大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
ガバナンスの整備	組織的文脈		1	セキュリティに関する法令や、契約等に規定された事項を考慮し、社内ルールを策定、教育・周知すること。	★4	・セキュリティに関連する以下の事項を把握した上で、社内ルールを策定すること - 自社が関連する法令(事業法、個人情報保護法等) - 所管省庁や関係団体における基準等 - 取引先等が提示する制限事項等も含めた、関係者からの要求事項 ・上記事項の改定状況について、年１回以上の頻度又は必要に応じて確認を行い、社内ルールの見直しを行うこと ・策定・見直した社内ルールを教育・周知すること	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和5年度版) 1.1(4) **自動車GL No.9, 11 (LV1)**		
	役割/責任/権限	1	2	セキュリティを担当する部署及び従業員を決定し、責任及び権限を割り当てること。	★3	・セキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を明確化すること ・平時のセキュリティ推進活動に必要な連絡先リストを整備すること	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和5年度版) 2.1.1(1)(4)(5)(6) **自動車GL No.13 (LV1)**		
					★4	・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、情報セキュリティ委員会等の経営判断ができる体制を設置していること	ISO/IEC 27001:2022 4.4, A.5.4 政府統一基準(令和5年度版) 2.1.1(2) **自動車GL No.14 (LV2)**		
			3	サイバー攻撃や予兆を監視・分析をする体制を整備すること。	★4	・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すること ・入手した情報やログの相関分析等により、サイバー攻撃の予兆やインシデントの発生の検知を可能とし、適切な対応が導き出せる体制を構築すること ※相関分析： 複合的なログなどで分析してセキュリティインシデントの予兆や痕跡を見つけ出す手法	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和5年度版) 7.1.4 **自動車GL No.16 (LV1), No.17 (LV2)**	○	
		2	4	秘密保持契約又は守秘義務契約を規定し、遵守させること。	★3	・役員、従業員、社外要員(派遣社員等)を対象に、自社の守秘義務を策定し、文書化すること ・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること ・退職時又は期間満了時に会社の機密情報を持ち出させないこと	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**		
					★4	・自社の機密情報を取扱う役員又は従業員に、守秘義務の誓約書を提出させること(社外要員除く) ・派遣社員、受入出向社員について、派遣元、出向元の会社と業務開始前に守秘義務を締結すること ・当該守秘義務では、業務で知り得た情報を外部に漏えいさせない旨の記述を設けること	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.5,6 (LV2)**		
	ポリシー	3	5	自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。	★3	・自社のセキュリティ対応方針を策定し、文書化すること ・セキュリティ対応方針(ポリシー)を役員、従業員、社外要員(派遣社員等)から容易に確認できる状態にすること ・定常的に、かつ、セキュリティ対応方針の改正時に役員、従業員、社外要員(派遣社員等)へと周知すること	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和5年度版) 2.1.3(2) **自動車GL No.1,3 (LV1)**		

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
	監督	4	6	セキュリティ対策状況を定期的に棚卸し、見直しを行うこと。	★3	・以下の事項について、年1回以上の頻度又は必要に応じて、最新の内容となっているか等の確認を行い、結果を見直しに利用すること - 平時の体制 [No.1] - 自社以外の組織が管理・提供し、自組織の資産が接続している情報システムの一覧 [No.5] - 機密区分に応じた情報の管理ルールの順守状況 [No.10] - 重要度に応じた情報機器、OS、ソフトウェアの管理ルールの順守状況 [No.11] - ユーザID及び管理者IDの一覧 [No.12,13] - インシデント発生時の体制 [No.27] ※[ ]内の番号は、対応する要求事項(★3)の番号を指す。	**CE A7.9** ISO/IEC 27001:2022 10.1, 10.2 政府統一基準(令和5年度版) 2.3.1, 2.4.1 **自動車GL No.15, 20, 58, 62, 78, 117 (LV1)**		
