JNSA
Network Security Forum 2024
パネルディスカッション

私の見る
アクティブサイバーディフェンス

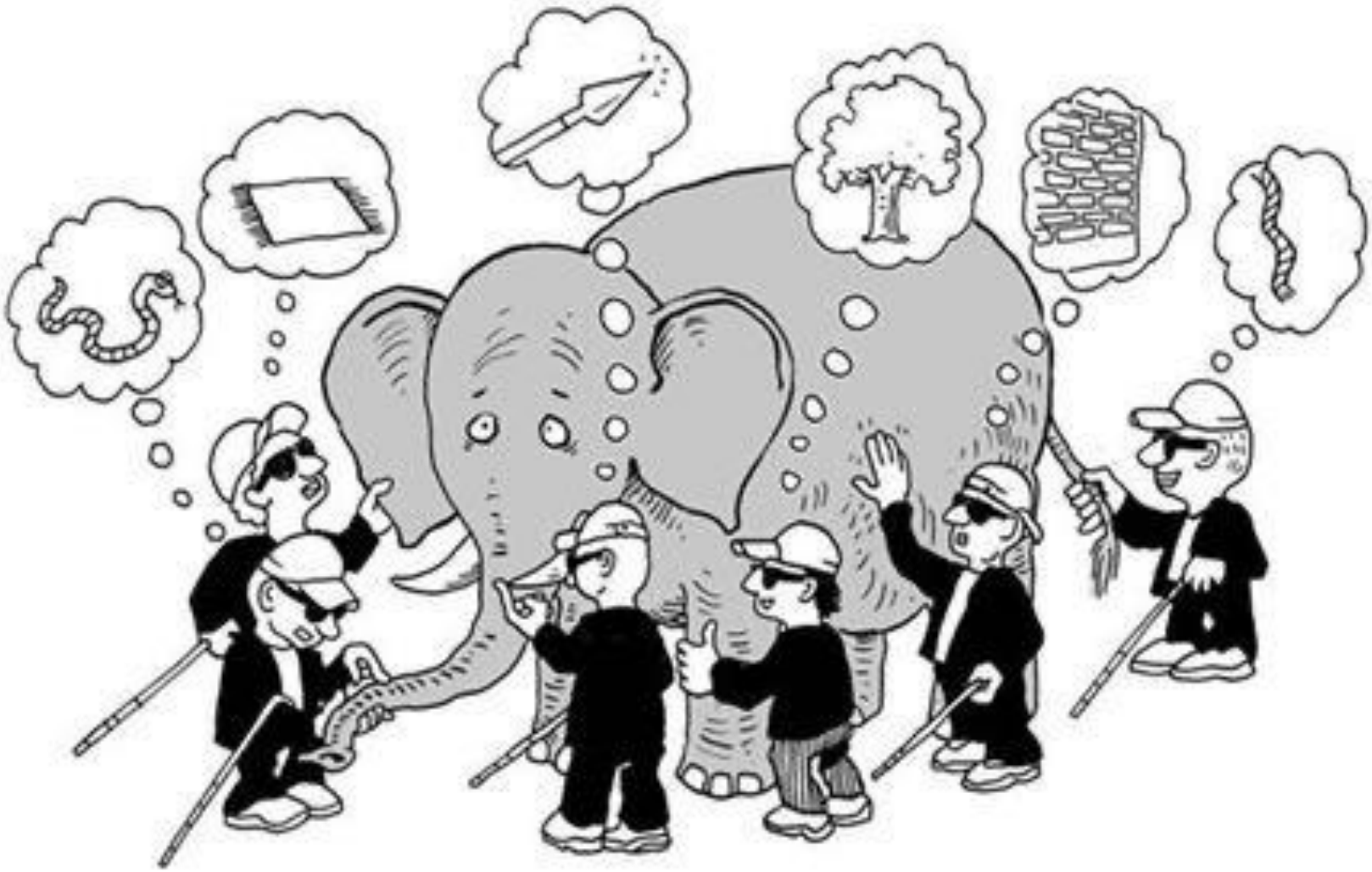
元陸上自衛隊システム防護隊長
国立研究開発法人情報通信研究機構　主席研究員
工学博士
伊東　寛

