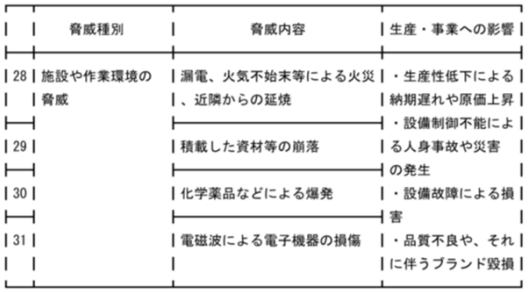
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」に対する意見募集結果の概要、及び具体的なガイドラインの修正内容

提出No.	No.	提出者	提出意見	提出意見に対する考え方
001	1	個人	■3.1.6. ステップ1-6：ゾーンの整理と、ゾーンと業務、保護対象の結びつけ ・想定読者にとって更に理解しやすくなるように、ゾーンを設定する意図目的を補足したほうが良いと考える。読み進めていくと、それは「あるゾーンにある保護対象資産の制御権を乗っ取られた際に、別のゾーンへ侵害が及ぶことを抑止し、被害を極小化するため」だと分かるが、読者の「何のために？」を解消するために一文あると良い。 上記の観点を大事にしながら、個社・業界の性質に則って作業の粒度を調節してもらえれば良いことが伝わると良いと考える。	いただいた御意見のとおり、修正いたします。 具体的には、ゾーンを設置する目的を追記いたします。 修正箇所：3.1.6.
001	2	個人	■3.1.6. ステップ1-6：ゾーンの整理と、ゾーンと業務、保護対象の結びつけ ・同じ業務を行うが、棟が分かれているなどの理由から、別LANになっている場合でも、それらを同名でゾーン設定しても良いか？（そのような状況にある場合は棟またぎでグルーピングするのが正解か？）この点について、ちょっとした注釈かコラムに追加すると、ここで疑問を持ち立ち止まってしまう読者：特に工場セキュリティを初めて検討する方も読み進められると考える。 ※少し個別具体的なケースなので、ガイドラインに反映させなくても良いかもしれませんが	いただいた御意見のとおり、修正いたします。 具体的には、ゾーンの定義・考え方を追記するとともに、棟が分かれている場合についての考え方を追記いたします。 修正箇所：2.6.
001	3	個人	■表 3-12 保護対象と関連する業務、脅威、影響の関係（例） ・（些末だが）一部文字化けしており読みづらい。	いただいた御意見のとおり、読みづらい点を修正いたします。 修正箇所：表3-12
001	4	個人	■表 3-12 保護対象と関連する業務、脅威、影響の関係（例） ・本ガイドラインではサイバーフィジカルセキュリティに焦点を当てているので、表のどの項番にも登場する「自然環境の脅威」はそれぞれ一番下に記載するで良いのでは。 -> 「表 3-21 想定脅威に対応するセキュリティ対策(例)の全体像」も同様。	いただいた御意見のとおり、修正いたします。 具体的には、表3-14、表3-15、表3-24について、「自然環境の脅威」をそれぞれ一番下の行に記載いたします。 修正箇所：表3-14、表3-15、表3-24
001	5	個人	■表 3-23 ネットワークにおけるセキュリティ対策（例） ・内部秘匿に関する対策に記載のある「ゲート機器」の定義をしたほうが良い。	いただいた御意見のとおり、修正いたします。 具体的には、表3-26に「不正通信防止（ゲートウェイ）」を追記し、表内の用語と本文の表現の整合性を取るよう修正いたします。 修正箇所：表3-26
001	6	個人	■表 3-23 ネットワークにおけるセキュリティ対策（例） ・利用者制限に関する対策で、「パスワード(定期)変更」に加えて「or 複雑なパスワードの設定」と追記したほうが良いのではないか。（複雑性については末尾注釈挿入）実態としては、有事の際を除いてすべての管理対象機器のパスワードを変更することは受け入れ難いケースが多いので、オプションとして複雑なパスワードを設定し恒久的に使用することも選択肢にあるという点、提示するのが良いと考える。付録E-1.チェックリストの2-10ではパスワード強度の言及がある。 -> 「表 3-24 機器におけるセキュリティ対策（例）」も同様。	いただいた御意見も踏まえ、修正いたします。 具体的には、表3-26、表3-27に「パスワードポリシーの策定」を記載し、「複雑なパスワード設定」が効果的な場合と「パスワード（定期）変更」が効果的な場合について追記いたします。 修正箇所：表3-26、表3-27
001	7	個人	■表 3-23 ネットワークにおけるセキュリティ対策（例） ・ログ取得に関して、最低限の対策が「ー」となっていることに違和感を感じる。ログを取得していないと、「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）」-> 運用・管理面のセキュリティ対策 -> A) サイバー攻撃の早期認識と対処 が成り立たないという懸念がある。 工場内の保護対象資産の中には、負荷がかかることや仕様に起因してログ出力できない機器があることも事実だが、 最低限：機器内ログ取得（処理負荷への影響を考慮） 中：＋IDSログ連携 高：＋ログ分析の仕組み整備 ぐらいがしっくりくる。 -> 「表 3-24 機器におけるセキュリティ対策（例）」も同様。 ※工場サブワーキンググループの皆さまで既に議論された内容であればすみません	いただいた御意見のとおり、修正いたします。 具体的には、表3-23において、「最低限」に「機器内ログ取得（処理負荷への影響を考慮）」、「中」に「＋IDSログ連携」、「高」に「＋ログ分析の仕組み整備」と修正いたします。 また、表3-24において、「最低限」に「システムログ取得（処理負荷への影響を考慮）」、「中」に「＋操作ログ取得・ログ連携」、「高」に「＋ログ分析の仕組み整備」と修正いたします。 修正箇所：表3-26、表3-27
001	8	個人	■表 3-24 機器におけるセキュリティ対策（例） ・利用ポートに関する対策に記載のある「媒体検査」「内容検査」の定義をしたほうが良い。読者にとっては馴染みの無い単語に思える。	いただいた御意見のとおり、修正いたします。 具体的には、「媒体検査」は「持込媒体の検査」、「内容検査」は「持込媒体のシステムチェック等」に修正いたします。 修正箇所：表3-27

001	9	個人	■表 3-24 機器におけるセキュリティ対策（例） ・ログ取得に関する対策では、「業務ログ」よりも「操作ログ」のほうが馴染みがある。	いただいた御意見のとおり、「業務ログ」を「操作ログ」に修正いたします。 修正箇所：表3-27
001	10	個人	総じて、多角的な視座に立ったガイドラインで、非常に読みやすかったです。 本ガイドラインで謳われている考え方を伝導する解説員が多く生まれ、セキュリティの継続的な担保がDX後押しの材料になるという文化が日本で醸成されること、結果として多くの産業で新たな付加価値が生み出されていくことを、心から願っております。	本ガイドラインに対する肯定的な御意見として承ります。
003	12	企業	・該当箇所 P24、「3.1.7. ステップ1-7：ゾーンと、セキュリティ脅威による影響の整理」の「表 3-11 一般的な脅威と生産への影響（例）」 ・意見内容 No.1-3の「脅威種別」が「不正侵入」となっている。「不正侵入」は「脅威の種別」というより、「脅威の手段」である。No.1-3はNo.4-17の「脅威種別」と見比べると以下の通りとしてはどうか。 ・理由 「不正侵入」が実施された結果の脅威として、No.4-17の「脅威種別」にも当てはまることからレベル感があっていないことが判る。 フィジカルな脅威を書きたいと思われるので、その部分を記載した。	いただいた御意見を参考に、修正いたします。 具体的には、表3-14は、不正侵入は手段であるため項目1,2の脅威種別・脅威内容・生産・事業への影響について、全面的に修正いたします。また、項目3についてはネットワークを介した不正侵入を前提としつつ、別の御意見も参考に、内部から外部への通信を含め修正いたします。 修正箇所：表3-14

	脅威種別	脅威内容	生産・事業への影響
1	機器の盗難、システム・機材に対する破壊	ゾーン内に侵入し、機器に対する直接的な破壊、盗難	・生産性低下による納期遅れや原価上昇 ・設備故障、盗難による損害
2		ゾーン内に侵入し、不正接続によるシステムやデータの破壊、盗難	
3		（欠番）	

004	13	企業	・該当箇所 P24、「3.1.7. ステップ1-7：ゾーンと、セキュリティ脅威による影響の整理」の「表 3-11 一般的な脅威と生産への影響（例）」 ・意見内容 No.18-21に「自然環境の脅威」があるが、「火災」がない。火災による被害のケースも検討する必要があるのではないか？ その他、工場の場合「積載した資材の崩落」、「化学薬品などによる爆発」、「換気不十分による窒息」等の「施設や作業環境の脅威」としてこれらをまとめてはどうか？  ・理由 フィジカルの脅威としては比較的発生頻度が高くリスクも高い「火災」が欠落しているため。「施設や作業環境の脅威」として、その他の脅威と共にまとめる。	いただいた御意見のとおり、修正いたします。 具体的には、表3-14において、脅威内容に「火災による機器・設備等の焼失」を追加いたします。また、脅威種別「施設や作業環境の脅威」として、脅威内容、生産・事業への影響を追加いたします。 修正箇所：表3-14
005	14	企業	・該当箇所 P40の枠内の対策 ・意見内容 対策に「（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、その他にも「体制面での対策」や「運用面での対策」、「教育面での対策」等もあるのでは？ （３）体制面での対策 ａ．セキュリティ対策を実施する組織体の構築 ｂ．リスクアセスメントの実施体制の構築 ｃ．監査体制の構築 etc （４）運用面での対策 ａ．セキュリティ対策の為のルール策定 ｂ．ルールのマニュアル化、手順書化 etc （５）教育面での対策 ａ．セキュリティ意識教育の実施 ｂ．工場内のルール、マニュアル、手順書等の周知徹底 ｃ．セキュリティ事故対応訓練の実施 ｄ．教育状況の監査 etc ・理由 人に対する対策が入っていなかったので追加しました。特に中小企業では予算の都合上、システムや装置、機器等に費用をかけることができないケースがありますので、人による対策も重要視されるべきです。	いただいた御意見のとおり、修正いたします。 具体的には、体制や運用面での対策は、ステップ1-1 (1)経営目標等の整理や(3)内部要件／状況の整理で自社の状況を確認しており、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いたします。 修正箇所：3.2.2　ステップ1-1(1)(3)

	脅威種別	脅威内容	生産・事業への影響
28	施設や作業環境の脅威	漏電、火気不始末等による火災、近隣からの延焼	・生産性低下による納期遅れや原価上昇 ・設備制御不能による人身事故や災害の発生
29		積載した資材等の崩落	
30		化学薬品などによる爆発	・設備故障による損害
31		電磁波による電子機器の損傷	・品質不良や、それに伴うブランド毀損

006	15	企業	・該当箇所 P54の「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）」 ・意見内容 「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である。その上で、「ステップ3：セキュリティ対策の実行」の中ではステップ2の中で決められたことを実施することを記載し、如何にして実施内容を工場の従業員等に周知徹底させるか等の啓蒙活動について記載するのが良いのではないか？ ・理由 「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）」では、「セキュリティ対策の実行」ではなく、「計画・対策・運用体制の不断の見直し（PDCAサイクルの構築）」について語られている。ので、表題と記載内容が一致していない。「計画・対策・運用体制の不断の見直し（PDCAサイクルの構築）」については、ステップ2にて対策の立案と一緒に検討するのが正しいのではないか？	いただいた御意見を踏まえ、修正いたします。 具体的には、ステップ毎の実施事項を整理し、ステップ2は「セキュリティ対策の立案」のままとしますが、ステップ3は「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）」に修正いたします。 修正箇所：3.3.　ステップ3
007	16	企業	・該当箇所 P66の「ステップ3」の続き ・意見内容 「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？ 記載内容としては以下の通り。 ステップ4：セキュリティ対策実施の監査と評価 ステップ4-1：セキュリティ対策の実施状況の監査 　ステップ2にて実施が決まったセキュリティ対策について、実施期限以降に監査を実施して実施状況とその効果を確認する。管理・運用状況については、担当者にヒアリングを行い、実施状況や効果を確認する。 ステップ4-2：監査結果の評価 　ステップ4-1にて実施した監査結果を元にして、評価を行い、実施できなかった項目を実施できるようにするための方法を検討するなど対応を行う。また実施したにもかかわらず効果が表れなかった対策については対策方法の見直しを行う。体制やルール等に問題がある場合は、体制やルール等の見直しを行う。 ・理由 ステップ3までに実施した内容について、監査や評価される場所がない。 PDCAを回すのであれば、「ステップ2」をPlan、「ステップ3」をDo、「ステップ4」をCheck, Actionとして回していくのが良いのではないかと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、ステップ3において、実施・運用状況とその効果の確認、及び評価・見直しについて追記いたします。 修正箇所：3.3.　ステップ3
008	17	企業	・該当箇所 P10の「図 2-2 ゾーンの定義例」の図の内容（※同じ絵を流用した図も同様） ・意見内容 制御ゾーンや生産管理ゾーンから直接インターネットに接続できる経路（OAゾーンを経由することなく、直接インターネットに繋がる経路）を図に記載してはどうか？ ・理由 実際問題として、制御ゾーンからセンサーネットワークに繋がるなど、インターネットに直接つながるケースは多く、工場と執務室が別の建屋になっている場合はほとんどのケースでそれぞれがインターネットに接続していて、一部の大企業の工場でなければ専用線で繋がるケースは少なく、逆に例題の図が一般的ではなくなっている。 現在発生しうる環境（制御ゾーンなどから直接インターネットに繋がる）も考慮しなければ、セキュリティのリスクが何処にあるか把握できない。 現状のままであれば、流れるデータを監視する場合、OAゾーンにセキュリティ機器を設置して監視すればよいイメージである。しかし、ゾーンそれぞれからインターネットに繋がる場合、ゾーンそれぞれに監視する仕組みが必要となる。現状の図からでは、その様なケースを抱えた工場から見た場合、そこにそのようなリスクがあることが見えてこないので、その様なケースも考慮した図の方が良いと思われる。	いただいた御意見を踏まえ、修正いたします。 具体的には、想定工場としては現状のままとし、制御ゾーンや生産管理ゾーンから直接インターネットに接続する経路の存在やその際も対策のステップは同じ進め方で問題ない点について、注釈に追記いたします。 修正箇所：2.3.

