

職務記述書

サイバーセキュリティテクニカルアドバイザー		
役割・責任	<p>防衛省・自衛隊では、日々高度化、複雑化するサイバー領域における脅威に対応するため、サイバー防衛能力の抜本的強化が必要と考えており、サイバー防衛を担う部隊の強化、人材の確保・育成、システム・ネットワークの充実・強化など様々な取組を行っている。</p> <p>かかる取組を促進すべく、サイバーセキュリティテクニカルアドバイザーは、サイバー領域における最新技術やサイバー攻撃の最新動向等に関する高度な知識・スキル及び豊富な経験・実績をもとに、防衛省・自衛隊全体のサイバー防衛能力強化のために必要な施策の実施について、最高情報保証責任者（CIS0）及び情報セキュリティ部門などに助言等を行う。</p>	
業務内容 詳細	1. サイバーセキュリティ体制の強化	・防衛省・自衛隊のサイバーセキュリティ体制の強化を図る上での各種課題（組織体制、システムなど）の解決に資する研究を行い、その成果に基づいて助言を行う
	2. サイバーセキュリティ関連規則	・サイバーセキュリティに関連する規則の改善を図る上での各種課題の解決に資する研究を行い、その成果に基づいて助言を行う
	3. 人材の育成・確保	・防衛省・自衛隊のサイバー人材の採用や育成の強化に関して研究を行い、その成果に基づいて助言を行う
	4. サイバーセキュリティに関する最新技術の研究	・防衛省・自衛隊におけるサイバーセキュリティに関する最新動向の調査及び分析などに関して研究を行い、その成果に基づいて助言を行う。
レポート ライン	<p>サイバーセキュリティテクニカルアドバイザーは、上記第1項～第4項に係る研究成果を CIS0 である整備計画局長に報告するとともに、研究成果に基づいた助言を行う。これらの実施に当たり必要な調整は、整備計画局サイバー整備課に対して行う。その他必要に応じて、防衛省・自衛隊の各部署との間で意見交換等を行う。</p>	
求められる 経験	実務	・民間あるいは公的機関におけるセキュリティコンサルティングの業務経験

		<ul style="list-style-type: none"> ・民間あるいは公的機関におけるセキュリティソリューションに関する設計開発の業務経験
	管理	<ul style="list-style-type: none"> ・セキュリティやシステム分野の部門あるいは個別プロジェクトにおけるマネジメントの経験
求められるスキル・知識	情報収集・分析	<p>サイバーセキュリティに係る以下の分野を含むことを想定（ただし、すべてを網羅することは要求しない）</p> <ul style="list-style-type: none"> ・サイバー攻撃の手法やサイバーセキュリティの最新動向に関する知識・情報 ・脆弱性に関する知識・情報 ・サイバーセキュリティ対策に関連するAIの最新技術にかかる知識・情報 ・サイバーセキュリティに関する諸外国の動向に関する知識・情報
	機器	<ul style="list-style-type: none"> ・サイバーセキュリティに必要な機器に関する知識・情報
	人材	<ul style="list-style-type: none"> ・サイバーセキュリティに関する人材の採用、配置、育成における知識・情報
	課題形成力	<ul style="list-style-type: none"> ・情報システム及びそれを運用する組織を対象としたサイバーセキュリティに係る状況把握・分析・課題の発見
	課題解決力	<ul style="list-style-type: none"> ・課題解決のための施策の具体化
期待される特性・行動	サイバーセキュリティに関して、防衛省・自衛隊の施策に結実する研究及び助言を行うため、責任感が求められる。また様々な課題を捉える広い視野と、一つのやり方に固執しない柔軟性が求められる。	
情報アクセス権限	<p>業務遂行上必要となる情報（特定秘密は含まない。）</p> <p>※1 防衛省入省後、秘密の取扱いに関する適格性の確認を行う。</p> <p>※2 自衛隊法第59条の規定により、守秘義務が課される。</p>	