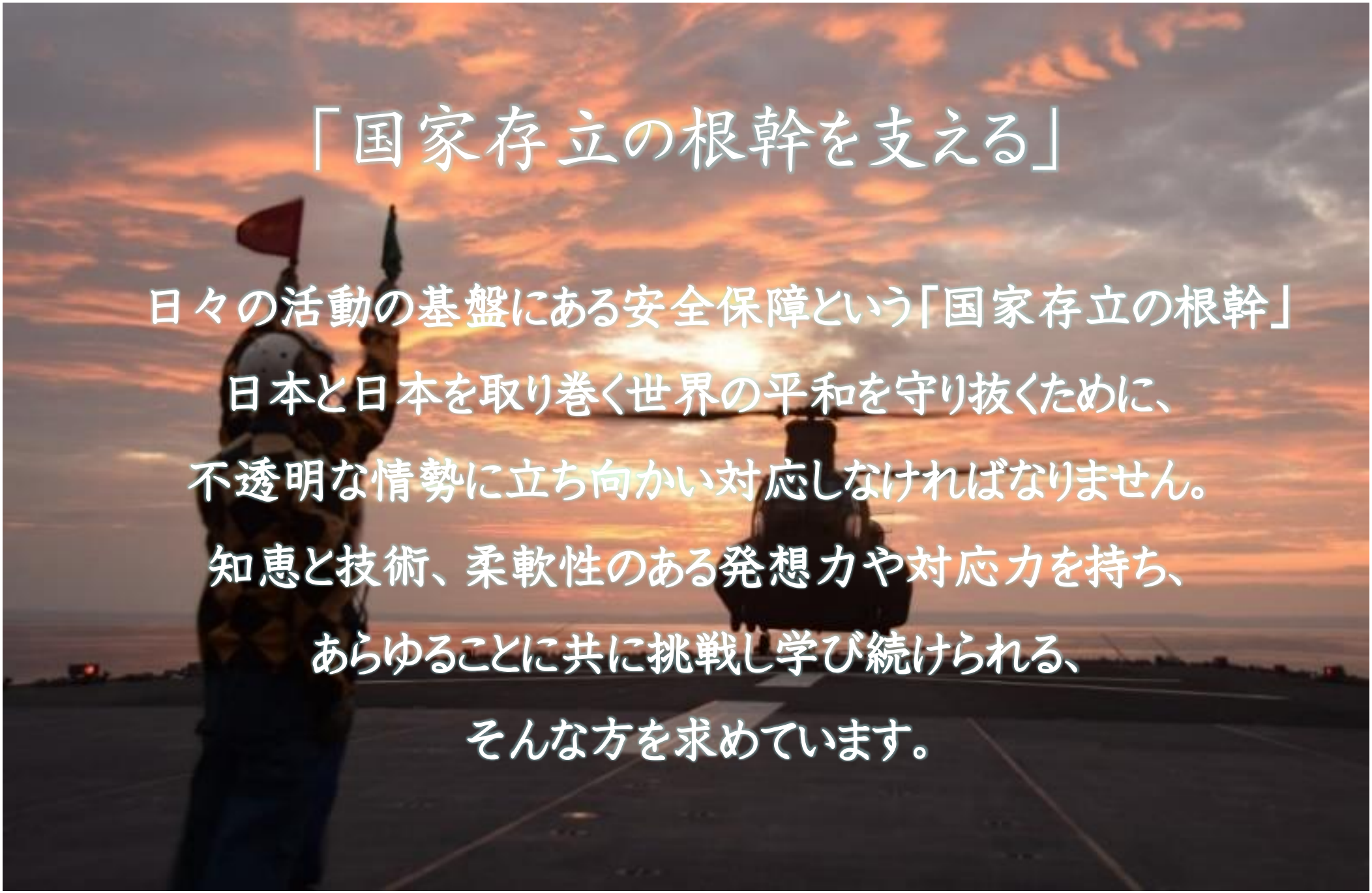
