ベンチマーク抽出結果（別紙）
チェック項目に基づき、各ベンチマーク内の記載を確認した結果を記載する。また、チェック項目ごとにNIST が提供するサイバーセキュリティフレームワークとの対応関係も合わせて提示する。

抽出軸		NISTフレームワーク対応	サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0		米国政府機関 制御システムセキュリティガイドライン（全般） 1.0版		IoTセキュリティガイドライン ver 1.0		中小企業の情報セキュリティガイドライン 第３版	
指示	カテゴリ		記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容
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	経営者のリスク認識	(−)	0	－	1	P35 ・定性的リスク分析のアウトプットは、全体的な可能性と結果のランキングを持つ資産またはシナリオのリストで構成されます。これらの順位に基づき、項目に対する適切な対応を決定することは、経営者の責任である。	2	P14 要点1. 経営者がIoT セキュリティにコミットする (2)解説 IoT においては、リスクが多様化・波及し、企業の存続に関わる影響をもたらす可能性がある。また、そのリスク対策にはコストを要するため、開発現場の判断を超える場合も多いと想定される。そこで、経営が率先して対応方針を示すことが必要と考えられる。	2	P6 1.情報セキュリティ対策を怠ることで企業が被る不利益 （企業が被る主な不利益） ・金銭の損失 ・顧客の喪失 ・業務の停滞 ・従業員への影響（以下、略）
	経営者によるセキュリティポリシーの策定・宣言	(ID.GV−1)	2	P58 ・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する。	1	P45 ・セキュリティポリシーは、組織が許容可能なレベルのセキュリティを維持するための一貫したプログラムに従うことを可能にする。ポリシーは、企業レベルで確立されたガバナンスまたは管理ポリシーから、セキュリティ管理の詳細を定義する運用ポリシーまで、組織内のさまざまなレベルで定義される。最も具体的なレベルのポリシーは、セキュリティ監査がコンプライアンスを測定するための、組織の文書となる。 ・セキュリティポリシーとは、組織が機密かつ重要なシステムリソースをどのように保護するかを指定または規制する規則である。ポリシーには、何が必須であるかが明確に示されている。ポリシーは必須であり、曖昧でないため、監査が可能になる。また、組織のセキュリティポリシーは、法律、規制、契約上の義務も考慮に入れている。セキュリティポリシーは、監査が組織の実際の運用をテストするための物差しとなる。	2	P14 要点1. 経営者がIoT セキュリティにコミットする (2)解説 「サイバーセキュリティ経営ガイドライン」を踏まえIoT セキュリティに関する基本方針を策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。また、そのために必要な体制・人材を整備する。	2	P12 3.経営者は何をやらなければならないのか （2）実行すべき「重要7項目の取組」 取組1 情報セキュリティに関する組織全体の対応方針を定める（以下、略）
	法律・業界ガイドラインの把握	(ID−GV−3) (DE.DP−2)	2	P59 ・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。 P90 ・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	0	－	2	P14 要点1. 経営者がIoT セキュリティにコミットする (3)対策例 経営層が「サイバーセキュリティ経営ガイドライン」を踏まえ、経営層のリーダーシップに基づいてIoT セキュリティに取り組むようにする。	1	P13 3.経営者は何をやらなければならないのか （2）実行すべき「重要7項目の取組」 取組7 情報セキュリティに関する最新動向を収集する（以下、略）
	その他		0	－	0	－	0	－	0	－
サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	(−)	2	P43 バリュークリエイションプロセスに関わるステークホルダーとの関係 ・ステークホルダーとの関係性を基礎として、継続的に自組織を取り巻くステークホルダーの関係性に関する全体像を把握し続け、組織間でサイバーセキュリティ上の役割と責任を明確化しておくことが重要である。 P57 ・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	0	－	0	－	2	第2部 P22 4.本格的に取り組む （1）管理体制の構築 ① 責任分担と連絡体制の整備（以下、略）
	関係者の役割と責任の明確化	(ID.GV−2)	2	P64 ・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。 P69 ・職務及び責任範囲(例：ユーザー/システム管理者)を適切に分離する。 P90 ・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	0	－	2	P52 要点20. IoT システム・サービスにおける関係者の役割を認識する (3)対策例 ①IoT 機器メーカやIoT システム・サービス提供者及び利用者の役割の整理 IoT 機器メーカ及びIoT システム・サービス提供者は、分野ごとに想定されるインシデントのシナリオを検討し、リスクの特定を行った上で、関係者ごとの役割を整理する。 整理した役割については、IoT システム・サービス提供者が公開するWeb や配布するドキュメント（サービス約款・マニュアル等）、提供するIoT 機器の画面等に記載・表示を行い、関係者に対してサービス開始までに周知し、システム・サービスの利用者が確認した上で、サービスの利用が開始できるような仕組みを整備する。	2	P22 4.本格的に取り組む （1）管理体制の構築 ① 責任分担と連絡体制の整備（以下、略）
	リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	(ID−GV−4)	0	－	0	－	0	－	0	－
	その他		0	－	0	－	0	－	0	－
サイバーセキュリティ対策のための資源（予算、人材等）確保	対策の明確化・費用評価・予算確保	(−)	2	P50 ・国内外の様々なガイドライン等を参照した上で、参照した文書による分類をベースに、対象とするスコープ(例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か)、対策を導入・運用する際の相対的コスト等の観点を考慮してセキュリティ対策を選択できるように、セキュリティ対策例をHigh-Advanced、Advanced、Basic の三段階のレベルに分けて示している。 P60 ・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	0	－	0	－	2	P23 4.本格的に取り組む （2）IT利活用方針と情報セキュリティの予算化（以下、略）
	人材の確保、役割の理解	(PR.AT−2) (PR.AT−3) (PR.AT−4) (PR.AT−5)	0	－	1	P50 ・セキュリティポリシーは、ポリシー自体に必要な変更を判断するために監視される。セキュリティポリシーの監視は、各ポリシー及び手順文書の一部であり、企業のセキュリティポリシーは、全体的なアプローチを定めている。各運用ポリシー及び手順文書には、ポリシーや手順そのものをいつ、誰がレビューし、更新するかが記載されている。 ・トレーニングプログラムは、新入社員、オペレーション、メンテナンス、アップグレード、後継者育成のために用意されるべきです。トレーニングプログラムは十分に文書化され、構造化され、運用環境の変化を取り入れるために一定期間ごとに更新されるべきである。	0	－	0	－
	組織内の人材育成	(PR.AT−1)	2	P72 ・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 P72 ・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	1	P50 ・セキュリティポリシーは、ポリシー自体に必要な変更を判断するために監視される。セキュリティポリシーの監視は、各ポリシー及び手順文書の一部であり、企業のセキュリティポリシーは、全体的なアプローチを定めている。各運用ポリシー及び手順文書には、ポリシーや手順そのものをいつ、誰がレビューし、更新するかが記載されている。 ・トレーニングプログラムは、新入社員、オペレーション、メンテナンス、アップグレード、後継者育成のために用意されるべきです。トレーニングプログラムは十分に文書化され、構造化され、運用環境の変化を取り入れるために一定期間ごとに更新されるべきである。	0	－	0	－
	セキュリティ人材のキャリアパス・待遇の設定	(−)	0	－	0	－	0	－	0	－
	継続的なセキュリティ対策の実施	(PR.AT−1)	1	P72 ・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	1	P50 ・セキュリティポリシーは、ポリシー自体に必要な変更を判断するために監視される。セキュリティポリシーの監視は、各ポリシー及び手順文書の一部であり、企業のセキュリティポリシーは、全体的なアプローチを定めている。各運用ポリシー及び手順文書には、ポリシーや手順そのものをいつ、誰がレビューし、更新するかが記載されている。 ・トレーニングプログラムは、新入社員、オペレーション、メンテナンス、アップグレード、後継者育成のために用意されるべきです。トレーニングプログラムは十分に文書化され、構造化され、運用環境の変化を取り入れるために一定期間ごとに更新されるべきである。	0	－	0	－
	その他	(PR.AT−1)	0	－	0	－	0	－	0	－

ベンチマーク抽出結果（別紙）
チェック項目に基づき、各ベンチマーク内の記載を確認した結果を記載する。また、チェック項目ごとにNIST が提供するサイバーセキュリティフレームワークとの対応関係も合わせて提示する。

抽出軸		NISTフレームワーク対応	サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0		米国政府機関 制御システムセキュリティガイドライン（全般） 1.0版		IoTセキュリティガイドライン ver 1.0		中小企業の情報セキュリティガイドライン 第３版	
指示	カテゴリ		記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容
