（お知らせ）

令和６年５月１７日
防　　衛　　省

「防衛産業サイバーセキュリティ基準に係る説明会」の開催について

防衛産業に新規参入する企業に対する防衛産業サイバーセキュリティ基準に係る説明会を以下の通り開催しますのでお知らせします。

１　趣旨

近年、増加するサイバー攻撃については、ネットワーク内部へ入り込む手段等が巧妙化するなど、情報が外部に流出するリスクが高まってきています。

こうした状況を受け、防衛省においては、装備品等の調達におけるサイバーセキュリティ体制の強化を図るため、令和３年度末に、防衛産業サイバーセキュリティ基準を整備し、令和５年４月以降、防衛関連企業（防衛省の契約相手方及びその下請負者）においては、サイバー攻撃の早期発見・対処等に対応した情報システムへの改修等が進められております。

防衛装備品への活用が可能な技術や製品を有する企業が防衛産業に新規参入する場合においても、防衛産業サイバーセキュリティ基準に基づく、強固な情報保全体制の構築が必要となることから、説明会を実施し、防衛産業サイバーセキュリティ基準に基づく構築時における疑問の解消等の機会を創出することを目的としています。

２　開催日時・場所等（別紙参照）

・東京開催：令和６年６月６日（木）及び７日（金）
（両日ともに１０時から１７時）
開催場所：東京都千代田区丸の内３－３－１　新東京ビル　７Ｆ
主な対象：（１日目）経営層
（２日目）社内規則の作成担当者
現地定員：１５０名（１社当たり２名まで）
オンライン定員：５００回線（実施方法：ＺＯＯＭを予定）

・各地区開催：別紙参照

３　参加登録

令和６年５月２２日（水）、防衛装備庁のＨＰにおいて、募集受付を開始
（先着順に受付し、定員に達し次第締切）

別紙

開催に関する事項について

今回募集の対象

地区	開催回	開催日	主な対象	実施メニュー	開催場所	定員
東京	１日目	6/6	経営層	社内規則策定及び承認要領等について説明を実施予定。	東京都千代田区丸の内３－３－１新東京ビル７Ｆ（デロイトトーマツ Seminar Room）	現地：150 名（１社当たり２名） オンライン：500 名
	２日目	6/7	社内規則の作成担当者	より具体的な社内規則の策定要領について説明を実施予定。		

参考：次回以降募集

地区	開催回	開催日	主な対象	実施メニュー	開催場所	定員
東北地区	第１回	各地区各回の開催日については、別途お知らせいたします。	情報システムの構築・管理者	管理策の具体的な構築要領等を例示や図解等により、説明を実施予定。 （同一内容により実施するため、ご都合の良い日時にて参加可能）	各地区各回の開催日については、別途お知らせいたします。	現地：20 名（１社当たり２名）
	第２回					
	第３回					
	第４回					
	第５回					
関東地区	第１回					
	第２回					
	第３回					
	第４回					
	第５回					
近畿・中部地区	第１回					
	第２回					
	第３回					
	第４回					
	第５回					
中国・四国地区	第１回					
	第２回					
	第３回					
	第４回					
	第５回					

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）

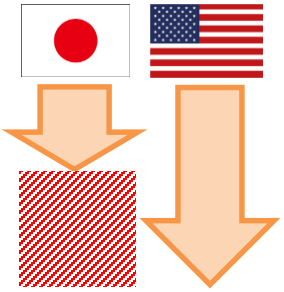
防衛産業サイバーセキュリティ基準

情報システムのサイバーセキュリティ対策

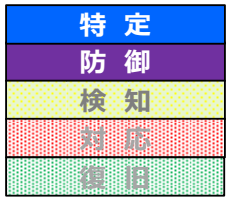
・保護すべき情報を取り扱う情報システムに対するサイバー攻撃に関し、早期発見・対処のための措置内容をより具体化

サイバー攻撃を防止する対策

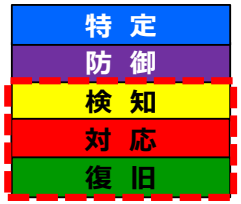
攻撃を受けた後の対策



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