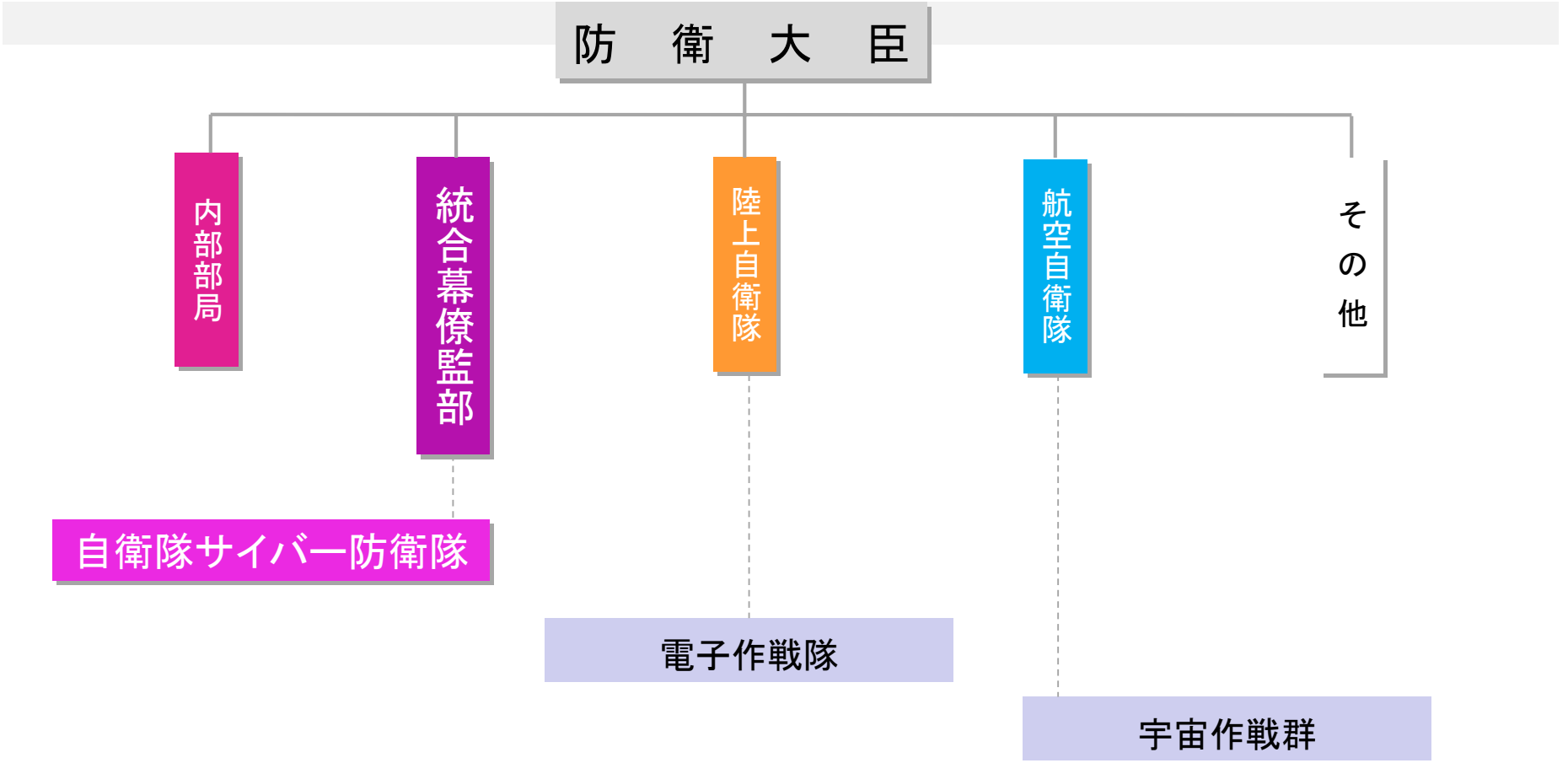
サイバーセキュリティ要員の募集

