ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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	共通項判断		自工会/部工会-サイバーセキュリティガイドライン 2.0 版		ネットワーク機能付き事務機セキュリティガイドラインVer.1.00		通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0		制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）		スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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	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	(—)	0.69	7	1	P10 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	0	–	0	–	0	–	0	–
	経営者によるセキュリティポリシーの策定・宣言	(ID.GV-1)	1.15	9	2	P7 ・自社の情報セキュリティ対応方針（ポリシー）を策定している ・自社の情報セキュリティ対応方針を策定し、文書化すること ・自社の情報セキュリティ対応方針（ポリシー）の内容を確認し、必要に応じて見直ししている 【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針ポリシー の内容を確認、改善 1 回以上 /年 ※別途、重大な変化が発生した場合には迅速に対応すること(以下、略)	0	–	0	–	0	–	0	【ガイドA-2】R MO.4 ・スマートホーム向けのIoT機器を遠隔から管理する事業者のシステム内部や管理対象のIoT機器が取得する情報や外部に渡す（通信する）情報および保存されている個人情報等を含むデータ管理などのポリシーを提示すること。（(2) スマートホーム向けのIoT機器を遠隔から管理する事業者向け） 【ガイドA-3】SO.6 ・住まい手に関する個人情報等を含むデータ管理などのポリシーを提示し、順守すること。（(3) スマートホーム向けのサービス事業者向け）	2	–
	法律・業界ガイドラインの把握	(ID-GV-3) (DE.DP-2)	1.00	7	2	P9 ・情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している。（以下、規則, 対象, 頻度について略） ・法令の変更に伴い、ルールを適宜見直ししている（以下、規則, 頻度について略）	0	–	0	–	0	–	0	–
	その他		0.00	0	0	–	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	(—)	1.23	9	2	P10 情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること 【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	0	–	0	–	0	–	0	–
	関係者の役割と責任の明確化	(ID.GV-2)	1.23	10	2	P10 情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること 【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	0	–	0	–	1	P4 ・本書では、制御システムを管理・設計・運用・保守する現場ユーザを対象とし、制御システムをよりセキュアに構築・運用するための指針を示す。以降の節の表に記載しているA/B/C/Dは以下のとおり定義する。 A：管理者 B：設計者 C：保守担当者 D：オペレータ	0	
	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)	0.62	5	1	P10 情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること 【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	0	–	0	–	0	–	0	–
	その他		0.00	0	0	–	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	(—)	0.38	4	1	P10 情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任を明確化すること ・連絡先リストを整備すること 【規則】 ・情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、 組織的に経営判断できる体制を設置していること	0	–	0	–	0	–	0	–
	人材の確保、役割の理解	(PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)	0.92	8	2	P13-15 【目的】マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する ・電子メールのマルウェア感染に関する社内への教育を行っている（以下、規則, 対象, 頻度について略） ・インターネットへの接続に関する社内への教育を行っている（以下、規則, 対象, 頻度について略） ・機密区分に応じた情報の取り扱いに関する教育を行っている（以下、規則, 対象, 頻度について略） ・標的型メール訓練を実施している（以下、規則, 対象, 頻度について略） ・各部署の情報セキュリティ管理者に対して、組織内でその対策とマネジメント手法に関する教育を実施している（以下、規則, 対象, 頻度について略）	0	–	0	–	1	P13 ・社外の作業者に保守作業等の作業をやむなる際に、安全上の注意事項、禁則事項、機密情報の管理について明確に教育すること。	0	–
	組織内の人材育成	(PR.AT-1)	0.77	6	2	P13-15 【目的】 マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する（以下、研修内容については、当該ページ内にて個別に記載を確認）	0	–	0	–	0	–	0	–
	セキュリティ人材のキャリアパス・待遇の設定	(—)	0.15	1	0	–	0	–	0	–	0	–	0	–
	継続的なセキュリティ対策の実施	(PR.AT-1)	0.62	6	1	P15 教育・訓練の内容を必要に応じて見直ししている 【頻度】 ・教育・訓練実施前後、もしくは１回／年以上	0	–	0	–	2	P6 ・オペレータや保守担当者に対し、たとえば、パスワードの管理方法や、メモリカード、USB メモリの取り扱い、パソコンを利用する際のルールの徹底など、定期的に、セキュリティに関する教育を実施することを推奨する。	0	
	その他	(PR.AT-1)	0.00	0	0	–	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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 が定義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	共通項判断		自工会修工会・サイバーセキュリティガイドライン 2.0 版		ネットワーク機能付き事務機セキュリティガイドラインVer.1.00		通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0		制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）		スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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	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)	0.69	6	1	P18 機密区分に応じた情報の管理ルールを定めている 【規則】 ・以下の内容等を含む管理ルールを定めること ・機密の特定 ・機密区分のレベル判定と表示 ・区分に応じた取り扱い方法 ・取り扱いエリアの区分及び制限 【対象】 ・情報資産（情報）	0	–	0	–	0	–	0	–
	経営戦略を踏まえたリスクの把握	(ID.RA-3) (ID.RA-1)	0.92	8	2	P18~19 高い機密区分の情報資産情報を一覧化している 【規則】 一覧には、対象情報、管理者名、部署名、保管場所、保管期間、開示先、連絡先などを含むこと 【対象情報】 ・No.54 で定めた機密区分のうち、高レベルの機密に該当する情報資産	0	–	0	–	0	–	0	–
	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)	0.62	6	2	P20 情報資産において「機密性」「完全性」「可用性」の 3 要素が確保できなくなった場合のリスクを特定できている 【規則】 ・対象の情報資産に情報セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握すること（以下、対象、観点、方法、頻度について略）	0	–	0	–	0	–	0	–
	リスク対応計画の策定	(ID.RA-6) (ID.RM-3)	0.85	7	2	P20 必要に応じて経営層へ業務影響及び対策を報告し、セキュリティ業務に関与している社内部署と共有している 【規則】 ・No.66 で把握した業務影響に対する対策方法及び対応を策定し、報告・共有すること ・報告に際し役員からの指示があった場合、これを関係部門へ共有すること 【対象】 ・情報セキュリティの総括責任者、関係部門 【頻度】 ・１回以上／年	0	–	0	–	0	–	0	–
	残留リスクの識別	(ID.RA-6) (ID.RM-3)	0.23	3	0	–	0	–	0	–	0	–	0	–
	その他		0.38	3	0	–	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)	1.46	10	0	–	1	P17 ・PSTNファクスモデムがファクスプロトコルを用いた利用者データの送信又は受信だけにしようされ、ファクスモデム経由のネットワーク経由のネットワーク通信はできないことが顧客向けお公開情報、又は申請資料に記載されていること。 ・外部から保護されたネットワーク内でご製品を使用することをユーザーに伝えていること。	0	–	2	P7 ・制御システムを接続するネットワークは業務用ネットワーク（情報システム）との間に、ファイヤーウォールでDMZ(De-Militarized Zone)を設置して、業務用ネットワークから制御システムネットワークへメールを送らないようにしたり、制御システムネットワークからインターネット接続もしないようにしたりする対策を推奨する。	2	【恣付A-1】MO.1 ・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。 【恣付A-1】MO.4 ・IoT機器およびIoT機器を含むシステムで通信相手に対するアクセス制限機能を実装すること。（以下、略） 【恣付A-1】MO.9 ・以下のようなリソースや資産保護の機能を実装すること。・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護する機能を実装すること。（以下、略） 【恣付A-2】MO.13,MO.14 ・IoT機器に保存される鍵、認証情報や個人情報等の重要なデータを保護すること。・耐タンパー性が必要な情報を取り扱う場合、耐タンパーデバイスを利用すること。（以下、略）
	脆弱性診断の実施・対応	(PR.IP-12)	1.15	8	2	P27 脆弱性の管理体制、管理プロセスを定めている 【規則】 ・脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること ・脆弱性情報 脅威情報を収集する情報源、ツール、頻度を定めること ・収集した情報の対応要否判断基準・対応手順を定めること ・対応履歴を記録し、月次でチェックすること 社外へ公開している サーバー について、本器修機前および稼働後に脆弱性診断を 実施し、判明した脆弱性に対して対策を行っている（以下、規則、対象、診断頻度について略）	0	–	0	–	0	–	0	–	2	P27 ・IoT機器に対して、新たに発見された脆弱性に対応するため、IoT機器のソフトウェアを適切にアップデートできる仕組みを具備することが望ましい。 【恣付A-1】MO.8 ・IoT機器およびIoT機器を含むシステムのソフトウェアやファームウェアをアップデートする機能を実装し、受容できない既知のセキュリティリスクおよびセーフティに関するバグーに対応していくこと。
	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)	1.46	11	1	P34 パソコン、サーバー には、マルウェア感染を検知・通報するソフトウエア（ウイルス対策ソフト）を導入している 【規則】 ・パソコン、サーバー ごとにウイルス対策ソフトを導入すること ・機器に応じた適切なスキャン範囲と頻度を規定し、スキャンを実行すること 【対象】 ・ネットワークに接続している全てのパソコン、サーバー	0	–	1	P7 ・適切なログ管理を実施することで、悪意ある第三者等からの不正侵入、不正操作等の情報セキュリティインシデント及びその予兆を検知。インシデント発生時には、この通信ログを別ファイルに保存できるように。あとからログデータを取り出して原因解析ができるようにすることを推奨する。	2	P7 ・制御情報系ネットワークと制御システムネットワークの間にもファイヤーウォールを設置して、ネットワークの通信ログをリングバッファ形式で設置し、インシデント発生時には、この通信ログを別ファイルに保存できるように。あとからログデータを取り出して原因解析ができるようにすることを推奨する。	2	P26 ・サイバー攻撃によって引き起こされた異常な動作を検知するために、一定期間記録を残す仕組みや、異常な動作が発生しても安全側に倒れるような機能を実装することが望ましい。 【恣付A-1】MO.3 ・IoT機器およびIoT機器を含むシステムの企画・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および、セーフティに関するバザードが残存しないこと。 【恣付A-2】MO.16 ・IoT機器およびIoT機器を含むシステムの企画・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および関連するセーフティのリスクに対応すること。
	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)	0.62	5	2	P36 ログを分析し、サイバー攻撃を検知する仕組みを導入している 【規則】 ・ログを常時分析し、異常発見時に通知する仕組みを導入すること ※ 分析対象 プロキシサーバー 、IPS/IDS 、ファイアウォール、エンドポイントのいずれか、または組み合わせ 監視時間 24 時間 /365 日 機能要件 インシデントアラートが即時発報されること、インシデントの速報レポートが作成され、通知されること	0	–	0	–	0	–	2	P26 ・サイバー攻撃によって引き起こされた異常な動作を検知するために、一定期間記録を残す仕組みや、異常な動作が発生しても安全側に倒れるような機能を実装することが望ましい。 【恣付A-1】MO.11 ・システエラーを発生させないようなセットアップ機能や、システエラーがあった場合には安全側に倒れるような機能を実装すること。
	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)	1.31	9	2	P12 マルウェア感染時の対応手順は、定期的に確認され、必要に応じて、改定していること 【規則】 ・世間動向や攻撃のトレンドなどをふまえ、教育・訓練内容の見直しをすること 【頻度】 ・１回 年以上	0	–	0	–	0	–	2	【恣付A-1】MO.3 ・IoT機器およびIoT機器を含むシステムの構成要素管理や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し、IoT機器およびIoT機器を含むシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。
	従業員に対する教育の実施	(PR.AT-1)	1.15	10	2	P13~15 ※研修内容については、当該ページ内にて個別に記載を確認	0		0		2	P6 ・メペレータや保守担当者に対し、たとえば、パスワードの管理方法や、メモリカード、USB メモリの取り扱い、パソコンを利用する際のルールの徹底など、定期的に、セキュリテイに関する教育を実施することを推奨する。	0	–