009	18	企業	・該当箇所 追加したほうが良いと思われる。付録などでも良いので、ガイドラインの中に記載して欲しいこと。 ・意見内容 工場セキュリティを考える際に、多くの工場から「古いPC」の問題を聞くので、「古いPC」が存在する場合、どの様なケースの場合、どの様な対策を実施すればよいかその指針を示す必要があると考える。例えば、以下のようなケースにて指針を記載する。 （1）バージョンアップできるが、バージョンアップしていないPCの場合 a. 今あるPCが使えているので継続して使っているケース b. 予算が無くて移行できていないケース （2）バージョンアップできないPCの対処方法 a.「バージョンアップできないPC」がネットワークに繋がっている場合 （インターネットに接続できるネットワークの場合） b.「バージョンアップできないPC」がネットワークに繋がっている場合 （閉じたネットワークの場合） c.「バージョンアップできないPC」がネットワークに繋がっていない場合 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 現在稼働している機器と接続するPCについて、稼働する為に必要となるドライバー等の接続プログラムが制限（特定のOS及び、特定のバージョンでなければ動作しない）を受けて、接続するPCがバージョンアップや機器の入れ替えなどの対応ができないケースがあり、そのまま放置することはセキュリティホールとなる可能性がある。 どの様に対処するかいくつかの方法論があるが、どの様なケースの場合、どの様な対策を実施すればよいか、多くの工場の方が悩まれていると思いますので、その指針を示す必要があるのではないかと考える。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
010	19	個人	番号：1 該当箇所：p.4 意見内容：フッタ 可用性、完全性、真正性、機密性の4要素をセキュリティ要素として挙げられていますが、通常、可用性、完全性、機密性の3要素に限定するか、真正性（Authenticity）、信頼性（Reliability）、責任追跡性（Accountability）、否認防止（non-repudiation）を足した7要素にすると思います。 理由：https://www.chusho.meti.go.jp/pamflet/hakusyo/H28/h28/html/b2_4_3_1.html	いただいた御意見のとおり、修正いたします。 具体的には、1.1の注釈において、真正性（Authenticity）を除いた3要素と、追加4要素を分けて記載いたします。 修正箇所：1.1.
010	20	個人	番号：2 該当箇所：p.13 意見内容：囲み枠（ステップ1） ステップ1-6に対応するのは3.1.6であり、ステップ1-7に対応するのは3.1.7のはずですが、そうなっていません 理由：冒頭の目次と矛盾しています	いただいた御意見のとおり、ステップ1-6・1-7をそれぞれ【3.1.6】【3.1.7】に修正いたします。 修正箇所：3.
010	21	個人	番号：3 該当箇所：p.25 意見内容：情報セキュリティとは別物に感じられる「自然環境の脅威」にまで言及されているのは素晴らしいと思いますが、火災にも言及すべきと思います。フランスのデータセンターが火災でデータ消失した事例もあります。 理由：https://gigazine.net/news/20220324-ovhcloud-fire-report/	いただいた御意見のとおり、修正いたします。 具体的には、表3-14の脅威内容に「火災による機器・設備等の焼失」を追加いたします。 修正箇所：表3-14
010	22	個人	番号4 該当箇所：p.72 意見内容：ホワイトリスト　「ホワイトリスト」、「ブラックリスト」といった呼称は避けられるようになってきていますので、「許可リスト」など代替の呼称も併記したほうが良いと思います。一方で、「ホワイトリスト」という呼称もまだまだ使われていますので、残した方が良いと思います。 理由：″NISTIR 8366: Guidance for NIST Staff on Using Inclusive Language in Documentary Standards https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8366.pdf Avoid terms that use ‘black’ to mean something bad or negative and ‘white’ to mean positive or less harmful″	いただいた御意見のとおり、修正いたします。 具体的には、「ホワイトリスト」の箇所に「許可リスト」を追加いたします。 修正箇所：付録A　用語／略語
010	23	個人	番号：5 該当箇所：p.98 2-6 意見内容：″システム構成図が作成している　→　システム構成図「を」作成している、あるいは、システム構成図が作成「されている」″ 理由：誤記	いただいた御意見のとおり、「システム構成図を作成している」に修正いたします。 修正箇所：付録E　チェックリスト
010	24	個人	番号：6 該当箇所：p.98　2-9 意見内容：″フラッシュカード　→　フラッシュデバイス（のほうが一般的と思います）″ 理由：誤記	いただいた御意見のとおり、「フラッシュデバイス」に修正いたします。 修正箇所：付録E　チェックリスト

010	25	個人	番号:7 該当箇所:p.99　3-1 意見内容:「ホワイトリスト」について、#4と同様の提案です 理由:#4と同様	いただいた御意見のとおり、修正いたします。 具体的には、「ホワイトリスト」の箇所に「許可リスト」を追加いたします。 修正箇所:付録E　チェックリスト
010	26	個人	番号:8 該当箇所:p.100　4-5 意見内容:"納入する工場システム機器　→　納入される工場システム機器"　この「工場システム機器」に関しては、工場は供給する側(サプライヤ)ではなく、利用する側(ユーザ)と思いますので、「する」よりも「される」のほうが適切だと思います	いただいた御意見のとおり、「納入される工場システム機器」に修正いたします。 修正箇所:付録E　チェックリスト
010	27	個人	番号:9 該当箇所:p.103 意見内容:このコラムの図すべてに「図0-1」など不自然な番号が振られています 理由:誤記	いただいた御意見のとおり、コラムの図番号を「図Ⅰ-x」「図Ⅲ-x」等に修正いたします。 修正箇所:コラム1
010	28	個人	番号:10 該当箇所:p.111 意見内容:このコラムは付録Fなので、「図C3-1」「表C3-1」などは不適切な番号だと思います。「C」は「コラム」の略と解釈することも可能ですが、そうすると、付録Cの図表番号の振り方と整合しません。 理由:誤記	いただいた御意見を踏まえ、コラムは付録Fとは独立のため、コラムの図番号を「図Ⅰ-x」「図Ⅲ-x」等に修正いたします。 修正箇所:コラム3
011	29	個人	--- 1 --- ・該当箇所 3.2.2. ステップ 2-2:想定脅威に対するセキュリティ対策の対応づけ (1) システム構成面での対策 1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 ・意見内容 対策例の記述として、「侵入検知システム(IDS)」と言う表現となっており、検知に重きが置かれている印象を与えている。但し、実際に「検知」だけでは通常該当の不正パケットは宛先ノードに到達しており、被害を事前に防止することができない。IPS(Intrusion Prevention System)と言う表現も併記をして、防御(攻撃パケット自体をブロックする)と言う対策も明示的に記載すべきではないか。実際に「表 3-23 ネットワークにおけるセキュリティ対策(例)」には、セキュリティ強度毎にIDSとIPSに関する記載がある。 提言:「侵入検知システム(IDS)」を「侵入検知／防止システム(IDPS)と言う表現に統一する ・理由(根拠) 「NIST SP 800-61」でもIDSではなく、IDPS(侵入検知／防止システム : Intrusion Detection and Prevention System)と言う表現で統一されており、Prevention(防御・防止)の表現も入っている。 【NIST SP 800-61参考記載】 3.2.3. 前兆と兆候のソース内の「表3-2 前兆と兆候の一般的なソース」 --- 1 ---	いただいた御意見を踏まえ、修正いたします。 「侵入検知システム(IDS)」だけではなく、「侵入検知システム(IDS)、侵入防止システム(IPS)」を併記する形に修正。 修正箇所:3.2.2(1)①　他

011	30	個人	--- 2 --- ・該当箇所 3.2.2. ステップ 2-2:想定脅威に対するセキュリティ対策の対応づけ (1) システム構成面での対策 1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 ・意見内容 昨今のセキュリティインシデントを分析すると、外部に漏れてしまった正規のID・パスワードを用いて（例えばVPN経由で）内部に侵入し、情報漏洩につながる事件が発生している。これらの攻撃は必ずしも脆弱性を利用するわけではなく、「表 3-23 ネットワークにおけるセキュリティ対策(例)」の通信監視・制御に記載されているようなIDS / IPSを利用した防御だけでは防ぐことができない。内部に侵入されうることを前提に、出口対策（インターネット出口におけるURLフィルタリングや通信ログ監視）に関しても対策例として記述すべきではないか。 提言：インターネット出口に関しても対策項目として記載する ・理由（根拠） 「NIST SP 800-61」でも事件の予防にて、「すべての接続ポイントのセキュリティを高めること」が重要と言う記述があり、特に他組織（インターネット）との境界対策は重要と読み取れる。 【NIST SP 800-61参考記載】 3.1.2. 事件の予防にて以下のように記述されている 「ネットワークセキュリティ ネットワークの境界では、明示的に許可されていないすべての 活動を拒否するように設定する。組織が適切に機能するために必要な活動だけが許可され るべきである。これには、モデム、VPN (virtual private network)、ほかの組織への専用線接 続といったすべての接続ポイントのセキュリティを高めることが含まれる。」 --- 2 ---	いただいた御意見のとおり、修正いたします。 具体的には、出口対策として「フィルタリング」を追加いたします。 修正箇所：3.2.2(1)①
011	31	個人	--- 3 --- ・該当箇所 3.2.2. ステップ 2-2:想定脅威に対するセキュリティ対策の対応づけ (1) システム構成面での対策 1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 ・意見内容 「ネットワークへの侵入行為を運用で早期に発見するための機能の利用」としては、ネットワーク・機器内ログをAI（マシーンラーニング）解析を行い、各機器の正常動作を自動でモデル化し、モデル情報を元にいつもと違う異常動作を検出する、そう言った振る舞い検知のテクノロジーを活用するべきではないか。 提言：AI（マシーンラーニング）技術を活用した振る舞い検知対策に関しても対策項目として記載する ・理由（根拠） 「NIST SP 800-61」でもインシデンと分析のためには、「正常動作の理解」が重要であると記載されており、昨今の複雑化する構成ではマニュアルに正常動作を管理するのは限界があるので、新しいテクノロジーを活用することも検討すべきである。 【NIST SP 800-61参考記載】 3.2.4. 事件の分析内の「 正常動作の理解」 --- 3 ---	いただいた御意見のとおり、修正いたします。 具体的には、「ログ取得：異常を早期発見するための機能の利用」を追記いたします。 修正箇所：3.2.2(1)①

011	32	個人	--- 4 --- ・該当箇所 3.2.2. ステップ 2-2:想定脅威に対するセキュリティ対策の対応づけ (1) システム構成面での対策 1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 ・意見内容 工場内のIoT機器に関しては、従来の制御装置・機器とは異なった特徴を持つことから、別の章を分けて具体的な対策に関して記述すべきではないか。 提言:IoT機器に関するセキュリティ対策を追記する --- 4 ---	いただいた御意見を踏まえ、修正いたします。 具体的には、IoT機器のセキュリティに関する参考文書を追記いたします。 修正箇所:3.2.2(1)②
012			ガイドライン案に言及されていらっしゃる暗号化ついて以下のとおり、意見を提出します。 暗号化は一部のシステムにしか記載がないが(例、ファイル保護)、サイバーセキュリティ対策において暗号化はデータ保護の基本でありファイル以外のシステムにも暗号化を推奨すべきと考えます。 暗号化技術の実装にあたり、「暗号鍵の管理」については言及されておりませんが、専用の暗号鍵管理システムまたはその暗号鍵管理システムが準拠しているセキュリティレベル(例、FIPS)を推奨すべきと考えます。 以下総務省サイバーセキュリティサイト、Cryptorec等でも「暗号鍵管理」の重要性は記載されております。 https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_structure_02.html https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf また、IoT セキュリティガイドライン ver 1.0においても、クラウド上のデータ蓄積形態に応じて、ファイルの暗号化やデータベースの暗号化を適用する等、クラウド上のデータの盗難や不正アクセスへの対策を行うと定義されておりますので(特に暗号鍵等の高い機密性が求められるデータは、必要に応じて HSM 等の専用の暗号装置や TEE、TPM 等の暗号技術の利用等を検討する)、暗号鍵管理としてHSM等の利用を推奨すべきと考えます。 https://www.soumu.go.jp/main_content/000428393.pdf 以上	―

013	33	企業	先程提出した意見書の個人情報に入力ミスがございましたので再度提出させて頂きます。こちらをご使用願います。 ―――――――――――――――――――――――――――――――――――――― ガイドライン案に言及されていらっしゃる暗号化ついて以下のとおり、意見を提出します。 暗号化は一部のシステムにしか記載がないが（例、ファイル保護）、サイバーセキュリティ対策において暗号化はデータ保護の基本でありファイル以外のシステムにも暗号化を推奨すべきと考えます。 暗号化技術の実装にあたり、「暗号鍵の管理」については言及されておりませんが、専用の暗号鍵管理システムまたはその暗号鍵管理システムが準拠しているセキュリティレベル（例、FIPS）を推奨すべきと考えます。 以下総務省サイバーセキュリティサイト、Cryptorec等でも「暗号鍵管理」の重要性は記載されております。 https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_structure_02.html https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf また、IoT セキュリティガイドライン ver 1.0においても、クラウド上のデータ蓄積形態に応じて、ファイルの暗号化やデータベースの暗号化を適用する等、クラウド上のデータの盗難や不正アクセスへの対策を行うと定義されておりますので（特に暗号鍵等の高い機密性が求められるデータは、必要に応じてHSM 等の専用の暗号装置や TEE、TPM 等の暗号技術の利用等を検討する）、暗号鍵管理としてHSM等の利用を推奨すべきと考えます。 https://www.soumu.go.jp/main_content/000428393.pdf 以上	本ガイドラインは、工場システムにおけるセキュリティ対策の全体的な枠組を提示するものであります。一方、具体的なセキュリティ対策は、産業分野や個社ごとに異なるものであり、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策を検討いたします。
014	34	企業	・該当箇所 (1).　P2　1.1項　工場セキュリティガイドラインの目的 ・意見内容 (1)P2 「1.1. 工場セキュリティガイドラインの目的」の記載において、 “インターネットにつなぐことで新たなセキュリティリスクを生む”と説明することで、「引き続き、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」との誤認識を与えるのではないか？ 「インターネット」ではなく、「ネットワーク」のような繋がることすべてを含んだ表現に変更するべき。	いただいた御意見を踏まえ、修正いたします。 「ネットワーク」に修正。 修正箇所：1.1.
014	35	企業	・該当箇所 (2).　P7　2.3項　想定生産ライン ・意見内容 (2)P7 2章に記載している想定工場において、外部ネットワークとの接続は自動倉庫遠隔保守用サーバのみで、設備ベンダの管理領域となっている。 昨今は制御ゾーン（生産現場）に含まれる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。より多くの機器やゾーンが外部ネットワークと接続することも想定すべきではないか。 （制御ゾーンに含まれる機器に対しても、セキュリティ対策の意識・理解が必要であることを推奨するべき。）	いただいた御意見を踏まえ、修正いたします。 具体的には、想定工場としては現状のままとし、制御ゾーンに含まれる機器が外部ネットワークと接続したり、外部クラウドが利用される場合のセキュリティ対策の必要性について、コラムとして追記いたします。 修正箇所：コラム4
014	36	企業	・該当箇所 (3).　P24　3.1.7. ステップ1-7：ゾーンと、セキュリティ脅威による影響の整理 ・意見内容 (3)P24 1行目の「脅威の種別の例」としての記載と、表3-11 一般的な脅威と生産への影響（例）の「脅威種別」の内容が一致していない。 1行目の記載は「脅威内容の例」とするのが正しいのではないか？	いただいた御意見を踏まえ、修正いたします。 具体的には、「脅威の種別の例」に合わせて、表3-14の「脅威種別」を記載いたします。 修正箇所：3.1.7、表3-14

014	37	企業	・該当箇所 (4). P30？44 3.2項（表3-24など） ・意見内容 (4)P30？45 3.2.2の各項で記載されているセキュリティ対策に関して、物理面での対策の記述に比べ、システム構成面での記述が抽象的に感じる。例えば、表3-24の「暗号鍵の管理」・「暗号鍵の厳密な保護」の記述であれば、「暗号鍵は定期的な更新を行う」・「暗号鍵は耐タンパデバイス（SAM, HSMなど）を用いて保管する」というような具体的な実践方法を記載すべき。	本ガイドラインは、工場システムにおけるセキュリティ対策の全体的な枠組を提示するものであります。一方、具体的なセキュリティ対策は、産業分野や個社ごとに異なるものであり、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策を検討いたします。
014	38	企業	・該当箇所 (5). P36 図3-4 ・意見内容 (5)P36 想定工場の構成に対して、実際にセキュリティ対策を実施した状態を3.2.1の図3-4としているが、付近に説明の記述がないため、具体的に何のセキュリティ対策がどのゾーンに実施されているかが分かりづらい。 各ゾーンの端末等へのセキュリティ対策、各ゾーン内の漏洩防止等の管理などを明記すべきと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、実施した対策について追記いたします。 修正箇所：図3-4
014	39	企業	・該当箇所 (6). P42 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 ・意見内容 (6)P42（誤記の修正） セキュリティ機器(ファイアウォール(FW)の「（」 ゲートウェイ機器)の導入の「）」をそれぞれ削除する。	該当箇所につきましては、別の御意見に伴う本文の修正により、削除いたします。
014	40	企業	・該当箇所 (7). P45 表 3-24 機器におけるセキュリティ対策（例） ・意見内容 (7)P45 脆弱性対策について、高レベルに「＋ソフトウェア更新」が位置付けられているのは、不適切です。ソフトウェア更新をしなくても、OSは古いままでも良いと勘違いさせる内容であり、最低限、又は中のセキュリティ対策強度であるべきだと考えます。 ※現実的にソフトウェア更新が工場環境において難しいという観点はあると思うが、そうであれば、セキュリティ対策強度「中」に記載がある、脆弱性診断や侵入可否検査（ペネトレーションテスト）で相当数の脆弱性が検出される事となり、実質的には、セキュリティパッチを適用しなくても良いとこの対策（例）から読み取れてしまい、セキュリティガイドラインにおける例示としては不適切だと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、表3-27において、ソフトウェア更新が望ましいものの、工場においては対応が難しい状況を鑑み、セキュリティ対策強度「中」に脆弱性が検出された後の回避策の適用を追記いたします。 修正箇所：表3-27
014	41	企業	・該当箇所 (8). P50 注釈21 ・意見内容 (8)P50 注釈21は、本項で紹介する物理対策を行う対象となる機器の具体例の説明である。データ可搬型の記憶デバイスが、ネットワークに接続しない機器の例示しかなく、これら以外は非対象であるような誤認を招く恐れがある。ここでは対象となる機器を列挙するべきではないか。（ネットワークに接続をするHDD/NASといった機器等）	いただいた御意見のとおり、修正いたします。 具体的には、「ネットワークに接続するHDD/NASなどの機器」を注釈に追記いたします。 修正箇所：3.2.2.(2)⑤
014	42	企業	・該当箇所 (9). P50 内部不正／過失の防止 ・意見内容 (9)P50 工場においては管理端末台数が多い事が多く、物理的なポート等の閉塞が困難なケースが予想される。ソフトウェア制御での閉塞の方が実現性が高い事もあるので、「物理的又は論理的な閉塞」と記載するのが例示として適切だと考えます。	いただいた御意見のとおり、表3-30では、「物理的又は論理的な閉塞」に修正いたします。 修正箇所：表3-30

