図目的を補足したほうが良い。個社・業界の性質を踏まえ、作業の粒度を調節すればよいことが伝わることが望ましい。	＜記載なし＞	・ゾーンを設定することにより、工場の機器やシステムを大きな括りの概念として俯瞰的に見ることが可能となり、あるゾーン内の保護対象がサイバー攻撃を受けた際、別のゾーンへ影響が及ぶことを抑止し、被害を極小化することを検討することが可能となる。
	125	ゾーンは論理的な区画だけなのか、物理的な区画も含まれるのか説明すべき。	・ゾーンとは、共通のセキュリティレベルを持つ領域であると定義する。	・ゾーンとは、業務の内容や重要度が同等である領域と定義する。同じゾーンに存在する保護資産に対しては、同等の水準のセキュリティ対策が求められる。
脅威と影響の整理	60	工場の脅威をグルーピングして記述した方がよい。1. 管理上の脅威（ISO27001）、2. 設備への脅威（IEC62443）、3. サイバー攻撃の脅威、4. 誤検知、誤動作による動作停止の脅威、5. 災害の脅威	・表3-11　一般的な脅威と生産への影響（例） （※ 脅威種別のみ抜粋） - 不正侵入 - 設備の異常な制御や破壊 - データ盗難・漏えい - データ改ざん・破壊 - 可用性低下 - 外部への攻撃の踏み台として利用 - 自然環境の脅威 - システム/機器の障害・故障 - 従業員の過失	・表3-14　一般的な脅威と生産への影響（例） （※ 脅威種別のみ抜粋） - 機器の盗難、システム・機器に対する破壊・不正操作 - 設備の異常な制御や停止 - データ盗難・漏えい - データ改ざん・破壊 - 可用性低下 - 外部への攻撃の踏み台として利用 - システム・機器の障害・故障 - 従業員、保守要員（設備ベンダ）の過失 - 施設や作業環境の脅威 - 自然環境の脅威
	93	自然環境の脅威とシステム／機器の障害・故障と、セキュリティとの関連性、意図を示した方が良い。		
	190	「ゾーン外からのネットワークを介した不正アクセス」については、外→内に限らず、内→外を想定した記述にすることが望ましい。		
	189	従業員の過失に加え、保守要員（設備ベンダ）のリスクも記載するのが望ましい。	＜記載なし＞	（注釈） ・なお、セキュリティ脅威への対策としてパッチの適用等を行うことにより、システム・機器の障害という別の脅威につながる場合もある。セキュリティ対策実施の際には、対策による影響の把握、障害が発生した場合にも事業・生産に影響しない対策範囲・スケジュール等を考慮する必要がある。
	13	「自然環境の脅威」に「火災」がない。その他「施設や作業環境の脅威」をまとめてはどうか。		

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方	
			旧	新
残存リスクへの対応	81	ステップ 2-3 に、対策後の残存リスクに対する対策方針の策定（サイバー保険への加入等）を追加しては。	＜記載なし＞	・システム構成面や物理面の対策後、なお残存するリスクの受容に向けては、対策方針の策定（例：サイバー保険への加入、事業継続計画（BCP）におけるセキュリティリスク対応の考慮※脚注 等）を行うなどのリスク管理策を講じることが考えられる。 （※脚注）例えば、初動対応・復旧手順の策定、代替手段の手配、利害関係者とのリスクコミュニケーション、及びその実効性を確保するために訓練・演習を行うことが考えられる。（サイバー攻撃を想定した訓練については、ステップ3(1)ライフサイクルでの対策②維持・改善面の対策も参照）
ネットワークにおけるシステム構成面でのセキュリティ対策	30	出口対策（インターネット出口のURLフィルタリングや通信ログ監視）に関しても記述すべき。	・「通信監視・制御：高」 ＋異常通信遮断 （IPS）	・「通信監視・制御：高」 ＋異常通信遮断 （IPS、フィルタリング）
	64	境界防御だけでは、ゾーン内の拡散を防げないのではないか。NDRなどの対策を例示すべき。	・「通信監視・制御：中」 通信状況可視化・監視、 異常検知（IDS）	・「通信監視・制御：中」 通信状況可視化・監視（NDR）、 異常検知（IDS）
	40	脆弱性対策の高「＋ソフトウェア更新」は、OSは古いままでも良いとの誤解を生むため、最低限又は中であるべき。	・「脆弱性対策：中」 ＋脆弱性診断、侵入可否検査	・「脆弱性対策：中」 ＋脆弱性診断、侵入可否検査 ＋回避策
	6	「パスワード(定期)変更」に加えて「複雑なパスワードの設定」を追記した方が良い。	・「利用者制限：最低限」 【略】 パスワード（定期）変更	・「利用者制限：最低限」 【略】 パスワードポリシー策定 （脚注） パスワードポリシーは工場の環境により定めることが望ましい。例えば、人員の入替が頻繁に発生する場合等はパスワードの（定期）変更が有効であるが、全ての管理対象機器のパスワード変更が難しい場合等には、複雑なパスワードを設定し使用することでもよい。
機器におけるシステム構成面でのセキュリティ対策	6	「パスワード(定期)変更」に加えて「複雑なパスワードの設定」を追記した方が良い。【再掲】	・「利用者制限：最低限」 【略】 パスワード（定期）変更	・「利用者制限：最低限」 【略】 パスワードポリシー策定

