「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【別冊：スマート化を進める上でのポイント】（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

本件の改正に直接関係しない御意見につきましては、個別の回答はお示ししておりませんが、貴重な御意見として承っております。
皆様の御協力に厚く御礼申し上げます。

提出No.	No.	提出者	提出意見	提出意見に対する考え方
001	1	企業	1. PDFで公開されているが、少なくてもしおり付きPDFにして電子的な可読性を確保すべきではないか。特に本書はDXを推進するために記載されたものであり、デジタルリテラシが高い方々が作成され、お手本となるようなデジタルでの提供が望まれる。さらに利活用を考えるとWord, Excelなどの編集可能なデータも有効になるのではないかと思われます。	いただいた御意見のとおり、修正いたします。 修正箇所：全体
001	2	企業	2. 1.2に「に工場のスマート化を進めている、もしくは検討している企業における？」と記載されています。しかし、公用文、法文等では、“又は”、“若しくは“等の使い方がルール化されている。階層がひとつの場合のorは、”もしくは”ではなく、“又は”を使うべき。	いただいた御意見のとおり、修正いたします。 修正箇所：1.2
001	3	企業	3. P5 2.1.1において「フィジカル空間とサイバー空間との結びつきが強くなり、その結果セキュリティリスクも上がると考えられることから、リスクに応じて適切なセキュリティ対策を行うことが重要である。」と記載されている。言いたいことは理解できますが、これだとスマート化によりリスクが増加し、それにより実施すべき対策も増えて、費用も増加するようにも読めてしまう。実施すべき対策もスマート化を意識したDXを考慮する必要がある。工場の(狭義の)スマート化とともに、そのセキュリティ対策もスマート化することにより、対策後のリスクを減少させることが必要だと考えます。スマート化とセキュリティ対策とを分けて説明しているが、両方を平行で進めていく必要がある。	いただいた御意見について、セキュリティ対策の見直しについても本文に触れているため、原案の通りとさせていただきます。また、セキュリティ対策のスマート化を達成するためには、新たなコストを負担する必要があるため、原案の通りとさせていただきます。
001	4	企業	4. P5 2.1.2において「外部ネットワーク接続の増加」と記載されている。その中の説明でもあるように「制御システムと情報システムとの接続の増加」も明記したほうがいいのではないかと思います。さらに、「工場システムが攻撃を受けるリスク」の増加だけではなく、工場システムを経由して情報システムが攻撃を受けるリスクの増加も十分検討していく必要がある。工場システムのセキュリティは、情報システムのセキュリティのセキュリティに比べて一般的に低い。このため、情報セキュリティシステムが、工場(制御)システムを経由して攻撃されるリスクを対策する必要がある。	いただいた御意見を踏まえて、工場システムを通じて接続するシステムが影響を受ける可能性についても追記いたします。 修正箇所：2.1.2
001	5	企業	5. P5 2.1.2「サプライチェーンの広がり」において、「自社で管理できない内容が増える可能性が高く」と記載されている。原理的にはサプライチェーンにおいてもそれを*管理*することは必要です。このため表現を「管理できない」ではなく、「直接的に管理できない又は困難な」とかにしたほうが誤解を招きにくいのかと思います。購入した外部機器などは、管理できないのではなく、管理しなくてはいけない。または、「自社のみで管理できない」として責任分界や役割分担が必要であることをここでも示す。	いただいた御意見のとおり、修正いたします。 修正箇所：2.1.2、2.1.3
001	6	企業	6. P6表2.1において「無線LAN 等の通信機能の利用」が「外部ネットワーク接続のリスク拡大」となっている。しかし、表の一番下の行が「外部システムとの連携」なので、この関係がわかりにくい。「外部ネットワーク接続のリスク拡大」の「外部」をとって「無線によるネットワーク接続のリスク拡大」にしたほうがいいのでは。	いただいた御意見については、通信機能として無線LAN以外に5Gなども想定しているため、「外部ネットワーク接続のリスク拡大」については、原案の通りとさせていただき、通信機能に5Gも含まれていることを明記いたします。 修正箇所：表2-1