	その他		0.31	2	0	–	0	–	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	(–)	0.31	4	1	P14 経営層が情報セキュリテイに関する役割と責任を理解するための機会を設けている 【規則】 ・経営層が役割と責任を理解するための説明の場を設けている ・説明内容を振返り、次回の説明内容を改善すること 【対象】 ・経営層や役員 【頻度】 ・１回以上／年	0	–	0	–	0	–	0	–
	外部監査の実施	(–)	0.62	5	0	–	0	–	0	–	0	–	0	–
	環境変化に応じたPDCAの整備	(PR.IP-7)	0.46	5	1	P11 定期的、または必要に応じて、事故時の体制を見直ししている 【頻度】 ・１回／年、もしくは、重大な情報セキュリティ事件・事故が発生した場合等	0	–	0	–	0	–	0	–
	リスクと取組状況の外部への公開		0.23	3	0	–	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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	共通項判断		自工会修工会・サイバーセキュリティガイドライン 2.0 版		ネットワーク機能付き事務機セキュリティガイドラインVer.1.00		通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0		制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）		スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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	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)	0.31	4	1	P11 情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任が明確化されていること ・情報セキュリティ事件・事故の基準や社内外組織との連絡先、ルートが明確化されていること	0	–	0	–	0	–	0	–
	初動対応マニュアルの整備	(PR.IP-9) (RS.RP-1)	0.92	7	1	P11 発生した情報セキュリティ事件・事故対応が実施され、事故の概要や影響および対応内容の記録がある 【規則】 ・情報セキュリティ事件・事故発生後の初動対応フローが整備されていること ・情報セキュリティ事件・事故の報告フォーマットが整備されていること	0	–	0	–	0	–	0	–
	インシデント対応専門チームの設置	(RS.CO-1)	0.54	5	0		0	–	0	–	0	–	0	–
	経営者への報告ルート・公開内容等の設定	(RS.CO-2)	0.38	5	0	–	0	–	0	–	0	–	0	–
	初動対応マニュアルの見直し	(RS.IM-1) (RS.IM-2)	0.31	4	1	P11 定期的、または必要に応じて、事故時の体制を見直ししている 【頻度】 ・１回／年、もしくは、重大な情報セキュリティ事件・事故が発生した場合等	0	–	0	–	0	–	0	–
	定期的な対応訓練の実施	(PR.IP-10)	0.46	6	1	P13-15 ※研修内容については、当該ページ内にて個別に記載を確認	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	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)	0.62	7	2	P37 事業継続上重要なシステムについては、管理に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている 【規則】 ・ 求められる復旧ポイントへ復帰可能なバックアップ及びトランザクションデータログを保管すること。 ・ 求められる復旧時間でリストアできる手順書を整備すること 【対象】 ・ 事業継続上重要なシステム	0	–	0	–	0	–	0	–
	復旧計画の見直し	(RC.IM-1) (RC.IM-2)	0.31	3	2	P12 マルウェア感染時の対応手順は、定期的に確認され、必要に応じて、改定していること 【規則】 ・世間動向や攻撃のトレンドなどをふまえ、教育・訓練内容の見直しをすること 【頻度】 ・ １ 回 年以上 情報セキュリティ事件・事故を含めた自社の事業継続計画又は緊急時対応計画は、定期的に確認され、必要に応じて改定していること 【頻度】 ・ １ 回以上／年	0	–	0	–	0	–	0	–
	組織内外の連絡先の整備	(RC.CO-1) (RC.CO-2) (RC.CO-3)	0.15	2	1	P11 情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している 【規則】 ・情報セキュリティを統括する役員（ CISO 等 ）や情報セキュリティ担当部署の役割・責任が明確化されていること ・情報セキュリティ事件・事故の基準や社内外組織との連絡先、ルートが明確化されていること	0	–	0	–	0	–	0	–
	定期的な対応訓練の実施	(PR.IP-10)	0.46	6	1	P13-15 ※研修内容については、当該ページ内にて個別に記載を確認	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	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)	0.31	3	2	P22 外部情報システムの一覧を定期的、または必要に応じて見直している 【規則】 ・定期的に棚卸を実施するとともに、新規あるいは利用中止するものを一覧に反映すること 【頻度】 ・ １ 回／年以上、かつ、新規開始あるいは利用中止時	0	–	0	–	1	P13 ・社外の作業者に保守作業等の作業をやむなく際に、安全上の注意事項、禁則事項、機密情報の管理について明確に教育すること。また、その教育の実績記録を保管すること。	0	
	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)	1.38	10	2	P21 IT 機器調達に対するセキュリティ要求事項を購入先と共有しており、購入時の評価結果を記録し保管している 【規則】 ・セキュリティ要求事項が購買契約等に明記されていること ・機器調達時に、セキュリティ要求事項の評価を実施し、結果が保管されていること ・定期的に棚卸結果が保管されていることを確認する 【対象】 ・ 社内ネットワークに接続する IT 機器 【保管状態の確認頻度】 ・ １ 回以上 年	0	–	0	–	1	P13 ・社外の作業者に保守作業等の作業をやむなく際には、事前に審査登録済みの作業者または会社カどうかをチェックすること。また、入退室の管理やオペレータを認証する仕組みを導入することを推奨する。	2	P27 ・スマートホーム向けIoT機器を提供する事業者は、IoT機器の誤操作や誤使用を防ぐため、「設置方法」、「使用環境」、「正しい使い方」、「IoT機器内に保存される情報」、「IoT機器が外部と通信する情報」、「サポート期間」など、IoT機器に関するガイドやポリシーを提供すること が望ましい。 ・また、このガイドには、発生しうるセキュリティインシデントや住まい手などへの危害についても記述しておくことが望ましい。 【添付A-1】MO.10 ・セキュリティ確保、セーフティ確保のために必要な事項だけでなく、IoT機器および IoT 機器を含むシステムに保存される情報や外部と通信する情報などを記載したガイドを提供すること。・サポートする端末化スイートや機器の代態等のセキュリティに関する情報はIoT機器の管理者機能などを介して提供すること。
	サプライチェーンのセキュリティ対策状況の把握	(–)	0.31	2	0	–	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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	共通項判断		自工会部工会-サイバーセキュリティガイドライン 2.0 版		ネットワーク機能付き事務機セキュリティガイドラインVer.1.00		通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0		制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）		スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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	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)	0.15	2	1	P10 【概要】 ・サイバー攻撃や脆弱性に関する公開情報、非公開情報を活用する体制を構築している	0	–	0	–	0	–	0	–
	関係団体への情報提供の実施	(ID.RA-2)	0.23	2	0	–	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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 が要求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を合わせて提示する。

抽出軸		NISTフレームワーク対応	共通項判断		鉄道分野における情報セキュリティ機保に係る安全ガイドライン 第４版		装備品等及び役務の調達における情報セキュリティ基準		ビル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第1版		電力制御システムセキュリティガイドライン JEAG 1111-2019	
カテゴリ内容	チェック項目		①スコア１超	②ガイドライン多（中分以上にあたる７事例）	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	(--)	0.69	7	1	P3 ・重要インフラ事業者等は、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場であり、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に記載された「機能保証（1.1.5(4)参照）の考え方」は踏まえ、サービスの提供に必要な情報システム（1.1.5(4)参照）のセキュリティを機保するなど、必要な対策に常に関与組むことが重要である。具体的には、情報セキュリティに係るリスクへの必要な備えや、有事の際の適切な対応体制を実現することなどであり、特に、経営層（1.1.6(1)参照）が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略上の位置付け、情報セキュリティに係るリスクマネジメントの実施等により、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要となっている。	1	P8 ・経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て、情報セキュリティ基本方針等の承認等を通じて、自社における情報セキュリティの確保に努めるものとする。	1	P28 ・新築の大規模オーナービルの場合、オーナーの意向に沿って最も自由にビルのサイバーセキュリティ対策を選択していけるものとなる。これから建設するビルであれば、全ての選択肢が選択可能であり、大規模ビルの建設コストを考えれば、サイバーセキュリティに当てるコストは相対的に比較的に小さいものと予想される。あとは、ビルの目的や用途の重要度等を考え、最も適当な選択肢を選んでいけば良い。なお、最低限実施すべきと考えられる対策については、基本的に全てを盛り込むことが望ましいと思われる。	2	P7 経営層の責任 ・経営層は電力制御システム等におけるセキュリティの確保について責任を負うこと。 ・経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラ以外の社会的責任を果たすための セキュリティ対策が実行されない可能性がある。
	経営者によるセキュリティポリシーの策定・宣言	(ID.GV-1)	1.15	9	2	P12 情報セキュリティ方針の策定・見直し 【主旨・目的】 ・重要インフラ防護のために、情報セキュリティ対策における根本的な考え方（以下、情報セキュリティ方針）を示す必要がある。 【対策項目】 ・最高情報セキュリティ責任者は、重要インフラ防護の目的、目指すべき姿、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を情報セキュリティ方針として策定すること。また、情報セキュリティ方針の策定・見直しに係る主旨組織、目的、権限、構成員、見直し要件等についても規定すること。経営層は、情報セキュリティ確保のため、情報セキュリティ対策に取り組むことを情報セキュリティ方針等に含め、組織の内外に対して宣言する。情報セキュリティ方針が妥当かつ有効であることを定期的な期間で確認するとともに、自組織を取り巻く状況に大きな変化が発生した場合にも確認する。	2	P5 情報セキュリティ基本方針等の作成及び変更 ・防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を作成し、経営者等の承認を得るものとする。 P5 情報セキュリティ基本方針等の周知等 ・保護すべき情報の管理全般に係る組織的な責任を負う者（以下「総括者」という。）は、情報セキュリティ基本方針等を取扱者に周知するものとする。	2	0	–	2	P7 経営層の責任 ・経営層は電力制御システム等におけるセキュリティの確保について責任を負うこと。 ・経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラ以外の社会的責任を果たすための セキュリティ対策が実行されない可能性がある。
	法律・業界ガイドラインの把握	(ID-GV-3) (DE.DP-2)	1.00	7	2	P2 「安全ガイドライン」の策定 ・各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。このことを踏まえ、「指針」においては、各重要インフラ事業者等の特性や行為に関する基準又は参考となる資料を「安全基準等」と呼び、次のとおり定めている。 ①関係法令に基づき国が策定するもの（強制基準） ②関係法令に準じて国が定めるもの（推奨基準）及びガイドライン ③関係法令や国民からの期待に応えるべく重要インフラ事業者等が自ら定めるもの（自主的な取組） ④関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定めるもの（内規）等	2	P5 ・防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を作成し、経営者等の承認を得るものとする。 P5 ・防衛関連企業は、情報セキュリティ基本方針等を内成又は変更する場合、本基準との適合性に関する防衛省の確認を受けるものとする。	1	P45 付録B 3DCC の建物設備システム/ファシリティズの関係 ・建物設備の情報インフラの類型セキュリティ対策モデルとして、日本データセンター協会が「建物設備システム/ファシリティズ」を発刊している。これは、データセンターをモデルケースとし、建物設備システムのセキュリティの考え方についてまとめたガイドラインで、21 の管理策を提示している。 この21の管理策では、物理的設計における管理策、建物設備システム構築時における管理策、設備システム運用における管理策に分類して、建物設備システムのセキュリティ対策の要件を分類、整理しており、どんにおけるライフサイクルの考え方を一部取り込んでいる。 ビルサプフォーミングループでは、この21 の管理策をベースとして参照しつつ、データセンター以外のビル全般にわたるスタークホルダによる議論で、より幅広い対象、状況に対応したガイドラインの策定を進めている。	2	P7 経営層の責任 ・経営層は電力制御システム等におけるセキュリティの確保について責任を負うこと。 ・経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラ以外の社会的責任を果たすための セキュリティ対策が実行されない可能性がある。
