サイバー戦争に踏み込む日本

小倉利丸 **toshi@jca.apc.org**

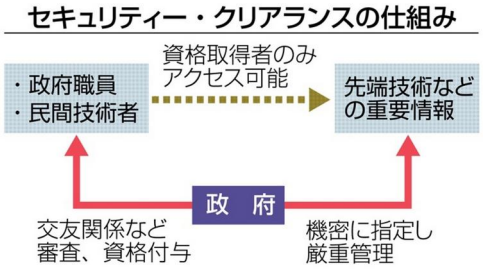
2024/10/1

能動的サイバー防御と健康保険証 廃止に反対する市民の集い

1．経済安保とセキュリティ・経済安保とセキュリティ・クリアランス

重要経済安保情報保護活用法

この法律は、国際情勢の複雑化、社会経済構造の変化等に伴い、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大している中で、重要経済基盤に関する情報であって我が国の安全保障を確保するために特に秘匿することが必要であるものについて、これを適確に保護する体制を確立した上で収集し、整理し、及び活用することが重要であることに鑑み、当該情報の保護及び活用に関し、重要経済安保情報の指定、我が国の安全保障の確保に資する活動を行う事業者への重要経済安保情報の提供、重要経済安保情報の取扱者の制限その他の必要な事項を定めることにより、その漏えいの防止を図り、もって我が国及び国民の安全の確保に資することを目的とするものです。
(内閣府）https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html



重要な経済情報を扱う者が対象であり、重要経済インフラの事業者という概念より幅広い。サイバー安保法制化の議論で関心を持たれているは中小企業における労働者の身元調査だ。どの重要インフラも末端は中小企業が担う場合が、多い。

セキュリティ・クリアランスの基本の枠組は、雇用している企業が身元のチェックを行い、政府がこれを認める、ということになっている。前提には政府が、交友関係などを含めて、資格審査が可能なだけの個人データをあらかじめ保有していなければならない、ということになる。つまり、民間がおざなりの調査をし、政府に資格審査能力がない場合、このシステムは、制度はあっても実体を伴わず機能しない。今後政府データの統合や相互、接続や官民連携が進めば、下記の「参考」で紹介したフランス型になりうるかもしれない。

(参考)フランスの場合。 2016 年、刑事訴訟法「重大事案 grand èvènement」という概念を設けた。テロの脅威となりうるイベントを対象とし、そのイベントまたはその付近で働く者（技術者、ボランティア、介助者、警備員など）は、行政調査を受けなければならない。この調査の後、国家保安調査部（SNEAS）が拘束力のある決定を下す。もし調査の結果、イベント関連の仕事に就かせることが不適とされた場合、当該は、イベントに参加することも働くこともできなくなる。2024 オリンピックに関しては 87 万件の調査が実施され、大会の安全を脅かす可能性のある 3,922 人が排除された。このなかには、S 記録（国家保安事項）を持つ 131 人と極左記録を持つ 167 人が就労を許可されなかった。フランスには、ACCReD と呼ばれる政府による安全保障上の身元調査のシステムがあり、ここには、不起訴、起訴後無罪の者、デモでの逮捕者も含む警察が関与したすべての人的情報も含まれる。このほか政治的意見、健康状態、ソーシャルネットワーク上での活動、宗教的信条なども収集している。(laquadrature.net 日本語仮訳 https://cryptpad.fr/pad/#/2/pad/view/fX-TC3kye2ĐWUzNSSf9Nu34t3+FLPCF9OrpPAHXBFPE/)

2．能動的サイバー防御(安保戦略)

「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」

2.1．能動的サイバー防御(安保戦略）の文言からの引用

サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向 け検討を進める。

(ア) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。
(イ) 国内の通信事業者が役務提供する通信に係る情報を活用(※)し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を 進める。
(ウ) 国、重要インフラ等に対する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、可能な限り未然に攻撃者のサーバ等への 侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、 内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、 サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設 置する。そして、これらのサイバー安全保障分野における新たな取組 の実現のために法制度の整備、運用の強化を図る。これらの取組は総 合的な防衛体制の強化に資するものとなる。

