ISO27001 要求事項と管理策対応表

要求事項	内容	-	管理策	内容
4.1	組織及びその状況の理解	\Rightarrow	-	-
		\Rightarrow	5.7	脅威インテリジェンス
	利害関係者のニーズ及び期待の理解	\Rightarrow	5.19	供給者関係における情報セキュリティ
		\Rightarrow	5.20	供給者との合意における情報セキュリティの取扱い
4.2		\Rightarrow	5.21	情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理
		\Rightarrow	5.22	供給者のサービス提供の監視、レビュー及び変更管理
		\Rightarrow	5.23	クラウドサービスの利用における情報セキュリティ
5.1	リーダーシップ&コミットメント	\Rightarrow	-	-
5.2	方針	\Rightarrow	-	-
	責任及び権限	\Rightarrow	5.1	情報セキュリティのための方針群
		\Rightarrow	5.2	情報セキュリティの役割及び責任
		\Rightarrow	5.3	職務の分離
		\Rightarrow	5.4	管理層の責任
		\Rightarrow	5.5	関係当局との連絡
		\Rightarrow	5.6	専門組織との連絡
		\Rightarrow	5.15	アクセス管理
5.3		\Rightarrow	5.16	識別情報の管理
		\Rightarrow	5.17	認証情報
		\Rightarrow	5.18	アクセス権
		\Rightarrow	8.1	利用者エンドポイント機器
		\Rightarrow	8.2	特権的アクセス権
		\Rightarrow	8.3	情報へのアクセス制限
		\Rightarrow	8.4	ソースコードへのアクセス
		\Rightarrow	8.5	セキュリティを保った認証
	計画策定	\Rightarrow	-	-
6.1.2	リスクアセスメント	\Rightarrow	-	-

7.1 一分 5.5.1 情報及びその他の関連資産の目録 3 5.1.1 情報の転送 3 5.1.1 情報の転送 3 6.2 雇用条件 3 6.4 製成手紙 4 分 6.5 雇用の終了又は変更後の責任 5 6.7 リモトワーク フ 4 6.7 リモトワーク フ 5 7.2 物理的でキコリティ保理 フ 6 7.3 オンイ、都駆びキコリティア県 フ 6 7.3 オンイ、都駆びキコリティア県 フ 6 7.3 オンイ、が開めると関係を発見 フ 6 7.5 物理的及び環境の脅威からの保護 フ 7 7.0 セコリティアルクリアスク・クリアスク・クリアスク・クリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスクリアスク・フリアスク・フリアスの表します。 フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスの表します。 フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスの表します。 フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリアスク・フリア					
7.1 計算 5.14 情報の配送 3 6.1 3 6.2 雇用条件 3 3 6.4 競車 3 6.5 雇用の終了又は変更後の責任 3 7.1 物理的セコリティリティ 3 7.1 物理的セコリティ 3 7.2 対理の以。環境のを由リティ 3 7.4 物理的セコリティ 3 7.5 セキュリティを使つべき付いの作業 3 7.6 セキュリティを使つべき付いの作業 3 7.7 カリアスク・クリアスクリアスク・クリアスクリアスクリアスクリアスクリアスクリアスクリアスクリアスクリアスクリアス			\Rightarrow		
7.1 対象 6.1 選考 6.2 雇用条件 窓内手続 ※ 6.5 雇用の終了又は変更後の責任 ※ 6.7 リモーレクー 物理的セネリティ機界 ※ 7.2 物理的セネリティの監視 ※ ※ 7.3 オンイス、部屋及び施設のセネリティの監視 ※ ※ 7.5 物理的なり表し現域の各域がたの保護 ※ ※ 7.6 セネリティを保つへき徹域での作業 ※ ※ 7.0 クリアデスク・クリアスクリーン ※ ※ 2 7.1 サポートコーディリティ ※ ※ 2 7.10 お護衛の監査及び保護 ※ ※ 7.12 サポートコーディリティ ※ ※ 7.12 サポートコーディリティ ※ ※ 7.12 サポートコーディリティ ※ ※ 3 68 総面の保守 ※ ※ 7.12 サポートコーディリティを保った処分又は再利用 ※ ※ 3 6.6 総理・おり上では対する保護 ※ ※ 3 7 マルウエアに対する保護 ※ ※ 3 8.8 技術の管理・他の企業機 ※ ※ 3 7.3 スポートの企業機 ※ ※ 3 8.8 技術の管理・センリティを保つた処分又は再利用 ※ ※ 3 7.3 スポートの企業機 ※ ※ ※ 3 8.8 技術の管理・センリティを保つた処分又は関連を持続を対しまする。 ※ <td rowspan="3"></td> <td rowspan="25"></td> <td>\Rightarrow</td> <td></td> <td></td>			\Rightarrow		
7.1 資源 6.2 雇用条件 ※ 6.4 第3年時 ※ 6.5 屋用の終了又は変更後の責任 ※ 6.7 リモートワーク ※ 7.1 物理的キュリティ境界 ※ 7.2 物理的と可能設して非常の作成をしてまります。 ※ 7.5 物理的及び環境の脅威からの保護 ※ 7.5 物理的及び環境の脅威からの保護 ※ 7.6 セキュリティを保つた意間域での作業 ※ 7.7 クリアテスク・フレーン ※ 7.8 装置の設置及び保護 ※ 7.1 サートユーティリティ ※ 7.1.1 サポートユーティリティ ※ 7.1.2 ケーブル配線のセキュリティ ※ 7.1.3 装置のセキュリティ ※ 7.1.4 装置のセキュリティを除た処分又は再利用 ※ 8.8 技術的施習性色管理 ※ 8.8 技術的施習性色管理 ※ 8.8 技術的機関性色管理 ※ 8.8 技術的機関性色管理 ※ 8.8 技術的機関性と同学を記し、教育及び訓練 7.2 力量 7.3 認識 会 6.6 ※ 25.10 情報をびその他の関連資産の許容される利用 できいより デジ・フリストリオリナー・ できいより デジ・フリストリオリナー・			\Rightarrow	5.14	情報の転送
