

ミサイル防衛の課題と展望(4)

副題「イージスアショアについて」

平成30年9月28日

一般社団法人国際平和戦略研究所



本説明の狙いと説明者紹介

- 本説明の狙い
 - 本説明は、一般社団法人国際平和戦略研究所が実施する標題セミナーの4回目の説明資料である。
 - セミナー参加者が副題に焦点を当てた内容について理解を得る事により、施策決定者に内容を反映していただき国が実施するミサイル防衛が適正に実施されることに貢献する。
 - 米朝会談を終え、北朝鮮による脅威は低下の様子を示しているが能力が低下しているわけではなくすでに保有している能力を基に準備すべきであるが、真の脅威は中国、ロシアである。
 - イーゼス・アショアは、高額、トップダウンにおける導入決定で反意もあるが、北朝鮮のミサイル脅威は継続され、中国、ロシアの弾道ミサイル、巡航ミサイル脅威に対処するためには、必須であると認められる。
 - 副題であるイーゼス・アショアの適正な導入整備に関し防衛省・自衛隊に民意を結集して進言する事を目的とする。
- 説明者
 - 氏名：坂上 芳洋
 - 経歴：防大卒、元海上自衛官、現防衛アナリスト
 - 一般社団法人国際平和戦略研究所理事
- 前提条件
 - 本説明は、説明者の経験と公刊資料並びに関係者とのインタビューからまとめたものである。
 - 本説明は、特定の企業・組織に利する事を目的とせず、また、一部の組織を非難する事を主目的することではなく純粋に中立的な立場で我が国のミサイル防衛及び日米同盟の維持向上を目的として提言するものである。
 - 内容によっては、米国ミサイル防衛庁及び米海軍を含む米政府の真意を確認し、我が国がイニシアティブをもって防衛力整備を実施する事を導く。
 - 一部は、米国側の理解を得るため、英語記述を加えている。



イージス・アショアの比較



現行システム
(ルーマニア・ポーランド)



平成31年度防衛省概算要求案
(根拠: 防衛省システム選定)



推奨案

イージス・アショア整備の懸案(総括)

標記について次のとおり総括し、各論は次ページ以降論述する。

- ・ イージス・アショアは、トップダウンで決定され不要論が蔓延しているが、**北朝鮮の脅威は依然継続し、脅威が進展する中国、ロシアに備える事が必須であるので必然の決断**である。
- ・ 本年7月30日の防衛省のイージス・アショア構成品選定結果による主レーダ**LMSSRの形態は未だ構想段階で日本独自に形態となり、設計、製造、試験、ミサイル射撃装備認定試験を日本政府が支弁する事が必定であることを政府防衛省は認識しているのか疑義**がある。また、LMSSR側が、新レーダーとして設計、プロトタイプ製造、初号機としての製造と包括的な試験計画並びに既存レーダーシステムより低コストで検証・検証計画を確定できるかも疑義があるところである。
- ・ 防衛省発表の平成31年度概算要求におけるイージス・アショアの経費が高騰している事、構成品選定結果と齟齬がある事：LMSSRを選択するが故の高騰かどうかまた、能力確認に関連する費用並びにミサイル発射装備認定試験の費用が含まれているかを明快にする必要がある。
- ・ LMSSRは、LRDRの技術に基づくとの米国ミサイル防衛庁の情報を根拠として防衛省が選択したが、構想段階であり、対抗馬である**米海軍がAir and Missile Defense Radar (AMDR)として選択し、PMRFで実運用、新造Aegis DDG用に製造中であるAN/SPY-6と比較にならない相違があることを度外視して選択したものである。日本独自であるため、研究開発、技術更新、整備運用はDCS調達であるが故に米国政府が保証するかについては、極めて重大な疑義を有し最大の関心事である。**
- ・ LMSSRが選択装備された場合、米海軍以外の日本を含む海外のAegis DDGのレーダ更新を目途としているとの情報があるが、それらの開発費を全て日本政府が負担することになる事を政府防衛省は現時点で予測しているのか疑わしい。加えて、ソフトウェアの更新と試験に関わる費用は、全て日本政府が支弁する必要があることを強調する。
- ・ これを要するに**イージス・アショアの構成品選定作業を再度実施し、整備の適正化を政官財（企業）及び国民の理解を一にして適切な防衛力整備を実施しなければならない。**
- ・ **米国ミサイル防衛省の進言が、米海軍を含む国防総省、米政府の総意に基づくものか再確認する事が必定である。**

サイバー防衛体制

2018年9月28日(金)

株式会社インテリジェントウェイブ

手塚 弘章



本日のストーリー

1. サイバー攻撃に関する日本の順位..... p.2
2. サイバー攻撃の怖さ..... p.3
3. 日本のサイバー防衛への取り組み..... p.6
4. 日本のサイバー司令部..... p.9
5. 日本のサイバー防衛隊..... p.10
6. 日本のサイバーセキュリティ戦略の概要.. p.11
7. 米国のサイバー防衛への取り組み..... p.13
8. 日本政府のサイバーセキュリティ予算.... p.14
9. サイバーセキュリティ軍を保有する国
のランキング... p.15
10. イスラエルの防衛体制..... p.18
11. 人間の限界を超えた攻撃..... p.19



サイバー攻撃に関する日本の順位（前回資料 1）

攻撃のターゲット上位10カ国 (数字は攻撃総数)

1位	アメリカ	2億2100万
2位	ブラジル	2420万
3位	イギリス	1420万
4位	日本	1340万
5位	ドイツ	1080万
6位	スペイン	1060万
7位	オーストラリア	700万
8位	インド	670万
9位	オランダ	580万
10位	シンガポール	450万

