経済産業省

参考資料1

工場システムのサイバーセキュリティ対策
アンケート調査票

工場システムのサイバーセキュリティ対策
アンケート調査票
＜業界団体向け＞

業界団体向けアンケート調査票（1/3）

※回答必須の設問

基本情報			
Q0	個人情報の取り扱いに同意する※	単一回答	同意する
Q1	氏名※	自由記述	
	氏名（フリガナ）※	自由記述	
Q2	団体名・協会名※	自由記述	
	役職※	自由記述	
Q3	貴団体・協会の会員数をお選びください。※ （正会員以外の会員も含み）	単一回答	・10社未満 ・10名～50社未満 ・50社～100社未満 ・100社～500社未満 ・500社～1,000社未満 ・1,000社以上
Q4	貴団体・協会の会員における企業規模の割合についてお選びください。※	自由回答	・大企業： ・中小企業： ・その他：
Q5	貴団体・協会の会員における製造業（工場を持つ企業）とサービス業の割合についてお選びください。※	自由回答	・製造業： ・サービス業： ・その他：
Q6	貴団体・協会の会員における業種（小分類）をお選びください。※	自由回答	産業別統計表を参考に選択肢を作成

貴団体におけるサイバーセキュリティ活動状況・展望			
Q7	貴団体・協会における脅威・インシデント等の情報共有に関するサイバーセキュリティ活動の実施状況についてお選びください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、 「3：実施済み」	単一回答	・国や関係機関等組織からの脅威・インシデント情報等の会員への提供 ・業界団体が収集した脅威・インシデント情報等の会員への提供 ・会員間の情報共有の仕組みの構築・運営 ・会員のインシデントに関する情報を元にした注意喚起や関連情報の提供 ・その他
	その他の場合：	自由回答	
Q8	Q7でご回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。	自由回答	

貴団体におけるサイバーセキュリティ活動状況・展望			
Q9	貴団体・協会におけるサイバーセキュリティ対策事例の共有に関するサイバーセキュリティ活動の実施状況についてお選びください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、 「3：実施済み」	単一回答	・会員のサイバーセキュリティ対策事例に関する情報共有 ・サイバーセキュリティ関連製品・ソリューション等の情報提供 ・インシデント対応に関するマニュアル等作成・提供 ・その他
	その他の場合：	自由回答	
Q10	Q9でご回答いただいたのサイバーセキュリティ活動について、具体的な内容があればご回答ください。	自由回答	
Q11	貴団体・協会が実施しているセキュリティ人材育成に関するサイバーセキュリティ活動についてお選びください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、 「3：実施済み」	単一回答	・セキュリティに関する教育・研修、セミナー等の実施 ・サイバーセキュリティ教育コンテンツの作成・提供 ・外部事業者のサイバーセキュリティ演習の提供 ・業界独自のサイバーセキュリティ演習の企画・実施 ・各社サイバーセキュリティ演習実施方法に関するマニュアル等作成・提供 ・国等が実施するサイバーセキュリティ演習への参加 ・その他
	その他の場合：	自由回答	
Q12	Q11でご回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。	自由回答	
Q13	貴団体・協会が実施している業界のセキュリティ向上に関する検討に関するサイバーセキュリティ活動についてお選びください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、 「3：実施済み」	単一回答	・会員が情報共有を行うための会議体の設置・運用 ・業界としてのセキュリティ方針・対策を検討する会議体の設置・運用 ・インシデント発生時のサポート（助言、対応支援） ・会員のサイバーセキュリティに関する意識や対策状況等の把握・実態調査 ・他の業界団体やISAC等とのサイバーセキュリティに関する連携 ・その他
	その他の場合：	自由回答	