→ 6.4 懲戒手続 → 6.5 雇用の終了又は変更後の責任 → 6.7 リモートワーク → 7.1 物理的セキュリティ境界 → 7.2 物理的入場 → 7.4 物理的セキュリティの監視 → 7.4 物理的とサーリティの監視 → 7.5 物理的及び環境的脅威からの保護 → 7.7 クリアテスケ・クリアスクリーン → 7.8 装置の設置及び保護 → 7.10 記憶媒体 → 7.10 記憶媒体 → 7.11 対策にトニーティリティ → 7.12 ケーブル配線のセキュリティ → 7.13 装置の保守 → 7.14 装置の保守 → 7.14 装置の保守 → 7.14 装置のセキュリティ → 7.13 装面の保守 → 7.14 装置のセキュリティ → 8.6 容量・能力の管理 → 8.7 マルフェアに対する保護 → 8.8 大の影響性の管理 → 8.9 構成管理 → 6.6 松密保持契約又は守秘義務契約 - 5.12 情報の分類 「特報の分類			\Rightarrow	6.1	選考
→ 6.5 雇用の終了又は変更後の責任			\Rightarrow	6.2	雇用条件
7.1 ⇒ 6.7 リモートワーク ・ 7.1 物理的とキュリティ(競渉のとキュリティ ・ 7.3 オフィス、部屋及び施設のセキュリティ ・ 7.4 物理的とネコリティの監視 ・ 7.5 物理的なア・ションへの以下及の自動からの保護 ・ 7.6 セキュリティを保つへき領域での作業 ・ 7.6 セキュリティの診断及の保護 ・ 7.9 ボース・カリアスク・クリアスク・リンスクリーン ・ 7.9 構作にある資産のセキュリティ ・ 7.10 対ボートューティリティ ・ 7.11 サポートューティリティ ・ 7.12 ケーブル配線のセキュリティ ・ 7.13 装置の使き ・ 7.14 装置の使き ・ 7.12 ケーブル配線のセキュリティ ・ 7.13 装置の使き ・ 7.14 装置のせきコリティを保力を処分又は再利用 ・ 8.6 容量・能力の管理 ・ 8.7 マルウェアに対する保護 ・ 8.8 技術的影響性の管理 ・ 8.9 構成管理 ・ 7.3 認識 ・ 6.3 情報とより子の意識向上、教育及び訓練 7.4 コミューケーション ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 ・ 7.1 <td< td=""><td></td><td>\Rightarrow</td><td>6.4</td><td>懲戒手続</td></td<>			\Rightarrow	6.4	懲戒手続
→ 7.1 物理的セキュリティ境界			\Rightarrow	6.5	雇用の終了又は変更後の責任
→ 7.2 物理的入退			\Rightarrow	6.7	リモートワーク
→ 7.3 オフィス、部屋及び施設のセキュリティ → 7.4 物理的セキュリティ医療 → 7.5 物理的のセキュリティ医療 → 7.5 物理的ので環境の脅威からの保護 → 7.6 セキュリティを保つべき領域での作業 → 7.7 グリアテスク・クリアスク・リファスクリーン → 7.8 英国の設置及び保護 →			\Rightarrow	7.1	物理的セキュリティ境界
⇒ 7.4 物理的セキュリティの監視			\Rightarrow	7.2	物理的入退
→ 7.5 物理的及び環境的脅威からの保護			\Rightarrow	7.3	オフィス、部屋及び施設のセキュリティ
7.1 対象 ⇒ 7.6 セキュリティを保つへき領域での作業 ⇒ 7.7 クリアデスク・クリアスクリーン ⇒ 7.8 装置のひを選及び保護 ⇒ 7.10 記憶媒体 ⇒ 7.11 サポートユーティリティ ⇒ 7.12 ケーブル配線のセキュリティ ⇒ 7.13 装置のセキュリティ ⇒ 7.14 装置のセキュリティを保った処分又は再利用 ⇒ 8.6 容量・能力の管理 ⇒ 8.7 マルウェアに対する保護 → 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.3 認識 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.4	物理的セキュリティの監視
→ 7.6 セキュリティを保つへき領域での作業 → 7.7 クリアデスク・クリアスクリーン → 7.8 装置の設置及び保護 → 7.9 構外にある資産のセキュリティ → 7.10 記憶媒体 → 7.11 サポートユーティリティ → 7.12 ケーブル配線のセキュリティ → 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 8.7 マルウェアに対する保護 → 8.8 技術の脆弱性の管理 → 8.8 技術の脆弱性の管理 → 8.9 構成管理 7.2 力量 → 6.3 情報セキュリティの意識向上、教育及び訓練 7.3 認識 → 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション → → 5.10 情報及びその他の関連資産の許容される利用 → 5.12 情報の分類 → 5.12 情報の分類 → 5.13 情報のラベル付け	7 1		\Rightarrow	7.5	物理的及び環境的脅威からの保護