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方	
			旧	新
ヒューマンエラー対策	E-1	ステップ2-2に、ヒューマンエラーに関する対策を追記しては。	＜記載なし＞	・なお、ヒューマンエラーへの対策として、セキュリティに関する業務に対する過失や疲労への対策、及びセキュリティに関するルールや意識付け・教育の不備等への対策についても考慮することが望ましい。
パッチ管理	E-8	パッチ管理とBCPは多層防御の重要な部分であるため、実用的な方法を追加する必要がある。	＜記載なし＞	＜表3-37に以下を追記＞ ・「管理対象」パッチ、「目的」パッチに関する情報の収集、適用状況の把握・管理、「運用ルール」可能な限り速やかにパッチ適用を検討し、未適用のパッチは適用計画を検討、「管理が必要な情報」 パッチに関する情報
人材育成	53	社員教育への注力について記載があっても良い。	＜記載なし＞	・工場システムに関わる従業員に対しては、サイバー攻撃のリスクや業務において必要なセキュリティ対策に関わる実施事項について理解を促すために、定期的な教育や周知を行うことが望ましい 。 ・工場システムのセキュリティ確保を職務とする従業員 に対しては、工場システムのセキュリティ確保に向けて必要な、最新のセキュリティ脅威や脆弱性、組織的・技術的に有効な対策に関する教育や、サイバー攻撃の発生時に適切に対応するためのルールや手順の理解及び模擬訓練なども有効である。 ・工場システムに関わる機器やサービスの提供者に対しては、納入される機器やサービスにおいて必要なセキュリティを理解し実装することが必要となることから、保守・運用を行うベンダには保守時に必要なセキュリティ対策について徹底するための教育が必要である。
情報共有	196	OT環境に適した情報収集は困難であり、業種により差がある等の課題を明記しては。	＜記載なし＞	・なお、工場システムにおける脅威は工場内のIT環境を中心に議論されるケースが多いが、リスクの高い産業機械や産業機械間のネットワークに関する脅威情報は国内では入手しづらいことから、業種や対象によって入手可能な情報に差があることに留意が必要である。こうした状況にあって可能な限り情報を入手・共有するためには、脅威情報や効果的な対策等、各社の対策に資する情報について、業界やコミュニティ等を通じて情報共有を行うことが望ましい。 産業機械等の脅威情報は、ベンダから入手できるよう事前に保守契約が必要である点に留意が必要。

	No.	意見の概要 ご意見の通りに対応 ご意見を参考に対応	意見に対する考え方	
			旧	新
チェックリストの記載項目	173	3.1節～3.2節の項目がチェックリストにあると良い。	＜記載なし＞	【0-1】 工場システムにおけるセキュリティ対策の検討・企画に必要な経営目標、外部要件、内部要件/状況を整理する。 【0-2】 工場システムにおける業務・保護対象の整理及び重要度の設定を行う。この結果を踏まえてゾーンを設定し、業務・保護対象を結びつけ、セキュリティ脅威との影響の整理を行う。 【0-3】 工場システムに関する内外の要件や、業務・保護対象・ゾーン等の情報の収集・整理結果に基づき、工場システムのセキュリティ対策方針を策定し、想定脅威に対する対策の対応づけを行う。