					★4	・以下の事項について、年１回以上の頻度又は必要に応じて、最新の内容となっているか等の確認を行い、結果を見直しに利用すること - セキュリティ対応方針、社内で運用するその他のセキュリティ関連ルール [No.5] - 情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)の一覧 [No.13] - 自社の情報機器が存在するネットワークを対象として作成したネットワーク図 [No.15] - 情報資産(情報)を対象として定義した管理ルールの順守状況 [No.16] - 高い機密区分の情報資産(情報)に関する一覧表の内容 [No.16] - 退職や期間満了時における機密情報、情報機器等の回収状況 [No.16] - 役員、従業員、社外要員(派遣社員等)に付与等したアクセス権 [No.25] - 持込みルール及び持出しルールの内容や遵守状況 [No.27] - 教育や訓練の内容 [No.27,28] - 意識向上に係る教育・研修の内容 [No.28] - パソコンへのソフトウェアのインストール状況 [No.42] ※[ ]内の番号は、対応する要求事項(★4)の番号を指す。	ISO/IEC 27001:2022 10.1, 10.2 政府統一基準(令和5年度版) 2.3.1, 2.4.1 **自動車GL No.40 (LV1), No.2, 7, 52, 55, 57, 61, 75, 91, 92, 98 (LV2)**, **No.43 (Lv3)**		
			7	定期的に経営層へ対策実態に関する報告を行い、結果を対策の推進に反映すること。	★4	・セキュリティ担当部署は、年１回以上、セキュリティを統括する役員(CISO 等)、関係部門に対して、No.6にて求める対策等の見直しの結果を踏まえたセキュリティ対策の実態及び今後の対策推進計画を報告し、結果を社内部署と共有すること ・報告に際し役員からの改善に向けた指示があった場合、セキュリティ担当部署は、当該指示内容を文書化、関係部門へ共有し、計画への反映や不備の是正等を実施すること	ISO/IEC 27001:2022 6.2, 9.3, A.5.35 政府統一基準(令和5年度版) 2.2.1(1) **自動車GL No.68 (LV1)**		
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	5	8	取引先と自社とのビジネス又はシステム上の関係を把握すること。	★3	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること	CE A2.9., A4.5. **自動車GL No.77 (LV1)**		
					★4	・機密情報を共有している取引先の一覧を作成していること ・会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化していること ・一覧表には取引に伴い授受／使用される情報資産とその取扱いを記載し、取引先と把握すること	**自動車GL No.70 (LV1)**		
		6	9	他社との間で、機密情報の取扱い方法を明確にすること。	★3	・機密情報を共有する取引先等との間で、業務開始前に機密情報の取り扱いについて、例えば以下の内容を含む取り交わしを行うこと - 機密情報の定義 - 機密情報の取扱い (表示、保管方法、複製可否、第三者への提供可否等) - 機密情報の返還	ISO/IEC 27001:2022 A.5.20 政府統一基準(令和5年度版) 4.1.1(2) **自動車GL No.44 (LV1)**		

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
			10	重要な機密情報等を取扱う取引先のセキュリティ対策状況を把握すること。	★4	・以下に示す条件のいずれか又は複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考に対策状況を把握すること [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する	ISO/IEC 27001:2022 A.5.19 政府統一基準(令和5年度版) 4.1.1(1)(2) **自動車GL No.42 (LV3)**		
			11	セキュリティインシデント発生時の他社との役割と責任を明確にすること。	★4	・子会社又は取引先と機密情報を共有する際、機密情報の取扱いとともに、セキュリティインシデント発生時の自社と子会社又は取引先の役割と責任を明確にした上で、以下を例とする事項について文書化すること - セキュリティインシデント発生時の相手方への通知義務 - セキュリティインシデント発生時の連絡先 - 再発防止策の協議方法	ISO/IEC 27001:2022 A.5.20, A.5.24 政府統一基準(令和5年度版) 2.2.4(1) **自動車GL No.46 (LV1)**		
			12	取引先との契約終了時に機密情報やアクセス権等を回収又は破棄すること。	★4	・機密情報を提供・共有する子会社、取引先を対象に、回収又は破棄すべき機密情報、アクセス権等のチェックシートを作成すること ・機密情報を提供・共有する子会社、取引先から、契約終了時にチェックシート等を使用し機密情報、アクセス権などを回収又は破棄すること	ISO/IEC 27001:2022 A.5.11 政府統一基準(令和5年度版) 4.1.1(4) **自動車GL No.43 (LV3)**		
