盗聴法に反対する市民連絡会主催
「デジタル監視社会はどこまで悪化したか？」（かながわ県民センター）

カナダの監視法制と戦争

２０２３年7月３０日
小笠原みどり

１．スノーデン告発から１０年

対テロ戦争下でアメリカが極秘裏に発達させた新しい大量監視の手法が判明する。

- デジタル通信基盤、特に通信ケーブルの変換地点に監視装置を埋めこむ。
- 通信事業者やインターネット会社が顧客の通信情報を政府に渡していた。
- 日本はアメリカの世界監視システムの主要拠点のひとつだった。

２．世界で拡大する監視法制

日本：共通番号（マイナンバー）法（２０１３年）
特定秘密保護法（２０１３年）
新安保法（２０１５年）
改定盗聴法（２０１６年）
共謀罪法（２０１７年）

カナダ：欧州評議会サイバー犯罪条約に署名（２００１年）
オンライン犯罪からカナダ人を守る法律（２０１３年）
テロリストからカナダを守る法律（２０１４年）
反テロリズム法律（２０１５年）
国家安全保障法（２０１９年）

３．パンデミック監視資本主義の台頭

新しいデジタル監視技術が緊急事態下で登場（接触追跡アプリ、ワクチン・パスポート、入国管理アプリなど）。ほとんどが失敗、市民の反発招く。

４．カナダで起きていること

諜報機関が中国大使館や中国系科学者らを新たな監視対象に。全国紙がカナダ安全保障諜報サービスの「内部告発者」を情報源に「中国がカナダの選挙に介入している」というキャンペーン。大学研究者と中国系技術企業のつながりも問題視され、研究費の申請に「国家安全保障ガイドライン」が導入される。ファーウェイなど大手企業との共同研究事業が中止になり、学問の自由が脅かされる。１９２３年の「中国人排斥法」から１００年目に、中国が急速に仮想敵国化している。

詳しくは拙稿「違法な大量監視を合法化すること」（英文）をご覧下さい。

Ogasawara, M. 2022. “Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada’s Legislative Response to the Expansion of Security Intelligence” *Canadian Journal of Law & Society* 37 (2): 317-338. Open access.

監視社会化とマイナンバー制度

2023.7.30　宮崎俊郎（共通番号いらないネット）

１．*2013.5.24*番号法成立から*2023.6.2*番号法改悪成立

2013.5.24　番号法成立
2016.1.1　運用開始・マイナカード交付開始
2020.9.1～2021.12.31　第１次マイナポイント（5,000円分）
（2020.6.1 2,135万枚交付16.8%）　（2021.12.1　5,057万枚39.9%）
2021.5.24　デジタル改革関連法案の成立
9. 1 デジタル庁発足
2022.1.1～2023.2.28　第２次マイナポイント　20,000円分
（2023.2.12　7,741万枚61.5%）
10.13 河野大臣「健康保険証2024年秋廃止」記者会見
2023.4. 1 オンライン資格確認開始
6. 2 番号法改悪案可決・成立
7. 9 申請9,743万枚（77.4%）交付9,337万枚（74.4%）
保有8,815万枚（70.0%）保険証登録6,493万枚（69.5%）

２．マイナンバー強制政策への転換の意味

①マイナカードの強制策の意味　民間利用の加速化

マイナカードは番号法に規定されて開始され、まさにマイナンバーを認証する媒体としてスタートした。ところがメインは電子証明書の本人確認機能であり、その発行番号（シリアル番号）に対して紐づけることが番号法の規制なしに実施可能となっている。保険証との紐づけもこの仕組みを利用している。）

特に民間との情報紐づけについては本人同意を原則とした「ＡＰＩ連携」という手法で拡大しようとしている。現在では多くの民間が本人確認機能を中心として利用している。つまり民間は安価で堅牢な公的個人認証を搭載した電子証明を利用したかったのだ。堅牢な本人認証の可能なマイナカードを強制的に持たせることで電子取引の確実性を担保するという民間の要請が下支えしていること見逃せない。

しかし、世界的にはナショナルカードをオールマイティに本人認証に使えるようにしている国家は極めて稀である。

②監視国家の基盤ツールの確立

今回の保険証廃止によるマイナ保険証への一本化は、実質的なマイナンバー強制の第一歩だ。遮二無二マイナカードを全員に持たせようとしているのは、外国人の在留カードの常時携帯義務をマイナカードに浸透させて「国内版パスポート」に仕上げる野望があるからだ。国家への忠誠を誓わせる「踏み絵」としても機能させたいのだろう。今回国家資格とマイナンバーを紐づける改定が行われたが、まさにこれは国家にとって非常時に必要な人材を効率的に利用していきたいという意思の表れであり、その頂点に徴兵制がある。