001	7	企業	7. P7「※ゾーンとは、業務の内容・重要度や設備環境など個社に応じて設定する領域を示す。」と記載されているが、「個社に応じて」が修飾する言葉は、「設定する領域」ではなく、「業務に内容・重要度」にして、「※ゾーンとは、個社の業務内容・重要度や設備環境などに応じて設定する領域を示す。」と変更してはどうか。	いただいた御意見を踏まえて、修正いたします。 修正箇所：2.1.3
001	8	企業	8. P7「ゾーンは、物理・サイバーが融合している場合もある。」と記載されている。物理とサイバーとが同一のゾーンもあれば、サイバーのゾーンが物理と異なっている場合もある。特に前者はイメージしやすいが、後者はイメージしにくい。特に物理のゾーンとサイバーのゾーンとをそれぞれをどのように考え分離していくかの記載があると非常に役立つのではないかと考えます。	いただいた御意見については、図3-2における視点の1つとして記載しています。本文中においてもこちらの視点を明記いたします。 修正箇所：3.1.6
001	9	企業	9. P8 3.1.1がある状態で、3.1の直下に文章を記載することをぶら下がり段落といい、JIS(日本産業規格)では禁止されている文書構成になっている。本書はJISではないので、それに従う必然はないですが、JISはISO/IECを元に世界的に誤解を招かない記載方法等として、それを禁止している主旨に鑑みると、それに準じた記載にしたほうがいいのではないかとおもいます。それ以降の章も同様。	いただいた御意見については、「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」（ガイドライン本編）も同様の文書構成であるため、原案のとおりとさせていただきます。
001	10	企業	10. P11 スマート化を進める上でのポイントとして「業界動向の確認」と記載されている。少し表現が誤解す業界も存在するのかと思います。例えば、「医療機器業界」は、医療分野の動向ではなく、医療機器の製造業者の動向を確認しないといけない。別な例だと自治体に機器、サービスを提供する事業の場合、お客様の業界動向と自社の製造業、サービス業との動向も確認しないといけない。つまり、BtoBの場合、自社の工場のスマート化を実施する場合は、その会社の事業の業界動向ではなく、スマート化する対象の業界動向を確認する必要がある。その後に、「工場システムや自社事業が対象とする規格や法制度の動向」は、前記の両方を意味しているように読めてしまう。	いただいた御意見を踏まえて、ご指摘本文にご指摘いただいた内容を追記いたします。 修正箇所：3.1.1
001	11	企業	11. P27「汎用品のハードウェアに対して調達者側でセキュリティ対策を行うことが難しいことから？検討の際には、調達者に求める以外に、」と記載されている。ここで「調達側」とは、どちらを指すのかがわからない？そのハードウェアのベンダー又は購入する側？	いただいた御意見を踏まえて、「利用者」と「提供者」に用語を統一いたします。 修正箇所：3.2
001	12	企業	12. P37 Software Bill of Material(SBOM)と記載されているが、通常、P38の記載にあるように“Materials”と最後にsをつける。	いただいた御意見のとおり、修正いたします。 修正箇所：3.3
001	13	企業	13. P45 誤植。最後の行の図C-6は、次のページの図の下にあるべき。	いただいた御意見のとおり、修正いたします。 修正箇所：付録C
001	14	企業	14. P45「遠隔保守サービスを自動倉庫ゾーンと分離させる。」と記載されている。これは非常に同意いたします。しかし、遠隔保守サービスの場合は、具体的にどこで分離するかを十分検討する必要があり、そこがセキュリティホールになる可能性が高い。例えば、工場内に設置する機器から外をゾーンに分離すると、工場内にあるVPN機器の脆弱性の保守、管理などの責任分界があいまいになる。どこで分離して、どこからどこまでが誰の責任になるかの観点も何かしら記載されるといいのではと思いました。	いただいた御意見を踏まえて、外部サービスとの責任分界に関する内容でゾーンの分離を行うことが重要である旨を、追記いたします。 修正箇所：付録C