リスクの特定	資産管理	7	13	ハードウェア、OS、ソフトウェアの情報に関する一覧を作成すること。	★3	・適用範囲内のパソコン、シンクライアントの製造元とOS及び台数を一覧化すること。 ・適用範囲内のサーバ、仮想サーバ、ハイパーバイザの製造元とOS及び台数を記入すること。 ・情報機器、OS、ソフトウェアについて、導入、設置、ネットワーク接続、セキュリティパッチ適用等のルールを含む管理ルールを定め、文書化していること	**CE A2.4, A.2.5** ISO/IEC 27001:2022 A.5.9, A.5.10 政府統一基準(令和5年度版) 2.1.2(1) **自動車GL No.59**, No.60 (LV1)		
					★4	・適用範囲内のスマートデバイスの製造元とOS及び台数を一覧化すること ・重要なシステムを構成する機器について、設定情報を一覧に含めること	**CE A2.4.1, A.2.6** ISO/IEC 27001:2022 A.5.9 政府統一基準(令和5年度版) 2.1.2(1)		
		8	14	ネットワークの情報に関する一覧を作成すること。	★3	・適用範囲内のネットワークを一覧化すること。その際、一覧の中に各ネットワークの所在地や目的に関する情報を含めること。 ・適用範囲内のネットワーク機器(ファイアウォールやルータを含む)を一覧化すること。その際、一覧の中に各機器の製造元とモデル、保守事業者に関する情報を含めること。	**CE A.2.7, A.2.8** ISO/IEC 27001:2022 A.5.9 政府統一基準(令和5年度版) 2.1.2(1), 5.2.2(1)		
					★4	・自社の情報機器が存在するネットワークを対象として、ネットワーク図を作成すること	政府統一基準(令和5年度版) 5.2.2(1), 5.2.3(1) **自動車GL No.74 (LV2)**		
		9	15	取引先等とのネットワーク接続を管理すること。	★3	・以下の内容を含む外部情報システムの利用ルールを定めること - 外部の情報サービスを利用する際のセキュリティ要件を定めること - 外部の情報サービスの利用時にセキュリティ要件を満たしているかサービス内容を確認し、自社の役員又は従業員が承認すること ・外部情報システムの接続先と守秘義務契約を締結すること	ISO/IEC 27001:2022 A.5.21, A.5.23 政府統一基準(令和5年度版) 4.2.2(1)(2), 4.2.3(2) **自動車GL No.76 (LV1)**		

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
		10	16	機密区分に応じた情報の管理ルールを定め 、それに基づく管理を行うこと。	★3	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること - 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 ・機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること ・高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと	CMMC LV1 3.8.3 ISO/IEC 27001:2022 A.5.10, A.5.12　A.5.13 政府統一基準(令和5年度版) 3.1.1(1)(3) **自動車GL No.54, 56 (LV1)**		
					★4	・退職や期間満了時には機密情報、情報機器等を回収すること - 回収物には、情報(印刷物、記憶媒体)、情報機器(パソコン、スマートデバイス)、アクセス権(ID、鍵)を含めること - 回収漏れが起こらない手順(例：回収物一覧のチェックシートの作成等)を整備、運用すること ・サーバ、会社支給のパソコン、スマートデバイス、外部記憶媒体の廃棄時(リース終了時含む)はデータを復元できないよう消去すること ※ディスクのフォーマットは、データを復旧される可能性があるため不可 ・サーバ、会社支給のパソコン、スマートデバイス、外部記憶媒体の記憶領域の消去を実施した記録又は業者の廃棄証明書を保管すること	CMMC LV1 3.8.3 ISO/IEC 27001:2022 A.5.11, A 7.14, A 8.10 政府統一基準(令和5年度版) 3.1.1(7), 5.2.4(1), 6.1.1(3), 6.2.1(3) **自動車GL No.7, 65 (LV2)**		
	リスクアセスメント		17	脆弱性の管理体制、管理プロセスを定めること。	★4	・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、文書化すること ・管理対象の情報機器における脆弱性の残存状況を把握すること ・対応履歴を記録し、月次でチェックすること	ISO/IEC 27001:2022 A.5.7, A.8.8 政府統一基準(令和5年度版) 7.2.1(1) **自動車GL No.125 (LV2)**	○	
攻撃等の防御	アイデンティティ管理とアクセス制御	11	18	ユーザID の発行・変更・削除の手続きを定めること	★3	・自社又は必要に応じて社外要員(派遣社員等)に対してユーザIDを作成し、承認するプロセスを確立し、文書化すること ・ユーザIDを共有しないこと ・やむを得ず共有IDが必要な場合は、共有IDを利用したユーザを特定できるようにすること ・ユーザIDが不要になった場合(例えば、ユーザが組織を退職した場合やIDが一定期間使利用されなかった場合)、速やかにユーザIDを削除又は無効にすること。 ・特別なアクセス権限が不要になった場合は、速やかに削除又は無効にすること(スタッフの役割が変わった場合等)。	CE A5.2, A7.1, A7.3 ISO/IEC 27001:2022 A.5.16 政府統一基準(令和5年度版) 7.1.1(2) **自動車GL No.113 (LV1), No.118 (LV2)**	○	