そして今狙われているのが医療と教育情報だ。これらの個人情報を生涯管理して綿密な国家管理の下に置くことこそが超監視社会の基盤整備なのだ。

３．マイナカードと他の証明書との一体化

（１）保険証との一体化

①2022年10月13日河野大臣の記者会見で保険証廃止を表明
前回の法改悪では健康保険法で「資格確認書」を発行できる規定を新設
しかし保険証廃止のメリットがほとんどなくデメリットを解消することに躍起な政府はマイナカード取得に暗証番号不適応者に免除したり、資格確認書の申請主義をなくしたりと迷走を続けているため、保険証廃止は目前か？

②病院や医療機関はマイナ保険証によるオンライン資格確認が必須化された。
規模の小さな診療機関にはかなり環境整備が重荷となり、廃院も検討されている。またシステム不具合によって資格確認できないケースが多発。いったん10割負担も出てきて、慌てて3割徴収に戻した。

③単なる保険者の資格確認にとどまらず、診療情報の共有化を通じて医療ＤＸ（医療データの一元管理）に道を開くもの。しかも莫大な利益がＩＴ業者に転がり込む。この構造は教育分野においても同様。

（２）運転免許証との一体化

①各県警の所有データを全国一元的に管理できるシステムの構築

②2020.10.16平井デジタル担当相・小此木国家公安委員長・河野規制改革担当大臣の歴史的3者合意。これまで抵抗してきた警察が一夜のうちに合意に至った背景は？今のところ従来の運転免許証の廃止は打ち出していない。

③単なる運転免許証システムにとどまるとは到底理解しがたい
⇒警察のマイナンバー制度利用に道を開く

（３）在留カードの一体化

①在留カードとマイナンバーカードの一体化について、所要の法律案を2022年（令和４年）の通常国会に提出し、2022年度（令和４年度）～2025年度（令和７年度）に政省令等の整備・システム改修、2025年度（令和７年度）から一体化したカードの交付を開始する予定である。

②在留カードは適法に中長期間在留することを証明する「証明書」と在留にかかる各種許可となる「許可証」としての二つの性格を併せ持つ。

③１６歳以上のものには「常時携帯義務」を課している。

④表面表記：在留カード番号・国籍・地域・氏名・生年月日・性別・住居地・写真
在留資格・就労制限の有無・在留期間・在留期間満了日・許可の種類・許可年月日・交付年月日・在留カードの有効期間満了日

⑤狙いは外国人管理の精緻化

⑥在留カードの常時携帯義務をマイナカードへ

（４）保険証・運転免許証の本人確認書類としての機能の剥奪
今年の５～６月に携帯３社は保険証を本人確認書類から除外した。
６月６日デジタル社会推進会議では本人確認書類をマイナカードに一本化して運転免許証や顔写真のない書類は廃止するという方針が示された。

４．いまこそ「書かない番号！持たないカード！」を！
番号強制社会への抵抗運動を！

（１）いまこそ「書かない番号！持たないカード！」

マイナカードの所持率は4分の3

政府の目標は3月末で対象者全員に持たせるということであり、いまだ10人に3人は持っていない状態。⇒追い込まれているのは私たちではなく政府だ！

これ以上所持率を増やさないことで、紙の保険証廃止を撤回へ追い込める。

マイナカードの取得は番号法上あくまで任意であり、強制は脱法行為だ！

（２）マイナカードの自主返納を呼びかける

　ＳＮＳを中心にマイナカードを役所に自主返納する運動が各地で起こっている。私たちも早い段階からマイナカードを取ってしまった方にも返すことができることを伝えてきた。

　しかし、返すだけではいったん紐づいたデータは消えない。保険証データは今のところ紐づけを解消することはできない。公金受取口座との紐づけはマイナポータルで解消可能。ほかの紐づけについては検証できていない。

　こうした状況の中での返納呼びかけはこうした状況も併せて説明が必要だ。

（３）デジタル強制を作らせない

　世界的に共通番号やカードによって民衆を一元管理している国家はごく少数にすぎない。日本はデジタル後進国だからマイナンバー制度を推進というロジックは世界的に通用しないことをさらに宣伝すべきだ。

