自動車産業サイバーセキュリティガイドライン Ver2.1公開

・自己評価結果の提出方法 システム化に伴う入力項目追加・誤記修正の為、自動車産業ガイドライン修正版（Ver.2.1）を公開

- システム化に伴う入力項目追加 ： 新規/差し替え選択欄の追加、共有先入力シートの追加
- 誤記修正箇所 ： 下記７項目 ※Ver.2.0から追加項目の規定はありません。（153項目から変更なし）

要求事項	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)
	10	Lv2	**個人情報をお持ちの会社については、個人情報に特化した社内ルールの規定があること**	【規則】 ・お客様個人情報の取り扱いにおける社内ルールを策定すること ［明確にする内容］ -個人情報の管理体制を確立 -取得時に利用目的を通知、明示 -本人の同意の範囲内で利用 -本人の同意なしに第三者提供しないこと -本人による開示・訂正・利用停止・消去などの要望に対応すること -個人情報の取扱いルールを定めること -個人情報保護法、GDPR、不正競争防止法等の情報セキュリティに関する法令・規則の情報収集を行うこと -情報漏洩した時の対応手順 ~~・策定した社内ルールを教育・周知すること~~ 【対象】 ・個人情報を取扱う業務担当者 ~~【頻度】~~ ~~（教育）~~ ~~・新規受け入れ時、かつ、１回／年~~ ~~（周知）~~ ~~・定常的に、かつ、ルールの改正時に周知すること~~	【規則制定の例】 ・個人情報取り扱いに関する会社規則を制定している ・部署ごとに個人情報管理台帳を作成し１回／年の棚卸を実施している 【教育・周知の例】 ・自社ホームページに個人情報保護に関するポリシーを掲載(GDPR含む)している ・コンプライアンス教育の一環として、個人情報保護についても教育している ・21 底して	情報セキュリティ対策フレームワークの構築	法務
	19	Lv1	**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	【初動対応フローの記載例】 ・No..24 記載の例を参照すること 【事件・事故発生時の報告フローの例】 ・No..18 記載の例を参照すること 【報告フォーマットの項目例】 ・発生 ・業務 ・原因 ・暫定 ・恒久 ・完了日時（恒久対策）		
	48	Lv3	**自社における他社の重要な機密情報の取扱い状況を把握している ↓ 他社から入手した重要機密情報が、自社内でどのように取り扱われているか実状を把握している**	【規則】 ・他社の重要な機密情報を自社で取扱った履歴を記録、保管すること ・適切に記録、保管されていることを確認し、必要に応じて是正すること 【記録、保管状況の確認、是正頻度】 ・1回以上/年	【取り扱い状況確認手法の例】 ・取扱い履歴(部署間での開示、再委託など)を記録、保管するルールを規定している ・許可された人のみアクセスできる場所に保管したことを示すアクセス権を設定している ・他社、自社の情報に関わらず、機密区分に応じた取扱いルールに従い取扱っている ・他社図面の取り扱いについて、技術部門共通ルールを定め、運用している ・機密保持契約書に従い、機密管理規準に則った取扱いの徹底を機密管理点検等で確認している	パートナー企業のリスク管理	情報セキュリティ

①【達成条件・達成基準の整合】
達成条件はルール規定のみだが、達成基準に教育・周知が含められている為、
教育・周知の記載を削除

②【達成条件・達成基準の整合】
達成基準に、初動対応フロー整備が規定されているが、
達成条件の内容（事故の概要や影響および対応内容の記録）と不一致の為、
初動対応フロー整備の記載を削除　（初動対応フロー整備はNo.24にて規定済み）

③文章の分かり難さを改善

要求事項	No.	レベル	達成条件	達成基準	他社事例 (参考事例を列記しており、 すべての遵守を求めているものではありません)	対象	担当領域 (回答者検討時の参考情報)
	63	**Lv3**	**情報資産(機器)は重要度に応じた管理ルールに沿って管理している**	【規則】 ・重要度に応じて、機器と搭載ソフトウェアが正規品である事をシリアル番号やハッシュ値を利用して定期的に確認すること 【頻度】 ・1回/年 以上(資産棚卸時等)	【ソフトウエア正規品確認の例】 ~~・改ざん後の不審動作をEDR（Endpoint Detection and Response）によるふるまい検知により確認~~ ・社内に配布するPCは、資産管理台帳で管 る。 ・会社貸与PCユーザーには管理者権限を与え れた管理者が実施する。また、インストール済の 年1回以上ライセンスに不足がないことを確認する。		
	67	**Lv3**	**セキュリティの要求事項を記載した開発標準を定め、定期的に見直している**	【規則】 ・情報システムのセキュリティ開発標準を定めること ・開発標準に則って、開発していることをチェックすること ・開発標準の内容を定期的に見直すこと 【見直し頻度】 ・1回/年	【開発標準の例】 ・開発プロセス（企画、設計、開発、テスト、移行）ごとにルールを定める ・開発に加えて運用・保守のルールを定める ・開発プロセスごとにゲートを設けて遵守状況のチェックを行う ・運用・保守の遵守状況を年1回チェックを行う	サーバー 情報セキュリティ対策フレームワークの構築	情報セキュリティ／IT
	106	**Lv2**	**業務およびデータの重要性に応じてネットワークを分離している。**	【規則】 ・業務内容やデータ重要性でシステムを分類し、専用のネットワーク毎に設置すること 【対象】 ・社外公開サーバー設置のネットワーク、 PCとサーバのネットワーク、工場ネットワーク／OAネットワーク等	【実践例】 ・インターネット公開サーバーはDMZに設置している ・PCとサーバーは、ネットワークを分 ・重要情報を取 ステムは専用のネットワークに設置している 工場ネットワークは専用のネットワークとしている		
セキュリティインシデントを想定し事業継続の要件に沿う復旧に必要なデータを準備できていること。	**153**	**Lv2**	**事業継続上重要なシステムについては、重要度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 ・求め 【対象 ・事業継続上重要なシステム	【バックアップ設計の例】 継続上重要なシステムは、求められる復旧ポイント、復旧時間、保管世 所を考慮して設計しリストア手順書も整備している	事件・事故対応	IT

④【達成基準・他社事例の整合】
他社事例の内容（不審動作の検知）が、達成基準と不一致の為、不審動作の検知の記載を削除

⑤誤記修正

⑥【対象の誤記修正】
達成基準の【対象】の内容が、他社事例【実践例】の一部の記載のみであった為、修正

⑦誤記修正
（重要度の「重」の字を追加）