

「IoT 製品に対するセキュリティ適合性評価制度構築方針案」に対する意見

・ 該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

3.1 制度の運用体制

・ 意見内容

CC が現行の制度であるが、EU はすでに NIS2 のための EU CC の導入を宣言していることもあり、このギャップを埋める必要がある。

・ 該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

3.2. 制度の対象とする製品範囲

・ 意見内容

対象となる機器がラベル取得後にソフトウェア含む機能を拡張更新した場合は、自己宣言による再度ラベルの取得が必要だと考える。

・ 該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

3.4. 制度で用いるセキュリティ要件・適合基準・評価手順

・ 意見内容

「図 3.4-2 セキュリティ要件の整理方針」には RED も含めるべき。CRA や RED、PSTI などでは脆弱性やインシデントに関連した報告義務がある。日本では JPCERT/CC および IPA が窓口となり、協調した運用が可能と考えられることから、義務化を並行して行うべきと考える。欧州で製品を販売する組織はそのための体制を構築する必要があることから、大きな負担にはならないと考えられ、寧ろ欧州のビジネスへの対応により製品のセキュリティおよび脆弱性やインシデント発生時の対処が、より速やかに行えるようになることは日本国内のサイバーセキュリティ態勢の向上の観点からも望ましいと考えられ、製造業社や販売業社が当該製品の脆弱性やインシデントに対処する窓口を設けるためにも IoT ラベリングの議論と並行して進めるべき。