(※)「国内の通信事業者」とある点に注目。「国外の通信事業者」には該当しない？

「役務提供」とは、私たちが通信事業者と契約して行なっている電話やメール、SNS のサービスを指す。したがって、「役務提供する通信に係る情報」とはメールなどの送受信サービスを行なう通信事業者が保有するメールなどのデータを政府が「活用」できるようにすることになる。一般に、メールの内容を通信事業者は読むことが可能である。したがって信頼できる通信事業者を選ぶこと、メールの内容を読まれないよう暗号化のサービスを使うことが必要になる。

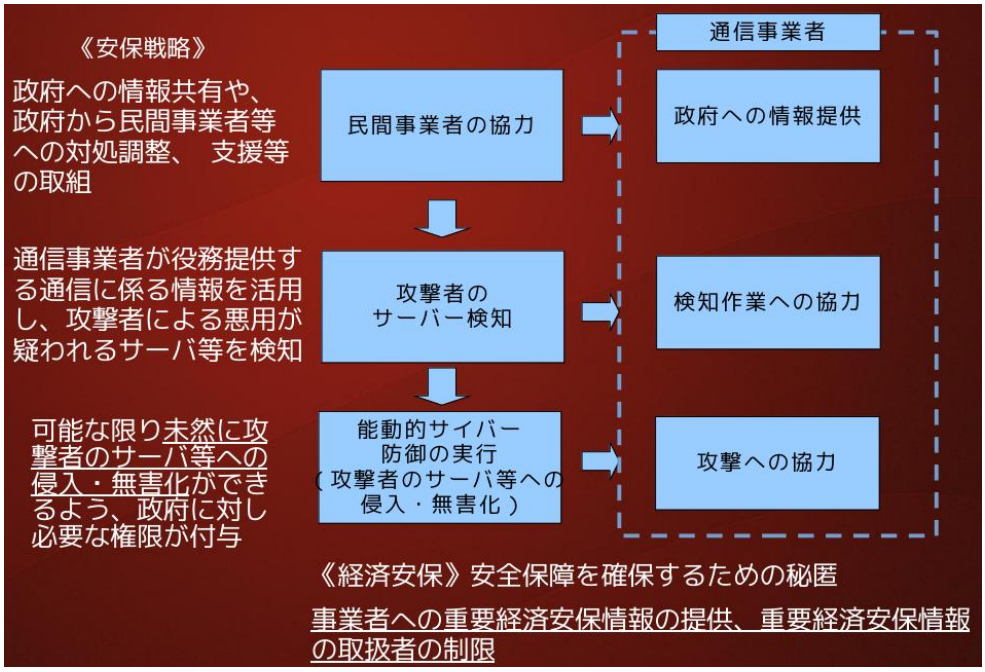
2.2．能動的サイバー防御(攻撃)の条件

- 武力攻撃に至らない重大なサイバー攻撃のおそれ
- 安全保障上の懸念に該当し、かつ「重大」である

問題点

- 現実の攻撃は存在しない。「懸念」「おそれ」の判断は？
- 導入される能動的サイバー防御の定義がない
- 政府にも自衛隊にも私たちのコミュニケーションインフラを防衛するだけの能力はない。だから政府は民間の通信インフラ企業を巻き込もうとしている。この点が実空間での戦力の構成と決定的に異なる。自衛隊であれ政府であれ、彼らだけの力で、サイバー攻撃の現状をリアルタイムで把握し、敵を特定し、攻撃するだけの力はない。なぜか？
    - 通信ネットワークを常時監視しているのは民間通信事業者である(私たちが契約しているプロバイダーは私たちのメールを読むことができるが、政府が読むためには裁判所の令状が必要だ)
    - 標的となるネットワークを特定したり攻撃するには民間通信事業者の協力なし

には不可能。



3．国家安全保障戦略における「サイバー」

《安保戦略》

- 政府への情報共有や、政府から民間事業者等への対処調整、 支援等の取組
- 通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知
- 可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与

《経済安保》安全保障を確保するための秘匿
事業者への重要経済安保情報の提供、重要経済安保情報の取扱者の制限

4．政府のスタンス

- 日本はサイバー攻撃の被害者である
- 通信の秘密よりも公共の福祉が優先する

しかし、この前提を受け入れるべきではない。

- 日本はサイバー攻撃の加害者である
- 通信の秘密に公共の福祉の制約を課すべきではない

5．サイバー安全保障有識者会議

5.1．趣旨と構成

「国家安全保障戦略」（2022 年 12 月 16 日閣議決定）に基づき、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、当該分 野における新たな取組の実現のために必要となる法制度の整備等について検討を行う」
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html