		12	19	管理者IDの発行・変更・削除の手続きを定めること	★3	・すべてのサーバ、ネットワーク機器について、システム管理者と責任者を定めること ・管理者権限を付与する従業員、社外要員(派遣社員等)を限定すること ・管理者に対して役割に応じた必要最低限の権限のみを付与すること ・システム開発を実施する従業員、社外要員(派遣社員等)が本番環境において、管理者権限で操作できないようにすること ・組織内でどの従業員、社外要員(派遣社員等)が管理者IDを持っているかを一覧化し、正確に把握すること。 ・管理者IDの付与・変更・削除は申請・承認制にすること ・管理者IDの付与・変更・削除及びサーバとネットワーク機器の設定内容の変更を行う権限を業務上必要な従業員、社外要員(派遣社員等)に限定すること	CE A7.4, A7.5, A7.6, A7.7, A7.8 ISO/IEC 27001:2022 A.8.2 政府統一基準(令和5年度版) 7.1.3(1) **自動車GL No.114 (LV1), 119 (LV2)**	○	○

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
		13	20	システムや情報の重要度に応じて認証の強度や実装方法を決定すること。	★3	・すべてのユーザIDについて、アプリケーションや機器へのアクセスを許可する前に、一意の認証情報(パスワード等)でユーザを認証すること ・重要な情報を取扱うと考えられるクラウドサービスにおいて、ユーザ及び管理者がサービスにアクセスする場合は、常に多要素認証を使用すること。 ・利用するクラウドサービスのうち、多要素認証をサポートしていないものを一覧化すること ・多要素認証で用いるものを含め、パスワードは、英大文字小文字、数字、記号を含めた10文字以上とすること ・多要素認証の実装においては、他で定義される要求事項を満たすパスワードに加え、以下いずれかの追加要素を利用すること - 所有物(例：ワンタイムパスワード、証明書) - 生体情報(例：指紋、顔、虹彩、静脈) ・管理者権限を持つ共有アカウントへのアクセスは、アクセスログを確実に取得すること	**CE A7.2, A7.14- A7.17** CMMC LV1 3.1.1, 3.5.2, LV2 3.5.3, 3.7.5 ISO/IEC 27001:2022 A.8.3, A.8.4, A.8.5 政府統一基準(令和5年度版) 7.1.1(1)，8.1.3(2)	○	○
					★4	・重要な情報を取扱うと考えられるシステムにおいて、★3で対象としているクラウドサービスへのアクセスに加えて、以下に示す場合は、常に多要素認証を使用すること - 管理者がインターネット経由でシステムにアクセスする場合 - ユーザがインターネット経由で特に機密レベルが高い情報を取扱うシステムにアクセスする場合	ISO/IEC 27001:2022 A.8.5 政府統一基準(令和5年度版) 7.1.1(1)，8.1.3(2) **自動車GL No.120 (LV3)**	○	
		14	21	社内システムを構成する端末にアカウントロック制御を実装すること。	★3	・業務で利用するシステムを構成する端末へのログオン(パソコンへのログオンやスマートデバイスのロック解除等)にあたって、設定が可能な場合、以下のいずれかを適用すること。 - 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。 - 試行が10回以上失敗するとアカウントをロックする。 ・上記のいずれも設定することができない場合、No.15で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。 ・パソコンや携帯電話のロック解除を行う場合、最低でも6文字以上のパスワード又はPINを利用すること。当該機器のロック解除用のパスワード等が他の認証にも使用される場合、別途示されるパスワードの管理に関するルールを適用すること。	**CE A.5.9, A5.10, A7.10** ISO/IEC 27001:2022 A.8.5 政府統一基準(令和5年度版) 7.1.1(1)	○	○
		15	22	パスワード設定に関するルールを定め、周知すること。	★3	・パソコン(シンクライアントを含む)、サーバ、スマートデバイス、クラウドサービスの利用者または管理者は、それらにおけるデフォルトパスワードを変更すること。 ・ユーザアクセスの認証にパスワードを利用する場合、以下の保護対策を講じること。 - パスワードは英大文字小文字、数字、記号を含めた10文字以上とする。 - 機器やサービス間でのパスワードの使い回しをしない。	**CE A4.3, A.5.3**, **A5.5**, **A7.10, A7.11, A7.12** ISO/IEC 27001:2022 A.5.17 政府統一基準(令和5年度版) 7.1.1(2) 自動車GL No.115 (LV1), No.116 (LV2)	○	
		16	23	パスワードの管理に関するルールを定め、周知すること。	★3	・紙のノートへの記載及び施錠保管、又はパスワード管理アプリの利用等により、パスワードを安全に保管すること。 ・パスワードの定期的な変更を強制しないこと。 ・パスワードの漏洩が判明した場合、又はその疑いがある場合に、速やかにパスワードを変更するための手順を整備すること。	CE A4.4, A5.6, A7.13 ISO/IEC 27001:2022 A.5.17 政府統一基準(令和5年度版) 7.1.1(2) **自動車GL No.115 (LV1),** **No.116 (LV2)**	○	