業界団体向けアンケート調査票（2/3）

※回答必須の設問

貴団体におけるサイバーセキュリティ活動状況・展望				
Q14	Q13でご回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。		自由回答	
Q15	貴団体・協会におけるセキュリティ課題について全てお選びください。※		複数回答	・会員企業のセキュリティの実態が把握できていない ・会員企業における共通のセキュリティ課題が明確にできていない ・業界団体にセキュリティに関する活動を推進するための知識・知見が不足している ・会員企業の実態を把握した上で、業界としてのガイドライン・指針等を策定するのが難しい ・会員企業に対して具体的なセキュリティ対策を示せていない ・特になし ・その他
		その他の場合：	自由回答	
Q16	Q15でご回答いただいた検討中のサイバーセキュリティ課題について、具体的な内容があればご回答ください。		自由回答	
Q17	貴団体・協会におけるサイバーセキュリティに関するガイドラインや文書の作成状況を対象範囲毎にお選びください。※ <選択肢> 「1：未作成」、「2：作成中」、「3：作成・公表済」		単一回答	・組織（例：企業が有する情報や、情報システムの設計・構築・運用に関するセキュリティ要件） ・工場（例：工場やプラント等の制御システムの設計・構築・運用に関するセキュリティ要件） ・製品（例：開発・製造する製品が備えるセキュリティ要件） ・サプライチェーン（例：部品、サービス、役務等提供を行う外部委託先に求めるセキュリティ要件） ・その他
Q18	Q17において「作成中」、「作成・公表済」とご回答いただいた方は、ガイドラインや文書の名称をご回答ください。※（複数ある場合は、すべて記載ください）		自由回答	

貴団体におけるサイバーセキュリティ活動状況・展望				
Q19	Q18にてご回答いただいたガイドライン・文書で参考にした文書について全てお選びください。※		複数回答	・サイバーセキュリティ経営ガイドライン ・中小企業の情報セキュリティ対策ガイドライン ・サイバー・フィジカル・セキュリティ・対策フレームワーク ・IoTセキュリティガイドライン ・ISO/IEC27000シリーズ ・NIST　サイバーセキュリティフレームワーク ・NIST　SP800シリーズ ・IEC62443シリーズ ・その他
		その他の場合：	自由回答	
Q20	Q19にてご回答いただいた文書を参考にした理由をご回答ください。		自由回答	

業界団体向けアンケート調査票（3/3）

※回答必須の設問

サイバーセキュリティに関するガイドラインの認知状況			
Q21	「サイバー・フィジカル・セキュリティ対策フレームワーク」の認知状況についてお選びください。※	単一回答	・フレームワークについて認知していて、内容についても確認している ・フレームワークについて認知しているが、内容までは確認できていない ・本アンケートで初めて知った
Q22	Q21について認知できた経緯について全てお選びください。※	複数回答	・他業界団体からの案内 ・経済産業省のHP ・セキュリティ関連セミナー等での案内 ・団体・協会内の上長等からの情報提供 ・セキュリティ関連ベンダ等からの案内 ・その他
Q23	「サイバー・フィジカル・セキュリティ対策フレームワーク」の活用状況についてお選びください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、「3：実施済み」	単一回答	・会員への周知を行っている ・ガイドライン作成の参考情報として利用している ・業界におけるサイバーセキュリティ施策検討の参考情報として利用している
Q24	「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）」の認知状況についてお選びください。 ※	単一回答	・ガイドラインについて認知していて、内容についても確認している ・ガイドラインについて認知しているが、内容までは確認できていない ・本アンケートで初めて知った
Q25	Q24について、認知できた経緯について全てお選びください。※	複数回答	・他業界団体からの案内 ・経済産業省のHP ・セミナーでの案内 ・社内の上司・同僚等からの情報共有 ・その他

サイバーセキュリティに関するガイドラインの認知状況			
Q26	「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）」の活用状況についてお答えください。※ ＜選択肢＞ 「1：未実施」、「2：一部実施」、「3：実施済み」	単一回答	・会員への周知を行っている ・ガイドライン作成の参考情報として利用している ・業界におけるサイバーセキュリティ施策検討の参考情報として利用している

工場システムのサイバーセキュリティ対策
アンケート調査票
＜個社向け＞

個社向けアンケート調査票（1/9）

※回答必須の設問

基本情報１			
Q1	氏名　※	自由記述	
	氏名（フリガナ）※	自由記述	
	メールアドレス　※	自由記述	
	電話番号　※	自由記述	
Q2	団体名・会社名　※	自由記述	
	役職　※	プルダウンから一つ選択	・役職なし ・主任相当 ・課長相当 ・部長相当 ・本部長・事業部長相当 ・役員以上