1980年慶應義塾大学大学院（修士課程）修了。同年、陸上自衛隊入隊。技術、情報及びシステム関係の部隊指揮官・幕僚等を歴任。この間、陸自初のサイバー戦部隊であるシステム防護隊の初代隊長を務めた。
2007年3月に退官し、以降、株式会社シマンテック総合研究所主席アナリスト、株式会社ラック ナショナルセキュリティ研究所所長、経済産業省大臣官房サイバーセキュリティ・情報化審議官、ファイア・アイ株式会社最高情報責任者等、約10年間にわたり官民のセキュリティ企業・組織で勤務。
2020年10月より国立研究開発法人情報通信研究機構(NICT)主席研究員。
工学博士。

主な著書に『「第５の戦場」サイバー戦の脅威』『サイバーインテリジェンス』『サイバー戦争論』などがある

本資料の内容は、公開情報に基づき、発表者が個人的に分析した成果によるものであり、政府関係機関、民間会社等の見解を代表するものではありません。

アクティブサイバーディフェンスとは



群盲像を撫でる

絵は以下のサイトより
https://www.countand1.com/2012/04/blind-men-elephant.html

・昔は、このように議論されていた

アクティブディフェンスとは（米国2016年）

防　御　　**攻　撃**

Into the Gray Zone — The Private Sector and Active Defense Against Cyber Threats-The Center for Cyber and Homeland Security (CCHS)、2016

アクティブ（サイバー）ディフェンスとは

米国ホームランドセキュリティの見解

- アクティブディフェンスは、**従来の受動的な防御と攻撃の間**にある一連のプロアクティブなサイバーセキュリティ対策を表す用語
- これらの活動は2つのカテゴリに分類される
- 技術的なもの
  - 防御側と攻撃側の間の技術的な相互作用を対象
- 政策的なもの
  - 防御側がインターネット上の脅威アクターとインジケーターに関するインテリジェンスを収集する操作
  - 悪意あるアクターの動作を変更できるその他の政策手段（制裁、起訴、貿易救済措置など）

Into the Gray Zone — The Private Sector and Active Defense Against Cyber Threats-The Center for Cyber and Homeland Security (CCHS)、2016

アクティブサイバーディフェンスとは

米国NSAの見解

- アクティブサイバーディフェンス(ACD)は、防御サイバー運用に対する国防総省(DoD)の全体的なアプローチの構成要素です。ACDは、国防総省とインテリジェンスコミュニティの防御サイバーセキュリティ機能の強化だけではありません。ACD定義の機能とプロセスを使用して、連邦、州政府、地方自治体の機関や組織、防衛請負業者、重要なインフラセグメント、および業界をサポートすることができます。脅威情報と分析、サイバー活動アラート、および対応アクションを迅速かつ自動的に共有および理解する能力は、高度なサイバー攻撃を正常に検出して防御するための努力の団結を可能にするために不可欠です。

- ACDは保護するネットワーク内でアクティブですが、攻撃的ではなく、その機能はネットワーク事業者や所有者によってインストールされたネットワークにのみ影響します。

https://apps.nsa.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm

2017年米下院に アクティブサイバーディフェンス確実性（certainty）法案が提出された

サイバー攻撃に対して自身のネットワークの境界を超えて行動をとることを許すもの

実施が許されるものとして

1. 対象のシステムに保存されてはいるが本来その持ち主のものではない情報を意図的に破壊すること、あるいはそれに関する情報を提供する
2. 限定された方法で、対象に物理的損害や経済的損失を与える
3. 公的な脅威を与える
4. 継続的な侵害者の大元に対するアトリビューションをするために偵察活動を実施する
5. 踏み台にされているコンピューターに対する侵入やリモートアクセスを行う
6. インターネットに悪い影響を与えていると断定された個人または主体に対して、永続的な切断を行う
7. 国家安全保障に関わるコンピューターなどを改めて防護する