	その他		0.00	0	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	(--)	1.23	9	1	P6 情報セキュリティ責任者 ・情報セキュリティ責任者は、情報セキュリティ対策の運用が可能となる組織のまとまりごとの長の責任者（組織のまとまりの単位が事業部であれば事業部長クラスが相当）であり、所管する組織の情報セキュリティ対策を推進及び運用するため、組織内の体制整備及び事務を行うこと。 また、組織内が実施手順を策定するとともに、情報セキュリティ対策の運用実態をセキュリティ監査し、実務レベルでの管理の仕組みを確立し、すべての取扱者への責務の周知や教育を行う等、個別対策を機能させる環境を整備すること。	2	P7-8 情報セキュリティの確保（以下、略） P15-16 ・経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、組織者は、SOC機能が事故等対処の各段階に対応し得る体制、責任及び手順を定めるものとする。（以下、略）	2	P32 ・リスクアセスメントを実施し、その結果を基に監理監査部からの「運用する管理体系」などを運用計画として定義・整備する。 P36 ・サーバ室、区画への入退室を適切に管理する。 ・関係者以外立ち入らせない。 P38 ・各種制御間の連結は、業界ごとに使われる規格の儀式外を使用する。 ・保守時の対応等も考慮して選択し導入する。 ・適切に管理された専用の室、区画の中に機器を設置する。 ・機器類は許可された作業員以外が容易に触れないようにする	2	P7 管理組織の設置 ・目的実現のためのセキュリティ管理責任組織を設置し、セキュリティガバナンスの構築を行うこと。 ・セキュリティ管理を推進する責任主体として、セキュリティ管理責任組織を設置し、電気事業者全体のセキュリティガバナンスの構築を行う。経営層はセキュリティの確保に必要な資源を準備し、実施可能な体制を構築する。なお、セキュリティ管理責任組織の設置にあたっては、セキュリティ面での戦略マネジメントに関する機能の配置にも留意する。 P9 役割（以下、略）
	関係者の役割と責任の明確化	(ID.GV-2)	1.23	10	2	P16 CSIRT 等の整備、関連部門との役割分担等の合意 【主旨・目的】 ・サイバー攻撃(又はその特性を考慮したBCP 等の実行)に必要な組織体制のひとつとして、CSIRT（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。CSIRT 等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。特に、制御システム保守運用の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応に制御システム関係運用部門の専門知識が要求されるため可能性を十分に認識しておく必要がある。また、サイバー攻撃に迅速に対応する観点から、情報セキュリティの専門知識を持つ組織を含めた対処体制を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及び情報セキュリティ関係機関との連携が有効である。（以下、対策項目について略）	2	p6 ・経営者等は、取扱者の指定の範囲を業務の遂行上必要最小限度に制限するとともに、次に掲げる事項に合意した者の中からふさわしい者を取扱者に指定するものとする。（以下、略） ・経営者等は、保護すべき情報に係る全ての情報セキュリティの責任を明確にするため、取扱者のうち、ふさわしい認める者を次に掲げる者に指定するものとする。（以下、略） p7 ・経営者等は、保護システムに係る全ての情報セキュリティの責任を明確にするため、保護システム利用者のうち、ふさわしい認める者を次に掲げる者に指定するものとする。（以下、略） p8 ・経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て、情報セキュリティ基本方針等の承認等を通じて、自社における情報セキュリティの確保に努めるものとする。	2	P32 ・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。 P34 ・防災センター（中央監視室）への入場者を登録（事前、都度）して管理するよう仕組みを入れる。 ・防災センター（中央監視室）への入退室をわたりチェック、管理するよう仕組みを入れる。 ・作業員の作業状況を常時監視する仕組みを入れる。 ・許可された作業員以外が作業できない仕組みを入れる。 P35 ・権限者以外、容易にシステム内部の構造が見られないようにする。	2	P9 役割の定義 ・システム関係者に対して、セキュリティに関する役割を明確にし、それぞれの役割を理解させる。なお、役割の定義にあたっては、システム関係者とセキュリティ管理責任組織が、互いに協力しながらセキュリティに関する取組み・管理を行えるよう留意する。）	1	P9 役割の定義 ・システム関係者に対して、セキュリティに関する役割を明確にし、それぞれの役割を理解させる。なお、役割の定義にあたっては、システム関係者とセキュリティ管理責任組織が、互いに協力しながらセキュリティに関する取組み・管理を行えるよう留意する。）
	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)	0.62	5	1	PS1 情報セキュリティ対策の運用状況把握 【対策の指針】 経営層は、情報セキュリティ対策の運用状況について、把握する。 【主旨・目的】 情報セキュリティ対策は、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、リスクマネジメントと情報セキュリティ対策が整合する取組となるように留意する。これらが整合するよう情報セキュリティ対策を経営層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営層も関与した全社的な体制の下で情報セキュリティ対策に取り組む必要がある。	2	P6 取扱者の指定等 ・経営者等は、取扱者の指定の範囲を業務の遂行上必要最小限度に制限するとともに、次に掲げる事項に合意した者の中からふさわしい者を取扱者に指定するものとする。（以下、略） ・経営者等は、保護すべき情報に係る全ての情報セキュリティの責任を明確にするため、取扱者のうち、ふさわしい認める者を次に掲げる者に指定するものとする。（以下、略） ・管理者は、取扱者にて指定した個人の氏名、生年月日、所属する部署、役職及び関係等を記載したリスト(以下「取扱者名簿」という。)を作成又は更新し、取扱者に保護すべき情報を取り扱わせる前に、防衛省の確認を受けるものとする。（以下、略） ・管理者は、取扱者の退職、異動、職務内容の変更などの理由により、保護すべき情報にアクセスする必要がなくなった場合は、取扱者名簿を更新するとともに、当該取扱者との面談等により、守秘義務を再確認するものとする。	0	–	0	–	2	P7 管理組織の設置 ・セキュリティ管理を推進する責任主体として、セキュリティ管理責任組織を設置し、電気事業者全体のセキュリティガバナンスの構築を行う。経営層はセキュリティの確保に必要な資源を準備し、実施可能な体制を構築する。なお、セキュリティ管理責任組織の設置にあたっては、セキュリティ面での戦略マネジメントに関する機能の配置にも留意する。
	その他		0.00	0	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	(--)	0.38	4	2	P27 （体制）の観点 予算・体制（委託先を含む）の確保 【対策の指針】 ・情報セキュリティ対策を計画に沿って進めるにあたり、情報システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクを考慮して適切に配分すること。	0	–	0	–	0	–	1	P4 ・「セキュリティ面での戦略マネジメント」とは、セキュリティ戦略の検討やセキュリティ事故対応の中核を担い、経営層との橋渡しを行うこと。また、セキュリティを経営・事業リスクのひとつとして認識した上で、経営計画や投資計画の策定にも関わること。
	人材の確保、役割の理解	(PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)	0.92	8	1	P29 人材育成・配置・ノウハウの蓄積 【対策の指針】 ・システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このことから、情報セキュリティ対策に係る担当者が変更になっても情報セキュリティ対策の水準を維持できるよう、ノウハウを組織するとともに、業効性を考慮した継続的な人材育成と配置を行う。また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＩＴに操作者も対象であることから、全社的に行う。さらに、情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を種保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び調金政策をあらかじめ検討しておくことが重要となる。	2	P11 ・防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。（以下、略） ・経営者等は、総括者、管理者、保護システム管理者、保護システム担当者に対しては、前項に掲げる事項に加え、それぞれの職責等に関する教育を行うものとする。 ・管理者は、新たな取扱者の指定、取扱者の異動及び職務内容の変更、保護システムの変更が生じる場合その他必要があると判断する場合に、第１項に規定する教育及び訓練を行うものとする。	1	P32 ・CLシステムに対して十分なセキュリティ知識を持った技術者の元で設計を実施する体制を整える。	2	P10 教育の計画・実施 ・システム関係者が役割に応じたセキュリティ教育を受けることができるように教育を計画及び実施し、セキュリティに関する知識とスキルを持つ人材を育成する。なお、セキュリティ教育は定期的に実施する。なお、実施にあたっては、組織として知識とスキルを継続的に蓄積できるよう人材の配置に留意するとともに、組織内の関係機関が提供する教育の場合や資格制度等の活用も考えられる。
	組織内の人材育成	(PR.AT-1)	0.77	6	2	P29 人材育成・配置・ノウハウの蓄積 【対策の指針】 ・システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このことから、情報セキュリティ対策に係る担当者が変更になっても情報セキュリティ対策の水準を維持できるよう、ノウハウを組織するとともに、業効性を考慮した継続的な人材育成と配置を行う。また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＩＴに操作者も対象であることから、全社的に行う。さらに、情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を種保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び調金政策をあらかじめ検討しておくことが重要となる。	1	P11 ・防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。（以下、略） ・経営者等は、総括者、管理者、保護システム管理者、保護システム担当者に対しては、前項に掲げる事項に加え、それぞれの職責等に関する教育を行うものとする。 ・管理者は、新たな取扱者の指定、取扱者の異動及び職務内容の変更、保護システムの変更が生じる場合その他必要があると判断する場合に、第１項に規定する教育及び訓練を行うものとする。	0	–	2	P10 教育の計画・実施 ・セキュリティ教育を計画し、実施すること。 教育効果の確認 ・セキュリティ教育の効果を確認すること。 ・システム関係者が役割に応じたセキュリティ教育を受けることができるように教育を計画及び実施し、セキュリティに関する知識とスキルを持つ人材を育成する。なお、セキュリティ教育は定期的に実施する。なお、実施にあたっては、組織として知識とスキルを継続的に蓄積できるよう人材の配置に留意するとともに、組織内の関係機関が提供する教育の場合や資格制度等の活用も考えられる。
	セキュリティ人材のキャリアパス・待遇の設定	(--)	0.15	1	2	P29 人材育成・配置・ノウハウの蓄積 【対策の指針】 ・システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このことから、情報セキュリティ対策に係る担当者が変更になっても情報セキュリティ対策の水準を維持できるよう、ノウハウを組織するとともに、業効性を考慮した継続的な人材育成と配置を行う。また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＩＴに操作者も対象であることから、全社的に行う。さらに、情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を種保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び調金政策をあらかじめ検討しておくことが重要となる。	0	–	0	–	0	–
	継続的なセキュリティ対策の実施	(PR.AT-1)	0.62	6	1	P29 人材育成・配置・ノウハウの蓄積 【対策の指針】 ・システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このことから、情報セキュリティ対策に係る担当者が変更になっても情報セキュリティ対策の水準を維持できるよう、ノウハウを組織するとともに、業効性を考慮した継続的な人材育成と配置を行う。また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＩＴに操作者も対象であることから、全社的に行う。さらに、情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を種保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び調金政策をあらかじめ検討しておくことが重要となる。	1	p11 情報セキュリティ教育及び訓練 ・防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。	0	–	0	–
	その他	(PR.AT-1)	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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が要求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を合わせて提示する。

抽出物		NISTフレームワーク対応	共通項判断		鉄道分野における情報セキュリティ機保に係る安全ガイドライン 第４版		装備品等及び役務の調達における情報セキュリティ基準		ビル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第1版		電力制御システムセキュリティガイドライン JEAG 1111-2019	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（※少なくとも2つあるまで参照）	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)	0.69	6	0	–	1	P2 ・保護すべき情報とは、装備品等及び役務の調達に関する情報のうち、防衛省が企業に保護を求める情報として指定したものをいう。 P8 保護すべき情報の分類 ・防衛関連企業は、保護すべき情報を他の情報から明確に区別できるよう適切に分類し、厳格に管理するものとする。 保護すべき情報の目録の作成等 ・管理者は、保護すべき情報を保管した場所、保存した保護システム、可搬記憶媒体等、保護すべき情報の管理状況を記載した目録を作成するものとする。	1	P19 ・図では企業という書き方をしているが、まず対象のアセット（資産）を明確化し、それに対して想定されるインシデントや被害レベルを設定し、リスクの特定を行う。 P19 ・ビルシステムにおけるサイバーセキュリティ対策を検討するとき、前提に述べたようにまずセット（資産）の明確化を行う。即ち対象となるシステムの構成として、どのような機器がひとつに接続されているかを把握する作業を実施する。同様に、各機器ごとんやのどこに置かれているから、物理的なセキュリティを検討するとき、重要な情報となる。	0	–
