

4-3. サイバーセキュリティ及びプログラム等改変システムに係る基準 (UN-R155 及び UN-R156)

- 適用範囲
 - 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。)

- 改正概要
 - サイバーセキュリティ及びプログラム等改変システムに係る基準は、サイバーセキュリティについては、保安基準の細目を定める告示の別添 120「サイバーセキュリティシステムの技術基準」により、プログラム等改変システムについては、同別添 121「プログラム等改変システムの技術基準」により、それぞれ自動運行装置を備える自動車に対して適用させている。
 - 今般、国連 WP29において、サイバーセキュリティ及びプログラム等改変システムに係る基準が新規則として採択されたことを踏まえ、保安基準においてもこれに対応する改正を行う。(詳細は別紙参照)
 - 加えて、自動運行装置を備える自動車以外の自動車においても安全対策を向上させるため、順次当該規制の対象とするような改正を行う。

- 改正時期(予定)

令和2年12月下旬

- 適用時期(予定)
 - 無線によるソフトウェアアップデートに対応している車両
新型: 令和4年7月1日
継続: 令和6年7月1日
 - 無線によるソフトウェアアップデートに対応していない車両
新型: 令和6年1月1日
継続: 令和8年5月1日

これまでの状況

- 2019年6月、国連WP29(自動車基準調和世界フォーラム)において、自動運転のフレームワークドキュメント(自動運転車の国際的なガイドラインと基準策定スケジュール等)に合意。
- 日本は、WP29傘下の専門家会議等において共同議長等の役職を担い、官民オールジャパン体制で議論をリード。
- 2020年6月に開催されたWP29本会議において成立。

主な要件

- サイバーセキュリティ及びソフトウェアアップデートの適切さを担保するための業務管理システムを確保すること。
- サイバーセキュリティに関して、車両のリスクアセスメント(リスクの特定・分析・評価)及びリスクへの適切な対処・管理を行うとともに、セキュリティ対策の有効性を検証するための適切かつ十分な試験を実施すること。
- 危険・無効なソフトウェアアップデートの防止や、ソフトウェアアップデート可能であることの事前確認等、ソフトウェアアップデートの適切な実施を確保すること。