基本情報２			
Q3	貴社が加入している業界団体等の名称を全てご記載ください※	自由記述、複数回答可	
Q4	アンケートの案内元の業界団体名をご記載ください（複数ある場合は、１つ選びご記載ください）。※	自由記述、単一回答	
Q5	貴社の業種（大分類）をお選びください。※ （「その他」は自由記述）	複数回答可	産業別統計表を参考に選択肢を作成
Q6	貴社の業種（小分類）をお選びください。※ （選択肢は、「小分類（大分類）」という表記にしています。Q5で選択した「業種（大分類）」が（　）内に記載されている選択肢からお選びください。）	複数回答可	産業別統計表を参考に選択肢を作成
Q7	貴社の総従業員数（正社員、準正社員を含む）をお選びください。※	単一回答	・50名未満 ・50名～100名未満 ・100名～300名未満 ・300名～1,000名未満 ・1,000名～10,000名未満 ・10,000名以上

基本情報２			
Q8	貴社の直近の年間総売上規模をお選びください。※	単一回答	・5,000万円未満 ・5,000万円～3億円未満 ・3億円～10億円未満 ・10億円～50億円未満 ・50億円～500億円未満 ・500億円～5,000億円未満 ・5,000億円以上
Q9	貴社が所持している国内の工場数をお選びください。※	単一回答	・5ヶ所未満 ・5ヶ所～50ヶ所未満 ・50ヶ所～100ヶ所未満 ・100ヶ所以上 ・その他
Q10	貴社が所持している国外の工場数をお選びください。※	単一回答	・所持していない ・5ヶ所未満 ・5ヶ所～50ヶ所未満 ・50ヶ所～100ヶ所未満 ・100ヶ所以上
Q11	貴社が工場で製造している製品の種類数をお選びください。※ （種類数は、型番単位でご回答ください。）	単一回答	・10種未満 ・10種～50種未満 ・50種～100種未満 ・100種～1000種未満 ・1000種～10000種未満 ・10000種以上 ・その他 （　　）
Q12	貴社の年間のIT予算額をお選びください。※ （IT予算額は開発費（ハードウェア費・システム開発費）と保守運用費（ハードウェア費・ソフトウェア費・通信回線費・外部委託費・その他）が含まれます。）	単一回答	・～100万円未満 ・100万円～300万円未満 ・300万円～500万円未満 ・500万円～1000万円未満 ・1000万円～1億円未満 ・1億円～10億円未満 ・10億円～30億円未満 ・30億円～50億円未満 ・50億円～100億円未満 ・100億円～ ・不明

個社向けアンケート調査票（2/9）

※回答必須の設問

基本情報２			
Q13	貴社の年間のセキュリティ予算額をお選びください。※	単一回答	・～100万円未満 ・100万円～300万円未満 ・300万円～500万円未満 ・500万円～1000万円未満 ・1000万円～1億円未満 ・1億円～10億円未満 ・10億円～30億円未満 ・30億円～50億円未満 ・50億円～ ・不明
Q14	貴社の年間の工場に関するセキュリティ予算額をお選びください。※	単一回答	・～100万円未満 ・100万円～300万円未満 ・300万円～500万円未満 ・500万円～1000万円未満 ・1000万円～1億円未満 ・1億円～10億円未満 ・10億円～30億円未満 ・30億円～50億円未満 ・50億円～ ・不明

デジタル技術の活用状況及びそれに係る課題			
Q22	貴社では2021年度下期から2022年度上期（2021年10月～2022年度8月）に、工場内、あるいは工場システムに影響を与えるセキュリティ事故が発生しましたか。あてはまるものを選びください。※	複数回答可	・コンピュータウイルスに感染 ・内部者（委託先を含む）の不正による情報漏えい、システムの悪用等のサイバーセキュリティ上のトラブル ・サイバー攻撃（DoS攻撃・DDoS攻撃、不正アクセス、標的型攻撃等） ・外部委託先に起因するサービスの停止・情報漏えい ・セキュリティ事故は生じていない ・わからない

デジタル技術の活用状況及びそれに係る課題			
Q23	「Q22」において「セキュリティ事故は生じていない」・「わからない」以外を回答いただいた方は、生じたセキュリティ事故の金銭的損害を概算でお選びください。 なお、金銭的被害とは、システム停止時間の逸失利益、対応人員の残業代等人件費、 原因調査や復旧のための外部委託費、復旧までの代替製品等購入・レンタル費、 取引先・顧客等への謝罪費、弁護士費用等を指します。	単一回答	・0円 ・10万円未満 ・10万円～100万円未満 ・100万円～300万円未満 ・300万円～500万円未満 ・500万円～1000万円未満 ・1000万円～1億円未満 ・1億円～10億円未満 ・10億円以上 ・わからない