014	43	企業	・該当箇所 (10). P62 3.3項(2) サプライチェーン対策 ・意見内容 (10)P62 3.3のサプライチェーンに関する対策について、製造工場は日本国内だけでなくグローバルなビジネスを行っている企業が多いため、世界情勢の考慮や各国の法案を確認するなどの観点も、付録Bとしてだけでなく本文内でも触れるべきではないか。	いただいた御意見のとおり、修正いたします。 具体的には、世界情勢の考慮や、各国の法制度、標準規格やガイドライン等に準拠した対策を進める必要がある旨を追記いたします。 修正箇所：3.3(2)
014	44	企業	・該当箇所 (11). P63 ・意見内容 (11)P63 本ガイドラインの本文は、このページまでであり、以降は付録でしょうか？ 本文と付録の境界がわかりづらいと感じます。	いただいた御意見のとおり、付録の冒頭に扉を挿入し、境界をわかりやすく修正いたします。 修正箇所：付録
014	45	企業	・該当箇所 (12). P98 付録E チェックリスト 2-6 「？の台帳を作成し、システム構成図が作成している。」 ・意見内容 (12)P98（誤記の修正） 「？の台帳を作成し、システム構成図〞を〞作成している。」	いただいた御意見のとおり、「システム構成図を作成している」に修正いたします。 修正箇所：付録E チェックリスト
014	46	企業	・該当箇所 (13). P98 付録E チェックリスト 2-8 「定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。」 ・意見内容 (13)P98 攻撃方法や脆弱性を特定しているだけでは何の意味もありません。脆弱性へ対応している、又は緩和策を講じている、といった特定後の対処を明文化すべきと思います。	いただいた御意見のとおり、「脆弱性へ対応している、又は緩和策を講じている。」に修正いたします。 修正箇所：付録E チェックリスト
014	47	企業	・該当箇所 (14). P98 付録E チェックリスト 2-11 「工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を削除している。」 ・意見内容 (14)P98 時間軸を入れるべき。「？〞速やかに〞削除している」とした方が良い。	いただいた御意見のとおり、「速やかに」を追記し、修正いたします。 修正箇所：付録E チェックリスト
014	48	企業	・該当箇所 (15). P99 付録E チェックリスト 3-1 「ウィルス対策がインストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリストを導入し、インストール不可能な端末では何らかの代替策（USB型のアンチウィルスなど）を導入している。」 ・意見内容 (15)P99 1.ウィルス対策がインストールできる端末、は表記がおかしい。〞ウィルス対策が〞を削除すると良い。 2.OT系機器（MES/SCADA/PLC）はアンチウィルスソフトを導入できないと思われるので、〞代替策（不審な動向や異常な通信が発生した際に検知する機器）〞とした方が良い。 ※WindowsやLinuxについて制限しているチェック項目文にはなっていない。	いただいた御意見のとおり、「ウィルス対策が」を削除し、修正いたします。 修正箇所：付録E チェックリスト

014	49	企業	・該当箇所 (16). P99 付録E チェックリスト 3-2 「アプリケーション／オペレーティングシステム（OS）にセキュリティパッチを 適用している。もしくは代替策を講じている。」 ・意見内容 (16)P99 時間軸、もしくは時間制限を付けた方が良い。 昨今、すべてのパッチを即時に当てている組織は無いと思われる。 修正パッチを適用した際の不具合などを考慮して、パッチ適用をしない場合もあるため、「重大な脆弱性については一定期間内（例えば1ヶ月以内）に修正パッチを適用している」といった記載が望ましい。	いただいた御意見を踏まえ、修正いたします。 具体的には、工場ではアップデートがすぐに実施できず、端末を使わなくてもよいタイミングで順次実施するのが実態であり、望ましい期間を設定するのは難しいことから、「重大な脆弱性については可能な限り速やかに」を追記いたします。 修正箇所：付録E チェックリスト
014	50	企業	・該当箇所 (17). P100 付録E チェックリスト 3-8 「工場内システムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析するか必要日数保存している。」 ・意見内容 (17)P100 「ログは定期的に分析する」と「必要日数保存している」に関しては、“or”文ではなく“&”文にすべき。 例えば、イベントログ（アラート）には対応すべきであり、ログを保存しておかないとサイバー攻撃を受けた際の調査作業に影響すると思われる。	いただいた御意見のとおり、修正いたします。 具体的には、「それらのログは定期的に分析し、必要日数保存している。」に修正いたします。 修正箇所：付録E チェックリスト
014	51	企業	・該当箇所 (18). P100 付録E チェックリスト 4-2 「工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を実施している。」 ・意見内容 (18)P100 時間軸を入れた方が良い。 「セキュリティ教育を業務開始時及び定期的に実施している。」が望ましい。	いただいた御意見を踏まえ、修正いたします。 具体的には、「業務開始」であると毎日の業務開始時と誤解を生むため、「契約開始時及び定期的に」として追記いたします。 修正箇所：付録E チェックリスト
014	52	企業	・該当箇所 (19). P97？100 付録E チェックリスト チェックリスト ・意見内容 (19)P97？100 下記の2つの観点をチェックリスト項目として追加すべきと考えます。 1.機器の初期設定を確認・判断する項目。 IoT機器ではベンダのデフォルト設定、デフォルトパスワードが侵害原因になっているケースも多い。NGとすべき場合などの具体例もあわせて、チェックリスト項目に入れるべき。 2.VPN装置の脆弱性対策に関する項目。 インシデント事例も多いので、敢えてチェックリストに入れておく方が良い。	いただいた御意見を踏まえ、修正いたします。 具体的には、1点目については、4-5 機器調達時の注意事項として注釈に追記いたします。また、2点目のVPN装置の脆弱性については、影響は大きいものの工場システムへの影響は限定的である場合も多いことから2-8の注釈に追記いたします。 修正箇所：付録E チェックリスト
014	53	企業	・該当箇所 (20). 全体 ・意見内容 (20)全体 社員教育への注力についても、もう少し記載があっても良い。	いただいた御意見を踏まえ、修正いたします。 具体的には、従業員及びサプライヤー・保守運用ベンダに対する教育について追記いたします。 修正箇所：3.3.(1)②、表3-38
015	54	個人	・2ページの最下行から上に2行目「言って」は「いって」のほうがよい。同3行目の例「いう」と同様に。	いただいた御意見のとおり、修正いたします。 修正箇所：1.1.
015	55	個人	・6ページの7行目「替える」は「換える」のほうがよい。109ページの3行目の例と同様に。	いただいた御意見については、原案のとおりとさせていただきます。

015	56	個人	・105ページの1行目「一つ」は「1つ」のほうがよい。41ページの6行目「3つ」と同様に。	いただいた御意見については、原案のとおりとさせていただきます。
015	57	個人	・105ページの8行目「不正侵入の防止」は「不正侵入を防止」のほうがよい。同10行目、13行目の例と同様に。	いただいた御意見のとおり、「不正侵入を防止」に修正いたします。 修正箇所：3.2.2.(1)
015	58	個人	・109ページの11行目「伸長・継続」は「伸長、継続」のほうがよい。「Continuity」は「伸長」を意味しないから。	いただいた御意見のとおり、「伸長、継続」に修正いたします。 修正箇所：コラム2
016	59	個人	スパイ防止法がない状態では、この様な形でしかサイバーセキュリティ強化の方法はないのかもしれませんが、早急にスパイ防止法を制定してください。	いただいた御意見に関しては、例えば、第201回国会における質問主意書（内閣衆質二〇一第六六号 令和二年三月三日）において、「お尋ねの「スパイ防止法」の制定（中略）については、様々な議論があるものと承知しているが、政府としては、今後とも、情報機能の更なる強化について検討を行ってまいりたい。」との見解が示されているものと承知しております。
017	60	企業	お世話になっております。 ガイドライン案の作成ありがとうございます。 案に対する直接的な意見に関しましては、日本工作機械工業会を通じて意見をさせて頂きます。 ここでは弊社としての考えを述べさせて頂きます。 工場にはどんな脅威があるかをグルーピングして記述したほうがよいと考えます。 具体的には5つの脅威があると考えております。 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 本ガイドラインは、3. サイバー攻撃の脅威が主に記述されています。 4. 誤検知、誤動作による動作停止の脅威の記述は無いようにみえます。 通常は4を恐れて設備を提供及び導入する側も対策がされていない会社が多いと考えます。 そこで、1？5の脅威があるということを読者と共有し、ガイドラインを構成することで読みやすく、利害関係者に賛同を得られると考えております。 以上よろしくお願いします。	いただいた御意見を踏まえ、修正いたします。 具体的には、工場の脅威について、誤検知や誤動作による動作停止の脅威も含めて整理し、「脅威の種別の例」として、表 3-14と整合性を取る形で修正いたします。 修正箇所：3.1.7.
018	61	個人	章番号：2、「2. 本ガイドラインの想定工場」 想定工場のネットワーク例が既に理想系になりすぎており現実から乖離していると考える。実際は設備系ネットワークとOAネットワークがこの様にきれいに分かれてない企業が多見されます。また工場内の設備・資産のネットワーク接続状況を把握できていないケースが多見されます。その様な企業向けに、ゾーン分けより前に資産の可視化や分離やセグメンテーションのステップをいれるべきではないでしょうか？また、その様な企業向けでも効果を発揮できるITシステムでの施策を例示するべきではないか？	本ガイドラインは、工場システムにおけるセキュリティ対策の全体的な枠組を提示するものです。一方、具体的なセキュリティ対策は、産業分野や個社ごとに異なるものであり、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策を検討いたします。
018	62	個人	章番号：2、「2. 本ガイドラインの想定工場」 工場システムでもクラウド利用や検討が増えている中で、想定工場のシステムでクラウドに関する指針が示されていないは不足を感じます。追加するべきだと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、想定工場としては現状のままとし、外部クラウドが利用される場合のセキュリティ対策の必要性について追記いたします。 修正箇所：2.
018	63	個人	章番号：3.1.4、「ステップ 1-4：保護対象の整理 」 無線LAN-APはAGVだけでなく他のセンサーやOA用PCなど多種多様な機器が接続されるはずです。利用を分ける必要があるのであれば明文化すべき、共用を想定するのであれば共用時の指針を明記すべきと考えます。	本ガイドラインは、工場システムにおけるセキュリティ対策の全体的な枠組を提示するものです。一方、具体的なセキュリティ対策は、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策を検討いたします。

018	64	個人	章番号：3.2.2、「(1)システム構成面での対策 」 例示されているのは境界防御だけで、ゾーン内の拡散（ラテラルムーブメント）を防げないのではないでしょうか？NDRなどの対策を例示すべきでと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、通信状況可視化・監視に（NDR）を例示として追記いたします。 修正箇所：3.2.2.(1)

019	65	企業	・該当箇所 P1 工場セキュリティについて知りたいこと ・意見内容 各項目についての詳細の記載箇所が明記されており、目的に応じて必要な部分だけ読み進めることができるのはよい。	本ガイドラインに対する肯定的な御意見として承ります。
019	66	企業	・該当箇所 P1 工場セキュリティについて知りたいこと ・意見内容 4 番の項目の記載箇所が（P56-68）となっているが、（P54-66）の間違いではないか。	いただいた御意見のとおり、正しいページ番号に修正いたします。 修正箇所：工場セキュリティについて知りたいこと
019	67	企業	・該当箇所 P2 1.1. 工場セキュリティガイドラインの目的 ・意見内容 箇条書き前に以下の文を追加 なお、昨今の設備はITの実装度合いが増加しているのに加え、攻撃は高度な技術を用いた自動化省人化が進んでおり、「自社工場を狙うものはいない」とはならないことに注意が必要である。 ・理由 自社工場に重要な情報は無く攻撃を受けないという方に向けて、等しく攻撃を受ける注意喚起をした方がよいと思います。	いただいた御意見を踏まえ、修正いたします。 具体的には、いずれの工場も高度な攻撃に狙われる可能性がある点について追記いたします。また、「【参考】攻撃者の動機」で記すように、たまたま攻撃した先が工場という場合もある点にも言及いたします。 修正箇所：1.1.
019	68	企業	・該当箇所 P2 1.1. 工場セキュリティガイドラインの目的 ・意見内容 箇条書き文を追記 ●IT セキュリティ分野で一般的なデータの保護だけでなく、不正操作に端を発した災害による、従業員の安全及び近隣住民への説明責任、資産棄損防止の観点から機器稼働等の維持や安全の確保が求められる。（安全を確保する要素としてHealth 健康　Safety 安全　Environment環境といわれる） ・理由 様々な機器がITで制御され、場合によっては火災等の被害が発生する可能性があり、従業員への安全、近隣住民への責任の為にもセキュリティ対策を実施するというメッセージを込めたらと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、箇条書き1文目の注釈として、ご指摘の点を追記いたします。 修正箇所：1.1.
019	69	企業	・該当箇所 P2 1.1. 工場セキュリティガイドラインの目的 ・意見内容 箇条書き文を追記 ●古い設備が運用されている場合など、既存システムに対する段階的なセキュリティ対策の導入が必要になる。なお、導入に際しては、都度対策といった対症療法では、効果が薄れ、支出が増大する。生産性への影響を計測した上で適切な対策、費用の支出を設計し対応すべきである。 ・理由 セキュリティ対策を都度都度実施すると対投資効果が問題となります。よって生産性への影響を確認した上で投資を行うという目的が重要とした方が良いと考えます。	いただいた御意見を踏まえ、修正いたします。 箇条書き2文めの注釈として、ご指摘の点を追記いたします。 修正箇所：1.1.

019	70	企業	・該当箇所 P2 1.1. 工場セキュリティガイドラインの目的 ・意見内容 箇条書きに以下文を追加 ●事務所側のセキュリティ対策と工場側のセキュリティ対策は異なる。 ・理由 現行の情報システム部は事務部門が担当、工場は生産技術部門が担当という会社も多くあると思います。情報システム部門の方が読むときに冒頭メッセージを入れた方がその後読みやすいと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、元の注釈6を本文に移動し、各者・各部門が置かれた環境や価値観は様々である点について記載いたします。 修正箇所：1.1.
019	71	企業	・該当箇所 P3 1.1. 工場セキュリティガイドラインの目的 ・意見内容 文内への追記 また、本ガイドラインは、業界団体や個社が情報セキュリティ上の脅威を組織全体で共有した上で、自ら対策を企画・実行するに当たり、 ・理由 セキュリティ対策はリスク管理であり、脅威の認識が基本になるかと考えております。よって、最初に脅威を組織全体で共有することが重要と考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、ご指摘の「自ら対策を企画・実行するに当たり」の「企画・実行」に脅威の認識も含めていることから、文章の追記は行いませんが、ステップ1-1(2)外部要件の整理、及びステップ1-7において、脅威の認識について記載いたします。 修正箇所：3.1.1.、3.1.7.
019	72	企業	・該当箇所 P4 1.1. 工場セキュリティガイドラインの目的 ・意見内容 参考部分への箇条書き追加 ・設備の規定外の作動による従業員の健康への影響。 ・　〃　　に端を発した災害による近隣住民の生活への影響 ・理由 目的にも記述し、参考にも同様の従業員の健康、及び近隣住民の生活への影響の追記をした方がよいと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、設備の期待外の作動に関する脅威と影響について追記いたします。 修正箇所：【参考】工場システムにおいてセキュリティ脅威により生じる影響の例
019	73	企業	・該当箇所 P5 1.2. ガイドラインの適用範囲 ・意見内容 本ガイドラインの想定読者は、例えば以下を想定しているが、情報セキュリティの推進は取締役会等の意思決定機関による体制の構築、体制を通じ、組織に指示することが前提となる。その上で、IT システム担当や生産関係部門の間で、 ・理由 各部門が様々なセキュリティ対策の意識及び実際に実施することは重要ですが、リスクは投資対効果が目にみえない領域です。よって、意思決定機関の率先が前提と考えます。	いただいた御意見のとおり、修正いたします。 具体的には、脚注5を本文に移動するとともに、セキュリティの推進には、経営層等意思決定を行う者による関与が重要である点を追記いたします。 修正箇所：1.2.
019	74	企業	・該当箇所 P5 注釈5 ・意見内容 注釈5　はおっしゃる通りですが、 弊社のDXオブザーバーに一読をお願いしたが、こうした人たちには当たり前のことのようでやったほうが良いと思いますという答えしか出てこないのも事実。 経営層の意思決定が1丁目1番地であるので、上記注釈がありましたが、本ガイドラインの簡易概要版を作成いただきたいです。これを理解できる人材は本当に限られますので。	いただいた御意見を踏まえ、注釈を本文に移すことで修正いたします。 修正箇所：1.2. なお、簡易概要版の作成に関する御意見につきましては、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