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	情報資産の優先順位付け	(ID.AM−1) (ID.AM−2) (ID.AM−3) (ID.AM−4) (ID.AM−5)	2	P28～36 ・三層構造モデルに基づき、分析対象となるバリュークリエイションプロセスを明確化し、各層における構成要素を把握する。 P56−57 ・システムを構成するハードウェア、ソフトウェア及びその管理情報(例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報)の一覧を作成し、適切に管理する。 ・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。（以下、略） P61 ・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	1	P34 ・リスクとは、一般に、特定の脅威が特定の脆弱性を悪用し、特定の結果をもたらす確率として表される損失の予想と定義される。リスクは、脅威、脆弱性、結果の関数であり、結果とは、特定の脅威又は脆弱性によって組織の資産又は財産に生じる特定の被害により組織が経験する負の影響である。脅威と脆弱性の構成要素は、可能性という言葉で表すことができる。可能性とは、特定の行為が発生する確率のことである。 ・資産所有者は、リスクをランク付けし、リスクの見積りに緩和策または修理のコストを含めるべきである。また、最小の財務的損失で最大のセキュリティエクスポージャーを緩和するための適切な対策を決定する必要があります。	2	P18 要点3. 守るべきものを特定する (3)対策例 ①守るべき本来機能や情報の洗い出し 2) 情報の洗い出し IoT 機器・システムが収集するセンサーデータや個人情報（プライバシー含む）、所有する設計情報などの技術情報を洗い出す。また、機能を構成するソフトウェアやその設定情報も読み出されて攻撃手法の考案に利用されたり、改ざんされて不正操作されるリスクがあるため、守るべきものとして洗い出す。	2	P44 5.より強固にするための方策 （6）詳細リスク分析の実施方法 手順①　情報資産の洗い出し（以下、略）
	経営戦略を踏まえたリスクの把握	(ID.RA−3) (ID.RA−1)	2	P36-40 ・自組織の事業に対して、各層の機能が脅かされることになると想定されるセキュリティインシデント及びそのセキュリティインシデントの結果、事業に影響がどの程度及ぶかについて、事業被害レベルとして設定する。（以下、略） P56 ・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。 ・自重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。 P61-62 ・セキュリティ対策組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。（以下、略）	1	–	0	–	2	P49 5.より強固にするための方策 （6）詳細リスク分析の実施方法 手順②　リスク値の算定（以下、略）
	リスクが事業にも足たらす影響の推計	(ID.RA−4) (ID.RA−5) (ID.RM−2)	2	P41 ・1.1 及び1.2 にて実施した内容を踏まえ、抽出したセキュリティインシデントにつながるような攻撃シナリオの検討、事業被害レベル、リスク源（脅威/脆弱性）の評価等を実施する。 P61 ・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 P85-86 ・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。（以下、略） P94 ・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	1	P34-35 ・健全なリスクアセスメントの方法論は、脅威に最も近いシステムから順に、階層的なアプローチで関連するすべてのシステムを分析する必要があります。基本的なリスクアセスメントのプロセスは、3つのステップで構成される。 1) は、初期リスクを評価します。 2) リスク軽減のための対策を実施する。 3) は、残留リスクを評価する。 このプロセスのステップ 2 とステップ 3 は、残存リスクを許容レベルまで低減するために必要に応じて繰り返される。 具体的には、第2ステップでは、既存のコントロールの評価と改善策又は追加対策を追加する計画を実施すること。リスクを決定するプロセスのより詳細な説明は、IEC 62443 の将来のパートで提供される予定である。	1	P34 要点10. 安全安心を実現する設計の整合性をとる (3)対策例 ②セーフティとセキュリティの相互の影響の確認（以下、略）	2	P49 5.より強固にするための方策 （6）詳細リスク分析の実施方法 手順②　リスク値の算定（以下、略）
	リスク対応計画の策定	(ID.RA−6) (ID.RM−3)	2	P42-48 ・1.3 で実施したリスク分析により抽出されたリスクに対して、回避、低減、移転、保有の内、いずれの対応をとるかを、発生時の被害の大きさ等に基づいて検討する。 P62 ・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。IoT 機器及びIoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	1	P35 ・定性的リスク分析のアウトプットは、全体的な可能性と結果のランキングを持つ資産またはシナリオのリストで構成されます。これらの順位に基づき、項目に対する適切な対応を決定することは、経営者の責任である。組織によっては、比較的高いレベルのリスクを受け入れるもの（積極的な成長企業など）もあれば、もともとリスクを嫌う保守的な企業もある。したがって、あるレベルの残留リスクが、ある組織には受け入れられ、別の組織には受け入れられないことがある。同じ会社であっても、個々の工場が異なるリスク許容度を示すこともある。経営陣は、自社のリスク選好度や許容度を明確に定義し、理解することで、特定された残留リスクへの対応レベルをより適切に分析できるようになるはずです。 ・産業用オートメーションおよび制御システムのセキュリティに対処することは、一般に新たなリスクを導入することにはなりませんが、既存のリスクに対する異なる視点に寄与する可能性があります。例えば、安全性に関するリスクは、産業オートメーションの文脈では通常、より注目されます。 産業オートメーションと制御システムのセキュリティは、リスク許容レベルを定義するプロセスを再発明する必要はなく、組織内の他のリスク管理手法から導き出すだけでよいのです。	0	–	2	P52 5.より強固にするための方策 （6）詳細リスク分析の実施方法 手順③　情報セキュリティ対策の決定（以下、略）