サイバーセキュリティ全般の基本対策状況について （サイバーセキュリティ経営ガイドラインのチェックリストを基にお聞きしております。）			
Q35	貴社における全社のサイバーセキュリティリスクの認識、組織全体での対応方針の策定についてお選びください。※ （例） ・経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している ・経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言している	単一回答	・未実施 ・一部実施 ・実施済み
Q36	「Q35」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q37	貴社における全社のサイバーセキュリティリスク管理体制の構築についてお選びください。※ （例） ・組織の対応方針（セキュリティポリシー）に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築している ・サイバーセキュリティリスク管理体制において、各関係者の役割と責任を明確にしている	単一回答	・未実施 ・一部実施 ・実施済み

個社向けアンケート調査票（3/9）

※回答必須の設問

サイバーセキュリティ全般の基本対策状況について			
Q38	「Q37」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q39	貴社における全社のサイバーセキュリティ対策のための予算確保についてお選びください。※ （例） ・必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している	単一回答	・未実施 ・一部実施 ・実施済み
Q40	「Q39」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q41	貴社における全社のサイバーセキュリティ対策のための人材確保についてお選びください。※ （例） ・組織内でサイバーセキュリティ人材を育成している ・セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施している	単一回答	・未実施 ・一部実施 ・実施済み
Q42	「Q41」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q43	貴社における全社のサイバーセキュリティリスクの把握とリスク対応に関する計画の策定についてお選びください。※ （例） ・特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、経営戦略を踏まえたサイバーセキュリティリスクとして把握している ・サイバーセキュリティリスクが事業にいかなる影響があるかを推定している	単一回答	・未実施 ・一部実施 ・実施済み

サイバーセキュリティ全般の基本対策状況について			
Q44	「Q43」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q45	貴社における全社のサイバーセキュリティリスクに対応するためのマネジメントの仕組みの構築についてお選びください。※ （例） ・意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、対応者などの責任分担等）を策定している ・サイバー攻撃の動向等を踏まえて、サイバーセキュリティリスクへの対応内容（検知すべきイベント、技術的対策の強化等）を適宜見直している	単一回答	・未実施 ・一部実施 ・実施済み
Q46	「Q45」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q47	貴社における全社のサイバーセキュリティリスクに対応するための技術的な仕組みの構築についてお選びください。※ （例） ・重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施している ・システム等に対して脆弱性診断を実施し、検出された脆弱性に対処している	単一回答	・未実施 ・一部実施 ・実施済み
Q48	「Q47」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	

個社向けアンケート調査票（4/9）

※回答必須の設問

サイバーセキュリティ全般の基本対策状況について			
Q49	貴社における全社のサイバーセキュリティ対策における PDCA サイクルの実施 についてお選びください。※ （例） ・経営者が定期的に、サイバーセキュリティ対策状況の報告を受け、把握している ・サイバーセキュリティリスクや脅威を適時見直し、環境変化に応じた取組体制（PDCA）を整備・維持している	単一回答	・未実施 ・一部実施 ・実施済み
Q50	「Q49」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q51	貴社における全社のインシデント発生時の緊急対応体制の整備についてお選びください。※ （例） ・サイバー攻撃の初動対応マニュアルを整備している ・インシデント対応の専門チーム（CSIRT等）を設置している	単一回答	・未実施 ・一部実施 ・実施済み
Q52	「Q51」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q53	貴社における全社のインシデントによる被害に備えた復旧体制の整備ついてお選びください。※ （例） ・被害が発生した場合に備えた業務の復旧計画を策定している ・復旧作業の課題を踏まえて、復旧計画を見直している	単一回答	・未実施 ・一部実施 ・実施済み
Q54	「Q53」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	

サイバーセキュリティ全般の基本対策状況について			
Q55	貴社における全社のビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握についてお選びください。※ （例） ・システム管理などについて、自組織のスキルや各種機能の重要性等を考慮して、自組織で対応できる部分と外部に委託する部分を適切に切り分けている ・委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている	単一回答	・未実施 ・一部実施 ・実施済み
Q56	「Q55」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	
Q57	貴社における全社の情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供についてお選びください。※ （例） ・マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPA への届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している	単一回答	・未実施 ・一部実施 ・実施済み
Q58	「Q57」で選んだ選択肢について、その実施状況を選んだ理由をご回答ください。	自由記述	

