TRIAS 99-023-02

サイバーセキュリティ業務管理システム試験

1. 総則

サイバーセキュリティ業務管理システム試験の実施にあたっては、「自動車の特定改造等の許可に関する技術上の基準に関する細目等を定める告示」（令和 2 年国土交通省告示第 787 号）に定める別添 2「サイバーセキュリティ業務管理システムの技術基準」の規定及び本規定によるものとする。

2. 試験条件

書面及び現地審査により試験を行うことができる。

3. 試験記録及び成績

試験記録及び成績は、付表の様式に記入する。

3.1. 当該試験時において該当しない箇所には斜線を引くこと。

3.2. 記入欄は、順序配列を変えない範囲で伸縮することができ、必要に応じて追加してもよい。

付表

サイバーセキュリティ業務管理システム試験記録及び成績

試験期日: 年 月 日 試験場所: 試験担当者:

○ 試験対象管理システム

社名: 管理システムの名称:

○ 試験成績

※各項目について適合性を裏付ける資料を添付のこと。書式は任意で構わない。

要件			適合性
3.		要件	
3.1.		試験機関は、審査のため、申請者がサイバーセキュリティ業務管理システムを導入していることを検証するとともに、本技術基準への適合性を検証しなければならない。	適 ／ 否
3.2.		サイバーセキュリティ業務管理システムは、以下の要件を満たさなければならない。	
	3.2.1	申請者は、試験機関に対し、サイバーセキュリティ業務管理システムが以下の段階を考慮していることを証明しなければならない。	適 ／ 否
	(1)	開発段階	
	(2)	生産段階	
	(3)	生産後段階	
	3.2.2	申請者は、サイバーセキュリティ業務管理システムにおいて使用されるプロセスにより、別紙に規定するリスク及び軽減策を含め、サイバーセキュリティを十分に考慮することが確保されていることを証明しなければならない。この場合において、当該プロセスは次に掲げるプロセスを含むものとする。	
	(1)	サイバーセキュリティを管理するための組織内で使用されるプロセス	適 ／ 否
	(2)	車両へのリスクの特定のために使用されるプロセス。当該プロセスにおいては、別紙のパートA に規定する脅威その他の関連する脅威が考慮されるものとする。	適 ／ 否
	(3)	特定されたリスクの評価、分類及び処理のために使用されるプロセス	適 ／ 否
	(4)	特定されたリスクが適切に管理されていることを検証するために導入されているプロセス	適 ／ 否
	(5)	車両のシステムのサイバーセキュリティをテストするために使用されるプロセス	適 ／ 否
	(6)	リスクアセスメントが最新に保たれていることを確保するために使用されるプロセス	適 ／ 否
	(7)	車両へのサイバー攻撃、サイバーセキュリティに対する脅威及び脆弱性の監視、検出及び対応のために使用されるプロセス並びに実施されたサイバーセキュリティを確保するための対策が、特定された新たなサイバーセキュリティに対する脅威及び脆弱性に照らして依然として有効であるかどうかを評価するために使用されるプロセス	適 ／ 否
	(8)	実施されたサイバー攻撃の分析に資する関連データを提供するために使用されるプロセス	適 ／ 否
	3.2.3	申請者は、サイバーセキュリティ業務管理システムにおいて使用されるプロセスにより、3.2.2.(3)の分類及び3.2.2.(7)の対応に基づき、サイバーセキュリティに対する脅威及び脆弱性のうち対応が必要なものが合理的な期間内に軽減されることが確保されることを証明しなければならない。	適 ／ 否
	3.2.4	申請者は、サイバーセキュリティ業務管理システムにおいて使用されるプロセスにより、3.2.2.(7)の監視が継続的であることを証明しなければならない。	
	3.2.4.1	初めて新規登録を受けた車両を監視対象に含めなければならない。	適 ／ 否
	3.2.4.2	サイバーセキュリティに対する脅威及び脆弱性並びにサイバー攻撃を車両のデータ及びログにより分析及び検知する能力を有さなければならない。この場合において、車両の所有者又は運転者に係る個人情報その他のプライバシーの保護に関する権利が尊重されるものとする。	適 ／ 否
	3.2.5	申請者は、3.2.2.の規定に関し、サイバーセキュリティ業務管理システムが、その契約するサプライヤー、サービス提供者又は申請者の下位組織との間に存在する関係をどのように管理するかについて証明しなければならない。	適 ／ 否

備考