別添 120　サイバーセキュリティシステムの技術基準

1.　適用範囲

この技術基準は、自動車（二輪自動車、側車付二輪自動車、三輪自動車、カタピラ及びそりを有する軽自動車、大型特殊自動車並びに小型特殊自動車を除く。）のサイバーセキュリティシステムに適用する。本技術基準は、アクセスについて権限のある者による車両へのアクセス並びに車両のデータ、機能及び処理能力に係る他の技術基準及び法令の規定の適用を妨げるものではない。また、本技術基準は、個人情報の保護に関する他の法令の規定の適用を妨げるものではない。

2.　用語の定義

2.1.　「サイバーセキュリティ」とは、車両及びその機能が、電気部品又は電子部品に対する脅威から保護されている状態をいう。

2.2.　「リスク」とは、自動車のサイバーセキュリティに係る脆弱性を悪用することにより、特定の脅威が組織又は個人に危害を与えるおそれをいう。

2.3.　「リスクアセスメント」とは、リスクの性質を理解し、リスクを分析（リスクのレベルを決定することをいう。）するための当該リスクの特定（リスクを発見、認識及び説明することをいう。）及びリスクを評価（当該リスク又はその重大さが受入可能又は許容可能であるかどうかを決定することをいう。）するための当該分析の結果とリスク許容基準（許容することができるリスクかどうかを判断するための基準をいう。）との比較に関する全体的なプロセスをいう。

2.4.　「脅威」とは、システム、組織又は個人に危害を与える可能性のある望まない事案の潜在的な要因をいう。

2.5.　「脆弱性」とは、１つ以上の脅威によって悪用されるおそれのあるデータ資産または軽減策（リスクを軽減する手段をいう。）の弱点をいう。

3.　要件

3.1.　自動車製作者等は、試験機関が本技術基準の要件への適合性を確認できるよう車両のリスクアセスメント並びにリスクがどのように対処及び管理されているかを実証しなければならない。この場合において、リスクアセスメントは、車両のシステム間の相互作用及びいかなる外部のシステムとの相互作用を考慮しなければならない。

3.2.　自動車製作者等は、車両の重要な要素を特定しなければならない。

3.3.　自動車製作者等は、既に運行の用に供している車両のためのソフトウェア、サービス、アプリケーション若しくはデータの保存又は実行のための専用環境が車両に存在する場合に適切な対策が取られていることを試験機関が確認できるよう実証しなければならない。

3.4.　自動車製作者等は、基準適合性の確認前に、実行されたセキュリティ対策の有効性を検証するために適切かつ十分な試験を実施しなければならない。