6月7日第一回会合
三つの部会を設置

- 官民の情報共有・民間支援
- 通信情報の利用
- 攻撃者のサーバ等の無害化

7月8日第二回会合
8月6日第三回会合
【連絡先】 内閣官房サイバー安全保障体制整備準備室

5.2. 有識者会議の議論の見方

- 原則(戦争放棄、人権)の観点から判断する
- 被害感情や国際情勢への不安感情を煽る言動にまどわされない
- 既存の自衛隊や警察の制度を既成事実として前提する議論に与しない
- サイバー領域は武器・兵器による殺傷行為と直接関係ないと思いこんではいけない
- 専門的にみえる議論の「わかりにくさ」は、反対の世論を抑える政府の作戦である

議員も有権者も素人。民主主義では素人が立法の主体。専門家に判断を委ねてはいけない

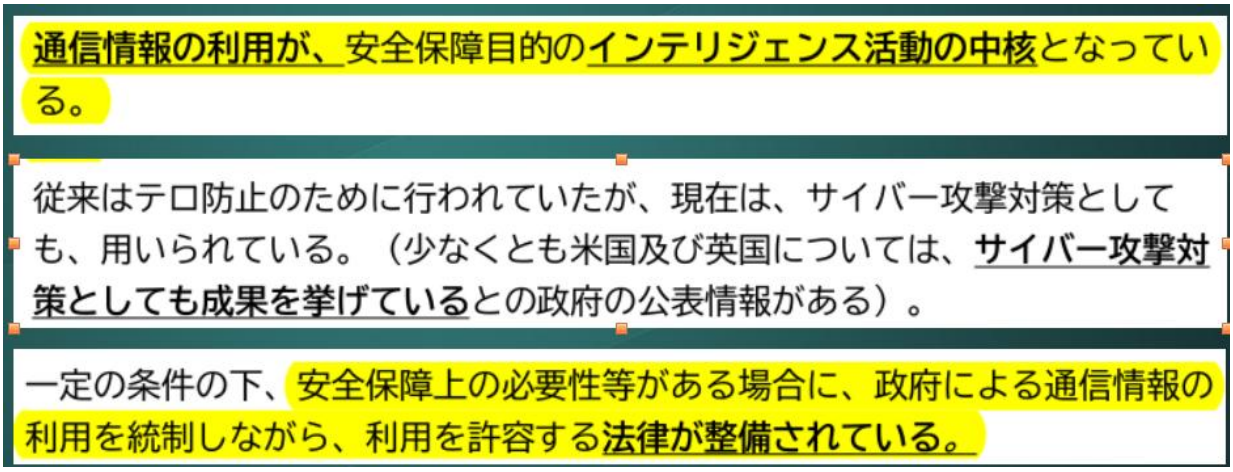
5.3. 第3回資料から(議論のポイント1)

アクセス・無害化を行うに当たっての判断のためにも、今まで以上に、サイバー攻撃に関する**詳細で十分な量の観測・分析の積み重ねが必要**。
平時からの分析が必要であり、令状主義*に基づく個別的かつ司法的なコントロールでは、通信情報の利用と通信の秘密の保護という両方の目的を適切に果たすことができない。

- 先制攻撃を前提とした「詳細で十分な量」の情報収集 ⇒これまで以上の網羅的な情報収集体制を構築できるようにすること
- 平時の情報収集の重視 ⇒ 今現在こそが重要であるということ。「緊急事態になれば何か新たな態勢がとられるだろう」ということではない。
- 令状主義の否定 ⇒ 憲法の規定を真っ向から否定する主張を政府側事務局が示している。