019	75	企業	・該当箇所 P7 2.2. 想定組織構成（P7） ・意見内容 以下の前提条件を追記 ・情報システム部門：OA(Office Automation)系を中心に、ネットワーク、サーバ、端末の管理を実施 セキュリティ担当者は不在で、ウイルス対策システム の可用性を確保するサーバ管理を実施 ・理由 本ガイドラインを全て読んだところ、本想定の組織では、セキュリティ担当者は不在のようです。よって、想定は、これから情報システム部で担当者を確保しようとしている会社を想定します。	いただいた御意見については、原案のとおりとさせていただきます。
019	76	企業	・該当箇所 P7～9 2.3. 想定生産ライン ・意見内容 自動倉庫の遠隔保守を除けば、想定が拠点のネットワーク内に閉じている。 ・理由 昨今の事情から、インターネット接続の活用、例えばクラウド技術の使用も想定に加える必要はないか。	いただいた御意見を踏まえ、修正いたします。 具体的には、想定工場としては現状のままとしますが、制御ゾーンに含まれる機器が外部ネットワークと接続したり、外部クラウドが利用される場合のセキュリティ対策の必要性について、参考として追記いたします。 修正箇所：2.3.
019	77	企業	・該当箇所 P8 図2-1 ・意見内容 図中に、本文の構成で説明している”ルータ（設備系-生産管理系）”に当たる装置・機器が無い。	いただいた御意見のとおり、本文から「ルータ（設備系-生産管理系）」を削除し、修正いたします。 修正箇所：図2-1
019	78	企業	・該当箇所 P11 表2-1 ・意見内容 表2-1など用語を統一した方が良い。「AGV」と「AGV(無人搬送車)」他にFW、ISC、IDS、OAシステムも同様	いただいた御意見のとおり、用語を統一し、修正いたします。 修正箇所：表2-1 他
019	79	企業	・該当箇所 P13 「3.セキュリティ対策企画・導入の進め方　本節では～」 ・意見内容 ”経営目標等の整理””外部要件の整理”を行うためには、まずP28表3-13のようなリスクを認識しなければならないので3.項の冒頭で表3-13を説明した方が分かり易いのではないか。 ・理由 一般的なリスクを認識してから活動を開始した方が良い。	いただいた御意見のとおり、修正いたします。 具体的には、脅威の認識については、ステップ1-1(2)外部要件の整理、ステップ1-7においても記載いたします。 修正箇所：1.1.
019	80	企業	・該当箇所 P13 2.6. 想定ゾーン ・意見内容 ステップ 1 (1)経営目標等の整理に追記 脅威の認識（管理上の脅威、設備機器の脅威、サイバー攻撃の脅威、誤検知誤作動の脅威、災害の脅威） ・理由 取り掛かる前に、自社の工場においてどのような脅威が存在し、想定会社における脅威の重要度を判断することを最初に記述するよう考えました。括弧内は具体的に脅威を示すことで理解が進むと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、脅威の認識については、ステップ1-1(2)外部要件の整理、ステップ1-7においても記載いたします。 修正箇所：1.1.

019	81	企業	・該当箇所 P14 2.6. 想定ゾーン ・意見内容 ステップ 2-3 を追記 2-3. 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） ・理由 リスクは対策してもゼロにはなりません。この残存リスクに対しての対策方針が必須と考えます。	いただいた御意見のとおり、残存リスクへの対応を追記し、修正いたします。 修正箇所：3.2.2.
019	82	企業	・該当箇所 P14　図3-1, P15　表3-2, P88　表C-1, P90　表C-3 ・意見内容 IEC 62443はシリーズ規格（規格群）である。 ”IEC 62443”は、”IEC 62443規格群”に修正する。	いただいた御意見のとおり、「IEC62443規格群」に修正いたします。 修正箇所：表3-2、表C-1、表C-3他
019	83	企業	・該当箇所 P15 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-1　セキュリティ対策を検討・企画する際に考慮すべき経営目標事項（想定工場における例）内に追記 安全上の問題の発生防止 及び近隣住民への被害防止 ・理由 設備のセキュリティ案件に対し、内外要件としての、優先度を決める際に、近隣住民への被害防止の考慮は必須であると考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、近隣住民への被害防止の観点も追加し、整理いたします。なお、内外要件の整理にあたって、どのような要素を考慮すべきかについて、その考え方やプロセス・道筋がわかるように表を追加いたします。 修正箇所：表3-1
019	84	企業	・該当箇所 P15 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-2　セキュリティ対策を検討・企画する際に考慮すべき外部要求事項（想定工場における例） 内のビジネス上の要求の最上位に追記内容として： 国内外の法令遵守の観点 例として：消防法、個人情報保護法、サイバーセキュリティ法、データ安全法等 ・理由 要件として、工場運営において法令を遵守する視点を盛り込む必要があると考えます。	いただいた御意見については、法令遵守の観点は3.1.1.(2)外部要件の整理、付録Bに記載済のため原案のとおりとさせていただきます。

019	85	企業	・該当箇所 P16 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-4 工場のセキュリティを運用・管理していくための体制の考え方（例）の工場システムの計画・・・に追記 ・メリット：生産性向上を考慮し工場システムの現状に即した検討が可能 ・デメリット：ITに詳しい担当者の異動後に、担当者が不在となるリスクがあり、セキュリティ対策の運営継続にに支障が生じる。ITが得意な担当者が不在であれば、保守業者に依存し、保守を終了した場合、同様に運営に支障が生じる。 ・理由 想定部門として生産技術部門の方がセキュリティ対策を行うメリットとして、生産性向上の考慮を追加しました。また、デメリットとして対策や運用の継続が課題になると考え、担当者が実施した場合、保守業者に依頼した場合の2種類のデメリットを考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、メリットについては追記いたしますが、デメリットについては、現在の「セキュリティに関する人財育成、ノウハウ蓄積が必要」に含まれますので、原案のままといたします。 修正箇所：表3-4
020	86	企業	・該当箇所 P16 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-4 工場のセキュリティを運用・管理していくための体制の考え方（例）のIT 関係部門で実施に追記 ・デメリット：事務エリアと同等のセキュリティ対策を実施しようとし、対策の方針が誤る可能性がある。また、設備の誤検知、誤作動のリスクが高まる。 ・理由 想定では情報システム部門ではセキュリティ担当者が不在のようにみえました。よって想定される情報システム部員は、自分の知識で工場の対策をすると想定しました。	いただいた御意見を踏まえ、修正いたします。 具体的には、「OAと同等の対策に捉われ、工場システムに適した対策方針の立案が困難。」を追記いたします。また、設備の誤検知、誤動作のリスクについては、「業務への影響を含めた分析が困難。」で記載しているため、原案のままといたします。 修正箇所：表3-7
020	87	企業	・該当箇所 P17 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-4 工場のセキュリティを運用・管理していくための体制の考え方（例）の企業全体のリスク・・・に追記 ・デメリット：火災や侵入犯罪とサイバー攻撃を同一視し、公的機関の全面支援、捜査体制が得られる前提で構築し、対策の方針に誤りが発生しやすい。 ・理由 想定される組織で総務部門の方は、火災や侵入の延長でセキュリティを進める可能性が高く、注意が必要と考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、「火災や侵入と同等の公的機関・捜査機関からの支援を期待し、工場システムに適した対策方針の立案が困難。」を追記いたします。 修正箇所：表3-7
020	88	企業	・該当箇所 P17 3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理 ・意見内容 表 3-4 工場のセキュリティを運用・管理していくための体制の考え方（例）のセキュリティ統括組織で実施に追記 ・メリット：サイバー経営ガイドラインで実施すべき内容と連携が可能となる。 ・理由 セキュリティ統括組織は、意思決定機関と緊密な連携があり、法令や、政府機関の指示をよく理解します。そこで、典型的なガイドラインについて、挙げました。	いただいた御意見については、「セキュリティの視点で全社横断的な維持・改善が可能」との文言に含まれること、また、体制を問わず「サイバーセキュリティ経営ガイドライン」を実践いただくことが重要であるため、原案のとおりとさせていただきます。

020	89	企業	・該当箇所 P19 3.1.4. ステップ1-4 ・意見内容 構成する機器の型番、ベンダー、脆弱性識別情報等も併せて作成すると良い。 ・理由 日々巧妙化するサイバー攻撃への追従や、インシデントへの迅速対応に必要。	いただいた御意見を踏まえ、修正いたします。 具体的には、ご指摘の点を注釈に追記するとともに、参照可能なドキュメントや事実等を参考情報として追記いたします。 修正箇所：3.1.4.
020	90	企業	・該当箇所 P19～20 3.1.4. ステップ1-4 表3-8、図3-2 ・意見内容 表3-8と図3-2は、登場する構成要素を合わせたほうが良い。 ・理由 誤解防止。	いただいた御意見のとおり、修正いたします。 具体的には、図3-2、表3-8について、構成要素の整合性を取るとともに、図を再掲のものに差し替えいたします。 修正箇所：3.1.4.
020	91	企業	・該当箇所 P23 表3-10 ・意見内容 表 3-10 ゾーンの概要（想定工場における例）「機密情報、重要情報」欄の追加。別紙1参照 ・理由 設備自体を防御するという視点ですが、設備を動作させる為の情報内容も重要と考えます。 そこで、本ガイドラインにそって参考として列追加し、内容を記述しました。 	いただいた御意見を踏まえ、修正いたします。 具体的には、わかりやすさの観点で列の順序を変更すると共に、関連する保護対象の列にデータを追加いたします。 修正箇所：表3-13
020	92	企業	・該当箇所 P24 表3-11 ・意見内容 表3-11 一般的な脅威と生産への影響（例）の2ページ目　9項および12項で、「脅威の種別」で示された「データ」の盗難・漏えいや改ざん・破壊などに対して、「脅威の内容」では、「パケット」の盗聴や改ざんがされることを問題にしていますが、「パケット」の意味が不明瞭なため、どういった脅威なのかが分かり難い	いただいた御意見を踏まえ、修正いたします。 具体的には、それぞれ「パケットの盗聴（通信データの盗聴）」「パケットの改ざん（通信データの改ざん）」と追記いたします。 修正箇所：表3-14、表3-24

表 3-10 ゾーンの概要（想定工場における例）

	関連する保護対象	機密情報、重要情報	関連する業務	名称	概要
1	・生産ライン ・保守端末 ・ルータ	【重要情報】 ・制御装置内の OS 及びプログラム情報 ・ルータ内のネットワーク設定	・生産（＋検査） ・生産状況監視（現場） ・部材補充（現場へ） ・メンテナンス	制御ゾーン ・（生産現場）	・製品を生産するための生産ライン、制御装置・機器などで構成されるゾーン
2	・AGV 制御 PC ・無線 LAN-AP ・AGV	【重要情報】 ・AGV 装置内の OS 及びプログラム情報 ・無線 LAN-AP 内の通信設定	・部材補充（現場へ）	自動搬送 ・ゾーン	・部材や完成品の運搬を行う AGV を運用するゾーン
3	・自動倉庫遠隔保守用サーバ ・自動倉庫	【重要情報】 ・倉庫サーバ内の OS 及びプログラム情報 ・自動倉庫動作指令手法情報	・部材補充（現場へ） ・部材補充（倉庫へ）	自動倉庫 ・ゾーン	・部材を保管しつつ、自動で入出庫する装置を運用するゾーン
4	・MES サーバ	【機密情報】 ・生産計画情報内の顧客情報 ・甚先で使用する部品、ソフトウェア情報	・生産計画設定 ・生産（＋検査） ・生産状況監視（現場） ・生産性分析 ・トレーサビリティデータ参照	生産管理 ・ゾーン	・生産計画の管理、トレーサビリティデータの管理などを行うサーバ群からなるゾーン
5	・SCADA	【重要情報】 ・生産状況の監視を実現する為の OS、プログラム、データベース情報	・生産状況監視（現場） ・生産性分析 ・トレーサビリティデータ参照	・生産状況 監視ゾーン	・生産状況や設備情報の取得・見える化を行う装置からなるゾーン
6	・OA 系サーバ ・OA 端末	ガイドラインの対象外	・生産計画設定 ・部材補充（倉庫へ） ・生産性分析	・OA ゾーン	・生産に直接関係ない業務を行うゾーン
7	・保守センタ・VPN 装置等 Firewall	【機密情報】 ・VPN 装置内の接続情報	・リモートメンテナンス	・リモート メンテナンスゾーン	・設備ベンダの保守センタが、自動倉庫をリモートで監視するためのゾーン

※リモートメンテナンスゾーンは、設備ベンダの管理領域であると想定。

020	93	企業	・該当箇所 P24～27 3.1.7　表3-11、表3-12 ・意見内容 セキュリティの脅威と並んで、突然、自然環境の脅威とシステム／機器の障害・故障が取り上げられている。 ・理由 セキュリティとの関連性、意図を示した方が良い。	いただいた御意見を踏まえ、修正いたします。 具体的には、工場の脅威について「脅威の種別の例」と整合性を取ることで、修正いたします。また、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も追記いたします。 修正箇所：3.1.7.
020	94	企業	・該当箇所 P25 表3-11 ・意見内容 表3-11 一般的な脅威と生産への影響（例）の2ページ目　17項の「生産・事業への影響」の列にある 　・捜査中のライン・・・・は、・操作中の誤記と思われます。	いただいた御意見のとおり、「操作中」に修正いたします。 修正箇所：表3-14
020	95	企業	・該当箇所 P26　表3-12, P31　表3-14 ・意見内容 各セルの1文字目が文字化けしている。	いただいた御意見のとおり、修正いたします。 修正箇所：表3-15、表3-17
020	96	企業	・該当箇所 P26～27、P31 ・意見内容 ガイドラインの内容に関する指摘・意見等はありません。目的を沿った形で丁寧にまとめられていると思います 表記に関しては1点指摘があり、p.26～p.27、p.31に使用されている表にて文字化けやカーニング不具合による文字の重なりが見られ、指定フォントや機種依存文字などが原因ではないかと推察されます。	いただいた御意見のとおり、見やすさについて修正いたします。 修正箇所：表3-15、表3-17
020	97	企業	・該当箇所 P27 【参考】攻撃者の動機 ・意見内容 攻撃者の動機は、ガイドラインの前半（1.1項）に移動した方が良いと考えます。 ・理由 初めに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よりインパクトがあるのではないかと考えました。	いただいた御意見を踏まえ、修正いたします。 具体的には、攻撃者の動機に関して1.1に記載いたします。 修正箇所：【参考】攻撃者の動機

020	98	企業	・該当箇所 P29 ステップ 1-7:【参考】経営層による取組の宣言の例　ポツ1について、以下のとおり修正。 ・意見内容 3.1.7. ステップ 1-7: ゾーンと、セキュリティ脅威による影響の整理　、【参考】経営層による取組の宣言の例に追記。別紙2参照。 ・理由 取組み宣言の例ではありますが、脅威を組織全体での認識を強調しました。また、政府の指示によるサイバー経営ガイドラインの遵守も宣言し、最終残存リスクを考慮することを記述しました。 経営層によるセキュリティ取組宣言の例: X 社は、電子機器メーカとして安定した製品供給が重要である。このため、生産ライン及び製品に対するセキュリティ確保が重要であり、組織的な対策推進を実施する。 • 目的:セキュリティ**脅威の**視点でのリスク評価に基づき実施目標を設定し、確実な実施と継続的な改善を図ることを目的とする。 • 方針:目的を実現するため、推進体制を整備するとともに必要な権限を委譲する。 • 体制:CEO 直下に **CISO 担当を置き、サイバー経営ガイドラインによる指示を自社内に適用するとともに、**推進組織を設置し、戦略的かつ全社統一的な視点で推進する。 • リスク評価:セキュリティ、業務継続、リスク対応の視点から総合的に実施する。 • **残存リスクへの対応:残存リスクにおいて財務、業績への著しい毀損の可能性がある場合は、サイバー保険への加入等によるリカバリ対策を実施する。** • 周知と教育・訓練:サプライチェーンの関係者に周知し遵守を徹底する。	いただいた御意見を踏まえ、「サイバーセキュリティ経営ガイドライン」の記載内容に合わせて修正いたします。 修正箇所:【参考】経営層による取組の宣言の例
021	99	企業	・該当箇所 P34 【参考】対策の深さ ・意見内容 まずは、対策の「深さ」を、「低、中、高」の語句で示していることに違和感があります。(「深い」が、「高い」)また、この直前までのP.32～33において、「セキュリティ要求レベル」を「低、中、高」で分類していたものに続いて、このP.34においても、同じ「低、中、高」としているため、あえて、それと関連付けて説明されようとしているのかも不明瞭です。	いただいた御意見のとおり、「対策の程度」に修正いたします。 修正箇所:【参考】対策の深さ
021	100	企業	・該当箇所 P34、P59など 付録への用語説明の追記。 ・意見内容 P34、P59など付録への用語説明の追記。(選定基準が分かっておりませんが)アクセスポート、CSIRT、CADA、物理アクセス制御、脆弱性情報、段取り掛け、高負荷攻撃、ファームウェア、外部記録媒体、ポータルメディア、可搬型の記憶デバイス、無線LAN、VLAN、社内LAN、無線LAN-APなど	いただいた御意見を踏まえ、付録への用語を追加し、修正いたします。 修正箇所:付録A　用語／略語