	残留リスクの識別	(ID.RA−6) (ID.RM−3)	1	P63 ・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	1	P35-36 ・リスクへの対応には、いくつかの可能性があります。組織は、それぞれの状況に応じて、いくつかの行動を組み合わせてとることができます（以下、略）	0	–	0	–
	その他		0		0	–	0	–	0	–
サイバーセキュリティリスクに対応するための仕組みの構築	重要端末への多層防御の実施	(PR.AC) (PR.DS)	2	P62 ・IoT 機器及びIoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。 P68 ・IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。 ・無線接続先(ユーザーやIoT 機器、サーバ等)を正しく認証する。 P69 ・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防ぐ。（以下、P70-84にかけて記載あり）	0	–	1	P40 要点14. 機能及び用途に応じて適切にネットワーク接続する (2)解説 提供するIoT システム・サービスの機能及び用途、IoT 機器の機能・性能等を踏まえ、ネットワーク構成やセキュリティ機能の検討を行い、IoT システム・サービスを構築・接続する必要がある。機能及び用途に応じて有線接続・無線接続のどちらを選択するかを検討した上で、セキュリティ対策を実施する必要がある。また、機能・性能が限られたIoT 機器については、IoT 機器単体で必要なセキュリティ対策を実現することが困難なため、IoT システム・サービス全体でセキュリティを確保することが必要である。	2	第2部　P41　5.より強固にするための方策 （5）技術的対策例と活用 ③　アクセス管理（以下、略）
	脆弱性診断の実施・対応	(PR.IP−12)	2	P62 ・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 P80 ・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。 P88 ・自組織の管理しているIoT 機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	1	P56 ・対策の有効性及び装置やシステムの固有のセキュリティ特性は、少なくともゾーンに関連するセ キュリティ特性を監査及び/又は試験する手順に基づいて、定期的に監査及び/又は試験を行う べきである。場合によっては、新たな脆弱性の発見も監査やテストの引き金になりえる。	2	P53 要点21. 脆弱な機器を把握し、適切に注意喚起を行う (2)解説 IoT 機器に脆弱性がある場合には、その脆弱性を突いたサイバー攻撃が行われる可能性がある。そのため、IoT システム・サービスの提供者が、提供しているシステム・サービスのために設置したIoT 機器のうち、脆弱性を持つものがネットワーク上に存在していないかどうかを確認することが被害の抑制に有効である。 そのためには、新たに設置するIoT 機器だけではなく、既存のIoT 機器を含めて、機器の情報を把握する手段を整備もしくは利用し、脆弱性を持つ機器を特定する必要ある。また、脆弱性が把握された場合には、該当するIoT 機器の管理者に対して、注意喚起を実施する必要がある。	1	第2部　P41　5.より強固にするための方策 （5）技術的対策例と活用 ④　システムセキュリティ管理（以下、略）
	検知すべきイベントの特定・迅速な検知のための体制構築	(DE.AE−1) (DE.AE−5) (DE.DP−3)	2	P76 ・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。 P76 ・IoT 機器、サーバ等にて稼動するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。 P85 ・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。 ・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。（以下、P87-90にかけて記載あり）	1	P54 SL(capability)-対策、装置、システムのセキュリティレベルの能力 ・SL(能力)は、ゾーンや導管のセキュリティに寄与する、ゾーンや導管内の装置やシ ステムの対策と固有のセキュリティ特性について定義される。これは、対策や装置やシステムが対応するセキュリティー特性に対する有効性の尺度である。対策、装置またはシステムによって対処される可能性のあるセキュリティ特性の例を以下に示す。（以下、略）	1	P39 要点13. 機器等がどのような状態かを把握し、記録する機能を設ける (2)解説 様々な機器やシステムがつながった状態では、何がどのように接続し、機器やネットワーク上のどこで何が発生しているかを把握することは容易ではない。異常の発生を検知・分析して、原因を明らかにしたり、対策を検討したりするためには、個々のIoT 機器・システムがそれぞれの状態や他機器との通信状態を収集・把握することが必要である。また、発生した異常の原因究明を行う際に必要となることから、収集した情報はログとして適切に記録することが必要である。このとき、ログとして保管しても、攻撃者等によりその内容を不正に消去・改ざんされてしまうと対策が打てなくなってしまうことから、正しく記録できるよう対策を講じる必要がある。また、IoT 機器・システムの中にはセンサーなど低機能のものも含まれており、単独で大量のログの管理や、ログの暗号化などの対策を行うことが難しい場合がある。そのような機器については、他にログを管理するための機器を用意するなどの対策を行う必要がある。	0	–