	経営戦略を踏まえたリスクの把握	(ID.RA-3) (ID.RA-1)	0.92	8	2	P55 「平時」の観点 【対策の指針】 ・情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に孤みつリスクを特定（リスク特定）する。特定したリスクについて、定性又は定量的なリスク分析（リスク分析）を行い、事業にのひような損害を与えるかといった具体的な影響等を決定する。リスク特定及び(リスク分析の結果について)は、前述のＰlan（計画）のリスク評価及び(リスク対応に)同じ。なお、重要インフラサービスを安全かつ持続的に提供するために、重要インフラの分野やサービス特性によっては、情報セキュリティリスクに加えて、HSE 等の観点はして、例えば、重要インフラサービスの提供を行う際の衛安全・衛生の確保や、重要インフラサービスの利用者の安全・健康の確保、重要インフラサービスに提供に伴う環境負荷の低減等が考えられる。	1	P18 ・組惑者は、前項に規定するリスク雪定を実施する場合は、連やかにその結果を記載した文書を作成し、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。 ・組惑者は、前項に規定するリスク雪定結果を記載した文書について、文書にんび保管する場合は、施錠したひかカー等により、データに保存する場合には、暗号化により、必要な期間保管又は保存するものとする。 ・組惑者は、第１項に規定するリスク雪定を実施する場合は、保護すべき情報及び保護システムへの不正なアクセス、開示、使用、改ざん及び破壊等が及ぼす被害、脅威及び脆弱性の程度を複合的に評価するものとする。	1	P19 ・図では企業という書き方をしているが、まず対象のアセット（資産）を明確化し、それに対して想定されるインシデントや被害レベルを設定し、リスクの特定を行う。 P19 ・いずれの図においても、場所そこに置かれる機器の関係においては、それは違いがないことが分かる。場所やそこに置かれる機器の脆弱性等も踏まえた時、ビルシステムに共通的に考えられるリスクポイントを整理したのが次図である。	2	P13 ・セキュリティ対策は、事業計画に沿ってセキュリティ管理責任組織のもとで策定した方針にしたがって計画し、対象システムやネットワーク構成を把握したうえで、最適なリスクアセスメント手法を用いて選択する。セキュリティ対策の実施が困難な場合は、残存リスクとして識別し、次の改善時に対応が検討できるように文書に残す。セキュリティ事故発生時も、影響を最小限にとどめることを基本的な考え方とし、サービス継続の観点にも留意し、対策を計画する。 P14 代表的なリスクアセスメント手法（例）（以下、略） P17 ・通信路上のセキュリティ機保が必要な区間を予め定め、その内容に従って通信プロトコルを選択することが望ましい。採用した通信プロトコルについては、ぜい弱性情報を定期的に収集することが望ましい。また、通信プロトコルをカスタマイズする場合は、当初のセキュリティ機能を損なうことがないように実装することが望ましい。
	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)	0.62	6	2	P55 「平時」の観点 【対策の指針】 ・情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に孤みつリスクを特定（リスク特定）する。特定したリスクについて、定性又は定量的なリスク分析（リスク分析）を行い、事業にのひような損害を与えるかといった具体的な影響等を決定する。リスク特定及び(リスク分析の結果について)は、前述のＰlan（計画）のリスク評価及び(リスク対応に)同じ。なお、重要インフラサービスを安全かつ持続的に提供するために、重要インフラの分野やサービス特性によっては、情報セキュリティリスクに加えて、HSE 等の観点はして、例えば、重要インフラサービスの提供を行う際の衛安全・衛生の確保や、重要インフラサービスの利用者の安全・健康の確保、重要インフラサービスに提供に伴う環境負荷の低減等が考えられる。	1	P18 ・組惑者は、第１項に規定するリスク雪定を実施する場合は、保護すべき情報及び保護システムへの不正なアクセス、開示、使用、改ざん及び破壊等が及ぼす被害、脅威及び脆弱性の程度を複合的に評価するものとする。	1	P19 一般的なサイバーセキュリティ対策のスキーム ・次に事業被害や脅威について分析と評価を行う。この評価結果をもとに、改善の必要な箇所を抽出しリスクの低減対策を実施する。	0	–
	リスク対応計画の策定	(ID.RA-6) (ID.RM-3)	0.85	7	2	P11 リスクアセスメント及び(リスク)対応 【主旨・目的】 ・情報セキュリティ対策は、日々の情報セキュリティ対策の運用状況に応じて適宜見直さなければ、新たな脅威に対応できない。そのため、情報セキュリティ対策の運用において発見・駄増したリスクを考慮し、既存の情報セキュリティ対策を適宜見直す必要がある。 【対策項目】 ・重要インフラサービスの安全かつ持続的な提供に重要な与える、情報セキュリティに係るリスク管理に管理すべく、次のような手順によって情報セキュリティリスクアセスメントを実施すること。なお、重要インフラサービスを安全かつ持続的に提供するためには、重要インフラの分野やサービス特性によっては、情報セキュリティリスクに加えて、HSE(ふくろ)参照)等の観点からのリスクも特定し、分析・評価を行うことが期待される。（以下、手順について略）	2	P15-16 ・経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、組惑者は、次に掲げる事故等対応の各段階に対応し得る体制、責任及び手順を定めるものとする。（以下、略）	0	P32 表4－１ 4.体制構築等 (4) セキュリティポリシー ・設計要件・運用要件を明記する。 P31 表4－１ 2.バックアップデータ／事業継続 (1) セキュリティポリシー ・システムのバックアップ方法を運用側と検討したうえでバックアップ方法を設計時に仕様を組み込む。 ・管理ポイントや運転スケジュール等、システムを運用するにあたっての要なデータについては、バックアップを取得する機能を具備する。	1	P13 ・セキュリティ対策は、事業計画に沿ってセキュリティ管理責任組織のもとで策定した方針にしたがって計画し、対象システムやネットワーク構成を把握したうえで、最適なリスクアセスメント手法を用いて選択する。セキュリティ対策の実施が困難な場合は、残存リスクとして識別し、次の改善時に対応が検討できるように文書に残す。セキュリティ事故発生時も、影響を最小限にとどめることを基本的な考え方とし、サービス継続の観点にも留意し、対策を計画する。
	残留リスクの識別	(ID.RA-6) (ID.RM-3)	0.23	3	1	P12 ・リスクアセスメントで抽出した情報セキュリティリスクに対し、具体的な対応方法を決定するこ。 ・リスク対応の選択肢には、「低減」「回避」「移転（共有）」「保有（受容）」があり、「事象の結果による重要への影響度合い」や「事象の発生可能性」等を踏まえて、適切に考え方られるものを選定するこ。	0	–	0	–	2	P33-39に当けて回表等を含め記載	2	P17 ・データが保管、改ざんされた場合のリスクを考慮し、必要に応じてデータを暗号化することが望ましい。暗号を用いる場合は、適用範囲、暗号アルゴリズムの種別、強度及び品質を考慮し、暗号方式も選択し、暗号鍵も適切に配付し、管理することが望ましい。 P20 ・予め許可された機器以外の接続を許可しない仕組みも講じることが望ましい。 ・通信相手が予め許可された機器であることを確認する仕組みも講じることが望ましい。 ・電力制御用ネットワーク内において、利用目的毎に応じてネットワーク分け留することが望ましい。
	その他		0.38	3	0	–	0	–	1	P24-26 ・ビルシステムに対するサイバーセキュリティ上のリスクを考えるよって、IT システムや他の制御システムとは違うビルシステム特有の特徴について、事前に把握しておくことが重ある。 ・ビルシステムの大きな特徴として、次のような点を挙げることができる。（以下、略）	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)	1.46	10	2	P18 格付けに応じた情報の保存 ・システム管理者は、サーバ装置、端末に保存された情報の格付けに従って、適切なアクセス制御を行うこと（以下、略） 情報の保存期間 ・取扱者は、サーバ装置、端末又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること（以下、略）	2	P25-26(付紙) 保護システムの領域の確定 ・防衛関連企業は、保護システム（保護すべき情報の保存又は当該情報へのアクセスを可能とする機器に限る。以下同じ。）における保護すべき情報を取り扱う領域を定め、イントラネット及び外部ネットワークとの境界に物理的又は論理的に制御可能な措置を行うものとする。 P26(付紙) 保護すべきデータの暗号化（以下、略） P27(付紙) アクセス制御方針（以下、略）	2	P33-39に当けて回表等を含め記載	2	P17 ・データが保管、改ざんされた場合のリスクを考慮し、必要に応じてデータを暗号化することが望ましい。暗号を用いる場合は、適用範囲、暗号アルゴリズムの種別、強度及び品質を考慮し、暗号方式も選択し、暗号鍵も適切に配付し、管理することが望ましい。 P20 ・予め許可された機器以外の接続を許可しない仕組みも講じることが望ましい。 ・通信相手が予め許可された機器であることを確認する仕組みも講じることが望ましい。 ・電力制御用ネットワーク内において、利用目的毎に応じてネットワーク分け留することが望ましい。
	脆弱性診断の実施・対応	(PR.IP-12)	1.15	8	2	P52 ソフトウェアに関する脆弱性対策 ・システム管理者は、情報システム上で利用するソフトウェアに関連する脆弱性情報の収集に努め、当該情報から情報システムのリスクを分析した上で、脆弱性ごとに対策計画を作成し、適切な対策を講ずること。ソフトウェアに関する脆弱性対策計画の作成にあたっては、以下【具体例について判断することが望ましい。（以下、具体例について略）	2	P38(付紙) 脆弱性スキャンの実施 (1) 保護システム管理者は、保護システム全体に対する脆弱性スキャンを定期的に行い、その結果を分析するものとする。 (2) 保護システム管理者は、社内外の脆弱性情報に加え、情報セキュリティに係る専門的な分析機関（以下「情報セキュリティ機関」という。）が発信する脆弱性情報やセキュリティに係る注意喚起及び脆弱性の情報を継続的に収集するために、当該脆弱性が保護システムに対し影響を与える可能性があると認められる場合に、保護システム全体に対し当該脆弱性に係る脆弱性スキャンを実施し、その結果を分析するものとする。 (3) 保護システム管理者は、前２号による分析の結果を記載した文書を作成するものとし、脆弱性が特定された場合は、本基準第１１項１項第４号及び第２項第１号の措置を行うものとする。	2	P31 表4－1 2.バックアップデータ／事業継続 (2) セキュリティポリシー P35 表4－2 21. HMI/HIM (8) セキュリティポリシー P36 表4－2 24.システム管理サーバ（ビルシステム主装置） (9) セキュリティポリシー P37 表4－2 31.コントローラ（DDC、PLC 等） (7) セキュリティポリシー	1	p17 ・通信路上のセキュリティ機保が必要な区間を予め定め、その内容に従って通信プロトコルを選択することが望ましい。 ・採用した通信プロトコルについては、ぜい弱性情報を定期的に収集することが望ましい。また、通信プロトコルをカスタマイズする場合は、当初のセキュリティ機能を損なうことがないように実装することが望ましい。
	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)	1.46	11	2	P37 ログの取得・管理 【主旨・目的】 ・情報システムにおけるログには、システムの動作履歴、取扱者のアクセス履歴、その他必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の重要インフラサービス障害（その予兆を含む。）を検知するための重要な材料となるものである。また、情報システムに係る脆弱性やインシデントの問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どのようにログ取得るが、また、改ざん等消失等が起こらないよう、ログが適切に保全されなければならない。（以下、対策項目略）	2	P34(付紙) システム監視の実施 防衛関連企業は、保護システムにおける不正なアクセス及び(攻撃、アカウント及び権限の不正な使用、不正な通信並びに悪意あるコード等（以下「不正なアクセス等」という。）の検知に必要な情報の収集を行うための機器の設置、ソフトウェアのインストール等を実施し、次に掲げる事項について保護システムの内部及び外部環境下における監視（以下「システム監視」という。）を実施するものとする。（以下、略） システム監視の実施に係る共通事項（以下、略） ア 防衛関連企業がシステム監視を実施する場合は、システム上の挙動を常時監視するとともに、第９第１項の規定により作成されたシステム上のログの分析結果を利用するものとする。 イ システム監視により不正なアクセス等を検知した場合は、保護システム管理者及び保護システム担当者にアラートが発せられるよう、保護システムを設定するものとする。	2	P34 表4－2 2. P37 表4－2 3.に次けて記載	2	P18 ・機器のマルウェア対策（以下、略） P19 1．不正プログラム防止（以下、略） 2．不正処理防止（以下、略） P20 1．接続制御（以下、略） 2．認証（以下、略） 3．ネットワーク分割（以下、略）
	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)	0.62	5	2	P33 構築の観点 【対策の指針】 ・重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機能性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。その際、ソフトウェアに関する脆弱性、不正プログラム、サービス不能攻撃等の様々な脅威に対して導入を要する情報セキュリティ機能、未然防止が困難な「重要インフラサービス障害発生後の拡大防止・早期復旧の対策に要する機能をできる限り明示するとともに、そもそもの不正侵入を防止するための対策に代えてまたは侵入されたら平常被害を防止するための対策について明示する。また、脆弱システム等は、一律に脆弱性対処ができない場合があるので、サイバーセキュリティ上のリスクを評価し把握した上で適切な対策をとる要がある。	1	P35(付紙) ・不正なアクセス等を検知した際の対応 ・保護システム管理者が第２項第１号イに規定するアラートを受けた場合又は検知ソフトウェアにより悪意のあるコードを検知した場合は、検知ソフトウェアによる脆弱性の情報を定期的に収集するとともに、検知された悪意のあるコードを含むファイル等のひつの、隔離若しくは削除又はそれらを適切に組み合わせた措置を実施するものとする。	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)	1.31	9	2	P11 ・情報セキュリティ対策に係るPDCA サイクルに沿って、主旨・目的、対策項目及び(具体例)をそれぞれ参考にて記述する。 ・なお、通常、Plan での分析結果を踏まえ対策を構じたと上、Do で実行に移し、一定期間経過後、Check で対策の見直しの必要性を評価し、Act で改善を実施するという流れになるが、実運用においては、Do での監視・検知の結果次第では、緊急で対策内容を見直すの要が生じる可能性がある。	2	P17 ・保護システム利用者が保護システムの脆弱性を発見又は探知した場合は、速やかに保護システム管理者に報告するものとし、保護システム管理者は、適切な対処を行うとともに、その内容、修正方法を記載した文書を作成し、組惑者に報告するものとする。 P27(付紙) ・保護システム管理者は、アセス制御方針を定期的に、及び情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合には、その都度見直しを実施し、必要に応じてアクセス制御方針を修正するものとし、修正した場合は前号による組惑者の承認を得るものとする。	2	P33 表4－2 1.ネットワーク(ウラント、情報系 NW、BACnet 等) 10 ネットワーク (3) ・不正接続の有無を定期的に点検する。 ・外部との接続や通信はファイアウォール等によ必要最小限に制限する。 P33 表4－2 1.ネットワーク(ウラント、情報系 NW、BACnet 等) 10 ネットワーク (4) ・ビルPに設置する外部接続回線を管理し、不明回線の有無等を定期的に点検する。 P34 表4－2 21.HMI/HIM (5) ・不正なアクセス操作を定期的に確認する仕組みを入れる。	2	P13 対策の点検・報告 ・セキュリティ対策が適切に実施されていることを定期的に点検し、セキュリティ管理責任者に報告する。これを行わない場合、残存リスクを正しく把握できず、適切な対策が実施されない可能性がある。 対策の改善 ・対策の点検結果に基づき、セキュリティ対策の見直しを検討する。また、環境の変化に応じて、セキュリティ対策の目的及び内容の変更を検討する。これを行わない場合、適切な対策が実施されず、ぜい弱性が露呈する可能性がある。