<table>
<tr>
<td>021</td>
<td>101</td>
<td>企業</td>
<td>・該当箇所
P38
3.1. ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理

・意見内容
表 3-21
想定脅威に対応するセキュリティ対策(例)の全体像　への追加。別紙3参照

・理由
保守会社を経由した侵入も充分あると考えますので、本項目を追加しました。

表 3-21 想定脅威に対応するセキュリティ対策(例)の全体像
<table>
<tr><th>No.</th><th>脅威種別</th><th>脅威内容</th><th>対策種別</th><th>対策内容</th></tr>
<tr><td>1</td><td rowspan="4">自然環境の脅威</td><td>大雨、洪水などによる浸水・漏水</td><td rowspan="2">(2)
物理面での対策</td><td>(2)①
建屋に関わる対策</td></tr>
<tr><td>2</td><td>有害生物の侵入</td></tr>
<tr><td>3</td><td>地震などによる機器の転倒・落下</td><td>(2)⑤
機器に関わる対策</td></tr>
<tr><td>4</td><td>落雷、洪水、地震などによる
停電・瞬断・電圧変動</td><td>(2)
物理面での対策</td><td>(1)②
電源／電気設備に関わる対策</td></tr>
<tr><td></td><td></td><td></td><td>(1)
システム構成面での対策</td><td>(1)②
機器における対策</td></tr>
<tr><td>5</td><td rowspan="4">不正侵入</td><td>ゾーン外からの物理的侵入</td><td>(2)
物理面での対策</td><td>(2)③
物理アクセス制御に関わる対策</td></tr>
<tr><td>6</td><td>ゾーン内での機器に対する
直接的な不正接続／アクセス</td><td>(2)
物理面での対策</td><td>(2)⑤
機器に関わる対策</td></tr>
<tr><td></td><td></td><td>(1)
システム構成面での対策</td><td>(1)②
機器における対策</td></tr>
<tr><td>7</td><td>ゾーン外からの
ネットワークを介した不正アクセス</td><td>(1)
システム構成面での対策</td><td>(1)①
ネットワークにおける対策</td></tr>
<tr><td></td><td>ゾーン外からの攻撃を受けた保守回線業者からの不正アクセス</td><td>(2)
業者との契約
システム構成面での対策</td><td>(1)①
ネットワークにおける対策</td></tr>
</table>
</td>
<td>いただいた御意見を踏まえ、修正いたします。
具体的には、保守会社等必ずしも攻撃者ではなく、攻撃を受けた組織から侵入を受ける場合もある点を考慮し、他の御意見も踏まえて脅威種別や脅威内容等を全体的に見直しいたします。
修正箇所：表3-14、表3-24</td>
</tr>
<tr>
<td>021</td>
<td>102</td>
<td>企業</td>
<td>・該当箇所
P41
「表3-22　運用支援」

・意見内容
セキュリティ対策活動として例えば”点検”を目的として従業員にウィルスメール対応訓練等を行う項目を追加してはどうか。

・理由
効果的な対策を具体的に示した方が分かり易い。</td>
<td>いただいた御意見を踏まえ、修正いたします。
ウイルスメール対応訓練は追記するが、システム構成面の対策ではないことから、表3-22ではなく、表3-35 維持・改善のために必要な活動（例）における「人材のスキル向上、育成」で記載。また、本文において、「周知・教育を定期的に行うことが望ましい。」の注記として、訓練を行うことで異変に気付けるようになることが望ましい旨について記載。
修正箇所：3.3.(1)②</td>
</tr>
<tr>
<td>021</td>
<td>103</td>
<td>企業</td>
<td>・該当箇所
P42
3.2.2. (1)

・意見内容
①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中段にある　・ゲートウェイ機器）の導入で、 “）”が残り、もしくは、語句が消えてる</td>
<td>いただいた御意見のとおり、「ゲートウェイの導入」に修正いたします。
なお、他の御意見を踏まえ「機器」は削除いたします。
修正箇所：3.2.2.(1)</td>
</tr>
<tr>
<td>021</td>
<td>104</td>
<td>企業</td>
<td>・該当箇所
P43
②機器におけるシステム構成面でのセキュリティ対策

・意見内容
端末・機器などの選定に対し、配慮すべき点があれば、記載が欲しい。</td>
<td>いただいた御意見を踏まえ、修正いたします。
具体的には、チェックリスト4-5の工場システム機器に対するセキュリティ基準として、注釈を記載いたします。
修正箇所：付録E　チェックリスト</td>
</tr>
</table>

021	105	企業	・該当箇所 P49 ・意見内容 ④水道設備に関わる対策　下から2行目の、上下水道だけではなく、⇒上水道だけではなく、の誤記と思われます	いただいた御意見のとおり、「上水道」に修正いたします。 修正箇所：3.2.2.(2)④
021	106	企業	・該当箇所 P50 脚注21, 表3-27 ・意見内容 “工作機器”は、”生産ラインの制御機器”とすべき。 （図3-4などに使われている用語を踏襲する。）	いただいた御意見のとおり、「生産ラインの制御機器」に修正いたします。 修正箇所：3.2.2.(2)④、表3-30
021	107	企業	・該当箇所 P52 【参考】入退管理の考え方 ・意見内容 「物理アクセス制御」の意味で「アクセス制御」という用語を使用している。付録Aの用語「アクセス制御」と意味が異なる。文書全体で統一した方が良い。	いただいた御意見のとおり、物理アクセス制御を意味する場合は「物理アクセス制御」に修正いたします。 修正箇所：【参考】入退管理の考え方
021	108	企業	・該当箇所 P55　表3-30, P61　表3-35 ・意見内容 表記揺れの修正。 “セキュリティ攻撃”は、“サイバー攻撃”とすべき。 （“サイバーセキュリティ攻撃”は除く。）	いただいた御意見のとおり、「サイバー攻撃」に修正いたします。 修正箇所：表3-33、表3-38
021	109	企業	・該当箇所 P58 3.3. ステップ 3 表 3-34 セキュリティ管理作業（例） ・意見内容 「ISMS等の情報管理ルール活用」という表現は適切か？ ・理由 ISMSが規定する範囲と差がある。	いただいた御意見を踏まえ、図書等の情報管理においてはISMSも活用可能であるため、「ISMS等の情報管理の考え方を活用したルール」に修正いたします。 修正箇所：表3-37
021	110	企業	・該当箇所 P59 3.3. 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） ・意見内容 【参考】運用管理体制（例）に以下分を追加 このため、運用・管理体制をどの程度のレベルで整備するかを検討する必要がある。この体制整備の例を提示する。 尚、運用体制は外部委託できるものの、管理体制を全て外部委託することは指示系統が行き届かなくなる可能性があり、すべきではない。本件を考慮しつつ体制を整備する。 ・理由 運用体制、管理体制はどこまで外部委託できるかという疑問を読者が頂く可能性があると思います。そこで、管理体制は全て外部委託できないことを記しました。	いただいた御意見を踏まえ、修正いたします。 具体的には、あくまでも管理責任は自社にあることに留意する点を追記いたします。 修正箇所：【参考】運用管理体制（例）

021	111	企業	・該当箇所 P60 3.3. ステップ3 ②維持・改善面のセキュリティ対策 ・意見内容 リスクベースで脆弱性を優先順位付けすることを加えると、より効果的ではないか。 KEV：既知の悪用された脆弱性 EPSS：脆弱性が悪用される可能性 ・理由 https://www.cisa.gov/binding-operational-directive-22-01https://www.first.org/epss/model	いただいた御意見を踏まえ、修正いたします。 具体的には、KEVやEPSSについて注釈に追記いたします。 修正箇所：3.3.(1)②
021	112	企業	・該当箇所 P61 3.3. ステップ3 表3-35 利用機器、及びソフトウェアの脆弱性情報の入手 ・意見内容 セキュリティ緩和策の提供を付記してはどうか。 ・理由 例えば、工場システムとの整合が取れているかの確認が必要。	いただいた御意見を踏まえ、修正いたします。 具体的には、緩和策の提供について追記いたします。 修正箇所：表3-38
021	113	企業	・該当箇所 P61 表3-35 維持・改善のために必要な活動（例） ・意見内容 表の最下段の「人材」に関する項目では、書かれているような「スキルの向上」や「教育、訓練」などは必要と思いますが、その一方で、せっかく構築したセキュリティ対策の運用上の煩わしさから、例えば、セキュリティキーを、現場の作業者間で使いまわす、あるいは、制御機器に差しっぱなしにするなど、実運用上のモラルが保たれていないと全く意味が無いので、そのような観点での「教育・しつけ」、あるいは、そのような運用を防止するシステムにまで到達しているかの、「定期的な監視、改善・見直し活動」なども重要になってくる、ことまで言及されてはどうでしょう。	いただいた御意見を踏まえ、修正いたします。 具体的には、「定期的な確認、改善・見直し活動」を追記いたします。 修正箇所：表3-38

021	114	企業	・該当箇所 P.61 ・意見内容 P.61に「セキュリティの基礎教育だけでなく、セキュリティ攻撃を発生させることによる模擬訓練を繰り返し実施する」とありますが、模擬訓練を実施するには社内の知識では乏しく、外部に頼らざるを得ない状況が大半と思います。しかしながら、信頼のできる外部業者、相場価格についても情報が少ないため、ある程度の指針があると助かります。	いただいた御意見を踏まえ、修正いたします。 具体的には、「模擬訓練」に注釈を加え、ICSCoE、CSSC、民間企業等でもプログラムを提供している旨を記載いたします。 修正箇所：表3-38
021	115	企業	・該当箇所 P63 表3-36 ・意見内容 クラウドサービスの記載あるが、もう少し踏み込んだ内容にして欲しい。 ・理由 クラウドサービス利用時の注意事項を一般論としてまとめて頂きたい。	いただいた御意見のとおり、修正いたします。 具体的には、クラウド関連の記載を追記いたします。 修正箇所：表3-39、コラム4
021	116	企業	・該当箇所 P64 ・意見内容 下請け事業者に対し、親事業者が複数存在する賃加工業者では、共通化が困難 ・理由 各親事業者が異なる対策を講じている事が考えられ、共通した対策が打てないと思われるから	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
021	117	企業	・該当箇所 P67 付録A　用語/略語 ・意見内容 用語/略語は、ガイドラインの前半（2項と3項の間）に移動した方が良いと考えます。 ・理由 用語/略語を理解したうえでガイドラインを読んだ方がよりわかり易いのではないかと考えました。一般的にJIS規格書もそのような構成になっています。	いただいた御意見を踏まえ、修正いたします。 具体的には、用語・略語がわからない場合は付録Aを読んでいただくよう追記いたします。 修正箇所：工場について知りたいこと
021	118	企業	・該当箇所 P67,P68 付録A ・意見内容 略語のみ記載され、説明がない項目がある。CPS、DCSなど想定読者は幅が広くレベルも様々、説明があったほうが親切。	いただいた御意見を踏まえ、修正いたします。 具体的には、説明を追記いたします。なお、DCS等、本文中にない用語は削除いたします。 修正箇所：付録A　用語／略語

021	119	企業	・該当箇所 P67～P73 付録A ・意見内容 本文中に参照されていない用語がある。(選定基準は？)DCS、オンライン操作、権限昇格攻撃、システム構成情報、実行モジュール、操作用表示端末、電子認証、踏み台攻撃、ポート番号、ユーザプログラム、エンジニアリングツール	いただいた御意見のとおり、修正いたします。 具体的には、本文中にない用語は削除いたします。 修正箇所：付録A　用語／略語
021	120	企業	・該当箇所 P67 付録A ・意見内容 IPS 侵入防止システム本文のP43表 3-23 ネットワークにおけるセキュリティ対策（例）では、「異常通信遮断(IPS)」の意味でもちいている。	いただいた御意見の通り、修正いたします。 具体的には、表3-26では、機能を記載した上で(　　)内に一般的な製品・システム名称を記載し、付録Aの説明としては原案の通りとさせていただきます。 修正箇所：表3-26
021	121	企業	・該当箇所 P68 付録A ・意見内容 アンドン カイゼンベース株式会社のホームページから引用されたのか。その場合は引用元を明記したほうが良い。https://kaizen-base.com/column/31481/	該当箇所につきましては、別の御意見に伴う本文の修正により、削除いたします。
021	122	企業	・該当箇所 P68 付録A ・意見内容 エンジニアチェーン 株式会社日立ソリューションズ東日本のホームページから引用されたのか。その場合は引用元を明記したほうが良い。https://www.hitachi-solutions-east.co.jp/products/ecm/outline/	いただいた御意見を踏まえ、修正いたします。 具体的には、「エンジニアリングチェーン」については経済産業省の文書から定義を記載いたします。 修正箇所：付録A　用語／略語
021	123	企業	・該当箇所 P69 付録A ・意見内容 完全性 本文中で「完全性[正常性]」と記載されている箇所が多い。統一してはどうか。クライアント、セグメント、トレーサビリティ、レシピ情報なども同様。	いただいた御意見のとおり、修正いたします。 具体的には、「完全性」については、本文においても表記を「完全性」に統一いたします。その他の用語についても統一いたしますが、レシピ情報は本文に記載がないため削除いたします。 修正箇所：付録A　用語／略語　他
021	124	企業	・該当箇所 P70 付録A ・意見内容 脆弱性 「コンピュータのハードウェアやプログラムにおける」とあるが、「プログラム」は「ソフトウェア」の方が良いのでは。	いただいた御意見を踏まえ、修正いたします。 具体的には、「脆弱性」については、IPAネットワークセキュリティ関連用語集から定義を記載いたします。その結果、該当箇所については削除いたします。 修正箇所：付録A　用語／略語
021	125	企業	・該当箇所 P70 付録A ・意見内容 ゾーンの説明 P34　表 3-19 各ゾーンのレベルに応じたセキュリティ対策例（主要対策のみを抜粋）では、物理的な区画もゾーンとしている。用語でも説明したほうが良い。(説明では「論理的な区画」とだけ書いてある。)	いただいた御意見を踏まえ、修正いたします。 具体的には、「ゾーン」の定義を修正し、本文に記載いたします。なお、「ゾーン」は、本ガイドラインにおいて定義した用語であるため、付録Aからは除外いたします。 修正箇所：付録A　用語／略語、2.6.