	意図しないイベントへの対応計画の策定	(DE.AE−4) (DE.DP−1) (DE.DP−4)	2	P75 ・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例：ヒト、モノ、システム)を確保する。	0		0	–	0	–
	サイバーセキュリティリスクへの対応内容の見直し	(DE.DP−5)	2	P75 ・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。 P90 ・セキュリティ事象の検知プロセスを継続的に改善する。	0	P56 ・対策の有効性及び装置やシステムの固有のセキュリティ特性は、少なくともゾーンに関連するセ キュリティ特性を監査及び/又は試験する手順に基づいて、定期的に監査及び/又は試験を行う べきである。場合によっては、新たな脆弱性の発見も監査やテストの引き金になるえる。	1	P47 要点18.出荷・ リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える (3)対策例 脆弱性情報を収集・分析し、ユーザや他のシステム・サービス提供者に情報発信を行い、ファームウェアアップデート等の必要な対策を行う必要がある。なお、アップデート版の取得は、必ずIoT 機器メーカ等の信頼できるWeb サイトからダウンロードする等、信頼できる経路で、電子署名等を利用して改ざんされていないことを検証したものを取得することに留意する。	1	第1部　P13 3.経営者は何をやらなければならないのか （2）実行すべき｢重要7項目の取組｣ 取組7　情報セキュリティに関する最新動向を収集する（以下、略）
	従業員に対する教育の実施	(PR.AT−1)	2	P72 ・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 P72 ・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。 P72 ・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	1	P47 ・また、セキュリティプログラムの重要な構成要素として、トレーニングを挙げることもある。また、ポリシーに違反した場合の結果も示すことができる。経営陣は、この方針を組織全体に伝え、すべての従業員が理解できるようにする必要がある。	0	–	1	第2部　P28　4.本格的に取り組む （5）点検と改善（以下、略）
	その他		2	P68 ・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。 P77 ・IoT 機器やソフトウェアが正規品であることを定期的(起動時等)に確認する。 ・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する ・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。（以下、P79,P82-83,P90にかけて記載あり）	0	–	0	–	0	–
サイバーセキュリティ対策における PDCA サイクルの実施	経営者への対策状況の報告	(−)	2	P63 ・自組織内におけるセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する	0	–	0	–	1	P28 4.本格的に取り組む （5）点検と改善（以下、略）
	外部監査の実施	(−)	2	P80 ・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	0	–	0	–	0	–
	環境変化に応じたPDCAの整備	(PR.IP−7)	2	P67 ・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。 P79 ・構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。 P80 ・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。 P90 ・セキュリティ事象の検知プロセスを継続的に改善する。	0	–	0	–	0	–
	リスクと取組状況の外部への公開		0		0	–	0	–	0	–
	その他	–	2	P78 ・IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。 P78 ・IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する。 P80 ・保護技術の有効性について、適切なパートナーとの間で情報を共有する。 ・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	0	–	0	–	0	–

ベンチマーク抽出結果（別紙）
チェック項目に基づき、各ベンチマーク内の記載を確認した結果を記載する。また、チェック項目ごとにNIST が提供するサイバーセキュリティフレームワークとの対応関係も合わせて提示する。