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
		17	24	人の異動に伴うアクセス権の管理ルールを定めて、運用すること。	★3	・業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権及び機密上の配慮が必要な場所や部屋への入室について、以下の内容等を含む管理ルールを定めること - アクセス権の発行・変更・削除は申請・承認制であること - 与える入室許可・アクセス権の範囲は必要な範囲に限定すること - 入室権限やアクセス権の棚卸について定めていること - 与えた入室許可・アクセス権の申請書又は台帳を管理していること	CE A7.4, A7.5 CMMC LV1 3.1.2 ISO/IEC 27001:2022 A.5.18 政府統一基準(令和5年度版) 7.1.2(1), 7.1.3(1) **自動車GL No.49 (LV1)**	○	
					★4	・重要情報を扱うシステムは、アクセス権を付与するための条件を明確にする ・重要情報を扱うシステムにおけるアクセス権の設定は、システム管理者の要件及び設定手順を明確にし、厳格な管理下で実施する。 ・重要情報を扱うシステムは、情報利用者とシステム管理者の権限を分離する等、個人に権限が集中しない環境とする。 ・重要情報を扱うシステムは、付与したアクセス権限の運用/利用状況を定期的に確認する。	ISO/IEC 27001:2022 A.5.18, A.8.2 政府統一基準(令和5年度版) 7.1.3(1) **自動車GL No.50 (LV2)**	○	
			25	サーバ等の設置エリアへの入退室を管理し、記録すること。	★4	・サーバ等の設置するエリアに入場可能な人を定めること。 ・サーバ等の設置エリアを施錠すること。 ・施錠が出来ないエリアにサーバが設置されている場合、サーバを専用ラックに入れて施錠すること。 ・管理者を定めて、施錠管理を行うこと。 ・入退場日時、入場者氏名等を含めて、サーバ等の設置エリアの入退場記録を取得し、少なくとも6 ヶ月間保管すること	CMMC LV1 3.10.1 ISO/IEC 27001:2022 A.7.1, A.7.2, A.7.3 政府統一基準(令和5年度版) 3.2.1 **自動車GL No.84, 85 (LV1)、No.86 (LV2)**		
			26	可搬媒体の持込み・持出しを制限すること。	★4	・パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器(BYOD)含む)を対象とした社内への持込みルールを定め、文書化すること ・パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器(BYOD)含む)、印刷物(図面等の機密書類)に関する社外への持出しルールを定め、文書化すること	ISO/IEC 27001:2022 A.7.10 政府統一基準(令和5年度版) 3.1.1(4), 8.1.1(1) **自動車GL No.91, 92 (LV2)**		
	意識向上及びトレーニング		27	経営陣を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること。	★4	・役員、従業員、社外要員(派遣社員等)を対象に、年１回以上の頻度で、セキュリティの重要性を再認識する機会を設けること ・特に職場特有のリスクの理解やルールの遵守が必要な場合、職場単位で重要なルールやリスクについて、年１回以上の頻度でリマインドすること ・以下のトピックについて、新規受け入れ時、かつ、年１回以上、教育資料配布・掲示、e ラーニング、集合教育等による教育を実施すること - 電子メールによるマルウェア感染の予防 - Web 閲覧によるマルウェア感染の予防 - 機密区分の定義と取り扱い ・上記取組みの実施状況を記録し、保管すること	ISO/IEC 27001:2022 A.6.3 政府統一基準(令和5年度版) 2.2.3(2) **自動車GL No.28, 29, 30 (LV1), No.34, 35 (LV2)**		
			29	IT又はセキュリティを担当する部署の職員に対して、最新の知識とスキルを維持するための教育・研修を実施すること。	★4	IT又はセキュリティを担当する部署の職員に対して、脅威及び対策の変化等、最新の知識とスキルを維持するための学びの機会を提供すること ・上記取組みの実施状況を記録し、記録として保管すること	政府統一基準(令和5年度版) 2.2.3(2) **金融GL 2.1.3④**		
		18	28	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。	★3	・役員、従業員、社外要員(派遣社員等)を対象に、新規受け入れ時、かつ、年1回以上の頻度で、セキュリティインシデント発生時の対応について、教育資料の配布・掲示に加え、e ラーニングまたは集合教育等による教育や訓練を実施すること ・実施した教育や訓練の実施内容、実施方法、実施時期、受講状況等を記録し、保管すること	ISO/IEC 27001:2022 A.6.3 政府統一基準(令和5年度版) 2.2.4(1) **自動車GL No.38 (LV1)**		