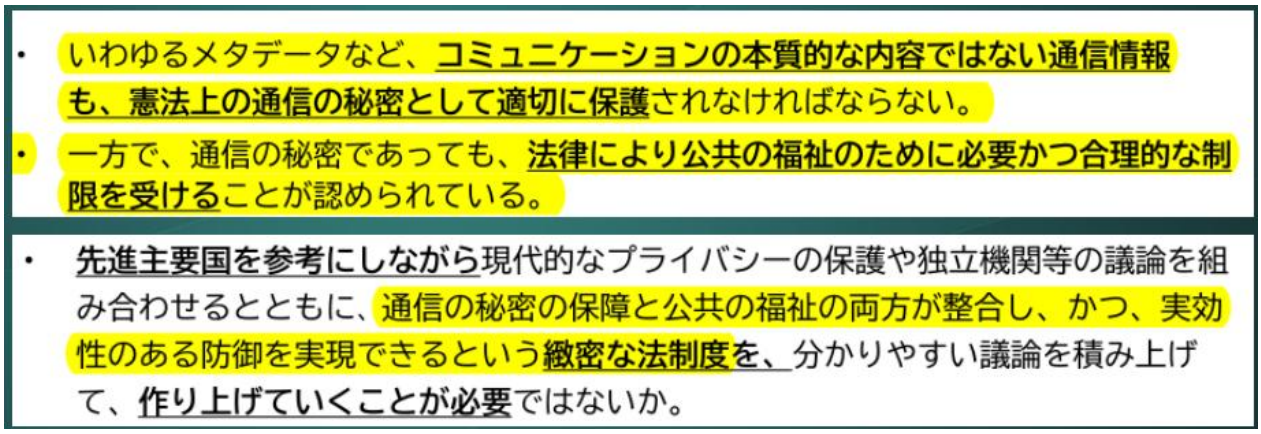
これらはいずれも、国連で現在検討されているサイバー犯罪条約の内容と重なるものだ。

5.4. 第３回資料から(議論のポイント 2)



- これらの基盤をなすインターネットはグローバルなシステムなので日本だけでは完結しないし、日本が制御できるわけでもない。国際的な連携が必須になる。(多国籍 IT 資本、日米同盟、多国間同盟、NATO などと経済連携が融合する構造が不可欠)
- テロ対策の転用
- 「インテリジェンス活動」とはスパイ活動のこと。諜報活動の中心が通信情報にあるということは、通信分野でのスパイ活動を可能にする法と技術の態勢を整えることになる。

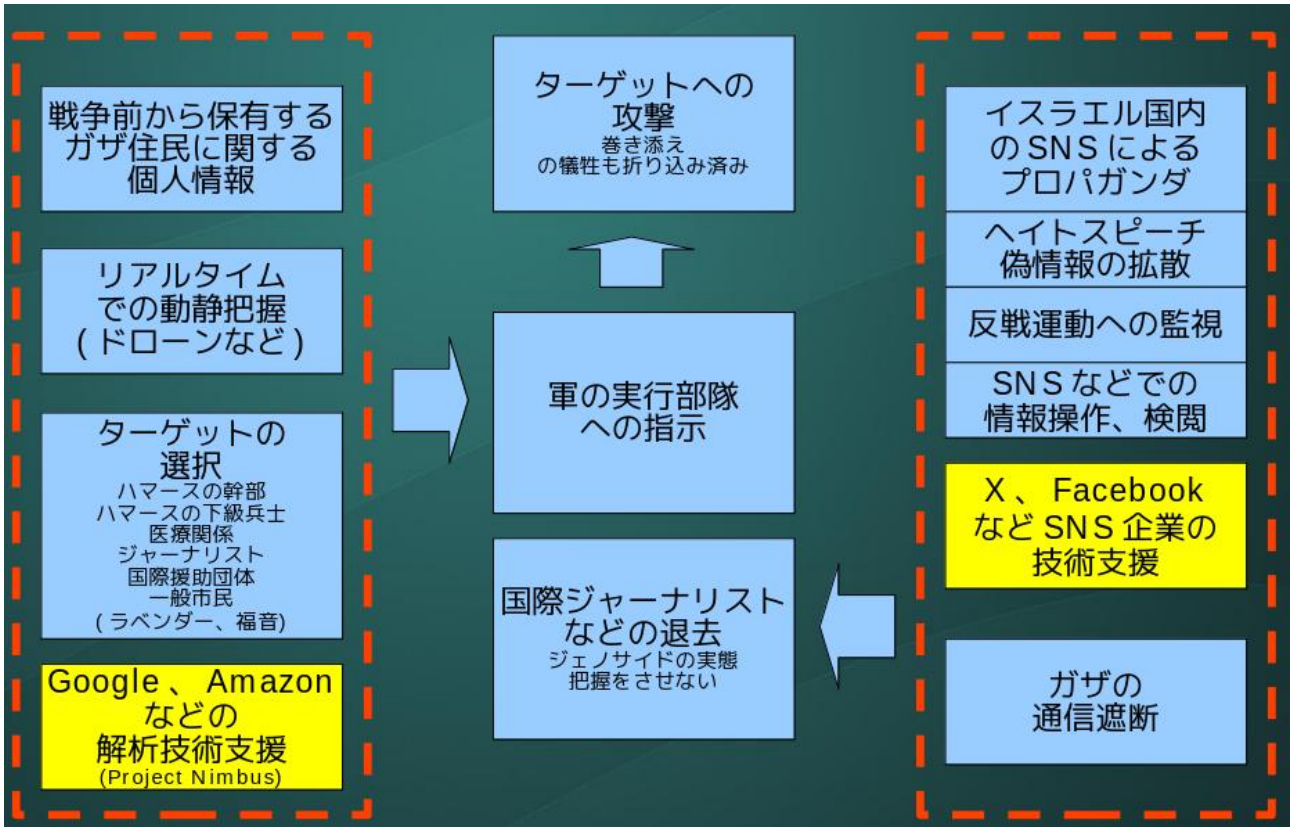
5.5. 第３回資料から(議論のポイント 3)