001	15	企業	15. 「サイバー・フィジカル・セキュリティ対策」のガイドラインということで、「2.1.2 外部ネットワーク接続の増加」とセキュリティとをどのように両立させるのかに関心がありました。「ゼロトラスト」を目指せとかの記載になっているか心配でしたが、「スマート化の状況により、ゼロトラストの考え方を採り入れることが有効な場合もある。」と適切に記載されていると感じました。さらに、スマート化のポイントとしてゾーンを主に置くことには、賛同いたします。今回ではなく、将来的に有識者の先生方に検討してもらいたい点として、サイバー・フィジカルを進展させていくと、ゾーン内のすべての通信、ゾーン間のすべての通信をサイバースペースにも反映する必要があると認識しています。そのためには、それらの通信の標準化が必要で、そのインターフェースを外だしして、そこをサイバーへの入り口としてセキュリティ確保を検討していく必要があると思っています。概略しか理解していませんが、具体的には、NEDOや日本ロボット協会などが実施されているORiN(ISO化されてISO20242-4としてIS発行)などのような考えが重要だと思っています。医療機器分野でもまだ適用範囲は狭いですが、ORiNの考えの元でOPeLiNKとして活用されています。	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。
002	16	企業	セキュリティ水準の異なるゾーン間の接続においては、一般的に情報システムで普及しているルーター、ファイアウォール、DMZを介した対応策が考えられる。 (例:ネットワーク間の境界にはファイアウォールを設置し、各方向の通信について必要最低限の通信のみを許可) しかし、情報システムとは異なり、制御システムへのサイバー攻撃はセーフティや環境への影響につながる危険性がある為、外部との接続においては、より強固なセキュリティ対策が求められるケースがある。そのため、制御システムから外部へのデータ送信を可能としつつ、データ送信を一方向だけに 制限するデータダイオードや一方向通信装置(機器で実現している一方向通信特性を活かして物理レベルで侵入を防御する装置)による対応策を講じることで、外部からの侵入を確実に拒否することが期待できる。 各ゾーンの定義を行う際に、上記の対策を打った物理レベルでの侵入防御を考慮したゾーン設計を入れることが可能であればこれを検討する方がより強固なセキュリティ設計ができると考えコメントさせていただきます。	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。
003	17	企業	1. 4頁:【参考】半導体セキュリティ規格SEMI E187の動向 意見:SEMIE187よりIEC62443の掲載を提案します。 理由: SEMIE187は半導体に特化しています。産業全体では、国際規格IEC62443の記載が適当と考えます。また、調達要件の事例は、防衛装備庁の例を挙げて良いかと考えます。インシデント例は国内事例が身近で良いと考えます。	いただいた御意見については、製造業におけるサプライチェーンセキュリティの取組例を説明したものであるため、新たな規格は追加せず、コラムのタイトルを修正し、意図をより明確にいたします。 修正箇所:1.2
003	18	企業	2.6頁: 2.1.3スマート工場でのセキュリティ対策のポイント 意見:重要なポイントとしての組織策(以下●項を追加) すべきと考えます。 ● ·インシデントの検知報告体制の考え方 工場内で発生する機器故障等のインシデントに加え、サイバーインシデントを検知、報告、初期対応、禁止行為の懲底等の体制、組織を構築する。 ・ゾーン設定の考え方 ・サプライチェーンの広がりに伴う責任分界や役割分担の考え方 理由:組織的なインシデント検知対応がセキュリティ対策として重要と考えます。	いただいた御意見については、一般的なOTにおけるインシデント対応に関しては、ガイドライン本編で記載しております。一方で、インシデント対応はサプライチェーンの広がりの一部として重要な考えであるため、「サプライチェーンの広がりに伴う責任分解や役割分担の考え方」においてインシデントに関しても明記いたします。 修正箇所:2.1.3