	従業員に対する教育の実施	(PR.AT-1)	1.15	10	1	P29 人材育成・配置・ノウハウの蓄積 【対策の指針】 ・システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このため、情報セキュリティ対策に係る担当者が変更になっても情報セキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとに、実効性を考慮した継続的な人材育成に配慮を行う。また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやテに関与者も対象とあることから、全社的に行うために、情報セキュリティ対策の推進役となるセキュリティ人材につて、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人首等を確保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び(資金政策をあらかじめ検討しておくことが重要となる。	1	p34(付紙) ・防衛関連企業は、保護システムにおける不正なアクセス及び変更、アカウント及び権限の不正な使用、不正な通信並びに悪意あるコード等（以下「不正なアクセス等」という。）の検知に必要な情報の収集を行うための機器の設置、ソフトウェアのインストール等を実施し、次に掲げる事項について保護システムの内部及び外部環境下における監視（以下「システム監視」という。）を実施するものとする。	2	P32 表4－1 3. 会社／業員の管理 （1）、表4－1 4. 体制構築等 （3）、表4－1 4. 体制構築等 （6） P34 表4－2 2. 防災センター（中央監視室） 21 HMI/HIM (1) 、表4－2 2. 防災センター（中央監視室） 22 保守用持ち込み端末 (1) P36 表4－2 2. 防災センター（中央監視室） 24 システム管理用サーバ（ビルシステム主装置） (10) P37 表4－2 31.コントローラ（DDC、PLC 等） (6) P38 表4－2 3.機械室／新館階点ボック2 31 コントローラ（DDC、PLC 等） (8)	1	p10 セキュリティ教育 1．教育の計画・実施 ・セキュリティ教育を計画し、実施すること。 ・システム関係者が役割に応じたセキュリティ教育を受けることができるように教育を計画及び実施し、セキュリティに関する知識とスキルを持つ人材を育成する。
	その他		0.31	2	0	–	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	(–)	0.31	4	1	P51 情報セキュリティ対策の運用状況把握 【対策の指針】 ・経営層は、情報セキュリティ対策の運用状況について、把握する。 【主旨・目的】 ・情報セキュリティ対策は、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、リスクマネジメントと情報セキュリティ対策が整合する効果的となるように組織する。このが整合するよう情報セキュリティ対策を経営層が担う全社的なリスクマネジメントの一部に位置付けるとともに、担当者のみならず経営層も関与した全社的な体制の下で情報セキュリティ対策に取り組む必要がある。（以下、対策項目略）	1	P19 セキュリティ監査の実施 ・組惑者は、１年に１回以上及び(将)社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定するセキュリティ監査計画に基づきセキュリティ監査を実施させるものとする。 P19 ・組惑者は、監査部門に、セキュリティ監査終了後、速やかにその結果を記録した文書を作成及び提出させ、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。	0	–	0	–
	外部監査の実施	(–)	0.62	5	2	P55–56 （2）情報セキュリティ対策の監査 【主旨・目的】 ・情報セキュリティの確保のためには、本ガイドラインに準拠して対策が適切に策定され、かつ運用されることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性 の有無(が疑問又は(はげしばなじない、そのために、取扱者による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を実施することが必要である。（以下、対策項目略）	2	P19 セキュリティ監査計画の作成等 (1) 防衛関連企業は、情報セキュリティ基本方針等に基づく措置の実施状況の確認及び(将)社の脆弱性の評価を客観的に行うため、監査部門を設置し、同部門には原則として最低１名は監査を受ける部署以外の取扱者を含むものとする。 (2) 監査部門は、次に掲げる事項を記載したセキュリティ監査計画を作成し、組惑者を通じて経営者等の承認を得るものとする。（以下、略） (3) 前号アの規定にかかわらずセキュリティ監査に関与する者に対する保護すべき情報及び保護システムに対するアクセス権限について、組惑者は当該セキュリティ監査の遂行上必要な権限を付与するものとする。 (4) 組惑者は、セキュリティ監査を通じて実施するために必要な情報を監査部門に提供し、その情報を利用及び分析させるものとする。 セキュリティ監査の実施 ・組惑者は、１年に１回以上及び(将)社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に、前項に規定す	0	–	1	P13–14 ・なお、セキュリティ対策の実施状況については、電力制御システム等の所管箇所とは別の組織、あるいは、外部の組織による監査等を実施することで、セキュリティ対策の継続的な改善の効果をより一層高めることが期待できることから、重要なシステムは適切なタイミングで、監査等を実施することが望ましい。
	環境変化に応じたPDCAの整備	(PR.IP-7)	0.46	5	2	P6 セキュリティ委員会 ・情報セキュリティ委員会は、情報セキュリティ対策に関する事業者内基準を策定し、必要に応じて見直しを行うこと。 また、適切な責任及び(資源配分によって、組織内におけるセキュリティを推進すること。 ・さらに、情報セキュリティに対する意識を醸成し、保つために、幹部を社じめとしたすべての取扱者等が情報セキュリティの重要性を認識し、対策を理解し実践するために必要な教育・訓練等を計画的に実施すること。	0	–	1	P19 一般的なサイバーセキュリティ対策のスキーム ・更にこれらの過程は随時レビューし、PDCA サイクルとして回していくことが重要である。即ち、リスクアセスメントやリスク対策は１回実施すればよいというものではなく、随時状況をとう、新たな脅威の発生や対策の構築などに対応していかなければならない。 ・こんにちには、例えば設計や建設の段階でセキュリティ対策を実施したうえも、その後の長期にわたる運用過程において、定期的に脆弱性情報を収集し、リスクアセスメントを実施して、必要に応じた追加対策を行うことが望まれるというこどである。	0	–
	リスクと取組状況の外部への公開		0.23	3	1	P26 事業関係、再発防止策等の公表 ・鉄道情報セキュリティ異在者は、個人データの漏えい等が発生した場合に、二次被害の防止、類似事案の発生回避等の観点から、可能な限り影響範囲などの事実関係、再発防止策等を公表するために必要な手続を整備すること。 P28 対外的な情報発信及び情報共有 【主旨・目的】 ・製造事故発生後は、事業者活動が関係者から見えなくな、何もしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講ずる必要がある。そのために、関係者との事前の協議が必要となる。（以下、対策項目略）	0	–	0	–	1	P32 情報の共有 ・自らの組織で見つかった電力制御システム等のぜい弱性や脅威について、他の組織でも同様の問題が発生し得ると判断した場合は、情報共有に務める。
	その他	–	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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 が定義するサイバーセキュリティフレームワーク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	共通項目		鉄道分野における情報セキュリティ確保に係る安全なガイドライン 第４版		装備品等及び役務の調達における情報セキュリティ基準		ビル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第1版		電力制御システムセキュリティガイドライン JEAG 1111-2019	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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)	0.31	4	1	P28 重要インフラサービス障害発生時の体制の整備 【主旨・目的】 ・重要インフラサービス障害が発生した場合には、早急にその状況を検出、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定めた上で責任者へ報告し、重要インフラサービス障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。（以下、対策項目、具体例略）	1	P17 情報セキュリティ事故等を発見又は検知した場合の処置 (1)全ての従業員は、情報セキュリティ事故等を発見又は検知した場合は、速やかに管理者（保護システムに係る場合は保護システム管理者）に報告するものとし、管理者は情報セキュリティ事故等対処計画に基づき速やかに対処するとともに、その旨及び対策（当該事故等に対するカギカッコ括弧内情報システム」及び「当該対処」の箇所）と情報等を記録した文書を作成し、組織者に報告するものとする。 (2) 保護システム利用者が保護システムの脆弱性を発見又は疑知した場合は、速やかに保護システム管理者に報告するものとし、保護システム管理者は、適切な対処を行うとともに、その内容、修正方法を記載した文書を作成し、組織者に報告するものとする。」	0	–	0	–
	初動対応マニュアルの整備	(PR.IP−9) (RS.RP−1)	0.92	7	2	P13 コンティンジェンシープン及び事業継続計画等の整備 【対策の指針】 ・重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対応態勢をあらかじめ整備することが重要となる。 そこで、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP：Business Continuity Plan）」（以下「BCP」という。）を策定する（または、これらに同等の方針を定めた計画を策定する）とともに、当該計画の実行に必要な組織体制を整備する。	2	P15-16 情報セキュリティ事故等対処計画の策定 ・経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、組織者は、次に掲げる事故等対処の各段階に対応し得る体制、責任及び手順を定めるものとする。（以下、略）	1	P32 体制構築等　（5） ・緊急時の対応手順書作成に不可欠。	2	P31 責任と手順 ・セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にする。また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直し実施する。手順にはセキュリティ事故対応および再発防止策の検討のための活動も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた機器管理体制の迅速なひとり上げ、及び体制間での密接な情報共有等の運用にも留意する。なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請がありば、これに協力する。
	インシデント対応専門チームの設置	(RS.CO−1)	0.54	5	2	P16 CSIRT 等の整備、関連部門との役割分担等の合意 【主旨・目的】 ・サイバー攻撃12クの特性を考慮したBCP 等の実行に必要な組織体制のひとつとして、CSIRT（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。CSIRT 等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応に制御システム等関連部門の専門知識が重要であり可能性を十分に認識しておく必要がある。また、サイバー攻撃に迅速に対応する観点から、情報セキュリティの専門知識を持つ組織を含めた対処体制を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及び情報セキュリティ関係機関との連携が有効である。（以下、対策項目略）	2	P16 ・情報セキュリティ事故等対処計画においては、前号の規定による対処体制等のほか、次に掲げる事項について措置を定めるものとする。 ア 保護システム管理者の下にヘルプデスク等を設置し、保護システム利用者に対し、情報セキュリティ事故等に関する必要な情報の提供等を行うこと。	0	–	1	P31 責任と手順 ・セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にする。また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直し実施する。手順にはセキュリティ事故対応および再発防止策の検討のための活動も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた機器管理体制の迅速なひとり上げ、及び体制間での密接な情報共有等の運用にも留意する。なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請がありば、これに協力する。
	経営者への報告ルート・公開内容等の設定	(RS.CO−2)	0.38	5	1	P16 CSIRT 等の整備、関連部門との役割分担等の合意 【主旨・目的】 ・サイバー攻撃12クの特性を考慮したBCP 等の実行に必要な組織体制のひとつとして、CSIRT（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。CSIRT 等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応に制御システム等関連部門の専門知識が重要であり可能性を十分に認識しておく必要がある。また、サイバー攻撃に迅速に対応する観点から、情報セキュリティの専門知識を持つ組織を含めた対処体制を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及び情報セキュリティ関係機関との連携が有効である。（以下、対策項目略）	1	P17 防衛省への報告 (1) 前活者は、前項第１号及び第２号に掲げる情報セキュリティ事故等の報告を受けた場合は、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、速やかにその詳細を防衛省（契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。）に報告するものとする。 (2) 前活者は、前号のほか、防衛関連企業の内部又は外部から情報セキュリティ事故等が発生した可能性又は将来発生する懸念の指摘があった場合は、当該可能性又は懸念の具体を含む把握し得る限りの全ての背景及び事実関係の詳細を速やかに防衛省に報告するものとする。 (3) 前活者は、前２号に規定する防衛省への報告については、それぞれ責任者及び連絡担当者等を明示した連絡系統図を含む報告要領を定め、責任者及び連絡担当者等に異動等があった場合には速やかにこれを更新するものとする。 (4) 前活者は、第１号の規定による情報セキュリティ事故等の詳細の防衛省への報告は、情報セキュリティ事故等対処計画に定められた期	0	–	1	P32 ・セキュリティ事故の報告 ・セキュリティ事故を検知した場合は、対応手順に従って報告を迅速に行う。検知したセキュリティ事故を記録し、後の対応に活用できるようにする。また、同種のセキュリティ事故が他の電力制御システムで発生していないかを確認し、発生状況に応じて対応する。セキュリティ事故の原因や対応等に関する情報は、再発防止策の検討などセキュリティ事故対応の見直しを含めて報告する。
	初動対応マニュアルの見直し	(RS.IM−1) (RS.IM−2)	0.31	4	0	–	0	–	0	–	1	P31 責任と手順 ・セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にする。また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直し実施する。手順にはセキュリティ事故対応および再発防止策の検討のための活動も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた機器管理体制の迅速なひとり上げ、及び体制間での密接な情報共有等の運用にも留意する。なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請がありば、これに協力する。
