防衛産業サイバーセキュリティ基準について

○ 近年、サイバー攻撃等のリスクが増大しており、防衛調達に係るサプライチェーン全体においても、サイバーセキュリティ対策を講ずることの重要性が高まっていることから、2022年３月に現基準である「防衛産業サイバーセキュリティ基準」を整備

【ポイント】

- 米国国防省が契約企業に義務付けている基準（NIST SP800-171[注１]）と同水準の管理策を採用
- 情報システムに対する攻撃者を特定・防御するという水際対策に加えて、「検知」・「対応」・「復旧」が強化されており、
- 情報システムのサイバーセキュリティ対策のみならず、物理的セキュリティ対策、組織的セキュリティ対策などを網羅的に規定
- 保護すべき情報を取り扱う全ての防衛関連企業（下請負を含む。）が対象

○ 特約条項[注２]に係る別紙及びその別紙に係る付紙として構成

注１　非政府機関でCUI（Controlled Unclassified Information:保護対象となる非秘密情報）を扱う情報システム・組織のセキュリティ標準（産業向け）

注２　契約の基本的な内容を補完する付加的な規定で、契約内容に応じて適用するもの

装備品等及び役務の調達における情報セキュリティの確保に関する特約条項

装備品等及び役務の調達における情報セキュリティ基準（別紙）

装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領（付紙）

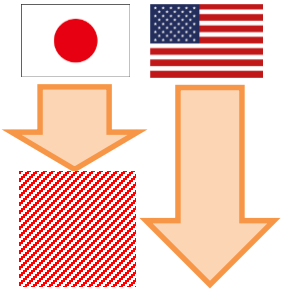
防衛産業サイバーセキュリティ基準

情報システムのサイバーセキュリティ対策

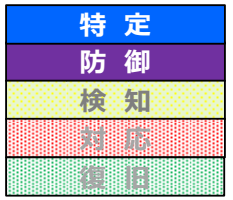
・保護すべき情報を取り扱う情報システムに対するサイバー攻撃に関し、早期発見・対処のための措置内容をより具体化

サイバー攻撃を防止する対策

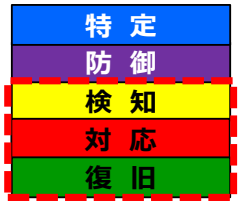
攻撃を受けた後の対策



旧基準



防衛産業サイバーセキュリティ基準（米国国防省基準ベース）



システムログや通信の監視、分析

不具合の修正・改善や被害の拡大防止

バックアップからのシステム再構成

サイバー攻撃に関し、早期発見・対処のための措置を従来よりも具体化