https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf

NICT

アクティブサイバーディフェンスとは

イギリス政府サイバーセキュリティ戦略

- コモディティ（サービスではなく物自体に関する）サイバー攻撃による被害を軽減することを目的とした国家サイバーセキュリティセンター（ National Cyber Security Centre;NCSC）のプログラム。
- 組織が脆弱性を見つけて修正し、インシデントを管理し、サイバー攻撃の遮断を**自動化**するのに役立つ多数の介入またはサービスで構成される。
- 一部のサービスは主に公共部門向けに設計されているが、他のサービスは、その適用可能性と実行可能性に応じて、民間部門または市民がより広く利用できるようになっている。

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

アクティブサイバーディフェンスとは

日本のとある識者の意見

- **自分たちの組織ネットワーク内**で行われるサイバーセキュリティのプロセスの一つ
- 偽装環境を作成して攻撃者を惑わしたり、攻撃者の情報を収集・特定して先んじて対処したりするもの
- ハックバックのような攻撃者に逆襲するような考え方は含まれない

NECサイバーセキュリティ戦略本部セキュリティ技術センターの
郡氏によるブログから　一部の言い回しを修正

NECセキュリティブログ
https://jpn.nec.com/cybersecurity/blog/220204/index.html

アクティブサイバーディフェンスとは

日本のとある識者の意見

- ACDとは、リアルタイムで攻撃を検知、分析し、ネットワークや国の境界を越えた合法的な対策の積極的な使用を組み合わせて、ネットワーク・セキュリティ侵害を軽減することと定義できる。