統合幕僚監部

自衛隊サイバー防衛隊


「国家存立の根幹を支える」
日々の活動の基盤にある安全保障という「国家存立の根幹」
日本と日本を取り巻く世界の平和を守り抜くために、
不透明な情勢に立ち向かい対応しなければなりません。
知恵と技術、柔軟性のある発想力や対応力を持ち、
あらゆることに共に挑戦し学び続けられる、
そんな方を求めています。

統合幕僚監部・自衛隊サイバー防衛隊の組織図



位　置　付　け	◆ 統合幕僚監部：防衛大臣を補佐する特別の機関 ◆ 自衛隊サイバー防衛隊：統合幕僚監部が直接管理する唯一の部隊

統合幕僚監部とは

▶自衛隊の運用に関する軍事専門的観点から防衛大臣を一元的に補佐

統合幕僚監部は、防衛出動や治安出動、災害派遣、国際平和協力活動をはじめとする陸・海・空３自衛隊の部隊行動等に際し、統一的な構想を立案し、その運用をつかさどる組織として設置され、軍事専門的観点から防衛大臣を一元的に補佐しています。

数々の国際平和協力活動、国内外で突発的に生起する自然災害等への対応のほか、ソマリア沖・アデン湾における海賊対処活動、さらには弾道ミサイルへの対処、東シナ海をはじめとする我が国の周辺海空域における警戒監視など、さまざまな活動に全力で取り組んでおり、我が国の平和と独立を守り、国の安全を保つために自衛隊の持つチカラを有効に活用して、任務を達成するための指示・調整を行っています。

統合幕僚監部には自衛官のみならず、多数の事務官・技官が配置されています。

海　賊　対　処　行　動

国際緊急援助活動

周辺海域の警戒監視

災　害　派　遣　活　動

新たな領域における能力強化

令和5年度以降に係る「国家防衛戦略」

宇宙・サイバー・電磁波といった新たな領域の利用の急速な拡大

陸・海・空における対応を重視してきた
これまでの安全保障の在り方の**根本的変更**

防衛力の強化の優先事項	宇宙・サイバー・電磁波といった**新たな領域**における**能力の強化**

統合幕僚監部における体制の強化

「国家防衛戦略」による防衛力強化優先事項

各自衛隊にも、
サイバー防護隊は存在するが……

統幕に「自衛隊サイバー防衛隊」設立

・サイバー防衛能力の根本的強化

・人員体制の拡充

一般職試験からの採用

▶サイバーセキュリティ要員の採用

自衛隊サイバー防衛隊において

〇サイバー攻撃等の脅威から情報システム等を防護

〇サイバーセキュリティに関する人材育成

〇隊員の能力向上等に関する業務等を実施

また、サイバーセキュリティ業務に関する企画立案及びその他一般的な行政事務を実施

近年の安全保障に係るサイバー攻撃等事象

凡例：政府機関等への攻撃　重要インフラ事業者等への攻撃　大規模、拡散型の攻撃

2015年1月、フランスの国際放送局がサイバー攻撃を受け放送停止

2016年6月、大企業や政府機関への攻撃（軍事資料流出）
2016年9月、韓国軍の内部ネットワークにサイバー攻撃（軍事秘密が流出）

2020年11月、カナダ政府は中国、ロシア、イラン、北朝鮮各国政府が関与する不正侵入プログラムが、電力供給システムに対するサイバー犯罪の面で大きな脅威だと警告。

2017年5月、フランス大統領選挙候補者に対するサイバー攻撃

2012年9月、政府機関等のウェブサイトへの攻撃
2015年5月、政府機関等への攻撃（年金情報流出）

2015年12月、ウクライナでサイバー攻撃による大規模停電
2017年6月、ウクライナ等でサイバー攻撃により政府機関等に被害

2013年8月、米ヤフーへのサイバー攻撃により30億件の個人情報が流出
2014年10月、ホワイトハウスの非秘密情報システムへの不正アクセス
2014年11月、米ソニー映画子会社に大掛かりなサイバー攻撃
2015年6月、米政府機関や米陸軍のウェブサイトへの攻撃
2016年7月、米民主党へのサイバー攻撃

2017年、北朝鮮に拠点を持つグループがﾊﾞﾝｸﾞﾗﾃﾞｨｼｭ中央銀行へのｻｲﾊﾞｰ攻撃で現金を強奪したとの認識を米シマンテック幹部が示す。

2019年、大手銀行の管理システムへの不正アクセス
2020年、化学メーカーの保有する技術情報の不正取得
2021年5月、富士通への不正アクセスにより、複数の政府機関の情報が流出