022	126	企業	・該当箇所 P71 付録A ・意見内容 バリューチェーン カオナビ人事用語集のホームページのホームページから引用されたのか。その場合は引用元を明記したほうが良い。 https://www.kaonavi.jp/dictionary/value_chain/	いただいた御意見を踏まえ、修正いたします。 具体的には、「バリューチェーン」については、各種資料を基に定義を記載いたします。 修正箇所：付録A　用語／略語
022	127	企業	・該当箇所 P72 付録A ・意見内容 ファイアウォール 本文中で、「ファイアウォール（アクセス制限）」や「ファイアウォール(FW)」と記載されている。統一したほうが良い	いただいた御意見を踏まえ、修正いたします。 具体的には、「ファイアウォール」に表記を統一し、「ファイアウォール（アクセス制御）機能」については「アクセス制御機能」に修正いたします。 修正箇所：付録A　用語／略語
022	128	企業	・該当箇所 P72 付録A ・意見内容 フリーアクセス 「フリーアクセスフロア」の説明になっている。	いただいた御意見のとおり、フリーアクセスの説明に修正いたします。 修正箇所：付録A　用語／略語
022	129	企業	・該当箇所 P77 B-1.2 ・意見内容 セキュリティリスクにおける評価、対策が主な内容であり、セキュリティインシデントの対応については既存文書が参考として記載されている程度になっています。インシデント対応についても本ガイドラインに必要な対応手順、フロー、注意事項を記載して頂ければと思います。	いただいた御意見を踏まえ、修正いたします。 具体的には、インシデント対応について追記いたします。 修正箇所：3.3.(1)①A）

022	130	企業	・該当箇所 P89 ・意見内容 (3) 経済産業省 IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF) 「社会的サポートも含めた4つの観点で、」は、図に合わせて、「セキュリティ・セーフティ要求の観点」と表現したほうが良いのでは。	いただいた御意見のとおり、修正いたします。 具体的には、「セキュリティ・セーフティ要求の観点」を追記いたします。 修正箇所:付録C　関係文書におけるセキュリティ対策の考え方
022	131	企業	・該当箇所 P90 表 C-3 ・意見内容 表 C-3 セキュリティ要求レベルと対比し、IEC 62443のレベルを利用した設定の例 レベルが1～3の3段階になっているが、P88「表 C-1　IEC 62443 におけるセキュリティレベル(脅威レベル)」ではレベル1～4の4段階である。合わせたほうがわかりやすいのでは。	いただいた御意見のとおり、修正いたします。 具体的には、IEC62443 セキュリティレベル3・4を、対応する要求レベルの「高」にいたします。 修正箇所:表C-3
022	132	企業	・該当箇所 P92 付録C 関係文書におけるセキュリティ対策レベルの考え方 表 C-8 マネジメントの成熟度を活用する例 ・意見内容 CMMIのレベルごとの「内容」は一般的か。レベル5は、繰り返し実施するので達成される状態を説明した方が良いのでは。	いただいた御意見のとおり、修正いたします。 具体的には、CMMIのレベル毎の内容について追記するとともに、レベル5について達成される状態を明示いたします。 修正箇所:表C-8
022	133	企業	・該当箇所 P92 表 C-7 ・意見内容 表 C-7　NISTのサイバーセキュリティフレームワークのレベルを活用する例 レベル1～4の内容を記載しているが、P89「表 C-2 NIST サイバーセキュリティフレームワークにおけるセキュリティレベル」のティア1～4と対応付けて表した方がわかりやすいのでは。	いただいた御意見のとおり、修正いたします。 具体的には、「表C-2 NISTサイバーセキュリティフレームワークにおけるセキュリティレベル」の記載を踏襲した表現に修正いたします。 修正箇所:表C-7
022	134	企業	・該当箇所 P93 「付録D 関連/参考資料」 ・意見内容 IEC62443やISO/SAE21434が記載されているが本文中の内容がそれら規格の何に準拠してるのかが記述してあると参考になると思う。 ・理由 これを実施すれば規格に沿った対策ができると理解できるから。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
022	135	企業	・該当箇所 P97 付録 E チェックリスト ・意見内容 チェックリストはよいと思うが、採点の 1～5 の判断基準が難しいと感じた。 ・理由 チェック項目の設問内容も複数の事項が記載あるので、もっと単純化して採点しやすくするといいと思う。	いただいた御意見を踏まえ、修正いたします。 具体的には、読者の状況に合わせて簡素化して用いるなどしてもよいとの旨を追記いたします。 修正箇所:付録E　チェックリスト

022	136	企業	・該当箇所 P97-100 「チェックリスト」 ・意見内容 ・チェックリストは便利であるが確認項目の内容が本文中に記載されておらずリンクしない。 ・参照欄の項目番号が荒すぎて該当部が探せない。 ・理由 チェックリストを実施するときに目的と方策がわからない。（何をどれぐらい）	いただいた御意見を踏まえ、修正いたします。 具体的には、チェックリストは具体的な対策をイメージし、実施状況を判断するためのものであるとの旨を追記し、本文とのリンクについては、番号に加えて見出しまで明示いたします。 修正箇所：付録E チェックリスト
022	137	企業	・該当箇所 P97 付録E チェックリスト ・意見内容 チェックリスト　2-6 「システム構成図が作成している。」は、「システム構成図が作成されている。」とした方が良い。	いただいた御意見のとおり、「システム構成図を作成している」に修正いたします。 修正箇所：付録E　チェックリスト
022	138	企業	・該当箇所 P102 付録E チェックリスト ・意見内容 例2：PLC の調達仕様書のセキュリティ要件指定の例を修正 X.X ペネトレーションテストの実施 公開されている脆弱性や攻撃手法に対し~~を用いたペネトレーションテストを実施し、~~必要都度、セキュリティリスクを低減するための緩和策を提示し、対策案を公開すること。 ・理由 調達時の要件として、設備は長期に渡る利用を考慮し調達時にペネトレーションテストよりも、利用し続ける上で、発見された脆弱性に対する緩和策の提供を受けることを条件としました。	いただいた御意見を踏まえ、修正いたします。 具体的には、当該箇所は調達仕様書の例として示したものなので、例はこのままとし、脆弱性の特定手法はペネトレーション以外にもある旨、及び調達後の利用時に、発見された脆弱性や攻撃手法に対する対策案や緩和策の提供を受けることも重要である旨を追記いたします。 修正箇所：付録F　調達仕様書テンプレート(記載例)
022	139	企業	・該当箇所 P103 コラム 1：工場セキュリティを巡る動向 ・意見内容 コラム 1：工場セキュリティを巡る動向は、ガイドラインの前半（1.1項）に移動した方が良いと考えます。 ・理由 初めに工場セキュリティを巡る動向を理解したうえでガイドラインを読んだ方がより理解が深まるのではないかと考えました。	いただいた御意見も参考に、修正いたします。 具体的には、工場セキュリティを巡る動向は参考の扱いとしますが、「工場セキュリティについて知りたいこと」における「工場セキュリティを巡る動向」についての記載を6項目目から3項目目に移動いたします。 修正箇所：工場セキュリティについて知りたいこと
022	140	企業	・該当箇所 P109 ・意見内容 コラム2 （1）工場システム自体の目的・機能、製品事業の伸張・継続、納期遵守から観たセキュリティ 「可用性確保(Availability)」となっているが、他と合わせると「可用性(Availability)」ではないか。コラム2(4)の「機密性確保(Confidentiality)」も同じ。コラム2(5)、およびP4の注釈の「真正性確保(Authenticity)」も同じ。P4の注釈の「責任追跡性確保(Accountability)」も同じ。	いただいた御意見のとおり、「可用性(Availability)」「機密性(Confidentiality)」「真正性(Authenticity)」「責任追跡性(Accountability)」に修正いたします。 修正箇所：1.1.、コラム2
022	141	企業	・該当箇所 P110 ・意見内容 コラム2 （5）製品のセキュリティ品質確保や製造責任から観たセキュリティ 「ソフトウェア」を「ソフトウェア(プログラム)」と記載しているが、「(プログラム)」は不要では。他の箇所では「ソフトウェア」としている。	いただいた御意見のとおり、修正いたします。 具体的には、「(プログラム)」を削除いたします。 修正箇所：コラム2

022	142	企業	・該当箇所 全般 ・意見内容 工場システムのセキュリティならば外来者に対するリスク管理として注意や規制を行う対策を加えて欲しい。 ・理由 入退場管理だけで良いのか疑問。	いただいた御意見を踏まえ、修正いたします。 具体的には、来訪者に対する注意や対策について追記いたします。 修正箇所：【参考】入退管理の考え方
022	143	企業	・該当箇所 全般 ・意見内容 本ガイドは大規模工場（ユーザ）向けで中小規模工場（ユーザ）はどこまで実施する必要があるのか判断できるか疑問。 ・理由 中小規模ユーザで最低限の対策をとるためには表３－２３や表３－２４が全て実施できるのか？	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
023	144	－	付録E チェックリストについて 以下の追記案を提案いたします。 3-6について、以下の追記を推奨します。 工場システムのリモートメンテナンスなどを目的とした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行っている。 運用的対策(システム関連等)について、以下のチェック項目も追加を推奨いたします。 工場システムで使われる組み込み機器(PLCやIoT機器など)のモデル情報、ファームウェア情報を把握し、関する最新の脆弱性情報を定期的に確認している。	いただいた御意見を踏まえ、修正いたします。 具体的には、チェックリスト3-6に「リモートユーザ毎の接続対象機器の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知」を追記いたします。また、2-8に、組込機器に関する脆弱性情報の定期的な確認について追記いたします。 修正箇所：付録E チェックリスト
024	145	企業	（1） ・該当箇所 全体 ・意見内容 今回策定いただいたガイドラインについては賛同いたします。JSSECでは、IoTセキュリティチェックシートを作成してOTとITの連携強化に努めており、このような活動が同ガイドラインの普及の一助になるものと考えております。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 以下、作成したチェックシートです。 https://www.jssec.org/dl/IoT_CheckSheet_ver2.1.pdf 併せて、P.81の業界、製品ごとのセキュリティ関連方針、ガイドライン等に本チェックシートも参考として追記いただければ幸いです。	いただいた御意見のとおり、修正いたします。 具体的には、表B-2に「IoTセキュリティチェックシート」を追加いたします。 修正箇所：表B-2
024	146	企業	（2） ・該当箇所 図1-1　製造業における事業所数・製造品出荷額等（2019年） ・意見内容 この図の説明が本文にないようで、唐突に出てきているようです。この図から読者に何が言いたいのかを本文に記載した方がいいと思います。	いただいた御意見のとおり、修正いたします。 具体的には、製造業も複数の業種に分けられており、出荷額や事業所数もそれぞれ異なっている旨を追記いたします。また、業種については一覧を別表でも提示いたします。 修正箇所：1.1.

024	147	企業	（3） ・該当箇所 P36の図3-4 要件に対する各ゾーンでの対策（例） ・意見内容 どのような対策をしたのかが分からないので、図の中に何の対策をしたのかを記載したらどうでしょうか？ 例えば、ゾーン間の通信制御、ログオン認証、入退室管理、ログ取得など前の表にある対策を図中に表現するとわかりやすくなると思います。	いただいた御意見のとおり、実施した対策について追記し、修正いたします。 修正箇所：図3-4

024	148	企業	（4）
			・該当箇所
			p.63: 表 3-36 取引先や調達先への主な確認ポイント（例）
			・意見内容
			- 「廃棄」に関する項目があると良い
			・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
			- 機器の「調達」については当該の表に記載があります
			- 同様に「廃棄」についても機器のライフサイクルの上で注意が必要な点と考えます
			- 廃棄時の注意点として以下があると考えます
			  - 個人情報・秘密情報などが漏えいするリスク
			
			参考情報: JSSEC IoTセキュリティチェックシート　第2.1版　解説編
			  - https://www.jssec.org/dl/IoT_CheckSheet_commentary_ver2.1.pdf
			  - Page-8: 12)IoT 機器の破棄や転売時に情報を読み出されるリスクを想定する
				いただいた御意見を踏まえ、修正いたします。
				具体的には、製品／部品購入時に廃棄時の情報漏えいリスクを考慮した取決めを実施しているか確認する旨を追記いたします。
				修正箇所：表3-39

024	149	企業	（5）
			・該当箇所
			p.6: 2.1. 想定企業 の 以下の箇条書き項目
			> 工場における有益な情報を見極めて収集し、状態を見える化し、得られた気付きを知見・ノウハウとして蓄積できている
			・意見内容
			- 当該項目はガイドラインの想定企業としては過大であるように見えます
			- 以下が明確であると良いと考えます
			  -（蓄積された知見の必要性）ガイドライン中で蓄積された知見がどの様に利用されているか
			  -（蓄積への道筋）前提として必要な場合、それを満たすための方法等が付録で紹介されると良い
			・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
			- 前提としている「蓄積された知見」がガイドライン中で参照されていないように見えます
			- 前提としては過大（それだけでDXに足を踏み入れている）ように見えます
				いただいた御意見については、本ガイドラインはDXが進む工場においても活用可能なものであるため、原案のとおりとさせていただきます。

024	150	企業	（6）
			・該当箇所
			p.103: コラム
			・意見内容
			- 以下のような代表事例に対して「ガイドラインがどのように寄与するか」の例示があると良い
			  - VPN機器の脆弱性を利用した事件
			  - https://www.jpcert.or.jp/newsflash/2020112701.html
			  - Mirai ボットネット
			  - https://www.jpcert.or.jp/at/2017/at170049.html
			  - マルウェア感染端末からの重要ネットワーク/情報へのアクセス
			  - JPCERT注意喚起(emotet)
			  - https://www.jpcert.or.jp/at/2022/at220006.html
			・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
			- 具体的なセキュリティに関する事件やニュースをトリガーとして参照される場合は多いと考えます
			- 事例への対応の例示はガイドライン利用のモチベーション向上につながると考えます
				いただいた御意見を踏まえ、修正いたします。
				具体的には、チェックリスト 2-8　脆弱性の特定と対応の注釈として、VPN機器の脆弱性を利用した事例と脆弱性への対応の重要性を記載いたします。
				修正箇所：付録E　チェックリスト
				
				なお、事例への対応についていただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

024	151	企業	（7） ・該当箇所 NIST CSFの表記について（p78, 93） ・意見内容 NIST Cyber Security Framework ⇒ NIST Cybersecurity Framework	いただいた御意見のとおり、「NIST Cybersecurity Framework」に修正いたします。 修正箇所：B-1.2(2)①、付録D　関連／参考資料

024	152	企業	（8） ・該当箇所 p76~77にて「重要インフラ」について記載されているので、 ・意見内容 6月17日にリリースされた「 重要インフラのサイバーセキュリティに係る行動計画 」についてp79の表（内閣サイバーセキュリティセンターの枠）に加えてもよいのではないか。 https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf	いただいた御意見のとおり、修正いたします。 具体的には、「重要インフラのサイバーセキュリティに係る行動計画」を追加いたします。 修正箇所：表B-1
025	153	個人	リモートアクセスについて P9図2-1　工場システムの例やP11図2-2　ゾーンの定義例等にありますとおり、ガイドライン現行案ではリモートアクセスは設備ベンダーの保守に限定されているように思われますが、社内ユーザーがHMIやMESサーバー、Historian等にリモートからアクセスすることも考えられます。 また、VPN装置兼Firewallといった従来のIT的なアプローチを想定しているようですが、OTならではのニーズもあるかと思われますので、そうしたニーズを整理して具体的な対策として盛り込むとより良くなるのでは、と思われます。 例えば、付録E　チェックリスト物理的対策3-6(P100)、3-7(P101)につきましては以下のとおり変更されることをご提案致します。 3-6:「工場システムのリモートメンテナンスなどを目的とした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）やネットワーク侵入防護（リモートユーザー毎の接続可能な端末の制限やメンテナンス期間外の機器への接続等　異常な行為の検知）などの保護対策を行っている。」 3-7:「工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知/防護システムを導入している。」 ご検討の程、何卒、宜しくお願い申し上げます。	いただいた御意見を踏まえ、修正いたします。 具体的には、3-6、3-7にそれぞれご指摘の点を追記いたします。 修正箇所：付録E　チェックリスト
―	154	企業	・該当箇所 内容 ・コメント 「内容」という見出しは、一般的には「目次」ではないかと思います。	いただいた御意見のとおり、「目次」に修正いたします。 修正箇所：目次
―	155	企業	・該当箇所 P1 ・コメント P1の表は、本書を読み進めるガイドとしてよいが、唐突感があるので、タイトルをつけるべきだと思います。	いただいた御意見のとおり、修正いたします。 具体的には、本ガイドラインを読み進めるガイドとして利用していただきたい旨を本文に追記いたします。 修正箇所：工場セキュリティについて知りたいこと
―	156	企業	・該当箇所 p4, P8 ・コメント セキュリティ要素の記載について P4の欄外[4]には、可用性、正常性[完全性]、真正性確保、機密性の4つがあげられており、責任追跡性はセキュリティ機能と記載されているが、P8では、真正性、責任追跡性がセキュリティ要素としてあげられている。この整合性を取るべきと思います。	いただいた御意見のとおり、修正いたします。 具体的には、真正性（Authenticity）を除いた3要素と、追加4要素を分けて記載いたします。 修正箇所：1.1.
―	157	企業	・該当箇所 P3, P106 ・コメント 統計情報の図は年度ごとに更新されるため、メンテナンスが大変なので載せない方がよいと思います。（P3、P106）	いただいた御意見を踏まえ、修正いたします。 具体的には、図1-1については、年度毎の変遷を示すことを目的としている訳ではないことから、グラフから読み取っていただきたい内容を本文に追記いたします。また、図0-5については削除し、意図を本文に記載いたします。 修正箇所：図1-1、コラム1

