

職務記述書（募集区分）

サイバーセキュリティ統括アドバイザー	
役割・責任	<p>防衛省及び自衛隊は、高度化・複雑化するサイバー脅威への対応として、サイバー防衛能力の抜本的強化を重要課題と位置付けており、防衛省次世代情報通信戦略に基づいて、AI や量子技術、エッジコンピューティング等の先端技術の活用、高信頼・低遅延通信インフラの整備、分散型ネットワークによるレジリエンス向上など、サイバー防衛能力の質的向上を進めているところである。</p> <p>この取組を加速するため、サイバーセキュリティ統括アドバイザーは、最新技術に関する専門知識と経験を活かし、CISO 等に対し、戦略的かつ実効的な助言を行う。</p>
業務内容詳細	<p>1. 暗号に関する体制強化</p> <ul style="list-style-type: none"> <li>・防衛省・自衛隊の暗号にかかる体制の強化を図る上での各種課題（体制構築、承認、運用、クラウドやドローンなどへの対応）等の解決に資する幅広い研究を行い、その成果に基づいて助言を行う。</li> </ul>
	<p>2. 各種暗号の研究</p> <ul style="list-style-type: none"> <li>・次世代情報通信戦略に基づき、耐量子計算機暗号等の次世代暗号技術や量子暗号技術等の活用に関する研究を行い、その成果に基づいて助言を行う。</li> </ul>
	<p>3. サイバーセキュリティ関連規則</p> <ul style="list-style-type: none"> <li>・暗号を含む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。</li> </ul>
レポートライン	<p>サイバーセキュリティ統括アドバイザーは、上記第1項～第3項に係る研究成果を CISO 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	<p>実務</p> <ul style="list-style-type: none"> <li>・暗号の開発及び運用にかかる業務経験</li> <li>・官公庁、企業、研究機関等での暗号技術に関する業務経験</li> <li>・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</li> </ul>

求められるスキル・知識	情報収集・分析	<ul style="list-style-type: none"> <li>・暗号技術に関する高度な専門知識</li> <li>・耐量子計算機暗号等の次世代暗号技術や量子暗号技術等の活用暗号技術に関する情報収集・分析</li> <li>・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）</li> <li>・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</li> <li>・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</li> </ul>
	課題形成力	<ul style="list-style-type: none"> <li>・課題形成のための状況把握・分析</li> </ul>
	課題解決力	<ul style="list-style-type: none"> <li>・課題解決のための施策の具体化、関係者における意思決定</li> </ul>
期待される特性・行動	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、関係者の意思決定を行うため、柔軟性も求められる。	
情報アクセス権限	業務遂行上必要となる情報（特定秘密は含まない。） ※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。 ※2 自衛隊法第59条の規定により、守秘義務が課される。	