個社向けアンケート調査票（5/9）

※回答必須の設問

工場におけるデータ分析・セキュリティリスク・リスク分析について			
Q59	貴社が所持している工場データ（例：生産計画・生産指示・設備状態・部材在庫量等）の利活用状況についてお選びください。※	単一回答	・データを利活用していない ・工場全体のデータの収集・蓄積を実施している（例：工場全体のデータを連携できるようデータベース等に保存している） ・収集・蓄積した工場全体のデータを用いて分析・予測している（例：蓄積しているデータを分析・予測し、生産計画変更や故障予測などに利用している） ・収集・蓄積したデータを用いた分析・予測結果より、制御・最適化を実施している（例：分析・予測結果を基に、工場の各機器をリアルタイムに自動操作などしている）
Q60	今後の工場データ利活用の意向についてお選びください。※	単一回答	・データ利活用の予定はない ・データ利活用を開始する予定である ・現状のデータ利活用状況を維持する予定である ・データ利活用を促進する予定である
Q61	工場のサイバーセキュリティリスクとして認識されているものについて全てお選びください。※	複数回答可	・工場システムへの不正侵入 ・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 ・外部へのサイバー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 ・特になし ・その他　（具体的に： [　　]）
Q62	貴社が所持している工場に対してサイバーセキュリティに関するリスク分析（例：リスクが顕在化した場合の事業被害に関する分析）の実施状況についてお選びください。※ （参考：「制御システムのセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」、情報処理推進機構）	単一回答	・毎年もしくはそれ以上の頻度で実施している ・3年に1回以内の頻度で実施している ・不定期に実施している ・実施していない

工場におけるデータ分析・セキュリティリスク・リスク分析について			
Q63	貴社において全社セキュリティ責任者（CISO（Chief Information Security Officer）の設置状況についてお選びください。※	単一回答	・設置している ・設置していない ・設置していないが予定がある
Q64	貴社において工場システムのセキュリティ責任者の設置状況についてお選びください。※	単一回答	・設置している ・設置していない ・設置していないが予定がある
Q65	貴社において、情報セキュリティ委員会（全社セキュリティインシデント対応や各種セキュリティ施策の審議・決定等の場）等の設置状況についてお選びください。※	単一回答	・設置している ・設置していない ・設置していないが予定がある
Q66	工場システムの構築・保守の外部委託状況についてお選びください。※	単一回答	・工場システムの構築・保守を外部委託している ・工場システムの構築・保守を外部委託していない ・該当しない
Q67	「Q66」で「工場システムの構築・保守を外部委託している」と回答頂いた方は、外部委託の契約時に契約書・仕様書等へのセキュリティ要件の取込状況についてお選びください。	単一回答	・契約書・仕様書等にセキュリティ要件を取り込んでいる ・契約書・仕様書等にセキュリティ要件を取り込んでいない

個社向けアンケート調査票（6/9）

※回答必須の設問

工場のサイバーセキュリティの具体の対策状況について ※経済産業省「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）」記載の対策の例示です。 回答は任意ですが、自社の工場におけるセキュリティ対策状況を確認できる設問となっていますので、ぜひご回答の上、自社の対策検討・推進にご活用ください。				
Q68	貴社の工場システムにおけるそれぞれの組織対策について、実施状況をお答えください。 （所持している工場によってセキュリティ対策状況が違う場合は、一番多くの工場に当てはまるものをお選びください。）	単一回答	・工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識をもっており、十分な予算・人員配置などの協力を得られる状態にある	・未実施 ・一部実施 ・実施済み ・実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し ・実施済みで、管理手順を文書化・自動化し、随時見直し ・該当しない・わからない
		単一回答	・工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている	
		単一回答	・工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている	
		単一回答	・工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている	
		単一回答	・工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの情報収集を行っている	

