日本安全保障貿易学会 2019 年年次大会（2019 年 3 月 9 日）
於　同志社大学

# 人工知能の安全保障上の可能性と情報の管理について

拓殖大学
教授　佐藤丙午

**〇はじめに：人工知能技術戦略（2017 年）**

**〇人工知能と安全保障**

「第三のオフセット」戦略と人工知能
新技術（Emerging and Foundational Technology）について
人工知能の兵器化について誤解と現実
各国ごとに異なる人工知能の兵器化の焦点
戦闘の方法の変化？：Multi-Domain Battle
Escalate to Deescalate への対応
通常抑止の意義（柔軟反応戦略の課題の克服？）
情報の多角化と攻撃方法の最適化
「新」兵器が及ぼす影響について
「30 大綱」と「中期防」：日本の防衛政策における人工知能

**〇CCW-GGE における LAWS：人工知能の位置づけ**

LAWS の議論の展開：人道法の枠内での議論の課題
「軍縮」と「人道」
CCW における議論の経緯
CCW-GGE（2018 年の結論）
「人間の管理」について
管理の定義
LAWS と人工知能
管理対象：「デザイン」と「運用」

**〇情報とアルゴリズム：「情報」の管理**

軍事における「可能性」と「信頼性」の問題
軍事における人工知能の活用について
「ビッグデータ」と「アルゴリズム」
軍事における「ビッグデータ」とは
「攻撃サイクル」と「ビッグデータ」
「アルゴリズム」と「データラベリング」：人的資本の問題
情報はなぜ保護されるべきなのか？

プライバシー
知的所有権
特許
それ以外？

**〇安全保障貿易管理における人工知能（情報とアルゴリズム）の扱い**

ECRA（輸出管理改革法）について
新技術（Emerging and Foundational Technology）の扱いについて
「リスト管理」の前段階
輸出を前提としない技術の管理
省庁間検討プロセスの今後

GAFA・アリババ・楽天・Yahoo などの民間企業に集まる「情報」の所有権と安全保障上の活用方法について

情報の国家管理の課題
オープン・ソースの「情報」の扱い
中国型治安モデル
「超」監視社会の安心と問題
SNS の管理

「人工知能」の拡散について
「信頼性」のない人工知能の活用方法：必要性と十分性について
リスト管理以外の方法は何か？

以上