抽出軸		NISTフレームワーク対応	サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0		米国政府機関 制御システムセキュリティガイドライン（全般） 1.0版		IoTセキュリティガイドライン ver 1.0		中小企業の情報セキュリティガイドライン 第３版	
指示	カテゴリ		記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容
インシデント発生時の緊急対応体制の整備	**組織内外の連絡先の整備**	(RS.CO−3) (RS.CO−4) (RS.CO−5)	2	P67 ・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。 P91 ・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	0	－	0	－	0	－
	初動対応マニュアルの整備	(PR.IP−9) (RS.RP−1)	2	P91 ・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。 P91 ・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	0	－	1	P52 要点20. IoT システム・サービスにおける関係者の役割を認識する (3)対策例 ①IoT 機器メーカやIoT システム・サービス提供者及び利用者の役割の整理 IoT 機器メーカ及びIoT システム・サービス提供者は、分野ごとに想定されるインシデントのシナリオを検討し、リスクの特定を行った上で、関係者ごとの役割を整理する。 整理した役割については、IoT システム・サービス提供者が公開するWeb や配布するドキュメント（サービス約款・マニュアル等）、提供するIoT 機器の画面等に記載・表示を行い、関係者に対してサービス開始までに周知し、システム・サービスの利用者が確認した上で、サービスの利用が開始できるような仕組みを整備する。	0	－
	インシデント対応専門チームの設置	(RS.CO−1)	2	P85 ・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	0	－	0	－	0	－
	経営者への報告ルート・公開内容等の設定	(RS.CO−2)	2	P93 ・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。 ・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	0	－	0	－	0	－
	初動対応マニュアルの見直し	(RS.IM−1) (RS.IM−2)	2	P96 ・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。 ・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	0	－	0	－	0	－
	定期的な対応訓練の実施	(PR.IP−10)	2	P72 ・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 ・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	0	－	0	－	0	－
	その他	－	2	P91 ・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。 P92 ・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う。 P95 ・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	0	－	0	－	0	－
インシデントによる被害に備えた復旧体制の整備	**業務の復旧計画の策定**	(ID.BE−5) (PR.IP−9) (RC.RP−1)	1	P93 ・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	0	－	0	－	1	P13 3.経営者は何をやらなければならないのか （2）実行すべき「重要7項目の取組」 取組5　緊急時の対応や復旧のための体制を整備する（以下、略）
	復旧計画の見直し	(RC.IM−1) (RC.IM−2)	0	－	0	－	0	－	0	－
	組織内外の連絡先の整備	(RC.CO−1) (RC.CO−2) (RC.CO−3)	1	P93 ・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	0	－	0	－	0	－
	定期的な対応訓練の実施	(PR.IP−10)	2	P72 ・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 ・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	1	P47 ・また、セキュリティプログラムの重要な構成要素として、トレーニングを挙げることもある。また、ポリシーに違反した場合の結果も示すことができる。経営陣は、この方針を組織全体に伝え、すべての従業員が理解できるようにする必要があります。	0	－	0	－
	その他	－	2	P93 ・事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。 P94 ・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。 P94 ・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	0	－	0	－	0	－