工場のサイバーセキュリティの具体の対策状況について				
Q69	貴社の工場システムにおけるそれぞれの運用的対策（システム関連等）について、実施状況をお答えください。 （所持している工場によってセキュリティ対策状況が違う場合は、一番多くの工場に当てはまるものをお選びください。）	単一回答	・システムが侵害・停止した場合の事業に対するリスクを検討している	・未実施 ・一部実施 ・実施済み ・実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し ・実施済みで、管理手順を文書化・自動化し、随時見直し ・該当しない・わからない
		単一回答	・工場システムにおける専用のセキュリティポリシが規定されていて、認知されている	
		単一回答	・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している	
		単一回答	・工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている	
		単一回答	・工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している	
		単一回答	・情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図が作成している	
		単一回答	・工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある	

個社向けアンケート調査票（7/9）

※回答必須の設問

工場のサイバーセキュリティの具体の対策状況について				
Q70	貴社の工場システムにおけるそれぞれの物理的対策について、実施状況をお答えください。（所持している工場によってセキュリティ対策状況が違う場合は、一番多くの工場に当てはまるものをお選びください。）	単一回答	・ウイ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また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	・未実施 ・一部実施 ・実施済み ・実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し ・実施済みで、管理手順を文書化・自動化し、随時見直し ・該当しない・わからない
		単一回答	・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	
		単一回答	・制御端末のオペレーティングシステムの使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している	
		単一回答	・工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）又は、入退室管理、外部の入室者への関係者の付き添いなど運用面での代替策を講じている	
		単一回答	・工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN 等）	
		単一回答	・工場内のネットワーク（情報システムとの境界含む）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	
		単一回答	・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	

工場のサイバーセキュリティの具体の対策状況について				
Q71	貴社の工場システムにおけるそれぞれの工場システムサプライチェーン対策について、実施状況をお答えください。（所持している工場によってセキュリティ対策状況が違う場合は、一番多くの工場に当てはまるものをお選びください。）	単一回答	・工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダー・構築事業者と連絡・連携体制を構築している	・未実施 ・一部実施 ・実施済み ・実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し ・実施済みで、管理手順を文書化・自動化し、随時見直し ・該当しない・わからない
		単一回答	・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	
		単一回答	・納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している	
		単一回答	・サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（監査実施など）を把握できている	
		単一回答	・納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある	
		単一回答	・新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている	
Q72	「Q68～Q71」で回答したセキュリティ対策以外に実施している対策がありましたらご回答ください。	自由記述		

個社向けアンケート調査票（8/9）

※回答必須の設問

サイバーセキュリティ全般における課題や要望について			
Q73	「Q4:アンケート案内元の業界団体名」てご回答いただいた業界団体が実施していることを認識しているサイバーセキュリティ活動についてお選びください。※	複数回答可	・脅威・インシデント等の情報共有 ・サイバーセキュリティ対策事例の共有 ・サイバーセキュリティ人材育成 ・業界のサイバーセキュリティ向上に関する検討・施策実施 ・サイバーセキュリティに関するガイドラインや文書の作成 ・その他
Q74	「Q73」にて「サイバーセキュリティに関するガイドライン・文書の作成」と回答いただいた方は、業界団体で公表されているサイバーセキュリティに関するガイドライン・文書の対象範囲を全てお選びください。	複数回答可	・組織（例：企業が有する情報や、情報システムの設計・構築・運用に関するセキュリティ要件） ・工場（例：工場やプラント等の制御システムの設計・構築・運用に関するセキュリティ要件） ・製品（例：開発・製造する製品が備えるセキュリティ要件） ・サプライチェーン（例：部品、サービス、役務等提供を行う外部委託先に求めるセキュリティ要件） ・その他
Q75	「Q73」にて「サイバーセキュリティに関するガイドライン・文書の作成」と回答いただいた方は、ガイドラインや文書の自社での利用についてお選びください。	単一回答	・利用している ・利用していない ・分からない
Q76	「Q75」にて「利用している」とご回答いただいた方は、具体的な利用方法についてご回答ください。	自由記述	
Q77	「Q4：アンケート案内元の業界団体名」にてご回答いただいた業界団体に期待するサイバーセキュリティ活動についてお選びください。※	複数回答可	・脅威・インシデント等の情報共有 ・サイバーセキュリティ対策事例の共有 ・サイバーセキュリティ人材育成 ・業界のサイバーセキュリティ向上に関する検討・施策実施 ・サイバーセキュリティに関するガイドラインや文書の作成 ・その他