大澤 淳 氏（中曽根康弘世界平和研究所 主任研究員））から
一部の言い回しを修正

WedgeONLINE
https://wedge.ismedia.jp/articles/-/32480?page=2

アクティブサイバーディフェンスとは

日本のとある識者の意見

- サイバー攻撃の監視（モニタリング）
- 攻撃の帰属（アトリビューション）の特定
- 攻撃への対応措置

を一連の活動として行うこと

『新領域安全保障 サイバー・宇宙・無人兵器をめぐる法的課題』（編・笹川平和財団新領域研究会）住田和明 氏（元陸将・元陸上総隊司令官）から一部の言い回しを修正

WedgeONLINE
https://wedge.ismedia.jp/articles/-/32674

NICT

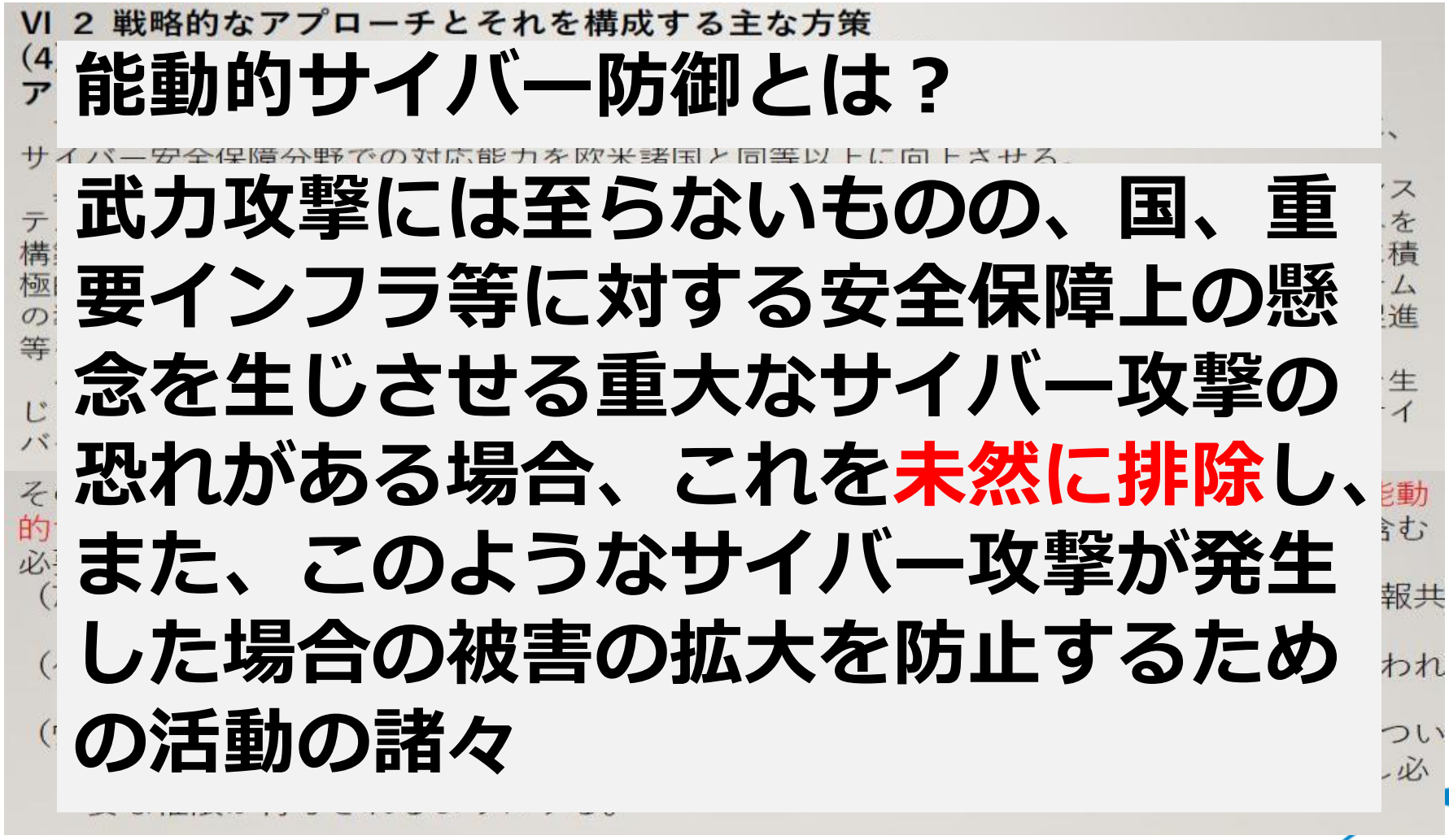
アクティブサイバーディフェンスとは

一般的に、受動的な対策にとどまらず、**反撃を含む**能動的な防御策により攻撃者の目的達成を阻止することを意図した情報収集も含む活動

新たな国家安全保障戦略等の策定に向けた提言

令和4年4月26日　自由民主党

アクティブサイバーディフェンス
国家安全保障戦略の該当部分



政府・防衛省の考え方と取り組み

- ACDについて、政府は「反撃能力」の一環として位置付けられるものではないとの見解
- ACDはあくまでも相手によるサイバー攻撃に対する防衛手段としての**対抗措置**であり、領域横断作戦などにおいて他の攻撃手段を補完する「武力行使」として運用されることは想定していない

- 自衛隊が行う「武力の行使」としてのサイバー攻撃については「法理的には、この必要な武力を行使することの一環として、いわゆる**サイバー攻撃という手段を我が国が用いることは否定されない**」との立場
- 2018年に策定された「防衛計画の大綱」では、「有事において我が国への攻撃に際して当該攻撃に用いられる相手方による**サイバー空間の利用を妨げる能力等**、サイバー防衛能力の抜本的強化を図る」と明記
- 国家防衛戦略には具体的な言及がないものの、防衛力整備計画では「我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の構築に係る取組を強化する」とし、「妨げる能力」について**「抜本的強化を図る」から「構築に係る取組を強化する」**と修正された
- 2027年度を目処に、自衛隊サイバー防衛隊などのサイバー関連部隊を約4000人に拡充し、サイバー要員を約2万人体制に強化すると共に、サイバー・スレット・ハンティング機能を強化し、重要インフラ事業者および防衛産業などの民間との連携強化を行うことが記述された
- 2023年1月には、内閣官房にサイバー安全保障体制整備準備室が立ち上げられ、現在、安全保障上の懸念を生じさせる重大なサイバー攻撃について、ACDの実施が行えるよう、包括的な法整備・体制整備の検討が進められている