	定期的な対応訓練の実施	(PR.IP−10)	0.46	6	1	P14 ・なお、重要インフラサービス障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含め必要がある。	1	P16 情報セキュリティ教育の実施 ・防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。（以下、略）	1	P32 体制構築等　（5） ・緊急時の対応手順書作成に不可欠。	2	P31 責任と手順 ・セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にする。また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直し実施する。手順にはセキュリティ事故対応および再発防止策の検討のための活動も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた機器管理体制の迅速なひとり上げ、及び体制間での密接な情報共有等の運用にも留意する。なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請がありば、これに協力する。
	その他	–	0.00	0	0	–	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)	0.62	7	1	P13 コンティンジェンシープン及び事業継続計画等の整備 【対策の指針】 ・重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対応態勢をあらかじめ整備することが重要となる。 そこで、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP：Business Continuity Plan）」（以下「BCP」という。）を策定する（または、これらに同等の方針を定めた計画を策定する）とともに、当該計画の実行に必要な組織体制を整備する。	1	P15-16 情報セキュリティ事故等対処計画の策定 ・経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、組織者は、次に掲げる事故等対処の各段階に対応し得る体制、責任及び手順を定めるものとする。（以下、略）	1	P31 バックアップデータ／事業継続（1） ・構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように"設計仕様"に加える。 ・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。	1	P31 セキュリティ事故の対応 ・作成した手順に従い セキュリティ事故の対応を行う。
	復旧計画の見直し	(RC.IM−1) (RC.IM−2)	0.31	3	0	–	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	(RC.CO−1) (RC.CO−2) (RC.CO−3)	0.15	2	1	P28 重要インフラサービス障害発生時の体制の整備 【主旨・目的】 ・重要インフラサービス障害が発生した場合には、早急にその状況を検出、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、重要インフラサービス障害による影響や範囲を定めた上で責任者へ報告し、重要インフラサービス障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。（以下、対策項目、具体例略） 対外的な情報発信及び情報共有 【主旨・目的】 ・緊急事態発生後は、事業者活動が関係者から見えなくなる、何をしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講ずる必要がある。そのために、関係者との事前の協議が必要となる。（以下、対策項目、具体例略）	0	–	0	–	0	–
	定期的な対応訓練の実施	(PR.IP−10)	0.46	6	1	P14 ・なお、重要インフラサービス障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含め必要がある。	1	P11-12 情報セキュリティ教育及び訓練 ・防衛関連企業は、取扱者に対し、次の各号に掲げる事項を含む教育及び訓練を１年に１回以上行うものとする。なお、教育及び訓練については、専門性の高い教育項目を含め、外部の知見を活用するなど適切に実施するものとする。（以下、略）	0	–	1	P33 周知と訓練 ・セキュリティ事故発生時の対応に関する周知や訓練を定期的に実施する。訓練の手法としては、手順の確認、連絡訓練、机上演習等が考えられる。また、他の電気事業者や重要インフラ事業者、組織外の関係機関等との合同の訓練・演習の機会を活用し、これに参画することも考えられる。
	その他	–	0.00	0	0	–	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)	0.31	3	1	P27 「体制」の観点 予算・体制（委託先を含む）の確保（以下、略）	0		0		0	
	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)	1.38	10	2	P28 委託先管理の仕組み 【主旨・目的】 ・事業者内の者に情報システムの開発、アプリケーション・コンテンツ（5.4(1)参照）の開発等を委託する際、取扱者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、事業者内で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。このリスクに対応するため、情報システムの開発、アプリケーションプログラムの開発等を外部委託する際は、委託先においても事業者内基準と同等の対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。 【対策項目】 ①事業者内における情報セキュリティ確保の仕組みの整備 ②委託先に講ずる情報セキュリティ対策の策定	0		1	P31 構成情報／管理情報(1) セキュリティポリシー ・構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように"設計仕様"に加える。 ・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。 P33 表4−2 1.ネットワーク(クラウド、情報系 NW、BACnet 等) ・リスクアセスメントを実施したうえで、発注の判断を行う。	2	P9 委託先等の対応 ・電力制御システム等に関連する委託先等のセキュリティ確保に関する役割を明確化する。また、委託先等に対して、セキュリティ確保の目的や対策を明確に伝達し、遵守させる取り決めを行う。なお、必要に応じて、遵守状況の確認等を実施することが望ましい。
	サプライチェーンのセキュリティ対策状況の把握	(–)	0.31	2	2	P28 外部委託実施における情報セキュリティ確保策の徹底 【主旨・目的】 ・情報システムの開発、アプリケーション・コンテンツの開発等を外部委託する際は、委託先選定、委託の実施において必要な対策を講ずる必要がある。（以下、外部委託の例、略） 【対策項目】 ①外部委託先の選定における手続の遵守 ②外部委託の実施における手続の遵守 システム管理者は、外部委託を実施する際に、委託先に誤り含むわせる業務における情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む。）、重要インフラサービス障害に対する対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む外部委託に関与契約を定めること。（以下、略）	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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	共通項判断		鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第４版		装備品等及び役務の調達における情報セキュリティ基準		ビル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第1版		電力制御システムセキュリティガイドライン JEAG 1111-2019	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（平均以上にあたる７事例）	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)	0.15	2	0	–	1	P36(付紙) ・保護システム管理者は、社内からの脆弱性情報に加え、情報セキュリティに係る専門的な外部機関（以下「情報セキュリティ機関」という。）が発信する脆弱性情報等セキュリティに係る注意喚起及び助言等の情報を継続的に収集するものとし、当該脆弱性が保護システムに対し影響を与える可能性があると認めた場合に、保護システム全体に対し当該脆弱性に係る脆弱性スキャンを実施し、その結果を分析するものとする。 P38(付紙) ・保護システム管理者は、社内文は前項第２号の情報セキュリティ機関から収集した情報に基づき、保護システム担当者、保護システム利用者（保護システムを利用する下請負者を含む。）等に対し、適切なセキュリティに係る注意喚起及び助言等を行うものとする。	0	–	0	–
	関係団体への情報提供の実施	(ID.RA-2)	0.23	2	0	–	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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 が要求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	共通項判断		スマートメーターシステムセキュリティガイドライン JEAG 1101-2019		元請け会社における情報セキュリティガイドライン 2020年11月 改訂		建設現場における情報セキュリティガイドライン 2020年11月 改訂		医療情報システムの安全管理に関するガイドライン 第5.2版	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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	(--)	0.69	7	2	P6 経営層のの責任 ・経営層はスマートメーターシステムにおけるセキュリティの確保について責任を負うこと。（勧告）	0	–	1	P7 最高責任者（現場所長）の役割 ・現場内の最高責任者として情報セキュリティの全体責任を負う。 ・必要な経営資源（人・物・金）の割り当てを行う。 ・セキュリティ責任者、セキュリティ担当者を任命する。 ・具体的なルールや手順の明文化を指示する。 ・セキュリティ責任者から遅守状況を把握し、改善指示を行う。	0	–
	経営者によるセキュリティポリシーの策定・宣言	(ID.GV-1)	1.15	9	2	P6 経営層の責任 ・経営層はスマートメーターシステムにおけるセキュリティの確保について責任を負うこと。（勧告） ・経営層は、スマートメーターシステムにおけるセキュリティの確保が事業遂行の重要な要素であることを認識し、スマートメーターシステムのセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、一般送配電事業者が重要インフラひとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	1	P7 情報セキュリティ基本方針を制定しましょう ・「情報セキュリティ基本方針 [1]（第1 版）参考資料－1」を制定します。 ・情報セキュリティ対策として各項目の具体的な手順やルールを定めます。 ・従業員および協力会社を含めた現場構成員に周知します。 ・定期的に手順・ルールの見直しを行い、変更した場合はその都度、現場構成員に周知することも必要です。	1	P6 情報セキュリティ基本方針の制定 ・現場所長は「情報セキュリティ基本方針 [1]（参考資料－1 に一例を示す）を制定し、情報セキュリティ対策として各項目の具体的な手順やルールを定め、協力会社を含めた現場構成員に周知する。 ・定期的に手順・ルールの見直しを行い、変更した場合はその都度、現場構成員に周知する。	1	P13 ISMS 構築の手順 ・ISMS の構築はPDCA モデルによって行われる。（以下略）
	法律・業界ガイドラインの把握	(ID-GV-3) (DE.DP-2)	1.00	7	2	P6 経営層の責任 ・経営層はスマートメーターシステムにおけるセキュリティの確保について責任を負うこと。（勧告） ・経営層は、スマートメーターシステムにおけるセキュリティの確保が事業遂行の重要な要素であることを認識し、スマートメーターシステムのセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、一般送配電事業者が重要インフラひとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	0	–	0	–	0	–	2	P3 本ガイドラインの読み方 ・本ガイドラインの大部分は法律、厚生労働省通知、他の指針等の要求事項に対応する対策を示すことを目的としており（以下略）
	その他		0.00	0	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	(--)	1.23	9	2	P6 管理組織の設置 ・スマートメーターシステムのセキュリティ管理責任組織を設置すること。また、スマートメーターシステムのセキュリティ管理責任組織と全社のセキュリティ管理責任組織との関係を明確化し、一般送配電事業者においてスマートメーターシステムに関するセキュリティガバナンスの構築を行うこと。（勧告） P9 第2－2条　役割（以下、略）	1	P7 情報セキュリティ管理体制を整備しましょう ・情報セキュリティ推進する会議体が管理体制を組織します。 ・建設現場が稼動すると、協力会社に対しても同様に、情報セキュリティ管理体制の構築を依頼します。	2	P6 情報セキュリティマネジメントシステムの構築 ・情報セキュリティを維持するために、「情報セキュリティ基本方針 [2]」を制定し、情報セキュリティ管理体制を整備。情報資産を調査・分類して情報資産管理台帳を作成する。 P12 現場事務所のエリア分類と情報セキュリティ対策 ・現場事務所内では、必要な情報セキュリティレベルによって分類し、それに応じた対策を実施する。 P14 情報資産の管理（以下、略）	2	P39 非常時に備えたセキュリティ体制の整備 ・非常時やサイバー攻撃などに対して、的確に対応できるためにセキュリティ体制を医療機関等においても構築することが求められる。非常時等においても要な原因関係の調査、必要なセキュリティ対応等に関する指揮、所管官庁等への報告などの体制については、医療の継続を確保する観点からも平常時から同様にする必要がある。 また、一定規模以上の病院や、地域と重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT等）を整備するなどが強く求められる。 P82 運用管理について【C最低限のガイドライン】 ・以下の項目を運用管理規程に含めること。（中略）
	関係者の役割と責任の明確化	(ID.GV-2)	1.23	10	1	P8 役割の定義 ・スマートメーターシステムに関連する者に対して、スマートメーターシステムに関するセキュリティ管理体制における役割を明確にし、それぞれが役割を理解したことを確認する。	1	P10 契約時の対応 ・協力会社に情報セキュリティ管理体制の構築を依頼しましょう	2	P7 情報セキュリティ管理体制の整備 ①情報セキュリティ管理体制 ②最高責任者（現場所長）の役割 ③セキュリティ責任者の役割 ④セキュリティ担当者の役割 ⑤JV 現場時の管理体制	2	P18 組織的安全管理対策（体制、運用管理規程） ・安全管理について、従業者の責任と権限を明確に定め、規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で医療情報システムを利用するかどうかに関わず遵守すべき事項である。（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)	0.62	5	2	P6 管理組織の設置 ・スマートメーターシステムのセキュリティ管理責任組織を設置すること。また、スマートメーターシステムのセキュリティ管理責任組織と全社のセキュリティ管理責任組織との関係を明確化し、一般送配電事業者においてスマートメーターシステムに関するセキュリティガバナンスの構築を行うこと。（勧告）	0	–	0	–	0	–	0	–
	その他		0.00	0	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	(--)	0.38	4	1	P5 「セキュリティ面での戦略マネジメントとは、セキュリティ戦略の検討やセキュリティ事故対応の中核を担い、経営層との橋渡しを行うこと。また、セキュリティを経営・事業リスクのひとつとして認識した上で、経営計画や投資計画の策定にも関わることもいう。	0	–	0	–	0	–	0	–