サイバーセキュリティ全般における課題や要望について			
Q78	「Q77」にてご回答いただいた期待しているサイバーセキュリティ活動について具体的な内容があればご回答ください。	自由記述	

工場セキュリティにおける課題・要望について			
Q79	工場システムのセキュリティ対策における組織的な課題について全てお選びください。※	複数回答可	・工場のサイバーセキュリティリスクについて経営層が理解していない ・工場システムのサイバーセキュリティを確保するための人材がいない ・工場システムのサイバーセキュリティ予算が少ない ・工場におけるインシデント対応体制がない ・その他
Q80	「Q79」にてご回答いただいた課題について具体的な内容があればご回答ください。	自由記述	
Q81	工場システムのサイバーセキュリティ対策を進める際の課題について全てお選びください。※	複数回答可	・工場システムのサイバーセキュリティを確保するために何から始めればよいかわからない ・複数の工場システムのサイバーセキュリティ対策状況を管理するのが難しい ・工場システムのサイバーセキュリティリスク分析方法が分からない ・異なる環境（例：新規/既設・規模・導入機器・データ利活用状況・国内/海外等）の工場システムをリスク分析するのが難しい ・異なる環境（例：新規/既設・規模・導入機器・データ利活用状況・国内/海外等）の工場システムに対する統一的な基準を構築するのが難しい ・その他
Q82	「Q81」にてご回答いただいた課題について具体的な内容があればご回答ください。	自由記述	

個社向けアンケート調査票（9/9）

※回答必須の設問

工場セキュリティにおける課題・要望について			
Q83	「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）」の認知状況についてお選びください。※	単一回答	・ガイドラインについて認知していて、内容についても確認している ・ガイドラインについて認知しているが、内容までは確認できていない ・本アンケートで初めて知った
Q84	「Q83」にて「ガイドラインについて認知していて、内容についても確認している」・「ガイドラインについて認知しているが、内容までは確認できていない」と回答いただいた方は、認知できた経緯について全てお選びください。	複数回答可	・業界団体からの案内 ・経済産業省のHP ・セキュリティ関連セミナー等での案内 ・社内の上司・同僚等からの情報共有 ・セキュリティ関連ベンダ等からの案内 ・その他
Q85	「Q83」にて「ガイドラインについて認知していて、内容についても確認している」と回答いただいた方は、現場での活用可能性についてお選びください。	単一回答	・活用できると考える ・活用に課題があると考える ・わからない
Q86	ガイドラインを活用するために国に期待する支援についてお選びください。※	複数回答可	・工場システムの構成事例を増やしてほしい ・具体的な対策を示してほしい ・対策に優先度をつけてほしい ・対策毎の具体的な実施方法の例がほしい ・リスク分析の具体的な実施方法がほしい ・ガイドラインについてのセミナーを開いてほしい ・その他
Q87	「Q86」にてご回答いただいた支援について具体的な内容があればご回答ください。	自由記述	

工場セキュリティにおける課題・要望について			
Q88	ガイドラインを活用するために業界団体に期待する支援についてお選びください。※	複数回答可	・業界の特徴的な工場システムの構成事例を基に記載してほしい ・業界のチェックリストを定めてほしい ・業界におけるガイドラインの利用方法を示してほしい ・業界としての統一的な対策内容を示してほしい ・業界としてのガイドラインを策定して欲しい ・その他
Q89	「Q88」にてご回答いただいた支援について具体的な内容があればご回答ください。	自由記述	
Q90	その他サイバーセキュリティ全般で国に期待する支援についてお選びください。※	複数回答可	・脅威・インシデント等の情報提供 ・サイバーセキュリティ対策に関する補助金・助成金 ・セキュリティ人材育成（例：サイバー演習・研修など） ・人事採用のための企業と情報セキュリティ人材のマッチング制度 ・サイバーセキュリティに関するガイドライン・文書の作成 ・サイバーセキュリティ対策に関して支援を行う専門家派遣 ・セキュリティが確保された製品・サービスが確認可能な認証・審査制度 ・セキュリティ対策に取り組む企業の表彰、優遇制度 ・インシデント発生時の相談窓口（情報提供や助言、対応支援） ・セキュリティ対策の必要性に関する普及活動 ・セキュリティに関する情報共有等を行うコミュニティ等の形成 ・その他
Q91	「Q90」にてご回答いただいた支援について具体的な内容があればご回答ください。	自由記述	