しかし

法・技術・組織・能力構築・連携 各要素における各国の防衛能力

1位	シンガポール
2位	アメリカ
3位	マレーシア
4位	オマーン
5位	エストニア
6位	モーリシャス
7位	オーストラリア
8位	ジョージア、フランス
9位	カナダ
10位	ロシア
11位	日本

出典：AKAMAI'S [STATE OF THE INTERNET] /
SECURITY Q1 2017 REPORT

出典：国際電気通信連合（以下ITU）

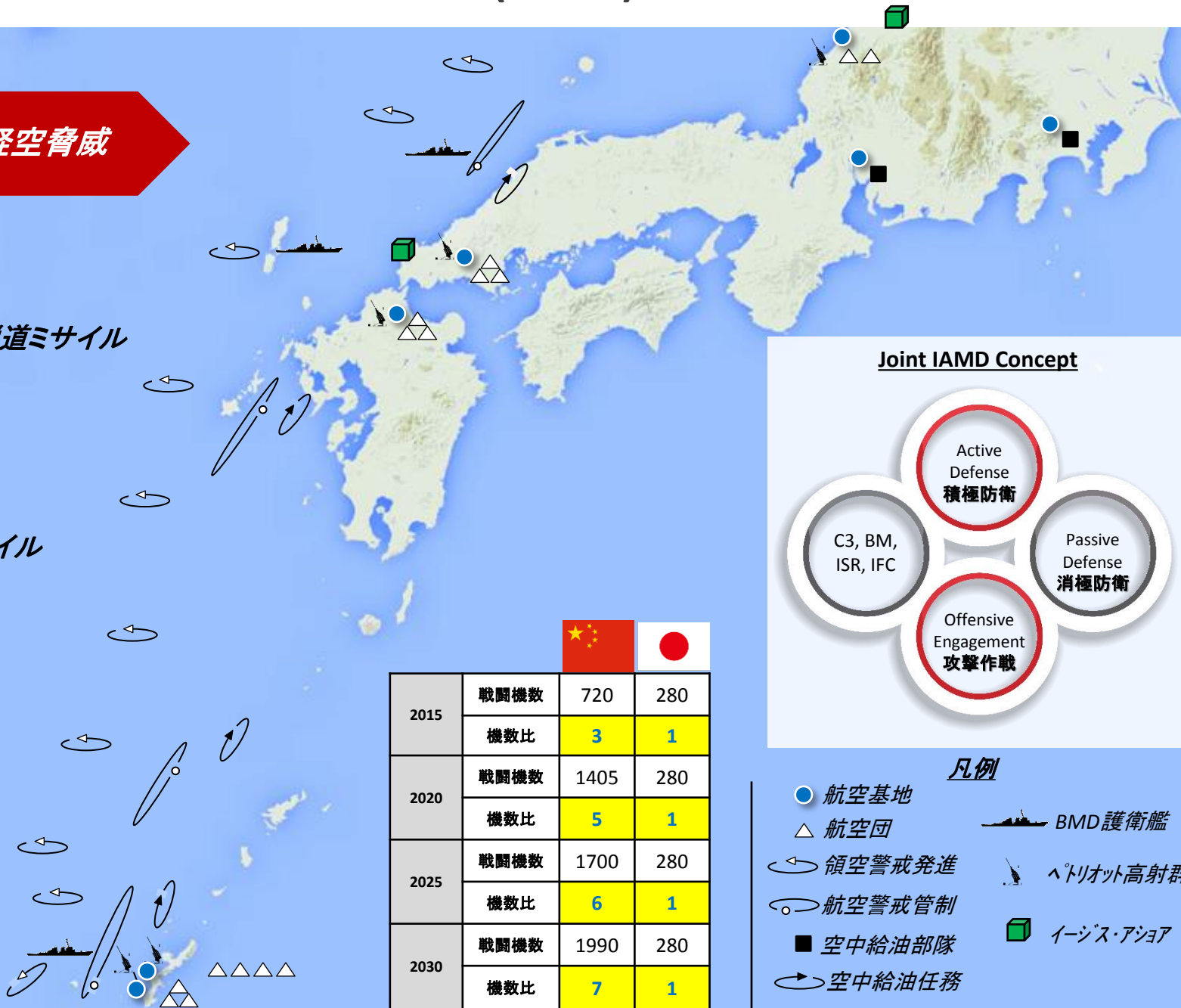
サイバー攻撃の怖さ（前回資料 2）

- ✓ 即時性…… 実行指示の直後から攻撃開始
 - ✓ 無差別…… ばら撒き攻撃では相手は無差別
 - ✓ 同時多発…… 同時に、複数の標的を攻撃
 - ✓ 場所無関係… 地球の裏側も時差なく攻撃
 - ✓ 材料費なし… 武器製造に材料は不要
- ⇒ 必要なのは、頭脳とコンピュータだけ



統合防空ミサイル防衛(IAMD)の運用イメージ

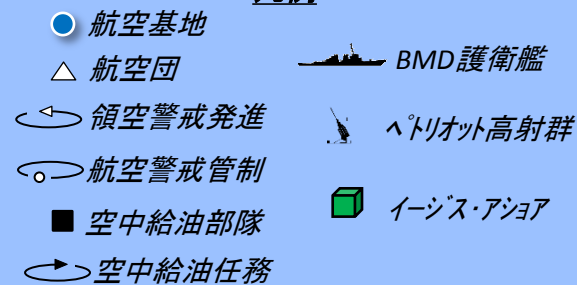
侵入してくる経空脅威



Joint IAMD Concept



凡例



2015	戦闘機数	720	280
	機数比	3	1
2020	戦闘機数	1405	280
	機数比	5	1
2025	戦闘機数	1700	280
	機数比	6	1
2030	戦闘機数	1990	280
	機数比	7	1