	人材の確保、役割の理解	(PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)	0.92	8	2	P9 教育の計画・実施 ・スマートメーターシステムに関連する者が役割に応じたセキュリティ教育を受けることができるように教育を計画し、少なくとも年に１回はセキュリティ教育を実施する。また、セキュリティ事故発生時に適切に対応できる知識とスキルを持つ人材を育成するための教育も実施する。なお、実施にあたっては、組織として知識とスキルを継続的に蓄積できるよう人材の配置に留意するとともに、組織外の関係期間が提供する教育の機会や資格制度等の活用も考えられる。	1	P11~13 契約期間中の対応 ・①情報セキュリティ教育を実施しましょう ・各社の責任者、作業員および回面等の情報資産を取扱う担当者に対し、情報セキュリティ 教育を実施します。 新規入場者教育時 ・情報セキュリティの必要性と最低限守るべきルール、情報セキュリティ事故発生時の対応方法について説明します。	0	–	0	–
	組織内の人材育成	(PR.AT-1)	0.77	6	2	P9 セキュリティ教育 １．教育の計画・実施 ・スマートメーターシステムに関連する者が役割に応じたセキュリティ教育を計画し、実施すること。（勧告） ２．教育効果の確認 ・スマートメーターシステムに関するセキュリティ教育が効果的に実施されていることを確認すること。（勧告） ・スマートメーターシステムに関連する者が役割に応じたセキュリティ教育を受けることができるように教育を計画し、少なくとも年に１回はセキュリティ教育を実施する。また、セキュリティ事故発生時に適切に対応できる知識とスキルを持つ人材を育成するための教育も実施する。なお、実施にあたっては、組織として知識とスキルを継続的に蓄積できるよう人材の配置に留意するとともに、組織外の関係期間が提供する教育の機会や資格制度等の活用も考えられる。	1	P11~13 契約期間中の対応 ・①情報セキュリティ教育を実施しましょう ・各社の責任者、作業員および回面等の情報資産を取扱う担当者に対し、情報セキュリティ 教育を実施します。 （以下略）	0	–	0	–
	セキュリティ人材のキャリアパス・待遇の設定	(--)	0.15	1	0	–	0	–	0	–	0	–
	継続的なセキュリティ対策の実施	(PR.AT-1)	0.62	6	0		1	P11~13 契約期間中の対応 ・①情報セキュリティ教育を実施しましょう ・各社の責任者、作業員および回面等の情報資産を取扱う担当者に対し、情報セキュリティ 教育を実施します。 朝礼、定例会議、協議会等 情報セキュリティ意識の向上のため、当該工事の関係者に対し、定期的・継続的に教育を実施します。	0		2	P29~ 人的安全対策 ・医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、人による誤りの防止を目的とした人的安全対策を実定するる必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。（以下略）
	その他	(PR.AT-1)	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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が要求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を合わせて提示する。

抽出軸		NISTフレームワーク対応	共通項判断		スマートメーターシステムセキュリティガイドライン JEAG 1101-2019		元請け会社における情報セキュリティガイドライン 2020年11月 改訂		建設現場における情報セキュリティガイドライン 2020年11月 改訂		医療情報システムの安全管理に関するガイドライン 第5.2版	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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)	0.69	6	0	–	2	P8 建設現場の重要情報には何があるかを特定しましょう ・2.1で述べた「工事に関する情報」が含いる。 ・情報ごに重要度を判断し、管理責任者・保管場所・閲所時の取扱い等を決定します。重要度の判定は、漏えいや喪失した場合の影響度により、3段階で判定します。 ・これらを、情報資産管理台帳として整備します。情報資産管理台帳の一例としては、「第1版」参考資料４ 2を参照して下さい。	2	P8 情報資産管理台帳の作成 （以下、略） P11 閲所時の対応 ・現場事務所は通常の事務所とは違いず有期」という特徴がある。現場終了時をあらかじめ想定した取組みが必要となる。具体的には、個別の情報資産について閲所時の取扱い状況(廃棄・返却等)を種類ごのように明記し、閲所後の情報漏えいの発生がないようにする。 P13~14 情報資産の管理 （以下、略）	2	P16 取扱い情報の把握 ・医療情報システムで扱う情報を全てリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリストは医療情報システム安全管理責任者が必要に応じて速やかに確認できる状態で管理されなければならない。（以下略）
	経営戦略を踏まえたリスクの把握	(ID.RA-3) (ID.RA-1)	0.92	8	1	P25 せい弱性の管理 ・せい弱性に関する情報を継続的に管理すること。（推奨）	0	–	1	P8 情報資産管理台帳の作成 ・重要度の判定は、情報資産ごとに下表の３段階に分類。重要度に応じた取扱いを規定化し運用を行う。参考資料－２ご情報分類ごの重要度の例を示す。当然工事案件の個別要件によっても見直しが必要である。どに、情報分類ごに分類内容の情報について判定を行うが望ましい。	2	P16 リスク分析 ・分類された情報ごと、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等の脅威を列挙する。医療機関等では一般ごの職員等への依頼に基づいて業務を進めているため、利用者の悪意や過誤を想定することに抵抗があると思われる。しかし、情報の安全管理を達成に説明責任を果たすためには、例えばご明らか可能性は低くても、万一ご備えて対策する必要がある。また、説明責任を果たすため、これらのリスク分析の結果は文書化して管理する必要がある。（以下略） P34 ・情報及び情報機器の持ち出し並びに外部利用について 情報又は情報機器の持ち出しについては組織的な対策が必要となり、組織として情報又は情報機器の持ち出しをどのように取り扱うかという方針が必要である。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可能限度や情報機器を用いた情報の持ち出しは想定されるため、リスク分析を実施し、対策を検討しておくことが必要である。（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)	0.62	6	1	P25 対応手順の策定 ・収集したせい弱性に対する対応手順を策定する。対応手順には、せい弱性が修正された機器やソフトウェア、通信プロトコル等を適用した場合の影響評価や、それらを適用できない場合の対応を含めておく。	0	–	0	–	1	P16 リスク分析 C、最低限のガイドライン ・リストアップした情報に対してリスク分析を実施すること。具体に関しては リスク分析に関する解説（別冊）を参照
	リスク対応計画の策定	(ID.RA-6) (ID.RM-3)	0.85	7	1	P12 対策の計画 ・セキュリティ対策は、事業計画に沿って経営層が策定した方針に従って計画し、リスクセスメントに基づいて選択する。財政的、技術的にセキュリティ対策の実施が困難な場合は、法令に反しない範囲において残存リスクとして識別し、次の改善時に対応が検討できるようにリスク管理する。スマートメーターシステムが安全に動作すること。必要な箇所にはバックアップを行うことを基本的な考え方として対策を計画し、セキュリティ事故発生時も、影響を最小限にとどめるようにする。	0	–	1	P13~14 情報資産の廃棄と再利用 ・現場事務所内のパソコンや共用のパソコン等情報機器を廃棄または再利用する場合は、その重要度に合わせた管理責任を定めこれを実施する。また、情報機器によって作成・印刷された文書等については、その保存期間を明示するなどの管理責任を定めこれを実施する。（以下、対策例略）	2	P16 リスク分析 C、最低限のガイドライン ・リスク分析により特ごされたリスクに対して、6.3 章~6.12 章に示す対策を実施すること。
	残留リスクの識別	(ID.RA-6) (ID.RM-3)	0.23	3	1	P12 対策の計画 ・セキュリティ対策は、事業計画に沿って経営層が策定した方針に従って計画し、リスクセスメントに基づいて選択する。財政的、技術的にセキュリティ対策の実施が困難な場合は、法令に反しない範囲において残存リスクとして識別し、次の改善時に対応が検討できるようにリスク管理する。スマートメーターシステムが安全に動作すること。必要な箇所にはバックアップを行うことを基本的な考え方として対策を計画し、セキュリティ事故発生時も、影響を最小限にとどめるようにする。	0	–	0	–	0	–
	その他		0.38	3	0	–	2	P16 契約終了時の対応 ・①情報資産の返却・廃棄・保管を徹底させましょう P17 現場閲所時の対応 ・現場閲所時においては、記憶媒体が紙か電子かを問わず、すべての情報について適切に保管・廃棄を行うことが必要です。機密保持契約書や【重要情報】貸出台帳」等も忘れずに保管してください。また、パソコンやプリンタなどをリース契約している場合は、リース契約機器の返却時に機器内に重要な情報が残存していないかの確認をすることが必要です。	0	–	2	P37 災害、サイバー攻撃等の非常時の対応 ・災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関等の様々な機能や人的能力に変化が生じる。その一方で、そのような事態下は医療の需要が高まり、平常時以上との対応が求められることもある。また、サイバー攻撃の場合は、自医療機関の診療等への影響だけでと、他医療機関へ影響が波及することもあり、適切な対応が求められる。このような事態に可能な限り対応するために、普段から想定されるかさんへんの準備等について、対策をとて、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（BCP：Business Continuity Plan）と呼ぶ。（以下略）
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)	1.46	10	2	P18 暗号 １．暗号の利用 ２．暗号鍵の管理（以下、略） P19 ネットワークの管理 １．ネットワークへのアクセス制御 ２．ネットワークの分離（以下、略）	0	–	2	P17 情報機器の運用管理 （以下、略） P19 アクセス制御 （以下、略） P19~20 ウィルス対策 （以下、略） P.20~21 ソフトウェアのインストール （以下、略）	2	P20 物理的安全対策 ・物理的安全対策とは、医療情報システムにおいて個人情報が入力、参照又は格納される端末や情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義した上で、以下の事項を考慮して、適切に管理する必要がある。（以下略） P21 技術的安全対策 （内容略） P42 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理 ・医療機関等において外部と個人情報を含む医療情報を交換する場合、医療情報システムを医療機関等が管理する内部ネットワークを通じた形のみかつ、ご接続」と利用することが原則とされた。（以下略）
	脆弱性診断の実施・対応	(PR.IP-12)	1.15	8	2	p25 せい弱性の管理 ・せい弱性に関する情報を継続的に管理すること。（推奨） ・スマートメーターシステムのせい弱性に起因するセキュリティ事故の発生を予防するために、実施することが望ましい事項である。実施にあたっては、次のような内容を勘案すること。 １．情報の収集 ・スマートメーターシステムに利用する機器やソフトウェア、通信プロトコル等におけるせい弱性に関する情報を定期的に収集する。 ２．対応手順の策定 ・収集したせい弱性に対する対応手順を策定する。対応手順には、せい弱性が修正された機器やソフトウェア、通信プロトコル等を適用した場合の影響評価や、それらを適用できない場合の対応を含めておく。	0	–	0	–	2	P7 不正ソフトウェア対策 ・たとえ個々にスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策には、スキャン用ソフトウェアを導入するだけでと、医療情報システム側の脆弱性を可能な限りかさくしておくことが重要である。そのために実施すべき対策として、セキュリティホール（脆弱性）が報告されいるソフトウェアへのパッチ適用、利用していないサービスや通信ポートの非活性化、マクロ等の利用停止、メールやファイルの無害化がある。 ネットワークとからの不正アクセス ・不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）もあるため、医療情報システムと外部ネットワークとの間体に応じて、IDS、IPSの採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ適用等の対策も講じておくことも重要である。
	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)	1.46	11	2	P19 ネットワークへのアクセス制御 ・スマートメーターシステムのネットワークに接続可能な機器を制御する。許可されていない機器からの通信は遮断するか、帯域を制限して影響を軽減する。 P21 マルウェア対策 ・スマートメーターシステムにおい、ネットワーク経由及び外部記憶媒体経由でのマルウェア対策を実施する。これを行わない場合、スマートメーターシステムへのマルウェアの侵入により、情報が保護できない可能性や正常なネットワークアクセスが確立できない可能性がある。マルウェア駆除に時間を要すると、スマートメーターシステムが長期にわたり利用できない可能性がある。	0	–	2	P9 情報セキュリティマネジメントシステムの運用 （以下、略） P15 ・情報資産の管理 （以下、略） ・ログ（記録） の管理 （以下、略）	1	P23 技術的安全対策 （内容略）
	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)	0.62	5	0	–	0	–	0	–	1	P23 ネットワーク上からの不正アクセス ・不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）もあるため、医療情報システムと外部ネットワークとの間体に応じて、IDS、IPSの採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ適用等の対策も講じておくことも重要である。
	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)	1.31	9	2	P12 対策の点検 ・セキュリティ対策を技術面・運用面から定期的に点検し、必要に応じて改善する。セキュリティ対策の点検は、セキュリティ対策の改善目的だけでなく、実施状況を利害関係者に説明できるように項目を検討する。また、内容に応じて第三者による評価を検討する。 対策の改善 ・対策の点検結果に基づき、セキュリティ対策の見直しを検討する。また、環境の変化に応じて、セキュリティ対策の目的及び内容の変更を検討する。	0	–	1	P8 情報セキュリティマネジメントシステムの運用 ・構築された情報セキュリティマネジメントシステムを下図のフローで運用を行い、情報セキュリティの維持・改善を図る。情報セキュリティ対策の実効性を確保していくためには、定期的に運用状況の確認・改善を行っていくことが必要である。 P10 情報セキュリティマネジメントシステムの運用 ・現場所長は運守状況の適否を判断し、問題があれば改善策をセキュリティ責任者に指示する。 ・セキュリティ責任者は改善の進捗や結果を現場所長に報告する。 ・チェック結果は記録に残す。	2	P23 不正ソフトウェア対策 ・たた、これらの不正ソフトウェアは常に変化しているため、検出するためのパターンファイルや検索エンジンを常に最新のものに更新しておく必要がある。 P32 医療情報システムの改造と保守 ・医療情報システムの可用性を維持するためには、定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があり、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があるため、想定される脅威に対するセキュリティ対策が必要になる。（以下略）