ちなみに、

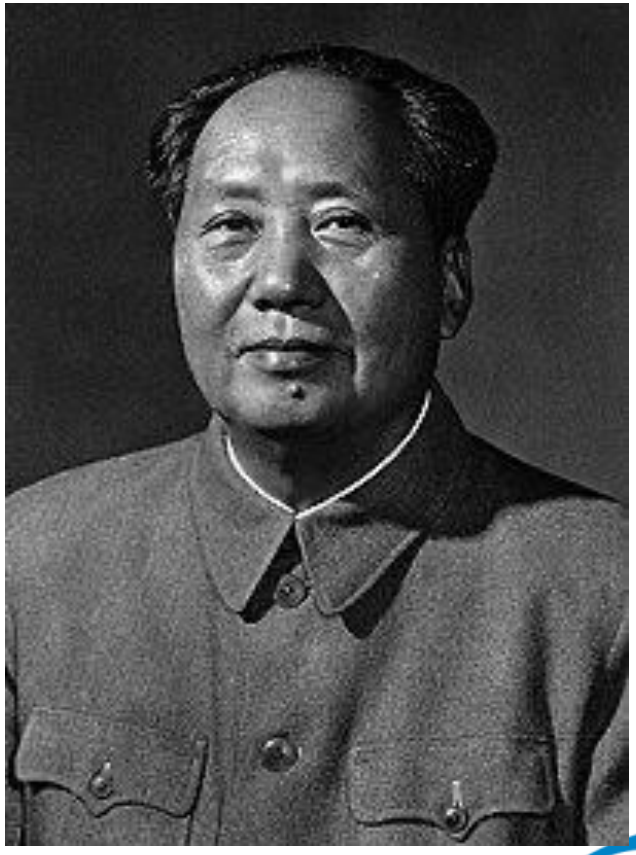
アクティブディフェンスという言葉は

軍事の世界ではかなり古い言葉

中国人民解放軍の「積極防御」

自分が弱い時は絶対戦うな、逃げ回れ

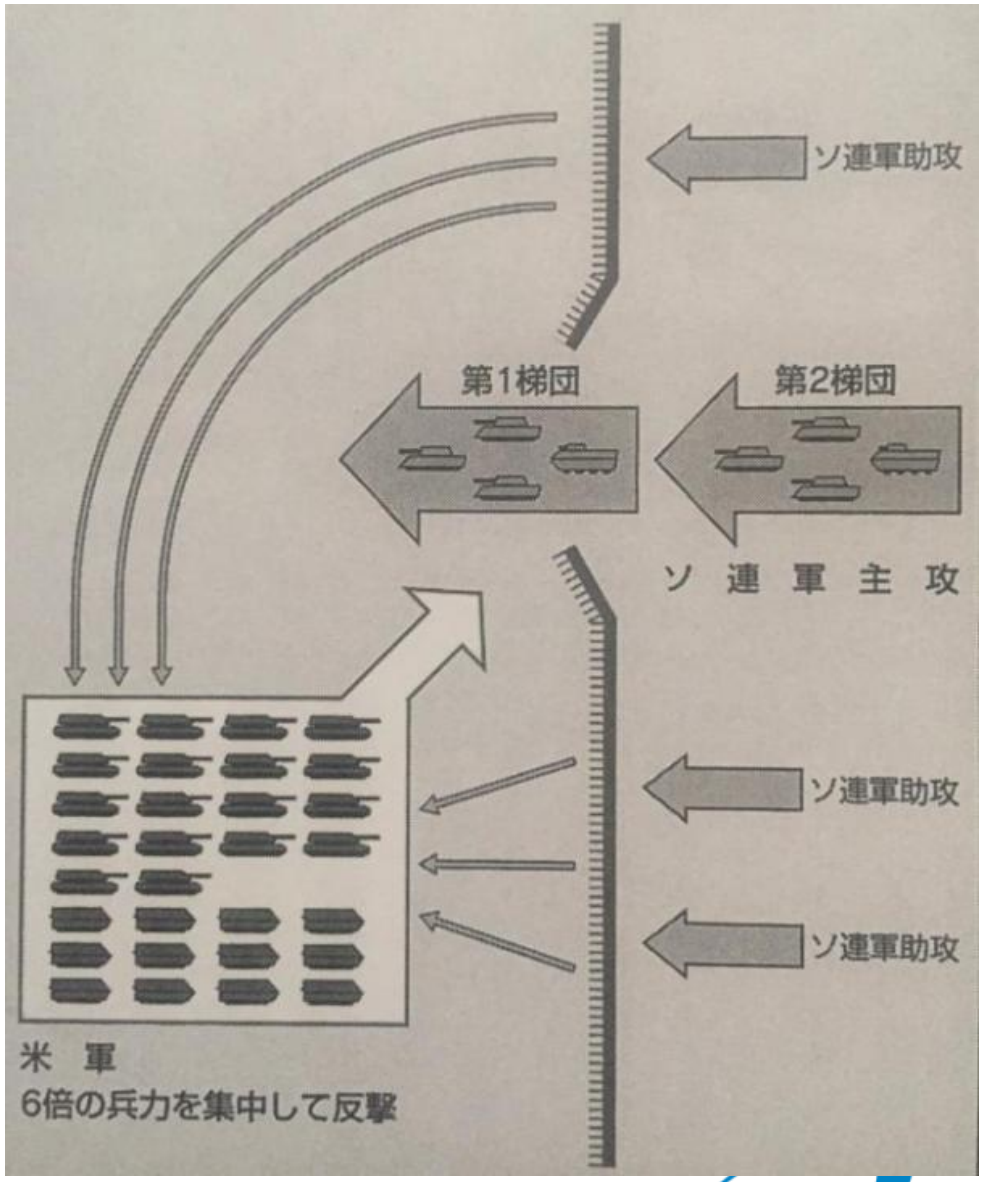
「遊撃戦論」毛沢東より



毛沢東の「積極防御」という思想は、1930年代の中国共産党の軍事戦略において重要な位置を占めていた。
これは特に長征（1934年から1936年）の期間中に発展し、その後も中国の軍事戦略の基礎として機能し続けた。
毛沢東は敵より劣る状況においても、積極的な防御策を通じて戦術的な優位を築くことを提唱した。

アクティブディフェンス

- 米陸軍教範*FM100-5*（*1976*年）
- 兵力の迅速な転用と集中



中国人民解放軍の「積極防御」

- 中国の2015年国防白書では
- 多くの関連する及び下位の教訓、原則を含めて、**戦略的には防衛**であり、**作戦および戦術的には攻撃**である両者が**一体化**したものと定義されている