	データセキュリティ		29	情報機器、情報システムの保管データを適切に暗号化すること。	★4	・社外に持ち出すパソコン、記憶媒体の機密情報を暗号化すること ・重要システム(インターネットに公開されているシステム、重要な社内システム)のデータベースを暗号化すること	ISO/IEC 27001:2022 A.8.24 政府統一基準(令和5年度版) 3.1.1(4)(6), 6.2.5(1) **自動車GL No.129 (LV3)**	○	

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
			30	重要データを適切な場所に保管するようルールを定め、周知すること。	★4	・マルウェアによる被害を受けた場合に業務に支障をきたす重要データはパソコン以外の社内ネットワーク上の相対的に安全な区域にあるサーバに保管するようルールを定め、役員、従業員、社外要員(派遣社員等)、受入出向者を対象に周知すること	**自動車GL No.100 (LV2)**		
			31	取引先等との情報共有や情報送信に関するルールを定め、周知すること。	★4	・以下を明文化し、役員、従業員、派遣社員、受入出向者へ周知すること -社外とファイル共有する場合は、信頼できる相手とのみ共有すること -送信履歴が残らない方法で、社外へファイル転送することを禁止すること ・上記取組みの実施状況を記録し、記録として保管すること	ISO/IEC 27001:2022 A.5.14 政府統一基準(令和5年度版) 3.1.1(6) **自動車GL No.135 (LV2)**		
		19	32	適切なバックアップを行うこと。	★3	・取得対象、取得頻度を定めて自組織で取扱うデータのバックアップを取得すること ・重要情報については、遠隔地を含めてバックアップを保管すること ・バックアップ対象ごとにリストア手順書を整備すること	ISO/IEC 27001:2022 A.8.13 政府統一基準(令和5年度版) 3.1.1(8) **自動車GL No.148, No.149 (LV1)**	○	
					★4	・事業継続上重要なシステムについて、復旧(システム再構築を含む)に係る目標等(No.45参照)に適合するよう、取得対象、取得頻度を定めてシステムバックアップを取得すること。 ・重要情報・システムについて、システム構築時、変更時、定期的(リスク応じて判断)に、定めた復元手順により、復元ができることを確認すること	ISO/IEC 27001:2022 A.8.13 **自動車GL No.151 (LV2)**	○	
	プラットフォームセキュリティ	20	33	ハードウェア・ソフトウェア等の安全な構成を確立し、維持すること。	★3	・パソコン、サーバ、スマートデバイスで使用していないソフトウェアをすべて削除又は無効化すること ・すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること ・サーバ及びネットワーク機器の設定変更を申請・承認制にすること	**CE A5.1, A5.8, A6.6, A6.7** ISO/IEC 27001:2022 A.8.9, A.8.19 政府統一基準(令和5年度版) 6.1.1(1)(2), 6.2.1(1)(2), 7.2.4(1) **自動車GL No.97**, 98, 102 (LV2)	○	
					★4	・不要サービスを無効化すること ・デフォルトユーザ ID の利用を停止すること ・利用するOS及びソフトウェアについて、ベンダーによる推奨セキュリティ設定を参考に設定を行うこと	ISO/IEC 27001:2022 A.8.9, A.8.19 政府統一基準(令和5年度版) 6.1.1(1)(2), 6.2.1(1)(2) **自動車GL No.101 (LV2)**	○	
			34	サポート期限の切れたハードウェア・ソフトウェアの利用停止や更改を実施すること。	★4	・サポートのある OS、ソフトウェアを利用すること ・やむを得ずサポート切れの OS、ソフトウェアを利用する場合は、更改計画を策定した上で、更改するまでの間、できる限り脆弱性悪用のリスクを低減すること	CE A6.6., A6.7. ISO/IEC 27001:2022 A.7.13, A 8.15 政府統一基準(令和5年度版) 6.2.1(2) **自動車GL No.123 (LV2)**	○	

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
			35	情報機器、情報システムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと。	★4	・インシデント発生時に調査を円滑に行うために必要なログとして、以下を取得、保管すること(※) [取得するログ(保管期間)] -ファイアウォールのログ(6 カ月)　※取引先等と接続する閉域網の入口に設置されるものも含む。 取得項目；日時、送信元 IP アドレス、送信先 IP アドレス -プロキシサーバのログ(6 カ月) 取得項目：日時、リクエスト元 IP アドレス、URL -認証サーバのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザID、成功/失敗 ・上記のログを脅威から保護するため、ログを保存するモノ、システムに「アイデンティティ管理とアクセス制御」において「重要な情報を取扱うと考えられるシステム」に課される要求事項(No.21)を適用すること ・上記で取得、保管しているログのうち、認証サーバのログについては、月１回以上の頻度でモニタリングを実施し、不審な認証試行を検知すること。 ※クラウドサービスの利用も対象に含む ※クラウドサービスを利用する場合、利用するサービスによって取得できるログの種類や取得方法等が異なることが想定されるが、以下の保管期間の規則を満たせない場合は、クラウドサービス選定時に、それを許容できるかを判断すること	ISO/IEC 27001:2022　A 8.15 政府統一基準(令和5年度版) 7.1.4(1) **自動車GL No.53, 143 (LV2), No.122 (LV3)**	○	