003	19	企業	3.6頁：2.1.3スマート工場でのセキュリティ対策のポイント 意見：「ゾーン設定の考え方」の冒頭部分に必要な理由を追加する。 工場内では、設置時期による様々なセキュリティレベル対応の製品が混在する。本製品群を通信機器により利用を制御することで、インシデント時は必要に応じてゾーン全体を遮断することでインシデントの拡散を防ぐ。 理由：工場のセキュリティ対策として、設備を中心としたゾーン設定が最も重要と考えます。	いただいた御意見を踏まえて、P.20の図3-2の視点の1つとして設備の導入時期について追記いたします。 修正箇所：2.1.3
003	20	企業	4. 6頁：2.1.3スマート工場でのセキュリティ対策のポイント 意見：「・サプライチェーンの広がりに伴う責任分界や役割分担の考え方」の冒頭部分に必要な理由を追加する。 スマート化が進むと、サプライチェーン間での情報が連携し、相互に生産性が向上する反面、責任分担点があいまいになりかねない。分担点を決め、インシデント検知体制、システム対策といったセキュリティ対策を決めておくことが重要である。 理由：工場内から様々な会社間で通信が拡大する際に「分担」を明確にします。	いただいた御意見を踏まえて、自社での管理範囲があいまいになるという点を理由の一部として追記いたします。 修正箇所：2.1.3
003	21	企業	5.8頁：工場をスマート化する目的の設定 意見：以下PDCAによる現場改善を冒頭に追加する。 ・工場をスマート化する目的の設定 自社工場の強み弱みを分析把握し、スマート化の目的を明確にするとよい。 スマート化及びセキュリティも導入直後から、現場での改善活動による育成が重要になる。このような改善活動が維持できるような仕組みの導入が重要である。 理由：後の記述(P30~) に、PDCAといった現場でも改善が記載されており、前半にも記載があるべきと考えます。	いただいた御意見については、スマート化の目的とPDCAを直接的には結びつけていないため、ステップ1.1での記載は見送りとさせていただき、原案のとおりとさせていただきます。また、後半の3.3節の②においても、PDCAの有効な考え方として現場を体制に含むことを明記しております。 修正箇所：3.3
003	22	企業	6. 13頁：インシデントが与える影響の把握および整理 意見：工場で発生するインシデントの影響の特徴を追記、修正する。 (現)工場システムに関連するインシデントは、工場への影響にとどまらず、自社事業や他社や工場の周辺環境にまで影響を与える可能性もある。 (新)工場システムに関連するインシデントは、誤作動による従業員や近隣住民の安全・健康への影響、有害物質の排出等による環境面への影響、及び工場システムの機能不全による製品の品質の不備の発生による製品購入者の安全・健康への影響、不良品の発生による廃棄時の大量ごみの影響を与える可能性もある。 理由：工場特有で発生する影響を意識し、以降のセキュリティ対策を進めていく必要があると考えます。	いただいた御意見については、ガイドライン本編での記載がすでにあるため、原案のとおりとさせていただきます。

003	23	企業	7. 14頁：スマート化を進めるうえでのポイント① スマート化の目的に照らした業務の広がり 意見：「広がり」という言葉を以下の「変更」と言い換えることを提案します。 ・スマート化の目的に照らした業務の変更 スマート化に応じたセキュリティ対策を検討するために、スマート化により変更が生じる業務を確認することが重要である。 ・業務の変更に応じたシステム範囲の拡大 スマート化によって業務が変更された、また新しい業務に応じたシステム範囲の業務手順を確認することが重要である。 理由：「広がり」という表現が従来の業務に「加える」という捉え方になると考えます。スマート化により、業務は追加、削除、変更され、今回は特に見過ごされ易い「変更」が着目されるようにすべきと考えます。	いただいた御意見については、本別冊はスマート化を進める企業を想定読者としており、スマート化においては業務を拡大する場合が多いため、原案の通りとさせていただきます。