2017年、サウジアラビアの石油化学工場の内部ネットワークへ侵入、攻撃

2011年以降、中東地域等で、非常に高度な情報収集型マルウェア「デューク一」「フレイム」「ガウス」を相次いで発見

2018年、米航空宇宙関連企業が保有する秘密情報への不正アクセス
2020年、Solar Winds社の監視ツールを介してアメリカ政府機関を含めた100弱の組織へ侵入

※資料源：一般報道等

2017年5月、150カ国以上でランサムェア「WannaCry」による被害

○諸外国の政府機関や軍隊などの情報通信インフラに対する攻撃が多発　これらの一部には、ロシア・中国・北朝鮮の政府機関や軍が関与しているとの指摘あり。また、非国家主体からのサイバー攻撃との指摘もあり
○サイバー空間における脅威の増大を受け、米国などでは、政府全体での取組や国防省レベルでの取組が進展

防衛省・自衛隊における取組状況

サイバー攻撃対処６本柱

① 情報システムの安全性確保

・ファイアウォール、ウィルス検知ソフトの導入
・ネットワークをDIIオープン系・クローズ系とに分離
・システム監査の実施　など

② 専門部隊によるサイバー攻撃対処

・サイバー防衛隊（共）、システム防護隊（陸）、保全監査隊（海）、システム監査隊（空）によるネットワーク・情報システムの24時間監視、高度なサイバー攻撃対処（ウィルス解析）

③ サイバー攻撃対処態勢の整備

・情報システムのセキュリティ対策基準の制定
・職員が遵守すべきセキュリティ対策の制定
・サイバー攻撃発生時の対処態勢の整備

④ 最新技術の研究

・サイバー演習環境構築技術の研究（模擬環境での対抗演習が実施可能）

⑤ 人材育成

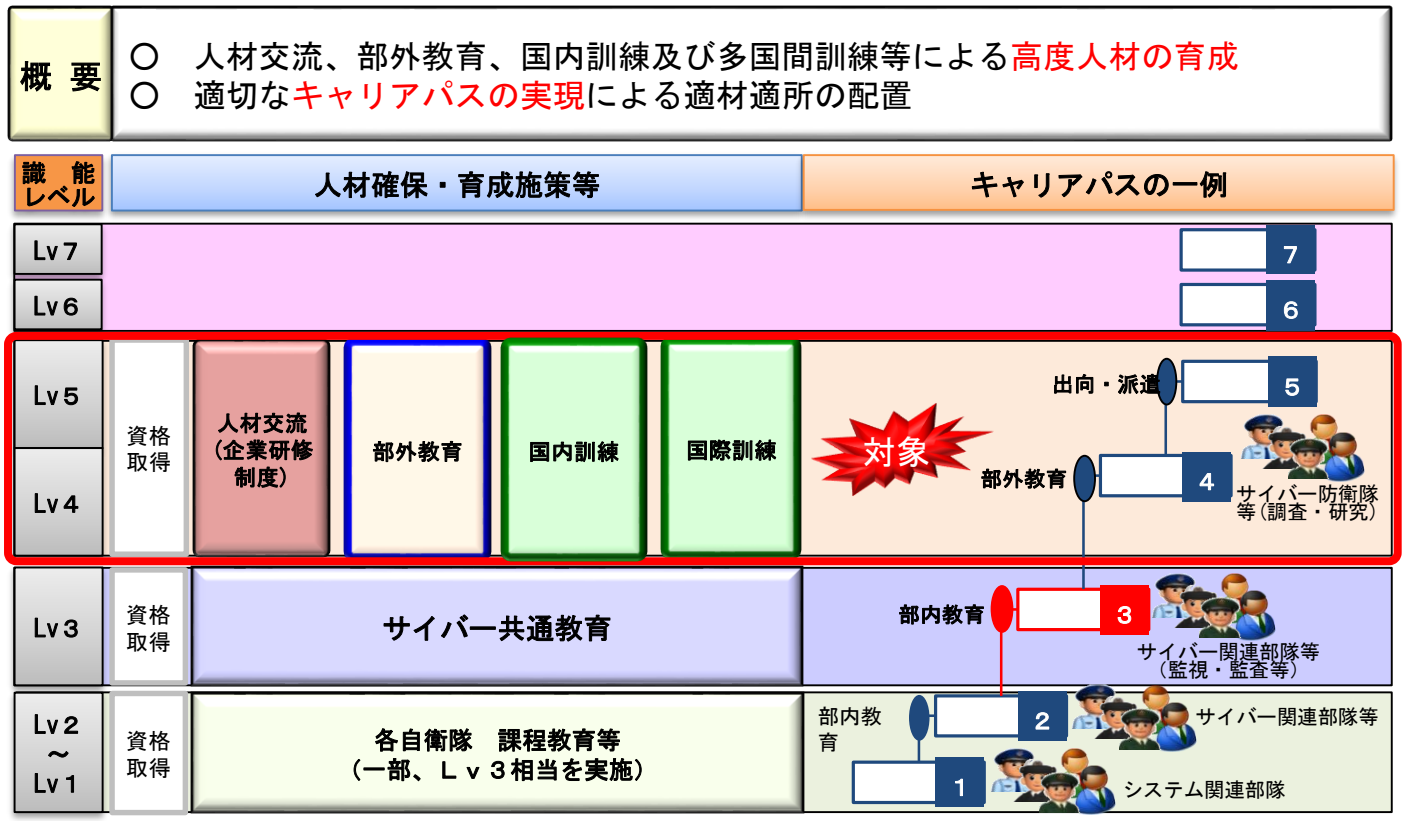
・人材育成のため、米国カーネギーメロン大学付属機関、国内大学院への留学や各自衛隊の専門課程における教育の実施
・セキュリティ意識の醸成のため、職場における教育、防衛大学校における専門教育の実施