―	158	企業	・該当箇所 P18,P31 ・コメント 業務の重要度に関する記載について P18表3－6とP31表3－15に同じ例が異なる表現で二度記載されているため、どちらかにまとめるべきと思います。「また、重要度については、・・・こうした考え方も参照することが有効である。」という文章も重複しています。	いただいた御意見のとおり、修正いたします。 具体的には、業務の重要度についてはより一般化する形で、工場において重要とする価値の要素を広く捉えるよう修正いたします。 修正箇所：表3-18
―	159	企業	・該当箇所 2章　本ガイドラインの想定工場 付録 E チェックリスト ・コメント チェックリストの確認項目毎に、最低限実施すべき項目、実施を強く推奨する項目、実施することが好ましい項目などの対応レベルのガイドを合わせて示すべきと考えます。業界・業種によっては想定工場ほどDXが進んでいない場合も想定されるが、それでもセキュリティ対策は必要です。本ガイドラインは業界・業種の事情に応じたガイドラインを作成する際に参照すべきものと定義されているが、対応レベルをガイドとして示すことは事情に応じたセキュリティ対策を検討する際の考え方として大いに参考になると思います。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
―	160	企業	・該当箇所 P31～33 P59 P90 P91 ・コメント 【レベル】という言葉の使い方 ・P31【参考】に記載されているセキュリティ要求レベルと、付録Cのセキュリティ対策レベルについて、本書での考え方、例えば、いつ、どこで、だれが、これらのレベルを考える必要があるのかを示すべきと考えます。 ・表 3-19 各ゾーンのレベルに応じたセキュリティ対策例（主要対策のみを抜粋） ・このため、運用・管理体制をどの程度のレベルで整備するかを検討する必要がある。この体制整備の例を提示する。（P59） ・P90 ”セキュリティ対策レベル”、 ”セキュリティ要求レベル” の違い ・P90 ”運用のレベル” とは？ ・P91 ”(3) マネジメントのレベル例” マネジメントのレベルとは？	いただいた御意見のとおり、修正いたします。 具体的には、「レベル」という用語については、一般的な用語に修正するなどして整理いたします。 修正箇所：【参考】セキュリティ要求レベルの考え方の例、【参考】対策の程度、付録C 関係文書におけるセキュリティ対策レベルの考え方
―	161	企業	・該当箇所 3章 コラム3 ・コメント 拠点間の脅威・被害・対策への言及 2章で取り上げられている想定企業には「複数の拠点に工場が存在し、それぞれの拠点で製品を生産」となっていますが、3章では、その拠点間の脅威や被害拡大・その対策の記載が抜けていると思われます。 コラム３：スマート工場への流れ：表C3-4にそのリスクの例は確認できましたが、DXやスマートファクトリーを意識した記載となっているので、拠点間も意識を強めてもよいのかなと思いました。	いただいた御意見を踏まえ、修正いたします。 具体的には、3章全般で拠点間の脅威も含めて記載していますが、特に①において拠点間の脅威について追記いたします。 修正箇所：3.2.2.(1)①
―	162	企業	・該当箇所 P55 ・コメント 3.3. ステップ3　のタイトルにはPDCAサイクルの構築とあるのだが、次ページで突如OODAプロセスが紹介されており、この関係が不明なため、説明が必要と思います。	いただいた御意見を踏まえ、修正いたします。 具体的には、3.3冒頭で「PDCAサイクル」と明記するとともに、①運用・管理面のセキュリティ対策では「A） サイバー攻撃の早期認識と対処（OODAプロセス）」と記載し、OODAプロセスがサイバー攻撃の早期認識と対処である旨を明確化いたします。 修正箇所：3.3.
―	163	企業	・該当箇所 P62 ・コメント 中小企業の読者の受け取り方の視点 中小企業が対策を取らないと、大企業が被害を受ける、という記載よりも「大企業のサプライチェーンに関わる中小企業が狙われるケースが増加しているので、中小企業が自分たちを守るために」といった書き方の方が、ポジティブにとらえてもらえるのではないでしょうか。	いただいた御意見のとおり、中小企業が自分たちを守るためという書き方に修正いたします。 修正箇所：3.3.(2)

―	164	企業	・該当箇所 P77, P93 ・コメント IEC 62443の説明が2か所（P77とP93）出てきますが、説明内容が異なっているので、統一していただきたい。	いただいた御意見を踏まえ、修正いたします。 具体的には、IEC 62443に関する説明内容を統一するとともに、付録Dについては、本文より具体的に説明いたします。 修正箇所：付録D　関連／参考資料
―	165	企業	・該当箇所 P77 ・コメント IEC 61508は、代表的な安全規格ではあるが、本ガイドで言及する必要はないのではないでしょうか。	いただいた御意見については、IEC 61508が産業機器のリスク低減の観点で参照されることがあるため、原案のとおりとさせていただきます。
―	166	企業	・該当箇所 付録B-1.2　セキュリティに関わる標準規格・ガイドライン準拠の要求 ・コメント 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」と同様に「主要規格との対応関係」も示されることが好ましいと考えます。 企業がセキュリティ対策に対して説明責任を果たす際、主要規格への対応をエビデンスとすることは容易に想像できます。今後本ガイドラインの活用を促すためにも主要規格との対応関係を明確にすることは重要であり、さらに対応関係を示すことは業界・業種の事情に応じたセキュリティ対策を検討する際の考え方として大いに参考になると思います。 出展：サイバー・フィジカル・セキュリティ対策フレームワーク　添付D	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
―	167	企業	・該当箇所 付録 D ・コメント 付録Dに関連する国際標準規格やガイドライン、チェックリストが示されているが、本ガイドラインで示されている3ステップの考え方や手法が、これらの規格やガイドラインにどのように関連付けられているかを示していただきたい。理由は、No.13と同じ。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
―	168	企業	・該当箇所 付録 D ・コメント 付録Dは、参考文献として別出ししてはいかがでしょうか。本文中にも参考文献参照番号を付け、記載順も本文での参照順などにするとよいと思います。	いただいた御意見を踏まえ、修正いたします。 具体的には、付録Dに記載の観点に関する説明を追記いたします。 修正箇所：付録D　関連／参考資料
―	169	企業	・該当箇所 付録　E　チェックリスト ・コメント チェックリストは、ステップ3の「不断の見直し」によって定期的に実施すべきであるため、その旨明示的に記載した方が良いと思います。 「工場セキュリティの現状を”定期的に”チェックしていただきたい。」	いただいた御意見のとおり、「定期的に」を追記し、修正いたします。 修正箇所：付録E　チェックリスト
―	170	企業	・該当箇所 付録 E チェックリスト全般 ・コメント 「付録 E-1チェックリスト」にある「工場ネットワーク」の定義が記載されていないと思いますので記載が必要ではないでしょうか？例えば、「図2-1工場システムの例」に記載されている「情報系ネットワーク」まで含めて「工場ネットワーク」と認識する人もいれば、「設備系ネットワーク」のみと認識する人もいると思います。	いただいた御意見のとおり、修正いたします。 具体的には、工場ネットワークの定義について追記いたします。 修正箇所：付録E　チェックリスト
―	171	企業	・該当箇所 付録 E チェックリスト全般 ・コメント 「付録 E-1チェックリスト」にある「工場ネットワーク」と「工場内のネットワーク」と表現を変えているように見受けられますが、両者の定義の違いを記載した方が良いのではないでしょうか？また、「工場システム」と「工場内のシステム」と表現を使い分けているように思いますが、両者の定義の違いを記載した方が良いのではないでしょうか？	いただいた御意見のとおり、修正いたします。 具体的には、、「工場ネットワーク」、「工場内のネットワーク」、「工場システム」、「工場内のシステム」の定義について追記いたします。 修正箇所：付録E　チェックリスト

―	172	企業	・該当箇所 付録 E チェックリスト全般 ・コメント 「付録 E-1チェックリスト」にある、「物理的対策」の定義がないように思いますが、いかがでしょうか？なお、本カテゴリ内の、3-1や3-2、3-3、3-5(VLANが例だとシステム的対策かなと)、3-6、3-7,3-8については、一般的には「物理的な対策」ではなくシステム的な対策あるいは論理的な対策だと思うので、読者は混乱すると思います。 3-5~3-8の「参照」列に記載されている参照先が「3.2.2(1)システム構成面での対策」、となっており整合性が取れていないように見受けられます。	いただいた御意見を踏まえ、修正いたします。 具体的には、チェックリストは、具体的な実施事項をイメージし、対策ができているか確認するためのものなので、本文に挙げた対策項目を全て含めている訳ではないことに留意頂きつつ、「参照」列については、本文との整合性を取って修正いたします。 修正箇所：付録E　チェックリスト
―	173	企業	・該当箇所 付録E チェックリスト全般 ・コメント 3.1節～3.2節あたりのチェック項目がチェックリストにあると良いかと思います。 手法は3.1～3.2記載の方法でも良いし、他の手法でも良い。何かしらの方法で脅威･リスクを分析、優先度づけすることが現実的な対策実施につながるのかと思います。	いただいた御意見を踏まえ、修正いたします。 具体的には、3.1～3.2に記載のステップ1～2の内容をチェックリストに反映いたします。 修正箇所：付録E　チェックリスト
―	174	企業	・該当箇所 付録 E 2-3 ・コメント システム関連対策　2－3　に記載の「工場システムからの電子メールやインターネットアクセスはポリシによって禁止されている。」について、「工場システム」は図2－2の定義例では「OAゾーン」も含まれるため、この内容の実現は難しいのではないでしょうか。	いただいた御意見を踏まえ、「工場システム」を「工場内のシステム」に修正いたします。 修正箇所：付録E　チェックリスト
―	175	企業	・該当箇所 付録 E 2-6 ・コメント 「付録 E-1チェックリスト」にある2-6「システム構成図が作成している」は「システム構成図を作成している」ではないでしょうか？	いただいた御意見のとおり、「システム構成図を作成している」に修正いたします。 修正箇所：付録E　チェックリスト
―	176	企業	・該当箇所 付録E 2-9 ・コメント 「工場内に外部記録媒体（USBメモリ、フラッシュカード）やポータルメディアの利用・持ち込みを制限している。」は、現実的な内容でしょうか。制限とは禁止ということでしょうか。禁止はしないけどこういう条件下で利用すること、といった内容はいかがでしょうか。 工場にはネットワークにつながっていない古い機器もあるため、なんらかの更新、データの移行、USBメモリ型ウイルス対策ソフトの利用など、様々な要因でUSBメモリを利用することが考えられます。また、工場の敷地が広く出入口が複数ある場合、持ち込み確認をするのも困難です。	いただいた御意見を踏まえ、2-9については「利用・持ち込みに関するルールを定め、運用している。」に修正いたします。 修正箇所：付録E　チェックリスト
―	177	企業	・該当箇所 付録E 2-10 ・コメント 「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でしょうか。 NISTや総務省では推奨されていません。少なくとも総務省と経産省で方針が異なりますと、混乱するもとになるかと思われます。	いただいた御意見を踏まえ、修正いたします。 具体的には、パスワードの設定は状況により適切な設定方法が異なるため、「パスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。」に修正いたします。 修正箇所：付録E　チェックリスト
―	178	企業	・該当箇所 付録 E 2-13 ・コメント バックアップしたデータの保護に対する言及 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。 復旧テスト・手順は確かに大事なポイントですが、昨今のランサム被害の事例からバックアップデータの保護も入れた方がよいと思いました。	いただいた御意見のとおり、修正いたします。 具体的には、2-13に「バックアップデータは保護された場所に格納するとともに、」を追記いたします。 修正箇所：付録E　チェックリスト
―	179	企業	・該当箇所 付録 E 3-1 ・コメント 「ホワイトリスト」という表現がありますが、差別用語と捉えられるリスクがあるため、「許可リスト」のような表現に見直してはいかがでしょうか？	いただいた御意見のとおり、修正いたします。 3-1のホワイトリストに「（許可リスト）」を追記いたします。 修正箇所：付録E　チェックリスト

―	180	企業	・該当箇所 付録 E 3-3 ・コメント 「付録 E-1チェックリスト」に「制御端末の」とありますが、「OA端末」は対象外なのでしょうか？	いただいた御意見を踏まえ、修正いたします。 具体的には、「制御端末の」は、全ての端末に適用するのは困難である可能性も考慮し、重要な端末の特定を意図したものですが、OA端末を対象外とするものではないため、「制御」を削除いたします。 修正箇所：付録E　チェックリスト
―	181	企業	・該当箇所 付録 E 4-2 ・コメント 「付録 E-1チェックリスト」にある、「工場システムセキュリティのメンテナンス等」とはどういう意味でしょうか？また、協力会社の人に「工場システムセキュリティのメンテナンス等」に関するセキュリティ教育をするという意味ですか？	いただいた御意見については、工場システムの保守・運用を行う際に、協力会社にセキュリティに関する教育を行うことを想定したもので、原案のとおりとさせていただきます。
026	182	企業	Society5.0では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを 構成することが可能ですが、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要となっております。 昨今、工場においても、国内外でのサイバー攻撃による被害が生じており、工場におけるサイバーセキュリティ対策が必要不可欠になっていることから、御省において、本ガイドライン(案)を取り纏められ、意見募集を行われたことは誠に時期を得たものであります。 弊社としては、今般のお取り組みに賛同致しますとともに、以下の意見を提出させて頂きます。 (1) ＜該当箇所＞ P.2 1.1 工場セキュリティガイドラインの目的また、一般低に、製造業/工場では ＜意見＞ 記載する順番を安全確保と事業/生産継続を変更してはいかがでしょうか。 安全確保(S:Safety) 事業/生産継続(BC:Business Continuity) 品質確保(Q:Quality) 納期遵守・遅延防止(D:Delivery) コスト低減(C:Cost) ＜理由＞ いかなる事業環境でも事業より人命優先という考え方が重要であり、記載順序の変更した方が良いのではないかと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、「安全確保」と「事業/生産継続」の記載順序を変更いたします。 修正箇所：1.1.
026	183	企業	(2) ＜該当箇所＞ P.2　1.1 工場セキュリティガイドラインの目的また、一般低に、製造業/工場では ＜意見＞ 記載内容にプライバシー要件を追加してはいかがでしょうか。 安全確保(S:Safety) プライバシー(P:Privacy) 事業／生産継続(BC:Business Continuity) 品質確保(Q:Quality) 納期遵守・遅延防止(D:Delivery) コスト低減(C:Cost) ＜理由＞ 製造業/工場では顧客ごとにカスタマイズした生産形態に対応している企業も増加しているように見受けられます。そのため、事務系IT環境で取得したプライバシーが含まれたデータを工場環境へデータ連携していく際、プライバシー要件を配慮していく必要があると考えます。 日本国内外問わずプライバシー要件が注目されています。対象範囲は生産現場におけるグローバルサプライチェーンとして考える必要があると思いますので、プライバシー要件の追加することが望ましいと考えます。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

026	184	企業	(3) ＜該当箇所＞ P.3 1.1 工場セキュリティガイドラインの目的 ＜意見＞ 3つのセキュリティ対策の必要性が記載されていますが、以下の内容を追加するのはいかがでしょうか。 例：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。 ＜理由＞ 工場等の製造現場の特徴として3つ例示されていますが、工場DX（デジタルトランスフォーメーション）の取組が推進されている企業が増えてきていることから、独自または組込型のハードウェアによる製造現場環境から、5Gやソフトウェアを採用する製造現場に環境が変化することが予想されます。また、クラウド環境やサプライヤーのシステムをインターネット等を通じて接続することも想定されます。そのため、ソフトウェアやクラウドが導入されていく製造環境、サプライラーと連携した製造環境に必要なセキュリティ対策の必要性を追加することが望ましいと考えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、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の必要性について追記いたします。 修正箇所：1.1.
026	185	企業	(4) ＜該当箇所＞ P.5 1.2. ガイドラインの適用範囲 ＜意見＞ 脚注5、6は重要なところなので、本文にて丁寧に説明し、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と考えます。 ＜理由＞ 工場システムのセキュリティ対策が進まない要因として、経営層の理解がないことや、部門間・担当間の立場や価値観の違いなどの摺合せができていないことなどにあると考えます。 例えば、事業/生産継続に対してサイバー攻撃によるインシデントの影響は直結している認識で、本ガイドラインを理解されることが望ましいと考えるため。	いただいた御意見のとおり、修正いたします。 具体的には、脚注5、6を本文に移動し、経営層及び部門間のコミュニケーションの重要性を明記いたします。 修正箇所：1.2.
026	186	企業	(5) ＜該当箇所＞ P.7 2.2想定組織構成 ＜意見＞ 生産技術・管理部門は設備系ネットワークを、情報システム部門は情報系・生産管理系ネットワークを管理していると思いますが、具体的に記載したほうが分かりやすくなると思います。 ＜理由＞ 図2-1をみるまでパソコンやサーバなど情報システム部門が全てを管理しているように誤認識したため。	いただいた御意見のとおり、修正いたします。 具体的には、各部門が管理する対象となるネットワークを追記いたします。 修正箇所：2.2.
026	187	企業	(6) ＜該当箇所＞ P.8 図2-1 工場システムの例図 ＜意見＞ ISA95等のリファレンスに沿った図に変更したほうが望ましい。 ＜理由＞ 想定した工場であるものの、構成は一般的に例示されたもののほうが、読み替えの助けになり共通認識を持つのが容易になると考えます。	いただいた御意見については、本ガイドラインでは、想定工場のシステムに関するモデルを元にリスク分析を行うのではなく、業務や保護対象の重要性を踏まえたゾーンを設定してリスク分析を行う手法を提示していることから、原案のとおりとさせていただきます。
026	188	企業	(7) ＜該当箇所＞ P.15 業務（想定工場における例） ＜意見＞ リモートメンテナンスの実施者に生産技術・管理部門を加えてはいかがでしょうか。 ＜理由＞ 想定の例ですが、セキュリティ対策としては、生産技術・管理部門が主体となることが望ましいと考えます。	いただいた御意見のとおり、修正いたします。 具体的には、リモートメンテナンスの実施者に生産技術・管理部門を追加いたします。 修正箇所：表3-8