003	24	企業	8. 16頁：スマート化を進めるうえでのポイント① 業務の広がりに伴う業務の重要度の見直し 意見：「広がり」という記述を「変更」と言い換えることを提案します。 ・業務の変更に伴う業務の重要度の見直し スマート化によって、変更された、また新しい業務に対して重要度の見直しを行うことが重要である。 理由：「広がり」という表現が従来の業務に「加える」という捉え方になると考えます。スマート化により、業務は追加、削除、変更され、今回は特に見過ごされ易い「変更」も着目されるようにすべきと考えます。	いただいた御意見については、本別冊はスマート化を進める企業を想定読者としており、スマート化においては業務を拡大する場合が多いため、原案の通りとさせていただきます。
003	25	企業	9. 17頁：表3-3スマート化を実現する上で追加されうる保護対象の例 意見：例では、外部サービス、装置・機器、ソフトウェア・業務プログラム、データのみが保護対象ですが、以下通信機器の追加を提案します。 保護対象：ネットワーク、構成要素： LAN,WAN,インターネット 理由：スマート化の重要な保護対象はネットワークが必須と考えます。	いただいた御意見については、ガイドライン本編での記載がすでにあり、今回の表は追加されうる保護対象の例を記載しているので、原案のとおりとさせていただきます。
003	26	企業	10. 19頁：技術の進化を踏まえ、スマート化を進める際の内外の接続の考え方の整理 意見：以下のような修正を加えることを提案します。 （現）スマート化を実現する上では、新たな業務の追加･更新が行われる。そのため、ゾーン設定を行う上で、業務の視点でゾーン内の扱うべき保護対象を詳細に整理することが重要である。そのため、以下の手順でゾーン設定を行う。 （新）スマート化の実現により、追加、変更される業務を考慮し、セキュリティ対策を実施する。そのために必要なゾーン、及びゾーンが外部と通信する出入口の設定（※）を改めて行うことが重要である。 （※）IEC62443ではコンジットという 理由：ゾーンを説明するのであれば、IEC62443に基づく「コンジット（※）」も説明した方が良いかと考えます。なお、ハンドブックですので、コンジットを物理的な扉や検問など拡大解釈してもよいかと考えます。P21から22には、ゾーン間の通信設計が述べられており、事前にゾーン間の設計を言っておいてもよいと考えます。 （※）コンジット(IEC62443用語)：単なる通信路ではなく、ゾーン間のセキュリティ水準の違いを維持する https://www.jpcert.or.jp/ics/20221027_ICSsecStandards-02.pdf	いただいた御意見については、本ガイドラインはIEC62443に基づいたものではなく、かつ、ステップ1-7の表3-4で該当の内容について確認しているため、原案の通りとさせていただきます。

003	27	企業	11.21頁：スマート化におけるゾーンごとのセキュリティ要件の考え方6 意見：参考となる文章内を以下のように変更を提案します。 6境界でセキュリティ対策を行うという従来の考え方に加え、保護資産に対し てセキュリティ対策を実施することを前提にした「ゼロトラスト」という考え 方がある。 理由： 6の備考はゾーンごとのセキュリティ要件の考え方を補足しています。但し、 ゼロトラスト（信頼しないことを前提としてすべての通信の中身を検疫する） に置き換えるような表現になっています。但し、工場のセキュリティの基本は 「ホワイトリスト方式（信頼した機器や通信のみ許可する）」であり、今後も この考え方は基本であり、基本に沿うよう備考を修正しました。	いただいた御意見については、ゼロトラストに置き換える意図にならない表現に修正いたします。 修正箇所：3.1.7
003	28	企業	12.27頁：クラウド利用時の対策 意見：以下の●項の追加を提案します。 ・自社の環境とサービスの利用条件 ・クラウドサービスの利用目的 ・インシデント発生時のサービス提供者の対応責任・対応方針 ・（データ移行の必要がある場合、）データ移行における信頼性 ● ・クラウドサービス通信遮断からの復旧後にデータの一貫性を保持する 理由：工場におけるクラウド利用時の通信遮断は、クラウド事業者理由のみでなく、自社のインシデントから安全を確保する為の遮断も想定する必要があるため、復旧後にデー―タの抜けや漏れを防ぐ内容を追加しました。	いただいた御意見を踏まえて、他の項目の記載粒度と合わせて追記いたします。 修正箇所：3.2.2