→ 7.8 装置の設置及び保護 → 7.9 構外にある資産のセキュリティ → 7.10 記憶媒体 → 7.11 サポートユーティリティ → 7.12 ケーブル配線のセキュリティ → 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 8.7 マルウェアに対する保護 → 8.8 技術の脆弱性の管理 → 8.9 構成管理 7.3 認識 → 6.3 情報とキュリティの意識向上、教育及び訓練 7.4 コミュニケーション → 6.6 秘密保持契約又は守秘義務契約 7.5 文書化した情報 → 5.12 情報及びその他の関連資産の許容される利用 → 5.12 情報のラベル付け	′.1		\Rightarrow	7.6	セキュリティを保つべき領域での作業
→ 7.9 構外にある資産のセキュリティ ⇒ 7.10 記憶媒体 → 7.11 サポートユーティリティ ⇒ 7.12 ケーブル配線のセキュリティ ⇒ 7.13 装置のセキュリティを保った処分又は再利用 ⇒ 8.6 容量・能力の管理 ⇒ 8.7 マルウェアに対する保護 ⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.3 認識 ⇒ 6.3 情報とキュリティの意識向上、教育及び訓練 7.4 コミュニケーション ⇒ 6.6 秘密保持契約又は守秘義務契約 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.7	クリアデスク・クリアスクリーン
→ 7.10 記憶媒体 → 7.11 サポートユーティリティ → 7.12 ケーブル配線のセキュリティ → 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 8.7 マルウェアに対する保護 → 8.8 技術的脆弱性の管理 → 8.9 構成管理 7.3 認識 → 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション → 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション → 7.10 情報及びその他の関連資産の許容される利用 → 5.12 情報の分類 → 5.13 情報のラベル付け			\Rightarrow	7.8	装置の設置及び保護
→ 7.11 サポートユーティリティ → 7.12 ケーブル配線のセキュリティ → 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 8.7 マルウェアに対する保護 → 8.8 技術的脆弱性の管理 → 8.9 構成管理 7.3 認識 → 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション → 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション → - - → 5.10 情報及びその他の関連資産の許容される利用 → 5.12 情報の分類 → 5.13 情報のラベル付け			\Rightarrow	7.9	構外にある資産のセキュリティ
→ 7.12 ケーブル配線のセキュリティ ⇒ 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 ⇒ 8.6 容量・能力の管理 ⇒ 8.7 マルウェアに対する保護 ⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.3 認識 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.10	記憶媒体
→ 7.13 装置の保守 → 7.14 装置のセキュリティを保った処分又は再利用 → 8.6 容量・能力の管理 → 8.7 マルウェアに対する保護 → 8.8 技術的脆弱性の管理 → 8.9 構成管理 7.3 認識 → 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション → 6.6 秘密保持契約又は守秘義務契約 7.5 文書化した情報 → 5.10 情報及びその他の関連資産の許容される利用 → 5.12 情報の分類 → 5.13 情報のラベル付け			\Rightarrow	7.11	サポートユーティリティ
7.14 装置のセキュリティを保った処分又は再利用 ⇒ 8.6 容量・能力の管理 ⇒ 8.7 マルウェアに対する保護 ⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.3 認識 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション ⇒ 6.6 秘密保持契約又は守秘義務契約 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.12	ケーブル配線のセキュリティ
⇒ 8.6 容量・能力の管理 ⇒ 8.7 マルウェアに対する保護 ⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.3 認識 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.4 コミュニケーション ⇒ - - 7.5 支書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.13	装置の保守
⇒ 8.7 マルウェアに対する保護 ⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.2 力量 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.3 認識 ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ - - み 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	7.14	装置のセキュリティを保った処分又は再利用