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	**システム管理の適切な委託の実施**	(ID.BE−3) (ID.BE−4)	2	P58 ・サプライチェーンにおいて、自組織が担う役割を特定し共有する。 P58 ・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	1	P49 ・セキュリティの問題には、サプライヤー、インテグレーター、保守サービスプロバイダー、コンサルタントなどの役割を担う下請け業者が関与する可能性のある業務が含まれます。下請け業者を対象とするセキュリティポリシーは、脆弱性を開く可能性のある下請け業者との相互作用に対処するものである。このポリシーでは、さまざまな関係者の責任を明確にする。プロジェクトが段階的に進行し、材料やシステムが納入されるにつれて変化する責任に対処する。この方針は、下請け業者との契約に一定の条件を書き込むことを要求する場合もある。 ・契約プログラマーを適切に管理しないと、アプリケーションの整合性が損なわれたり、プログラミングコードの保守性が損なわれたりする可能性があります。組織のプログラミングとドキュメンテーションの標準に従い、適切なテストを行い、信頼性が高く、タイムリーである、有能な契約プログラマーを見つけることが重要である。	0	－	2	P26 4.本格的に取り組む （4）委託時の対策（以下、略）
	委託先に実施を求めるセキュリティ対策の明確化	(ID.AM−6) (ID.BE−1) (PR.IP−8)	2	P51 ・企業等は、自組織のセキュリティマネジメント強化だけでなく、自身の関係するサプライチェーン上の取引先に対して、本フレームワークの特定の対策要件への準拠を求める等の手段により、取引先へのセキュリティガバナンスを強化することが可能である。 P59 ・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。 P63 ・自組織の事業に関係する自組織及び他組織(例：業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。 P64 ・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。（以下、P64-65にかけて記載あり）	1	P49 ・セキュリティの問題には、サプライヤー、インテグレーター、保守サービスプロバイダー、コンサルタントなどの役割を担う下請け業者が関与する可能性のある業務が含まれます。下請け業者を対象とするセキュリティポリシーは、脆弱性を開く可能性のある下請け業者との相互作用に対処するものである。このポリシーでは、さまざまな関係者の責任を明確にする。プロジェクトが段階的に進行し、材料やシステムが納入されるにつれて変化する責任に対処する。この方針は、下請け業者との契約に一定の条件を書き込むことを要求する場合もある。 ・契約プログラマーを適切に管理しないと、アプリケーションの整合性が損なわれたり、プログラミングコードの保守性が損なわれたりする可能性があります。組織のプログラミングとドキュメンテーションの標準に従い、適切なテストを行い、信頼性が高く、タイムリーである、有能な契約プログラマーを見つけることが重要である。	0	－	2	P26 4.本格的に取り組む （4）委託時の対策（以下、略）
	サプライチェーンのセキュリティ対策状況の把握	(−)	2	P63 ・自組織の事業に関係する自組織及び他組織(例：業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。 P65 ・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。 P66 ・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	0	－	0	－	0	－
	その他	－	2	P66 ・自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。 P67 ・取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。	0	－	0	－	0	－

ベンチマーク抽出結果（別紙）
チェック項目に基づき、各ベンチマーク内の記載を確認した結果を記載する。また、チェック項目ごとにNIST が提供するサイバーセキュリティフレームワークとの対応関係も合わせて提示する。

抽出軸		NISTフレームワーク対応	サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0		米国政府機関 制御システムセキュリティガイドライン（全般） 1.0版		IoTセキュリティガイドライン ver 1.0		中小企業の情報セキュリティガイドライン 第３版	
指示	カテゴリ		記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容	記載有無	記載箇所・内容
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	**業界団体を通じた情報共有の実施**	(ID.RA−2)	0	−	0	−	0	−	1	P31 5.より強固にするための方策 （1）　情報収集と共有 ①　情報収集の方法（以下、略）
	関係団体への情報提供の実施	(ID.RA−2)	0	−	0	−	0	−	1	P31 5.より強固にするための方策 （1）　情報収集と共有 ①　情報収集の枠組み（以下、略）
	その他	−	0	−	0	−	0	−	0	−