003	29	企業	13.27頁：汎用品の「ハードウェア」のセキュリティ対策 意見：以下の調達者側でセキュリティ対策が難しい「ハードウェア」へ留意する点と して、下線部及び●項の追加を提案します。 ▸ ハードウェアに対するセキュリティ対策の実施状況 ▸ 調達先の脆弱性対応状況 ▸ インシデント時の機器の保守（自社、業者）・運用の対応方針 ●▸ 保守業者へ脆弱性情報の提供及び対策提案を求める 理由：汎用品のセキュリティ対策は、インシデント発生時のみでなく、通常運用時の保守業者によるセキュリティ対応も重要と考えます。本記載では、社内のみで脆弱性情報の収集～対策を実施するよう読み取れたため、追記しました。	いただいた御意見を踏まえて、2点目の調達先に加えて、保守業者を追記いたします。 修正箇所：3.2.2
003	30	企業	14.28頁：ソフトウェアのセキュリティ対策 意見： OSS （オープンソース）を用いて自社開発する際、調達する際の両方の重視する点として、以下の●項の追加を提案します。 ●▸ ゾーン間の通信、社外との通信などセキュリティ対策上重要な箇所で、保守や脆弱性の対策が明確でないOSSの利用する際は特に注意する。 理由： OSS （オープンソース）を組み込んだソフトウェアの利用の対策は重要かと考えます。ゾーン間の通信や、社外通信の責任分担点といった、セキュリティ対策上重要な箇所でのOSS利用は特に注意すべき（基本は利用しない）と考えます。	いただいた御意見を踏まえて、ご指摘いただいた内容を追記いたします。 修正箇所：3.2.2

003	31	企業	15.29頁：（2）物理面での対策 意見：表3-6 スマート化の想定脅威に対応するセキュリティ対策例に以下の追加を提案します。 脅威種別：従業員・保守要員（設備ベンダ）の過失 脅威内容：ウイルスが混入したUSBメモリを装着した機器が異常な動作をする 理由：通信が制約された工場内のセキュリティ対策で、USBメモリはよく利用され、対策は考慮すべきであり、重要と考えます。	いただいた御意見については、ガイドライン本編での記載がすでにあり、今回の表は追加されうるセキュリティ脅威の例を記載しているので、原案のとおりとさせていただきます。
003	32	企業	16.32頁：表3-7サイバー攻撃の早期認識と対処における役割分担例「予防保全段階」 意見：表3-7では予防保全として脆弱性の情報の入手先として「ベンダ」のみから以下に「セキュリティ担当部署」追加を提案します。 予防保全段階：下記では、脆弱性情報がベンダから提供された、もしくはセキュリティ担当部署が入手した場合を示している。 監視段階：主な担当部署：ベンダ、セキュリティ担当部署 理由：現時点では、脆弱性情報を提供するベンダは非常に少なく、現実の運用に併せ「ベンダ」のみでなく「セキュリティ担当部署」を追加します。	いただいた御意見を踏まえて、本文にいただいた内容を追記いたします。 修正箇所：3.3
003	33	企業	17.32頁：表3-8サイバー攻撃の早期認識セ対処における役割分担例（被害発生段階） 意見：被害発生段階は、サイバー攻撃が原因か関係なく、通常と異なる事象が起きた際の対応である。以下の青下線のように、「現場責任者」追加を提案します。 監視段階(Observe) 主な担当部署：製造現場、意思決定者：現場部門長、現場責任者 理由：被害発生時の監視段階では、情報を早く入手する必要があり、現場部門長のみでなく、より現場に近い、現場責任者も加えてもよいかと考えます。	いただいた御意見を踏まえて、他の項目含めて粒度感を合わせるように修正いたします。 修正箇所：3.3