⇒ 8.8 技術的脆弱性の管理 ⇒ 8.9 構成管理 7.2 力量 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.3 認識 ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ - - 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	8.6	容量・能力の管理
⇒ 株成管理 ⇒ 株成管理 ⇒ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・			\Rightarrow	8.7	マルウェアに対する保護
7.2 力量 ⇒ 6.3 情報セキュリティの意識向上、教育及び訓練 7.3 認識 ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ - - 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	8.8	技術的脆弱性の管理
7.3 認識 ⇒ 6.6 秘密保持契約又は守秘義務契約 7.4 コミュニケーション ⇒ - - 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け			\Rightarrow	8.9	構成管理
7.4 コミュニケーション ⇒ - - 7.5 文書化した情報 ⇒ 5.10 情報及びその他の関連資産の許容される利用 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け	7.2		\Rightarrow	6.3	情報セキュリティの意識向上、教育及び訓練
7.5	7.3	認識	\Rightarrow	6.6	秘密保持契約又は守秘義務契約
7.5 文書化した情報 ⇒ 5.12 情報の分類 ⇒ 5.13 情報のラベル付け	7.4	コミュニケーション	\Rightarrow	-	-
7.5 文書化した情報 ⇒ 5.13 情報のラベル付け	7.5	文書化した情報	\Rightarrow	5.10	情報及びその他の関連資産の許容される利用
⇒ 5.13			\Rightarrow	5.12	情報の分類
→ 5.37 操作手順書			\Rightarrow	5.13	情報のラベル付け
			\Rightarrow	5.37	操作手順書

8.1	運用の計画策定及び管理	\Rightarrow	8.10	情報の削除
		\Rightarrow	8.11	データマスキング
		\Rightarrow	8.12	データ漏洩防止
		\Rightarrow	8.13	情報のバックアップ
		\Rightarrow	8.14	情報処理施設・設備の冗長性
		\Rightarrow	8.15	ログ取得
		\Rightarrow	8.16	監視活動
		\Rightarrow	8.17	クロックの同期
		\Rightarrow	8.18	特権的なユーティリティプログラムの使用
		\Rightarrow	8.19	運用システムへのソフトウェアの導入
	情報セキュリティリスク対応	\Rightarrow	5.24	情報セキュリティインシデント管理の計画策定及び準備
		\Rightarrow	5.25	情報セキュリティ事象の評価及び決定
		\Rightarrow	5.26	情報セキュリティインシデントへの対応
		\Rightarrow	5.27	情報セキュリティインシデントからの学習
		\Rightarrow	5.28	証拠の収集
		\Rightarrow	5.29	事業の中断・阻害時の情報セキュリティ
8.3		\Rightarrow	5.30	事業継続のためのICTの備え
		\Rightarrow	6.8	情報セキュリティ事象の報告
		\Rightarrow	8.20	ネットワークセキュリティ
		\Rightarrow	8.21	ネットワークサービスのセキュリティ
		\Rightarrow	8.22	ネットワークの分離
		\Rightarrow	8.23	ウェブフィルタリング
		\Rightarrow	8.24	暗号の利用

	監視、測定、分析及び評価	\Rightarrow	5.8	プロジェクトマネジメントにおける情報セキュリティ
1		\Rightarrow	5.31	法令、規制及び契約上の要求事項
		\Rightarrow	5.32	知的財産権
		\Rightarrow	5.33	記録の保護
		\Rightarrow	5.34	プライバシー及び個人識別可能情報(PII)の保護
		\Rightarrow	5.35	情報セキュリティの独立したレビュー
		\Rightarrow	5.36	情報セキュリティのための方針群、規則及び標準の遵守
		\Rightarrow	8.25	セキュリティに配慮した開発のライフサイクル
9.1		\Rightarrow	8.26	アプリケーションセキュリティの要求事項
		\Rightarrow	8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
		\Rightarrow	8.28	セキュリティに配慮したコーディング
		\Rightarrow	8.29	開発及び受入れにおけるセキュリティテスト
		\Rightarrow	8.30	外部委託による開発
		\Rightarrow	8.31	開発環境、テスト環境及び本番環境の分離
		\Rightarrow	8.32	変更管理
		\Rightarrow	8.33	テスト用情報
		\Rightarrow	8.34	監査におけるテスト中の情報システムの保護
9.2	内部監査	\Rightarrow	-	-
9.3	マネジメントレビュー	\Rightarrow	-	-
10.1	不適合、是正処置	\Rightarrow	-	-
10.2	継続的改善	\Rightarrow	-	-