		21	36	ハードウェア・ソフトウェア等へのセキュリティパッチやアップデートの適用に係る手続等を策定し、実行すること。	★3	・適用範囲内の情報システム・情報機器、ソフトウェアは以下の状態とすること - ライセンスが付与され、サポートされている - サポートが終了した場合に削除されるか、インターネットとの全てのトラフィックを遮断することで適用範囲から削除される - 可能であれば、自動アップデートが有効になっている ・以下のいずれかに該当する場合、アップデートプログラムがリリースされてから14日以内に、アップデートを行うこと - 当該アップデートが、ベンダーにより「重大」(Critical)又は「高リスク」(High Risk)と説明される脆弱性を修正するものである - 当該アップデートが、CVSS v3 の基本スコアが7以上の脆弱性を修正するものである - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない [対象] -会社支給のパソコンの OS、ブラウザ、Office ソフト -サーバの OS、ミドルウェア -会社支給のスマートデバイスのOS、アプリ -インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア	**CE A6.1- A6.5** CMMC LV1 3.7.1, 3.14.1 ISO/IEC 27001:2022 A.8.8 政府統一基準(令和5年度版) 7.2.1(1) 自動車GL No.124 (LV1)	○	○
		22	37	システムをマルウェア感染から保護すること。	★3	・ネットワークに接続しているすべての情報機器(パソコン、サーバ)に、ウイルス対策ソフトウェアを導入すること。 ・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。 ・ウイルス対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートすること。	CE A8.1- A8.3. CMMC LV1 3.14.2, 3.14.4 ISO/IEC 27001:2022 A.8.7 政府統一基準(令和5年度版) 7.2.2(1) **自動車GL No.136, No.137 (LV1)**	○	○
					★4	・パソコン/Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限すること	ISO/IEC 27001:2022 A.8.9, A.8.23 政府統一基準(令和5年度版) **7.2.4(1)** **自動車GL No.108 (LV2)**	○	

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
	技術インフラのレジリエンス	23	38	内外のネットワークを適切に分離し、境界部分を防護すること。	★3	・すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)及びルータについて、デフォルトの管理パスワードを強固で一意のパスワードに変更する、又はリモート管理アクセスを完全に無効にしていること。 ・ファイアウォール及びルータのパスワードを変更する手順を整備すること。 ・ファイアウォール及びルータに係る認証は、No.14-17に定める認証・パスワード設定等に関する基準を満たすこと。 ・全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、認証されていないインバウンド通信をデフォルトで遮断すること。 ・すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、インバウンド通信に関するファイアウォール・ルールが、担当者によって承認され、文書化されていること。 ・すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、不要になったファイアウォール・ルールを速やかに削除又は無効化すること。 ・ファイアウォール・ルールの変更をインターネット経由で行う場合、多要素認証を適用するか、又は信頼できるIPアドレスにアクセスを制限すること	CMMC LV1 3.13.5 **CE A4.1, A4.2, A4.3, A4.6 - A4.10** ISO/IEC 27001:2022 A.8.22 政府統一基準(令和5年度版) 7.2.4(1) 自動車GL No.103, 104 (LV2)	○	○
					★4	・利用中のOSが対応していない場合を除いて、すべてのパソコン、サーバにおいて、ソフトウェアファイアウォールを有効にすること。 ・社外公開サーバ、重要情報を扱うサーバ、工場ネットワーク/OA ネットワーク等について、専用のネットワークセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定すること。	**CE A4.1.1, A4.11** ISO/IEC 27001:2022 A.8.22 政府統一基準(令和5年度版) 5.2.1(3), 7.2.4(1) **自動車GL No.106 (LV2)**	○	
