- 提供する製品・サービスのセキュリティ対策に責任を持ち、「セキュア・バイ・デザイン」(※1)や「セキュア・バイ・デフォルト」(※2)の考え方に沿った対応(「サイバーインフラ事業者に求められる役割等に関するガイドライン(案)」への準拠や、JC-STARのラベル取得等)をお願いしたい。
- また、自組織も「サイバーセキュリティを実践する企業」であり、かつ、ユーザー企業にも影響を及ぼし得る存在であることを認識して、**サイバーセキュリティ対策に取り組む**ことをお願いしたい。

※1 「セキュア・バイ・デザイン」:IT製品(特にソフトウェア)が、設計段階から安全性を確保されていること

※2 「セキュア・バイ・デフォルト」:ユーザー(顧客)が、追加コストや手間をかけることなく、購入後すぐにIT製品(特にソフトウェア)を安全に利用できること。

趣旨・背景・補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が追うべきである(「責任のリバランス」)**、という欧米諸国を中心に提唱されている概念。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**の中でも、組織の改革を実行できる**経営層の意思決定者**による、製品開発の重要な要素としてセキュリティを優先させるという**コミットメントの重要性**が言及されている。今後、当該提言を踏まえた対応が全世界レベルで求められていくことが想定される。
- 経済産業省では、本文書も踏まえ、「**サイバーインフラ事業者に求められる役割等に関するガイドライン(案)**」を2025年3月に公表したところ。この中で、ITサービス・製品提供事業者に求められる責務として、セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用等についても提示している。加えて、**IoTセキュリティ適合性評価制度(JC-STAR)を構築・2025年3月に制度運用開始**し、セキュアなIoT製品を容易に選択できる環境整備を進めているところ。ITサービス・製品提供事業者におかれては、積極的にこれらのガイダンスや制度を活用いただきたい。経済産業省としては、引き続き、ITサービス・製品提供事業者が上記メッセージをより具体的に理解し、実践しやすい環境を整備していく。
- また、近年、**ITサービス・製品提供事業者におけるサイバー事案**もみられるところ、自らも「サイバーセキュリティを実践する企業」であり、**ユーザー企業にも影響を及ぼし得る存在**であることを認識して、対策に取り組んでいただく必要がある。

関係する政府文書・窓口等

- 内閣サイバーセキュリティセンター「[国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則](#)」に署名(令和5年10月)
- 経済産業省/内閣サイバーセキュリティセンター「[サイバーインフラ事業者に求められる役割等に関するガイドライン案](#)」(令和7年3月)
- IPA「[セキュリティ要件適合評価及びラベリング制度\(JC-STAR\)](#)」