- 「メタデータ」とは、メールでいえば、発信者と受信者のアドレス、通信の日時や配送経路などメール本文以外のデータ。これらを把握するだけで、人間関係をかなり正確に把握できる。
- 通信の秘密は公共の福祉によって制限されてよい、という解釈は間違い。憲法には公共の福祉による制限を認めていない。
- 通信の秘密と公共の福祉の両立は可能だ、という考え方も間違い。公共の福祉を優先させれば必ず通信の秘密は侵害される。
- 通信の秘密の最大の争点は、暗号の規制、パソコンやスマホを政府が監視できる技術の合法化になる。

6．サイバー戦争の具体例

6.1．ガザ戦争の場合（詳しくは『パレスチナ人のデジタルの権利、ジェノサイド、そしてビッグテックの説明責任』参照



(No Tech for Apartheit)イスラエルとの12億ドルのクラウド・コンピューティング契約「Project Nimbus」をめぐる抗議活動で、Googleが逮捕を命じた9人の労働者「Nimbus Nine」による声明

「Googleはイスラエル国防省のためにカスタムツールを構築し、ガザのパレスチナ人に対するジェノサイドが始まって以来、イスラエルの軍事的占領軍、イスラエル軍との契約を倍増してきた。Googleは嘘をつき続けることで、消費者やメディア、そして最も重要なこととして、私たちGoogleの労働者を軽視し、無視している。」 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/no-tech-for-apartheit_nimbus_nine_statement_jp/

Google、パレスチナのために声をあげる労働者への報復をやめよ-解雇された50人を復職させよ
2024年4月のGoogleによるジェノサイド加担に反対する全米行動でGoogleのオフィスに座り込んだ労働者など50名が解雇された問題に対して、Googleに対して解雇撤回を申し入れる行動が起きる
Googleは、4月16日にカリフォルニア州サニーベールにあるGoogle CloudのCEO

トーマス・クリアンのオフィス内と Google ニューヨークの 10 階共有スペースで行われた歴史的な全米の座り込みに対抗し、攻撃的な報復として、現場にいた参加者ではない人たちを含む 50 人の労働者を解雇した。この歴史的な労働者行動（ハイテク業界では初）を通じて、No Tech For Apartheid キャンペーンに参加するハイテク労働者たちは、Google が Project Nimbus として知られるイスラエルとの 120 億ドルの契約を打ち切るよう要求した。

6.2. NATO と日本の関係

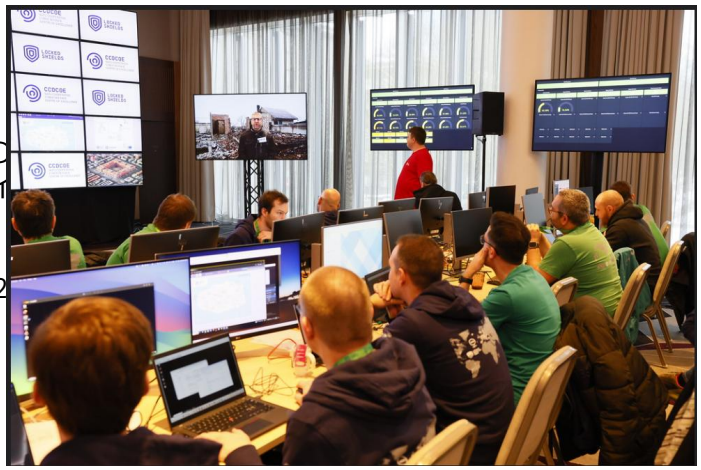
日本は NATO サイバー防衛協力センター(CCĐCOE)に正式加盟している。
防衛省は NATO 承認の研究機関だと説明しているが、センターのウエッブには以下の記述がある。