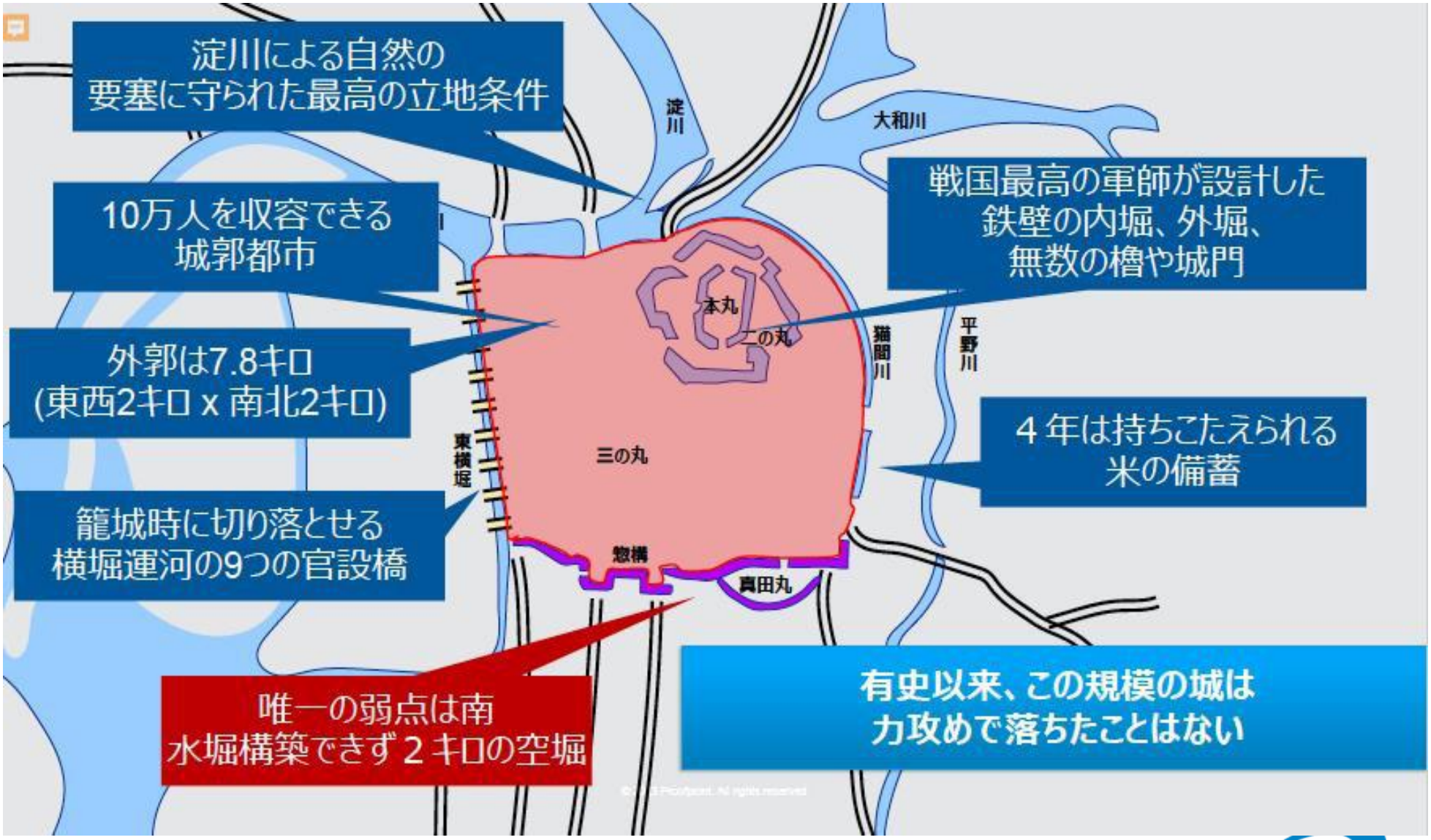
「中国の進化する軍事戦略」マクレイノルズ、原書房、2017年より

積極的防御に関する軍事上の一般的な見解

- 敵の攻撃を単純に防ぐ（普通の防御）のではなく
- 積極的に敵部隊を殲滅することで防御の目的を達成する

- つまり、守っているだけでは戦争に勝てない
- 敵の攻撃意図を挫く必要がある
- そのために敵の野戦軍主力を無力化する

積極的防御 こういう考えもあります



作図はプルーフポイント社の増田氏による

アクティブサイバーディフェンスについて

- **防御は、敵の企図を妨げられれば、必ずしも敵を撃破しなくても良い**
- これまで、物理的な世界の防御はこれでよかった。逆に言えば、防御という言葉の意味合いはここまででであった
- ところが、サイバーの時代では、このような守っているだけの防御は必ず負けてしまう
- そのため、より積極的な**主体**を相手にする広い防御の概念と言葉が必要となり、それを active defense と呼ぶことにした/したのではないか/すると良いかも


TBS