⑥ 他機関等との連携

・内閣サイバーセキュリティセンター、米軍、関係各国などとの情報共有

防衛省・自衛隊のサイバー攻撃対処態勢

○ 人材確保・育成



部外教育等の一例	
部外教育	・CISSP CBK Review Training ・SANS Training ・ハッキング技術 ・マルウェア解析ハンズオン ・TCP/IPプロトコル詳解
国内シンポジウム	・CODE BLUE@TOKYO ・白浜、越後湯沢、道後
国際シンポジウム	・FIRST総会 ・BlackHat and Defcon

※識能レベル（Lv1～7）
防衛省・自衛隊が必要とするサイバー人材を定義するため、省で定めたサイバーセキュリティ・スキルレベル。現在の防衛省・自衛隊の任務を遂行するためには、Ｌｖ５までの人材が必要となる。

【サイバーセキュリティのプロフェッショナルとして】

統合幕僚監部（自衛隊サイバー防衛隊）

入省3年目職員のコメント

●現在の職務内容について

私の勤務するサイバー防衛隊は、令和4年3月に新編された新しい部隊であり、防衛省・自衛隊の情報通信ネットワークの監視及びサイバー攻撃への対処を24時間体制で行っております。非常に高度な技術を必要とするため、業務の傍ら新しい技術の取得に追われる毎日ですが、やりがいを感じて勤務しております。

●仕事で心掛けていること

サイバーセキュリティの世界では技術が日進月歩で進化しています。業務に必要な最新の知識・技術を身に付け、それを業務で生かせるように心がけています。

●サイバー防衛隊の魅力

自衛隊の活動の基盤となる情報通信ネットワークを守る重要な職務に従事できることを非常に喜ばしく感じています。また、部内外教育、各種のサイバーコンテスト、サイバー攻撃対処訓練への参加等、人材育成に積極的に取り組む職場にとても魅力を感じています。

サイバーの世界で自分の力を生かしたい？

ＩＴの資格をたくさん取得したい？

Definitely, here !

意欲に溢れたあなたを待つ、

教育体制・勤務環境があります！

サイバー、ＩＴの世界に興味はあるけど、

ほとんど知識がない？

Welcome to CDC！

基礎から学べる

教育体制・勤務環境が整ってますよ！