	従業員に対する教育の実施	(PR.AT-1)	1.15	10	1	P9 セキュリティ教育 １．教育の計画・実施 ・スマートメーターシステムに関するセキュリティ教育を計画し、実施すること。（勧告） ・スマートメーターシステムに関連する者が役割に応じたセキュリティ教育を受けることができるように教育を計画し、少なくも年に１回はセキュリティ教育を実施する。	1	P11~13 契約期間中の対応 ・①情報セキュリティ教育を実施しましょう ・各社の責任者、作業員および関面等の情報資産を取扱う担当者に対し、情報セキュリティ 教育を実施します。（以下略）	2	P9 情報セキュリティ基本方針の宣言・周知 ・２．１情報セキュリティマネジメントシステムの構築」で記載した通り、「情報セキュリティ基本方針」を制定し、宣言・周知する。 情報セキュリティ対策の実施 ・具体的な実施方法については「３．情報セキュリティ対策の実施」で対策例を示しながら解説する。 情報セキュリティ教育の実施 ・セキュリティ責任者は、関係者全員に情報セキュリティ教育を年１回以上の頻度で実施する。（以下、略） P16 情報機器の運用管理 （以下、略）	2	P29 人的安全対策 ・医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、入ごる訓りの防止を目的とした人的安全対策を実施する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。（以下略）
	その他	–	0.31	2	0	–	2	P8 現場事務所のセキュリティは大丈夫ですか？ ・現場事務所においても、当該建設現場で要求される情報セキュリティレベルを勘案して下記事項の検討が必要です。 ・物理的セキュリティとも記載した現場事務所レイアウト（「第1版」3.1 参照）の検討・保安設備や保安システムの導入 ・現場事務所内ネットワーク構成の検討と回線の手配 ・適切な情報機器の手配	0	–	2	P31 情報の破棄 ・医療に係る電子情報は、破棄を確実に行うことにより、破棄に際しても安全性を確保する必要がある。しかし、例えばデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もあるため、注意しなくてはならない。（以下略）
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	(–)	0.31	4	0	–	0	–	1	P10 情報セキュリティマネジメントシステムの評価・見直しの実施 ・セキュリティ責任者またはセキュリティ担当者は定期的(年１回以上)に情報セキュリティマネジメントシステムのチェクを実施し、結果を現場所長に報告する。	0	–
	外部監査の実施	(–)	0.62	5	1	P11 実施状況の報告 ・セキュリティ対策の実施状況に関する報告事項を定め、適切に報告を行うことができる仕組みを構築すること。（勧告） P12 対策の点検 ・セキュリティ対策を技術面・運用面から定期的に点検し、必要に応じて改善する。セキュリティ対策の点検は、セキュリティ対策の改善目的だけでなく、実施状況を利害関係者に説明できるように項目を検討する。また、内容に応じて第三者による評価を検討する。	0	–	0	–	2	P88 運用管理について C、最低限のガイドライン (2) 管理体制（以下、略） ステップ3：全体の見直し及び確認評価 ・運用管理規程は単に策定すれば良いというものではなく、策定（Plan）された管理規程に基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Action）していかねばならない。このPDCA サイクルを適切に廻しながら、改善活動を伴う継続的な運用を行うことが重要である。
	環境変化に応じたPDCAの整備	(PR.IP-7)	0.46	5	0	–	0	–	1	P8 情報セキュリティマネジメントシステムの運用 ・構築された「情報セキュリティマネジメントシステム」を下図のフローで運用を行い、情報セキュリティの維持・改善を図る。情報セキュリティ対策の実効性を確保していくためには、定期的に運用状況の確認・改善を行っていくことが必要である。 P9 情報セキュリティマネジメントシステムの運用状況の確認 ・日常的に情報セキュリティマネジメントシステムの運用状況の確認を行う。 P10 情報セキュリティマネジメントシステムの評価・見直しの実施 （以下、略）	1	P88 運用管理について ステップ3：全体の見直し及び確認評価 ・運用管理規程の全体が作成された段階で、医療機関等の内部の関係者等にレビューを行い、総合的見点で実施運用が可能か評価し改善する。
	リスクと取組状況の外部への公開		0.23	3	1	P12 対策の点検 ・セキュリティ対策を技術面・運用面から定期的に点検し、必要に応じて改善する。セキュリティ対策の点検は、セキュリティ対策の改善目的だけでなく、実施状況を利害関係者に説明できるように項目を検討する。また、内容に応じて第三者による評価を検討する。	0	–	0	–	0	–
	その他	–	0.00	0	0	–	0	–	0	–	0	–

ガイドライン共通項抽出結果（別紙）
チェック項目に基づき、各ガイドライン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 が定義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	共通項判断		スマートメーターシステムセキュリティガイドライン JEAG 1101-2019		元請け会社における情報セキュリティガイドライン 2020年11月 改訂		建設現場における情報セキュリティガイドライン 2020年11月 改訂		医療情報システムの安全管理に関するガイドライン 第5.2版	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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)	0.31	4	0	−	0	−	1	P10 管理体制 ・関係者は情報セキュリティ事故が発生（可能性がある場合を含む）した場合、各社（JVの場合はスポンサー会社）で定められた連絡網に従って、速やかに現場所長またはセキュリティ責任者に報告する。 ・現場所長は本社等の関連部門へ連絡を行う。（以下、報告内容の一例略）	0	−
	初動対応マニュアルの整備	(PR.IP−9) (RS.RP−1)	0.92	7	2	P28 セキュリティ事故の対応 ・セキュリティ事故やセキュリティ事象の対応体制と手順を明確にすること。（勧告） 責任と手順 ・セキュリティ事故対応のための体制を作り、責任者の任命と報告体制の構築を行う。また、セキュリティ事故対応についての手順を策定し、定期的に見直しを実施する。手順には、セキュリティ事故対応だけではなく、再発防止策の検討も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた危機管理体制の迅速な立ち上げ、及び体制間での密接な情報共有等の連携にも留意する。 セキュリティ脆弱性とセキュリティ脅集の対応、（以下、略）	0	−	0	−	2	P37 非常時における事業継続計画 ・非常事態が発生している最中では適切な意思決定は望み難いので、事前にできる限り多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り下記の事項・フェーズごとに計画内容を事前審査等で検証することが望ましい。（以下、略）
	インシデント対応専門チームの設置	(RS.CO−1)	0.54	5	1	P28 責任と手順 ・セキュリティ事故対応のための体制を作り、責任者の任命と報告体制の構築を行う。また、セキュリティ事故対応についての手順を策定し、定期的に見直しを実施する。手順には、セキュリティ事故対応だけではなく、再発防止策の検討も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた危機管理体制の迅速な立ち上げ、及び体制間での密接な情報共有等の連携にも留意する。	0	−	0	−	1	P37 非常時に備えたセキュリティ体制の整備 ・一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなど対策が求められる。
	経営者への報告ルート・公開内容等の設定	(RS.CO−2)	0.38	5	1	P29 セキュリティ事故の報告 ・セキュリティ事故やセキュリティ事象の対応後には、規定に基づき、その経緯を経営層及び関係期間に報告する。報告は、再発防止策の検討及びセキュリティ事故対応の見直しに活用できるように予め決められた様式にしたがって実施する。また、需要家に影響がある場合は、内容に応じて社外へ公表を行う。	0	−	1	P10 管理体制 ・関係者は情報セキュリティ事故が発生（可能性がある場合を含む）した場合、各社（JVの場合はスポンサー会社）で定められた連絡網に従って、速やかに現場所長またはセキュリティ責任者に報告する。 ・現場所長は本社等の関連部門へ連絡を行う。（以下、報告内容の一例略）	0	−
	初動対応マニュアルの見直し	(RS.IM−1) (RS.IM−2)	0.31	4	0	−	0	−	1	P10 原因調査と分析 ・現場所長またはセキュリティ責任者は、情報セキュリティ事故を調査し、原因を究明 し、再発防止策を立案する。IT 面で専門的な知識を必要とする場合は、本社等の関連 部門へ支援を要請する。 ・現場所長は、再発防止策の進捗管理を図り、本社等の関連部門へ報告を行う。	1	P81 運用管理について ステップ３：全体の見直し及び確認評価 ・運用管理規程の全体が作成された段階で、医療機関等の内部の関係者等にレビューを行い、総合的視点で実施運用が可能か評価し改善する。 なお、運用管理規程は単に策定すれば良いというものではなく、策定（Plan）された管理規程に基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Action）していかなければならない、このPDCA サイクルを適切に廻しながら、改善活動を伴う継続的な運用を行うことが重要である。
	定期的な対応訓練の実施	(PR.IP−10)	0.46	6	1	P28 １．責任と手順 ・セキュリティ事故対応のための体制を作り、責任者の任命と報告体制の構築を行う。また、セキュリティ事故対応についての手順を策定し、定期的に見直しを実施する。手順には、セキュリティ事故対応だけではなく、再発防止策の検討も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた危機管理体制の迅速な立ち上げ、及び体制間での密接な情報共有等の連携にも留意する。 P30 周知と訓練 ・セキュリティ事故発生時の対応に関する周知や訓練を定期的に行うこと。（勧告）（以下、略）	0	−	1	P10 再発防止策の周知 ・現場所長またはセキュリティ責任者は、情報セキュリティ事故の原因と再発防止策を 現場関係者全員に周知する。	1	P7 事後責任について 2. 善後策を講ずる責任 ・また、医療情報について何らかの不都合な事態が生じた場合、善後策を講ずる責任として、以下のことが必要である。（以下、略）
	その他	−	0.00	0	0	−	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)	0.62	7	1	P31 サービス継続計画 ・スマートメーターシステムで提供する機能を定義し、それぞれの関連性を考慮してサービス継続のための計画を構築すること。（勧告） ・スマートメーターシステムで復開されるサービスの継続計画に事故発生時におけるセキュリティの維持に関する内容を含める。また、セキュリティが維持できないことによって事業継続に与える影響を検討し、事故発生時におけるセキュリティ水準を予め定める。本節における「事故」とは、サービス継続に支障を与える災害等の物理的な事象をいう。	0	−	0	−	1	P37 非常時における事業継続計画 ・非常事態が発生している最中では適切な意思決定は望み難いので、事前にできる限り多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り下記の事項・フェーズごとに計画内容を事前審査等で検証することが望ましい。（以下、略）
	復旧計画の見直し	(RC.IM−1) (RC.IM−2)	0.31	3	1	P31 改善の検討 ・サービス継続のための計画及び手順が目的を達成できることを定期的に確認及び検証し、改善策を検討する。（勧告） ・サービス継続のための計画及び手順が目的を達成できることを定期的に確認及び検証し、改善策を検討する。	0	−	0	−	1	P37 非常時における事業継続計画 ・非常事態が発生している最中では適切な意思決定は望み難いので、事前にできる限り多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り下記の事項・フェーズごとに計画内容を事前審査等で検証することが望ましい。（以下、略）
	組織内外の連絡先の整備	(RC.CO−1) (RC.CO−2) (RC.CO−3)	0.15	2	0	−	0	−	0	−	0	−
	定期的な対応訓練の実施	(PR.IP−10)	0.46	6	1	P31 サービス継続管理 （当該部分全般に記載） 事故対応 ・事故発生時の対応に関する周知や訓練を定期的に行うこと。（勧告） ・セキュリティ管理責任組織は、事故発生時でも最低限のセキュリティが確保できるように手順や対応策を確立し、文書化する。また、事故発生時の対応に関する周知や訓練を定期的に実施する。	0	−	0	−	1	P37 災害、サイバー攻撃等の非常時の対応 ・普段から想定されるがやるレベルの異常時について、対策を立て、文書化し、訓練を繰り返すことが有用である。
	その他	−	0.00	0	0	−	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)	0.31	3	0		0		0		0	
	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)	1.38	10	2	p8 委託先等の対応 ・スマートメーターシステムに関連する委託先等の役割を明確化する。また、委託先等に対して、セキュリティの実施目的や対策を明確に伝達し、遵守させる取り決めを行う。なお、必要に応じて、遵守状況の確認等を実施することが望ましい。」	2	P9 契約時の対応 ・①機密保持契約を必ず締結しましょう P10 ・②情報セキュリティルールを周知しましょう P16 契約終了時の対応 ・②機密保持契約内容の再確認	2	P6 JV 現場時の制定方法 （以下、略） P9 協力会社、委託先の管理 （以下、略） P10 関係者雇用終了時の対応 （以下、略） P11 JV 現場時の留意事項 （以下、略） P15 関係者間での情報共有 （以下、略）	2	P29 人的安全対策 ・医療機関等は、情報の盗難や不正行為、情報設備の不正利用等の以⼒解減を図るため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。（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	(−)	0.31	2	0	−	2	P7 情報セキュリティ管理体制を整備しましょう ・情報セキュリティを推進する元請会社の管理体制を組織します。 ・建設現場が稼動すると、協力会社に対しても同様に、情報セキュリティ管理体制の構築を依頼します。 P14 契約期間中の対応 ・②協力会社の実施状況を確認しましょう ・①情報資産の貸出し時は注意しましょう	0	−	0	−
	その他	−	0.00	0	0	−	0	−	0	−	0	−

ガイドライン共通項目抽出結果（別紙）
チェック項目に基づき、各ガイドライン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	共通項目判断		スマートメーターシステムセキュリティガイドライン JEAG 1101-2019		元請け会社における情報セキュリティガイドライン 2020年11月 改訂		建設現場における情報セキュリティガイドライン 2020年11月 改訂		医療情報システムの安全管理に関するガイドライン 第5.2版	
カテゴリ内容	チェック項目		①スコア１超	②記載ガイドライン多（半分以上にあたる７事例）	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)	0.15	2	0	－	0	－	0	－	0	－
	関係団体への情報提供の実施	(ID.RA-2)	0.23	2	1	P29 セキュリティ事故の報告と情報共有 ２．情報の共有 ・セキュリティ事故から得られた知見を、セキュリティ事故の予防及び再発防止に活用する仕組みを構築すること。（動告） ・自らの組織で見つかったスマートメーターシステムの脆弱性や脅威について、他社でも同様の問題が発生し得ると判断した場合は、しかるべき機関を通じて報告する。また、セキュリティ事故の再発防止策について周知を実施する。	0	－	0	－	2	P40 加重、サイバー攻撃等の非常時の対応 C、最低限のガイドライン ・不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じるおそれがあり多事業であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第１号 医政地発1029 第３号 医政研発1029 第１号 平成30 年10 月29 日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。
	その他	－	0.00	0	0	－	0	－	0	－	0	－