			39	社内から社外への不正な通信を遮断する対策を実施すること。	★4	・社内から不正なサーバへの通信を遮断する仕組みを導入すること	ISO/IEC 27001:2022 A.8.12 政府統一基準(令和5年度版) 7.2.4(1) **自動車GL No.146 (LV2)**	○	
攻撃等の検知	継続的モニタリング	24	40	ネットワーク上の適切な場所でネットワーク接続やデータ転送を監視すること。	★3	・社内外ネットワークの境界において、インターネットから社内への通信と社内から不正なサーバへの通信の双方について、ファイアウォール(又はファイアウォール機能を持つネットワーク機器)により不正アクセスをリアルタイム検知したり、遮断する仕組みを導入すること ・ファイアウォール(又はファイアウォール機能を持つネットワーク機器)からアラートが即時発報されること ・セキュリティ事象の速報レポートが作成され、通知されること ・アラートを受け取ったセキュリティ担当部署の担当者又は管理者等により当該事象がセキュリティインシデントに該当するかが判断されること	CMMC LV1 3.1.20, 3.14.6 CE A4.1 ISO/IEC 27001:2022 A.8.16 政府統一基準(令和5年度版) 5.2.3(1), 6.4.1(2), 7.1.6(1) **自動車GL No.142 (LV2)**	○	
					★4	・プロキシサーバ、IPS/IDS、ファイアウォール、エンドポイントのいずれか、又は組み合わせにより、以下の要件を満たす、異常時に通知する仕組みを導入すること -機器等からアラートが即時発報されること -機器等に関連したセキュリティ事象の速報レポートが作成され、通知されること	ISO/IEC 27001:2022 A.5.25, A.8.16 政府統一基準(令和5年度版) 5.2.3(1), 7.1.6(1) **自動車GL No. 142, 145 (LV2)**	○	
			41	ハードウェアやソフトウェアの状態や挙動を監視すること。	★4	・会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成すること ・利用を認めるもの以外のソフトウェアを役員、従業員、派遣社員、受入出向者が自由にインストールできないよう社内ルールを定めること ・外部から受け取ったファイルについて安全性を確認するため、ウイルス対策ソフトのリアルタイムスキャンを実行する、又は仮想環境上で安全性を確認するシステムを導入すること	ISO/IEC 27001:2022 A 8.7, A 8.16 政府統一基準(令和5年度版) 5.2.3(1), 6.2.1(2), 7.1.6(1) **自動車GL No.98, 130 (LV2)**	○	

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証の対象となると考えられる要求事項)
	有害イベントの分析		42	セキュリティインシデントとして扱う対象範囲を明確にし、運用していること。	★4	・以下の対象範囲を明確にすること -セキュリティインシデントとして扱う事象 -セキュリティインシデントのレベル ・No.41等で導入される機器等からのアラートを受け取った担当部署の責任者は、上記で定める対象範囲に基づき、以下を分析し、判断すること - 検知された事象がセキュリティインシデントに該当するか - （セキュリティインシデントに該当する場合）どのレベルのインシデントに該当するか	ISO/IEC 27001:2022 A.5.25 政府統一基準(令和5年度版) 7.1.4(1) **自動車GL No.23 (LV2)**		
インシデントへの対応	インシデントマネジメント	25	43	あらかじめ定めた手順に沿ってセキュリティインシデントに対応すること。	★3	・セキュリティインシデントへの対応手順を作成し、文書化すること ・対応手順には組織の必要に応じて以下の手順を含んでいること ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告 ・セキュリティインシデントの基準や社内外組織との連絡先、ルートを明確化すること ・セキュリティインシデント発生時におけるセキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を明確化し、文書化すること ・セキュリティインシデントの報告フォーマットを整備すること ・年１回以上、若しくは、社内外で重大なセキュリティインシデントが発生した際に、インシデント事例やその対応策を社内部署へ共有していること	ISO/IEC 27001:2022 A.5.24, A.5.26 政府統一基準(令和5年度版) 2.2.4(1)(2) **自動車GL No.16, 18, No.19, No.24 (LV1)**		
インシデントからの復旧	インシデント復旧計画の実行		44	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。	★4	・事業継続上重要なシステムについて、自然災害や情報機器の故障・不具合への対応を念頭に、以下の対策を構じること -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し、文書化すること	ISO/IEC 27001:2022 A 5.30 政府統一基準(令和5年度版) 5.3.1(1) **自動車GL No.153 (LV2)**		