Fujii_T CYDEF 2018

１　氏名及び役職名等（Name and Title）

藤井敏彦、防衛装備庁長官官房審議官
Mr. Toshihiko Fujii, Assistant Commissioner, Acquisition, Technology & Logistics Agency, MoD, GoJ

２　略歴（CV）

昭和 62 年 4 月　通商産業省入省
平成 12 年 9 月　日本機械輸出組合ブラッセル事務所
16 年 7 月　経済産業省貿易経済協力局貿易管理部特殊関税調査室長
19 年 7 月　経済産業省通商政策局通商機構部参事官
22 年 7 月　同部総括参事官
24 年 1 月　経済産業省資源エネルギー庁エネルギー交渉官
25 年 6 月　経済産業省通商政策局通商政策課長
26 年 7 月　経済産業省資源エネルギー庁国際資源エネルギー戦略統括調整官
27 年 7 月　経済産業省資源エネルギー庁資源・燃料部長
28 年 6 月　関東経済産業局長
29 年 7 月　現職に就任

Apr.1987 Joined the Ministry of International Trade and Industry
Sep.2000 Japan Machinery Center for Trade and Investment Brussels Office
Jul.2004 Director, Office for Trade Remedy Investigations, Trade Control Department, Trade and Economic Cooperation Bureau, METI
Jul.2007 Director, Multilateral Trade System Department, Trade Policy Bureau, METI
Jul.2010 Principal Director, Multilateral Trade System Department, Trade Policy Bureau, METI
Jan.2012 Counselor, Energy Negotiation, Agency for Natural Resources and Energy, METI

Jun.2013 Director, Trade Policy Division, Trade Policy Bureau, METI
Jul.2014 Deputy Commissioner for International Affairs, Agency for Natural Resources and Energy, METI
Jul.2015 Director-General for Natural Resources and Fuel Department, Agency for Natural Resources and Energy, METI
Jun.2016 Director-General, Kanto Bureau of Economy, Trade and Industry
Jul.2017 Assistant Commissioner, ATLA (Acquisition, Technology and Logistics Agency), Ministry of Defense

３　参加枠（Time Slot）

APR 4, 1005-1035 Key Note Speech

４　講義要約（Abstract）

「今後の防衛調達におけるサイバーセキュリティ対策」
防衛省・自衛隊では、自らのサイバー攻撃対処能力の向上はもとより、パートナーである防衛産業のサイバー攻撃対処能力の向上についても重要な課題と認識しており、昨今の高度なサイバー攻撃に備えた防衛産業向けの有効な対策について検討を開始している。
今回のワークショップでは、防衛装備品の調達を所管する防衛装備庁において検討を行っている「今後の防衛調達におけるサイバーセキュリティ対策」について、担当の防衛装備庁長官官房審議官から発表する。

"Cybersecurity Policies for Defense Industries in Future"
Since MOD/SDF recognizes not only how important is to improve our own cyber defense capabilities but those of the defense industries as a whole, we will start by discussing effective policies to prevent the recent high cyber attacks. In this cyber workshop, the Assistant Commissioner in charge of cyber security in Acquisition, Technology and Logistics Agency will address the issue of " Cybersecurity Policies for Defense Industries in Future " currently discussed in ATLA, which is responsible for policies of defense equipment procurement.

positions early in his career, including serving as Acting Deputy Undersecretary for Defence Policy, a Director of Policy Planning, and an Adviser to the Minister of Defence. Mr Lifländer also served as a Defence Counselor at the Embassy of the Republic of Estonia in the United States and as a Defence Counselor at the Delegation of the Republic of Estonia to NATO.
Mr. Lifländer received a direct commission in the Estonian Defense Forces (Infantry) and has been awarded with the Estonian Defence Forces Distinguished Service Decoration as well as Distinguished Service Decorations of the Estonian Ministry of Defence.
Mr. Lifländer received his Bachelor of Science Degree in Engineering from the United States Military Academy, West Point. He received his Master of Arts in Security Studies from Georgetown University's Center for Security Studies (CSS) in the Edmund A. Walsh School of Foreign Service.

３ 参加枠（Time Slot）

APR 4, 1040-1110 Key Note Speech

４ 講義要約（Abstract）

「新しいドメイン、古き課題: NATO の直面するサイバー課題」
将来のいかなる事件、紛争または危機において、サイバー的要素を含まないものは想像し難い。そして、これは現在すでに我々が直面している環境でもある。その意味は、能力開発の分野に「魔法の弾丸」はないということだ。実際のところ、サイバーに内在する技術的特徴は、勃興するサイバー脅威に対抗するソリューションを、希にウィジェット調達するようなものだ。この特殊なサイバーの課題に対処するためには、モノの要素から、より幅広く、より実践的な変革が求められている。つまり、それは人材登用、ドクトリン、訓練及び組織改編に関わる課題を意味する。NATO は共同作業により、より良い成果が得られることを発見した。サイバー空間を航空、陸上及び海上に並ぶ作戦ドメインとして認知する意志決定により、多くのものが生まれた。われわれは前に進み始めた、この仕事は前進の終点を意味するのではなく、むしろ始まりを意味する。

"New Domain, Old Challenges - NATO meeting the challenge of cyberspace"
It is difficult to imagine any future event, conflict or crisis that would not include a cyber component, given that this is the environment that we are all operating in already today. What this means for capability development is that there is no cyber 'magic bullet'. In fact, the inherent technical characteristics of cyber mean that solutions to emerging cyber threat are rarely going to be about widget acquisition. If we are to respond to the unique challenges of cyber we will have to have a much wider and more practical change than

addressing the material element alone. This means addressing challenges such as manning, doctrine, training and organizational issues. NATO is founded on the idea that we can achieve more when we work together. A lot is happening as a result of a decision to recognise cyberspace as an operational domain, alongside air, land and sea. While progress is being made, this work must be regarded as the beginning, rather than end, of progress.