003	34	企業	18.35頁：（2）サプライチェーン対策「被害発生段階」 意見：ガイドライン別冊では、上記の観点を基にスマート化に更なる検討が必要とし 確認ポイントを整理している。箇条書きポイントに●項の追加を提案します。 ・クラウド利用時の留意事項、表3-10クラウド利用時の留意事項 運用・保守： ・クラウドサービスと業務の切り分けや運用ルールを明確化しているか ・クラウドサービスで取り扱う情報の機密性は確認しているか ・クラウドサービスの利用方法を理解している担当者がいるか ・クラウドサービスのユーザを適切に管理しているか ・クラウドサービスが停止した際のバックアッププランを準備しているか ●・クラウドサービスを遮断した際の遮断期間中の稼働及びデータ復旧のプランを準備しているか ・クラウドサービスを介し調達先や他社ネットワークと接続されているか 理由：工場システムでのクラウド利用・運用時は、クラウド事業者理由のみでなく、自社インシンデント理由で遮断する場合もあります。本遮断から復旧した場合のプランも必要であり、追加するのが良いと考えます。	いただいた御意見を踏まえて、別の項目にご指摘いただいた内容を追記いたします。 修正箇所：3.3

004	35	企業	3.2.2(1)2機器におけるセキュリティ対策について。 （2）物理面での対策にデータ盗難や改ざんの脅威種別がありますが、対策内容の（1）2に具体的な記載がありません。 また、本紙「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」の「表3-27危機におけるセキュリティ対策(例)」にバックアップ（データ、機器）の記載がありますが、別冊の(1)2にはバックアップの記載がありません。 上記の理由から、(1)2に以下の段落追加をご提案いたします。 「サイバー攻撃の被害に遭ったとしても被害を少しでも小さくし、情報システムの復旧を早めるための対策として、システムやデータのバックアップがある。 バックアップデータを端末及びサーバ装置やネットワークから切り離して保管すると、より安全なサイバー攻撃対策となる。バックアップデータは改ざんや盗難への対策として、上書き不可設定や暗号化されることが望ましい。」	いただいた御意見については、ガイドライン本編での記載がすでにあるため、原案のとおりとさせていただきます。
004	36	企業	3.3(1)1運用・管理面のセキュリティ対策について。 本紙「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」の「表3-37セキュリティ管理作業(例)」に装置・機器バックアップの記載があります。別冊にも以下のとおり、33項最初の箇条書きに1つ追加することをご提案いたします。 「・定期オフラインバックアップ、セキュリティインシデント発生後に未感染状態へ復旧（リストア）できる機器の導入」	いただいた御意見については、ガイドライン本編での記載がすでにあるため、原案のとおりとさせていただきます。
005	37	個人	＞27頁 ＞クラウド利用時の対策 「工場においてスマート化を進める際には、クラウドサービスを利用することが考えられる。」とあるが、そのような事は通常無いであろう。 なるほど、外部の者が行う発注等について受けるための、あるいは他の外部と連携するシステムについて運用を行う基盤としてクラウドが用いられたりする事はありえようが、しかし、工場についてのスマート化のためにクラウドサービスを使うなどという事は、色々な観点からありえない事であるはずである。 そもそもインターネットとの通信などは工場においては必要性があるわけではなく、インターネットとの通信があるだけでそこに脆弱性や秘密漏洩の問題が発生する。（はっきり言って、「工場のスマート化」のためには、クラウドサービスはあまり使わないべきである。生産システムとの連携があるシステムの運用等についてはともかくとして。） そのような問題があるにも関わらず、クラウドサービスの利用の提示をするなどというのは、経済産業省の狂いを示すものであるが、やめていただきたいものである。 あくまで、生産システムとの連携を行う受発注のシステム等について使う可能性があったりするだけであるはずであるので、例としてそのようなものを示すとともに、一般的にそうであるような記述をするのは止められたい。記述を改められたい。	いただいた御意見については、工場のスマート化においてクラウドサービスが必ずしも必要ではありませんが、工場のスマート化の事例として、生産状況の見える化や保守業務の効率化等でクラウドサービスを利用しているケースが確認できていることから、原案の通りとさせていただきます。