> 「CCĐCOE は、2008 年 5 月 14 日に他の 6 か国--ドイツ、イタリア、ラトビア、リトアニア、スロバキア共和国、スペイン--とともにエストニアの主導で設立された。北大西洋評議会は、同じ年の 10 月にセンターに完全な認定と国際軍事組織の地位を授与することを決定した。」

つまり、センターはれっきとした軍事組織の地位を NATO の最高意思決定機関である大西洋評議会自身が授与している。この事実を防衛省は「研究機関」と位置づけるという意図的と思われるミスリードによって、隠蔽した。ちょうど 22 年 11 月は安保防衛 3 文書の議論の渦中だったはずだ。この時期に加盟したのは、安保防衛 3 文書の成立を見越して、自体を先取りしたといえる。

防衛省が言及していないことで重要なことは、日本と同時にウクライナも正式加盟した点だ。ウクライナは、センターへの加盟を NATO 正式加盟への第一歩と位置づけている。
https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/

6.3. NATO サイバー防衛演習：ロックド・シールズ



6.3.1. 自衛隊の資料から(2024 年)

１　ＮＡＴＯサイバー防衛協力センター（ＣＣＤ
「ロックド・シールズ２０２４」に参加し、サイ
セキュリティ動向の把握を図る。　※ＣＣＤＣＯ
of Excellence
２　参加時期　2023 年 4 月 23 日（火）から同月 2
３　実施場所　市ヶ谷等

演習統裁部はタリン（エストニア）に置かれるが、演習参加者は自国からオンライン形式で参加
４．演習参加予定国（日本以外） ＮＡＴＯ加盟国を含む約４０か国
５．参加部隊等(下線部は今年新規の参加)
（１）内部部局、統合幕僚監部、陸上自衛隊陸上総隊司令部、陸上自衛隊システム通信団、海上自衛隊システム通信隊群、航空自衛隊作戦システム運用隊、航空自衛隊航空システム通信隊、自衛隊サイバー防衛隊、防衛研究所
（２）内閣官房サイバー安全保障体制整備準備室、内閣官房サイバーセキュリティセンター（ＮＩＳＣ）、警察庁、外務省、経済産業省、情報処理推進機構（ＩＰＡ）、情報通信研究機構（ＮＩＣＴ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）、重要インフラ事業者等(※)
（３）英国 英国防省(昨年は、オーストラリアと合同チームを編成して参加)

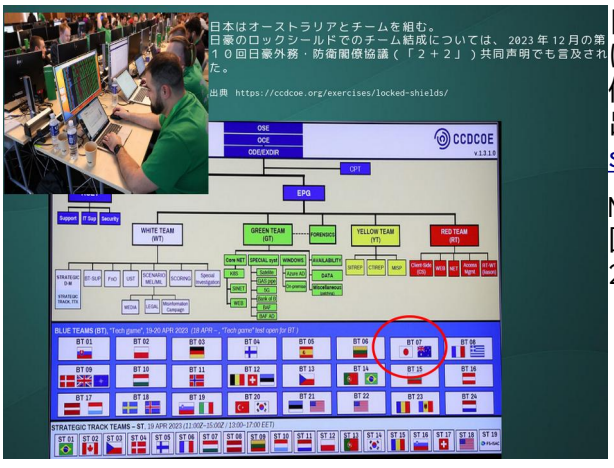
(※)ネット上で把握できた企業としては、日鉄ソリューションズ、中部電力、Fortinet、ESET など(23 年には NTT 各社が参加) CCDCOE のウエッブサイトには以下の民間企業の協力があったと記されている。Havelsan,Singapore University of Technology and design, Accenture, FS-ISAC, Fortinet, Clarified Security, AWS, Red Hat, Aselsan, NATO StratCom COE,Siemens, Fujitsu, TalTech, Artic Security, Bittium, CR14, BHC, SpaceIT, Stamus Networks, Forestall, Microsoft, Palo Alto Networks, EstoniaDefence Forces, Telia, Atech, Startex Security.