026	189	企業	(8) ＜該当箇所＞ P.24 表3-11 一般的な脅威と生産への影響（例） ＜意見＞ 従業員の過失に加え、保守要員（設備ベンダ）のリスクについても記載するほうが望ましいと考えられます。 ＜理由＞ 保守作業あるいは環境による事故発生リスクが、従業員の過失よりも懸念されます。「工場内部の過失・不正」の記載があります、同意であったとしても、従業員と保守要員は別機能のため、明記にしたほうが望ましいと考えます。	いただいた御意見のとおり、「従業員の過失」を「従業員、保守要員（設備ベンダ）の過失」に修正いたします。 修正箇所：表3-14、表3-24
026	190	企業	(9) ＜該当箇所＞ P.24 表3-11 一般的な脅威と生産への影響（例） ＜意見＞ 脅威種別　不正侵入の脅威内容に、「ゾーン外からのネットワークを介した不正アクセス」とありますが、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と考えられます。 ＜理由＞ 標的型攻撃等による、外部に出ようとする不正通信（バックドア通信/コネクトバック通信）の脅威を示すため ※P34の活動抑止に「他ゾーンへの通信」とあるのでそれに対応する形で示されていると理解の助けになると考えられます。	いただいた御意見のとおり、外部から内部のみならず、内部から外部への不正通信を想定した記載に修正いたします。 修正箇所：表3-14
026	191	企業	(10) ＜該当箇所＞ P.34 表3-19 各ゾーンのレベルに応じたセキュリティ対策例（主要対策のみを抜粋） ＜意見＞ 以下3点の修正をご提案いたします。 ・区分の侵入防止を「侵入防止・異常検知」にする。 ・要件を「外部ネットワークからの侵入防止」を修正し、「ネットワークにおける侵入防止・異常検知」とする。 ・高に「産業ネットワークの可視化」を入れる。 ＜理由＞ ICS固有のシステムやネットワークプロトコルに対する資産管理や脅威発生に気づく仕組みが必要と考えられます。	いただいた御意見を踏まえ、修正いたします。 具体的には、異常検知については「運用支援」に含まれるため、ご指摘の1点目・2点目については現状のまま、3点目の「工場内のネットワークの可視化」については、「アラート監視」の高に追加いたします。 修正箇所：表3-22
026	192	企業	(11) ＜該当箇所＞ P.38 表3-21 想定脅威に対するセキュリティ対策（例）の全体像 No.6 ＜意見＞ システム構成面での対策で「ネットワークにおける対策」を追加することが望ましいと考えられます。 ＜理由＞ 上記ICSセキュリティを想定した対策を明示した方が良いと考えられます。	いただいた御意見のとおり、「システム構成面での対策」に「ネットワークにおける対策」を追加し、修正いたします。 修正箇所：表3-24
026	193	企業	(12) ＜該当箇所＞ P.41 表3-22 システム構成面のセキュリティ対策の目的概要No.7 ＜意見＞ 検知のところを「異常検知」としたほうが望ましいと考えられます。 ＜理由＞ 不正か否かがわからないことも想定され、何を目的とするか明確にするため「異常」という言葉を用いるのが適切と考えられます。	いただいた御意見のとおり、「検知」を「異常検知」に修正いたします。 修正箇所：表3-25
026	194	企業	(13) ＜該当箇所＞ P.42　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 ＜意見＞ ネットワークにおける対策として「想定外・異常通信が発生していないこと」を3つ目の目的として記載することが望ましいと考えます。また「産業ネットワークの可視化・異常検知」を考えられる実施策として追加することが望ましいと考えます。 ＜理由＞ ICSセキュリティでは、インターネットプロトコル以外の産業制御用プロトコルなど、記載のような通常のセキュリティ製品では検知が困難な通信が流れているため、これら通信に異常が起きた場合の脅威を把握することは困難です。よって、侵入防止だけでなく、異常検知を目的とする機能を実装する必要があると考えられます。	いただいた御意見を踏まえ、修正いたします。 具体的には、「想定外・異常通信が発生していないこと」を3つ目の目的として記載するとともに、表3-26の「通信状況可視化・監視」と整合を取った実施策を本文に記載いたします。 修正箇所：3.2.2.(1)①、表3-26

026	195	企業	(14) ＜該当箇所＞ P.52【参考】入退管理の考え方 ＜意見＞ 個人認証を必須とし（単なる携帯カード識別ではなく）、また、その認証と端末へのアクセス認証、敷地内での位置の把握まで連動することが望ましいと考えられます。 ＜理由＞ 重要な点は入退室管理ではなく、「誰がどこで何をした」かであると考えるため。 一般的な執務環境での実装は困難かもしれないが、工場等の専用設備であれば可能と考えます。	いただいた御意見のとおり、「～連動することが望ましい」と追記し、修正いたします。 修正箇所：【参考】入退管理の考え方
026	196	企業	(15) ＜該当箇所＞ P.59 C) 情報共有 ＜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など課題を明記してはいかがでしょうか。 ＜理由＞ OT環境に影響を与えるのは生産管理等の工場内でのOA環境が中心に議論されるケースが多いですが、保守リスクの観点でいえば、産業機械側の直接的なリスク（あるいは産業機械間のネットワーク上のリスク）の方が懸念され、その脅威情報は国内ではほぼ見受けられません。サプライチェーン先にこれを求めるのは現実的ではないと考えられます。	いただいた御意見のとおり、修正いたします。 具体的には、情報共有の課題を追記するとともに、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や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を追記いたします。 修正箇所：・3.3.(1)①C）
027	197	個人	・表 3-23 ネットワークにおけるセキュリティ対策（例）P43 ・付録E チェックリスト 技術的対策 3-6 利用者制限の対策として、多要素認証の記載はありますが、ユーザーの信頼性の担保だけでなく、デバイスの健全性(サイバーハイジーン)も確認した上で、アクセスを許可すべきなので、デバイスの検疫、信頼性担保をするという対策項目として追加すべきです。 対策をしないと例えば個人所有のデバイスや許可をされていないデバイスでアクセスされる可能性もあるので、マルウェア感染リスクや、情報漏洩のリスクが高まります。	いただいた御意見のとおり、修正いたします。 具体的には、接続機器の健全性の確保について、表に注記いたします。 修正箇所：付録E　チェックリスト、表3-26
028	198	個人	＜意見1＞ P.13, 14 > ステップ 1-6 ゾーンの整理と、ゾーンと業務、保護対象の結びつけ > ステップ 1-7 ゾーンと、セキュリティ脅威の影響の整理【3.1.6】 ステップ1-6, 1-7の2つのステップはあくまでゾーンとしてエリアを分割した場合でのステップに過ぎず、別の言葉で定義すべき。 理由としては、保護対象とセキュリティレベルを定義していく際、一様にゾーンという言葉で広く定義するのは現状の複雑な工場システムを考慮すると難しいと考えられる。	いただいた御意見については、業務や保護対象の重要性を踏まえたゾーンを設定してリスク分析を行う手法を提示していることから、原案のとおりとさせていただきます。
028	199	個人	＜意見2＞ P.15 > 表 3-1 セキュリティ対策を検討・企画する際に考慮すべき経営目標事項（想定工場における例） 各表の例に対して、各企業の工場は異なる部分も多く、本資料内の内容は想定工場における例として特殊であるため、例として提示するのは構成として不適当であると考える。 もしくは、提示するのならばより詳細に記載したほうがイメージとしては持ちやすいと考える。 例のイメージが先行してしまい実際に検討する場合「何を注意して考えればいいのか」といったような要素も含めてフレームワークとして提供すべきではないかと考える。	いただいた御意見を踏まえ、修正いたします。 具体的には、想定工場の事例を書くのみではなく、どのような要素を考慮すべき事項として考えればよいかについて、その考え方やプロセス・道筋がわかるように表3-1、表3-3、表3-5の各表を追加いたします。 修正箇所：表3-1、表3-3、表3-5

029	200	企業	初めに、このようなガイドライン策定の取り組みに深く感謝致します。生産現場におけるセキュリティの確保が急務であるにも関わらずその具体的な方法に戸惑う企業は数多くあり、こうしたガイドラインが大きな助けになることは間違いありません。ありがとうございます。 こちらにて、シスコシステムズ合同会社従業員有志の意見を取りまとめてコメントいたします。従業員有志の意見であり、シスコシステムズ合同会社を代表するものではないことを申し添えておきます。 1.1 工場セキュリティガイドラインの目的 本ガイドラインの動機づけとして、生産システムがサイバー攻撃者からみて比較的脆弱で攻撃し易い対象であるという点を主たる動機付けにすると良いのではないでしょうか。案の記述ではインターネット接続の機会拡大が主たる動機付けとされていますが、これは俗に「エアギャップ神話」と呼ばれる誤解に呼応しており、この誤解を補強してしまいかねないと考えます。言い換えると、読者に「インターネットに繋がないのならばこのガイドラインは自分には無関係なのだ」と誤読させてしまう可能性を心配しております。繋がなくても危険はありガイドラインに従った対策をすべきであるとの認識を明瞭に示し、必要とされる全ての方に届くように記述を改善できるのではないでしょうか。	いただいた御意見のとおり、修正いたします。 具体的には、従来の工場システムが脆弱である点、インターネット接続の機会拡大に限らず、ネットワーク接続やDXの進展、サプライチェーンの拡大、サイバー攻撃の高度化/一般化等、様々な観点で工場システムのセキュリティ対策の必要性について記載いたします。 修正箇所：1.1.
029	201	企業	2. 本ガイドラインの想定工場（1/3） 具体的な想定工場の設定と同時に抽象的な論理モデルも定義したほうが良いのではないでしょうか。想定工場を定義することは、読者が具体的なイメージを描き易くなる点で優れており、このアプローチ自体には賛同いたします。心配なのは、想定工場とは異なる工場を持つ読者が自社工場へどのように当てはめて良いか戸惑ったり、自社には無関係なガイドラインであると誤解してしまったりする可能性です。 そこで、論理モデルとしてPurdue Modelを導入すると良いのではないでしょうか。Purdue Modelは広く認知され参照されており、市場にある各種のセキュリティ製品・ソリューションもPurdue Modelに基づいてあるいは念頭に設計されているものが多くあります。Purdue Modelを抽象モデルとし、その具体例を想定工場で示すことで、読者が抽象モデルを自社工場へ当てはめたり想定工場を自社工場へ読み替えたりする上での助けになるのではないかと考えます。 論理モデルにPurdue Modelを導入すると、想定工場でのゾーン分けもこれに基づくレベル分けにした方がより良くなるのではないでしょうか。そのようにすれば、論理モデルと具体例である想定工場との対応が理解し易くなります。すると、想定工場と異なる工場を持つ読者でもモデルと想定工場の対応を参考にモデルと自社工場の対応関係を自力で読み取ることができるようになると考えます。このようにすることでガイドラインをより多くの工場で活用しやすい、より有用なものにできるのではないでしょうか。	いただいた御意見については、本ガイドラインでは、想定工場のシステムに関するモデルを元にリスク分析を行うのではなく、業務や保護対象の重要性を踏まえたゾーンを設定してリスク分析を行う手法を提示していることから、原案のとおりとさせていただきます。
029	202	企業	2. 本ガイドラインの想定工場（2/3） 上と異なる観点からのコメントです。 ガイドラインの中に、ローカルブレイクアウトを行う場合の指針が盛り込まれていると良いのではないでしょうか。クラウド利用が進むと、大容量通信の需要が増し、コスト低減圧力が高まります。従来は工場からインターネットを利用する場合には企業のデータセンターを経由して中央からブレークアウトしていた企業が、強い大容量通信需要に応えるために、安価なインターネット接続サービスを直接工場に引き込む、いわゆるローカルブレークアウトを導入し始めています。安易なローカルブレークアウトはセキュリティを損ないます。一方でセキュリティ対策が決まらないからといってローカルブレークアウトを戸惑うことは、生産性の向上ひいては工場の競争力を削ぐことにもつながります。本ガイドラインがローカルブレイクアウトに関しても指針を提供することで、ガイドラインの有用性がますます高まるのではないでしょうか。	いただいた御意見を踏まえ、修正いたします。具体的には、ローカルブレイクアウトについて記載いたします。 修正箇所：コラム4
029	203	企業	2. 本ガイドラインの想定工場（3/3） 上の二点とはまた異なる観点からのコメントです。 ベンダーによるメインテナンス等を目的としたリモートアクセスに関しては企業ガバナンスの観点をガイドラインに取り入れると良いのではないでしょうか。このようなリモートアクセスの需要はますます高まっています。また、多くの設備ベンダーがリモートアクセスに留まらず設備を常時クラウドに接続することでもたらされる付加価値を訴求するようになってきています。従って、設備と設備ベンダーが提供するクラウドサービスとの間のリモートアクセスを含む接続に対する統治は今後ますます必要になってきます。案では、このような通信の統治についてもっと深い検討の余地があるように見えます。	いただいた御意見を踏まえ、修正いたします。 具体的には、企業における通信の統治について脚注にて追記いたします。 修正箇所：コラム4
029	204	企業	3. セキュリティ対策企画・導入の進め方 セキュリティ対策は継続的永続的なものであり、それを妥当なコストで実現する必要があるという観点を主軸にすると良いのではないでしょうか。案ではステップ 3 がサイクルとなることや変化に応じてステップ 1 に戻ることが確かに言及されてはいます。しかし、その記述はそれほど強調されていません。全体として読んだとき、セキュリティ対策を単発のプロジェクトとして実行する事柄であるかのように誤読されてしまうのではないかと心配しております。基本方針の策定等を頻繁に繰り返す必要はありませんが、実行段階は継続的なものになっていなくてはならないことはもっと強調されても良いのではないでしょうか。	いただいた御意見のとおり、修正いたします。 具体的には、継続的にサイクルを回す重要性を記載いたします。 修正箇所：3.

029	205	企業	3.1.4. ステップ 1-4:保護対象の整理 保護対象の整理に始まる、保護対象を把握する一連のステップは、保護対象をカテゴリーに分けて整理する段階ではステップ1のような上流工程で行うのが適切と思いますが、個々の保護対象個体を整理把握する段階は後段の継続的実行段階に組み入れた方が良いのではないでしょうか。 工場は生産性向上や安全性向上を継続的に希求するがゆえ、常に変化しています。また大企業では絶えず生産ラインの新設と解体、あるいは生産する製品の変更のための組み替えが行われています。従って常に保護対象が増減します。工場はmoving targetなのです。 ステップ1の保護対象の整理からの一連のステップを、カテゴリーではなく個々の保護対象を把握整理することと読者が誤読してしまうのではないかと心配しております。ここを誤読した場合、保護対象の整理を一種の棚卸しプロジェクト的に人手と手間をかけて実行してしまう可能性があります。そうすると、コストがかかり過ぎて保護対象個体の把握を継続的に実行できなくなり、帳簿上の保護対象と工場の実態が乖離してしまいます。 常に変化する工場の実態を継続的にかつ妥当なコストで掌握し続けなくては、セキュリティ対策が実態から乖離してしまうということを読者にはっきりと示す必要があるのではないでしょうか。 そのようなことを実行するためには、自動的かつ継続的に保護対象を検出・認知・追跡する何らかの自動化されたシステムを持つ必要があるということが自ずと導かれます。ガイドラインでその具体的方法にまで言及する必要はないかも知れません。しかし、人手による棚卸しのようなことでは変化する工場の実態について行けないという点を読者に認識してもらうことは大切なのではないかと思います。 最後に、このような取り組みに改めて深く感謝申し上げると共に、この取り組みが実を結び日本の産業により良いセキュリティと競争力がもたらされる事を心より願っております。	いただいた御意見を踏まえ、修正いたします。 常に変化する環境を踏まえて必要に応じて見直しをすることを自動化等のツールも活用しつつ、行うことを追記いたします。 修正箇所：3.1.4.