6.3.2. ロックドシールズ演習にみるサイバー戦争の特徴

- 自衛隊だけで完結しない
- 他省庁の参加
- 民間事業者(通信事業者、インフラ事業者(電力など）)
- 他国の部隊との共同行動

軍隊だけで完結しないのは、情報インフラの基盤を民間が掌握し、その末端には PC やスマホを武器にする人達がいる。
他省庁や民間が巻き込まれるために、国際法上保護されるはずの民間人規定がほとんど機能しない。全ての人間が敵として標的とされる。

6.3.3. 2023 年の場合を例に(日本はオーストラリアとチームを組む)



日豪のロックシールドでのチーム結成については、2023 年 12 月の第１０回日豪外務・防衛閣僚協議（「２＋２」）共同声明でも言及された。
出典 https://ccdcoe.org/exercises/locked-shields/

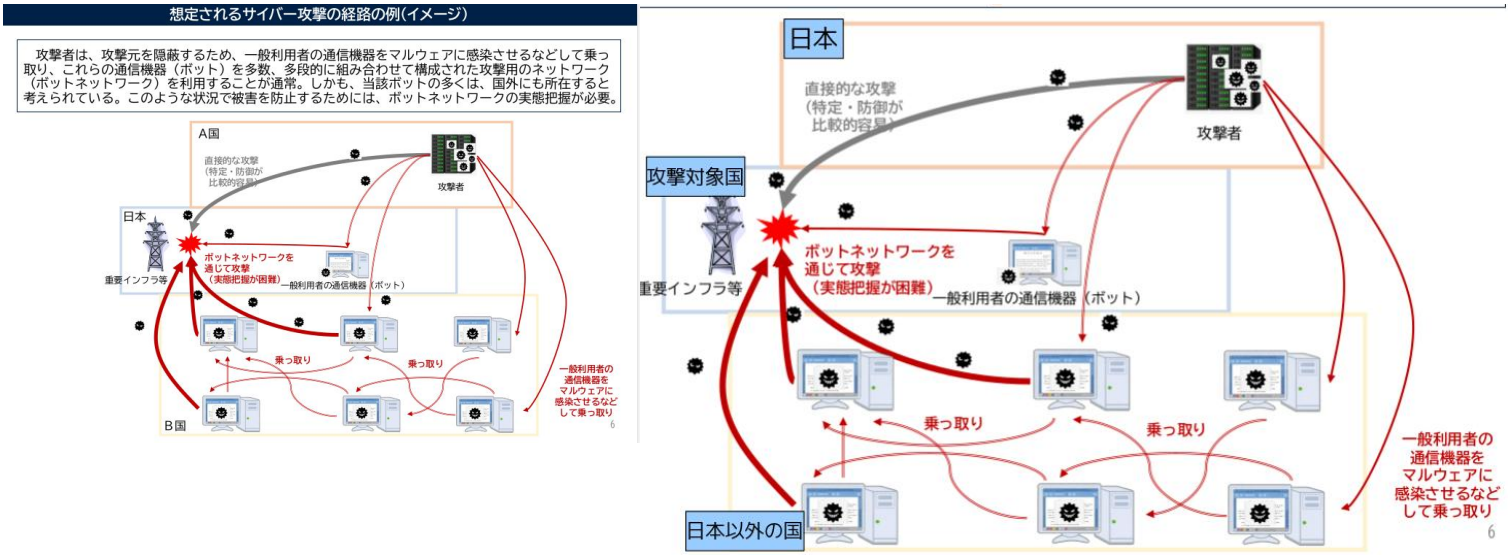
NTT 広報
国際サイバー防衛演習「Locked Shields 2023」に NTT グループが参加

「NTT グループは、4 月 18 日から 21 日まで開催される、NATO サイバー防衛協力センター（CCDCOE: Cooperative Cyber Defence Centre of Excellence）主催の国際サイバー防衛演習「Locked Shields 2023」に参加します。
NTT ドコモ、NTT コミュニケーションズ、NTT データ、ならびに NTT セキュリティ・ジャパンにとって、今回は昨年に引き続き、2 度目の参加になります。本演習は

約 40 か国が参加し、架空の国に対するサイバー攻撃を想定して行われるものです。
日本チームは、同志国や団体との連携を深め、サイバーインシデント対応能力を共同で強化するため、今回は、オーストラリアとチームを組み、日本の政府機関や民間企業、オーストラリア国防省とともに参加します。」

上は中部電力と東北電力のインフラ会社

7．サイバー戦争のイメージ(左：有識者会議資料、右はＡ国を日本とした場合)



サイバー攻撃では、攻撃そのものを秘匿したり偽装する。そもそも日本が攻撃していることを公然とは認めないだろう。攻撃の拠点が日本国内にはない可能性も高い。直接的な殺傷能力がある無人機攻撃や爆撃標的の「生産」に注目しがちだが、むしろ、日本が加害国としてやりそうなことは、身元を偽装して相手国のインフラへに対して攻撃を仕掛ける手法になる場合があることを念頭に置く必要がある。

上図のサイバー攻撃の概念図の左図は有識者会議の資料(通信情報の利用に関するテーマ別会合 第１回資料としてサイバー安全保障体制整備準備室が提出した資料のもの)で、日本がＡ国から攻撃されると想定したもの。能動的サイバー防御では日本が攻撃者になるので、この図のＡ国を日本とした場合を右図に示した。ここにあるように、攻撃者は、自らが攻撃者であることを秘匿して第三国を経由して攻撃する。こうした事態を前提にして、

サイバー戦争の当事国であることそのものを明かにするための特別な対応が必要になる。

こうしたサイバー攻撃は、必ず情報戦とリアルにおける軍事作戦が連動する。情報戦の主戦場はマスメディアではなく SNS での一般市民による敵への憎悪の拡散が必須の要件になる。

8. まとめ

敵基地攻撃能力の問題も含めて、現代の戦争は、サイバー領域との有機的な結びつきなしにはありえないことを反戦・平和運動が自覚することが重要になっている。

この場合、従来の反戦平和運動の領域を越えて以下の点が極めて重要になる。

- 平時こそが有事である。情報戦(情報収集と監視、世論操作)への対処は今すぐ必要になる。
- 私たちのインターネットへの接続そのものが「戦場」の一部を構成している。官民の膨大な個人データの収集と解析の入口になるのが私たちのネットでの通信行為そのものである。また、ネットでの言論が戦争や憎悪を扇動する空間になる。
- 福祉や社会保障など私たちの権利に関わる個人情報もまた戦争に動員される。特に、個人情報の網羅的な収集と政府や企業による自由な利活用が将来的に戦争を遂行する上での重要な資源になりうる。
- 特に、私たちが日常的に依存せざるをえないコンミュニケーション・サービスの企業がジェノサイドやアパルトヘイトに加担していることを軽視してはならず、可能な対応を工夫する。すでに、Google、Facebook、X、Amazon は明確な戦争加担企業であり、私たちの個人データを大量に保有する日本の通信事業者が NATO の軍事演習に正式に参加していることを軽視してはならない。
- このことを自覚して、戦争に加担しないコミュニケーションのありかたを運動圏の文化として確立すること。
- **これまでの各国のサイバー攻撃の状況をえると、日本が能動的サイバー防御を発動したことそれ自体を公表しない可能性が高い。また、どこか他の国を経由した攻撃や金銭目的を偽装する手法もサイバー領域では常套手段である。実空間での先制攻撃とは全く異なる状況になることに十分な関心をもつ必要がある。**
- **立法事実として現実にあるサイバー攻撃の被害と世論の不安感情から政府は国家のサイバー安全保障の必要性を強調する。しかし、国家の安全保障と私たちのサイバーセキュリティとは相容れない観点であることをしっかり確認することが大切。**

参考資料(小倉のブログから)

能動的サイバー防御関連の記事

https://www.alt-movements.org/no_more_capitalism/

サーバー戦争や監視社会問題の記事(反監視情報)

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/

上の URL を入力するのが面倒なばあい、「小倉利丸 ブログ」「小倉利丸 反監視情報」などで検索してみてください。

能動的サイバー防御批判(有識者会議資料に関して)その 1

https://www.alt-movements.org/no_more_capitalism/blog/2024/06/16/yushikishakaigi_hihan-1/

能動的サイバー防御批判(有識者会議資料に関して)その 2(終)

https://www.alt-movements.org/no_more_capitalism/blog/2024/06/20/yushikishakaigi_hihan-2/