　ただし、社会をデジタル化していこうとする力学は全世界的に進められている。通貨についてもデジタル通貨を主流としていく流れができつつある。それらはすべて記録されていく社会のことだ。

　これらのデジタル強制に対して私たちはあくまでデジタルとアナログの選択を自らの生き方として選択可能な社会を作り出していきたい。

　自分たちの情報は自分たちでコントロールできる情報主権を確立したい。

（４）当面の目標は来年秋までに保険証廃止の撤回

　街頭宣伝・デモ・集会などを通じて保険証廃止撤回を幅広く訴えかけていきたい。すでに政府の強引で支離滅裂な対応に市民の怒りは高まっており、あと一歩ではないだろうか。

広がる顔識別カメラシステム
これとどうたたかうか

２０２３年7月３０日
角田富夫（共謀罪 No！実行委員会）

１、個人情報保護委員会、顔識別カメラシステムを容認

ⅰ、2021 年、JR 東日本の顔識別カメラシステム稼働

容認した個人情報保護委員会へも批判、世論の批判の前に有識者会議を設置

ⅱ、「犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会」

この会議には、この問題に詳しい山本龍彦氏（慶応大学）や森弁護士らも参加。

2022 年、有識者会議 7 回開かれ、報告書案を作成、本年 1 月～2 月、パブコメ実施　3 月 29 日、パブコメに踏まえ個人情報保護委員会「犯罪予防や安全確保のための顔識別能力付きカメラシステムの利用について」公表

※第 8 回有識者検討会（２０２３・３）議事概要は、検討会の雰囲気を知る上で重要、個人情報保護員委員会は有識者にどんどん意見をいわせ、同システムに批判的な有識者の取り込みをはかった面があるが、うまくいったかどうかわかりません。

ⅲ、個人情報保護委員会の結論

予想されたことですが、顔識別カメラシステムについての是非は議論されず、同システムの運用にあたっては個人情報保護法に踏まえ対応することを事業者にもとめています。つまり、個人情報保護のために、同法の修正などはなかったということです。

この点、顔識別機能付きカメラシステムにより、「長期にわたり特定の個人を追跡することが可能」、「被撮影者が非撮影社自己の個人情報が取り扱われている事実を認識できず、またその取扱いを受容するか否かを選択することができない状況で、撮影範囲に入った全ての者の顔画像を自動的、無差別かつ大量に取得することができる」（１２ページ）など、同システムの危険性を指摘しながら、同法になんらの修正などを加えなかったことは同委員会が、個人情報の保護ではなく、利用に重点を置いていることが改めて明らかになりました。

私達は、顔識別カメラシステム問題について、国会でその是非、是とする場合、運用基準の明確化などについて議論を求めていきたいと考えています。そのうえで、今後運動を進めていく上で重要な足がかりがありました。

２、顔識別カメラシステムの利用にあたっての通知・公表義務

ⅰ、個人情報保護委員会「犯罪予防や安全確保のための顔識別機能付きカメラシステム

の利用について」では、同システムの利用にあたっては利用目的の特定（１７条１項）、通知・公表（法２１条）がもとめられることになりました。

この点は、極めて重要と思われます。

いわゆる防犯カメラについては、設置状況からみてその利用目的が明確な場合は、通知・公表の義務から例外（第２１条４項４号）とされてきましたが、それがなくなりました。

この事自体はすごく重要なことと考えています。

別紙「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」参照

ⅱ、チェツク運動の重要性

別紙や「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」をみればわかりますが、いままでの事業者からみればこれを実施することは大変です。

本当に、同システムの利用にあたって「透明性の確保や適正な運用」がおこなわれているかチェックしていくことが重要と思われます。

例えば、ここ横浜駅を見た場合、同システムの利用についての掲示がおこなわれているか、行なわれているとしたらどこかなどを確認し、JR 東日本、個人情報保護委員会に質問をしていくことなど。

※個人情報保護委員会は、複数のでは入り口がある場合、一ヶ所に掲示されていればよいとしています。

ⅲ、国会での議論を喚起していくことの重要性

３、たたかいはこれから

ⅰ、広がる顔識別監視システム

イ、「工業会　日本万引防止システム協会」

ウォークスルー型の顔識別カメラシステムを店舗増加

２０１９年　３１９店→　２０２１年　６８６店

ロ、JR 西日本、本年顔認証改札の実証実験

ハ、JR 東日本　「鉄道をもつ IT 企業」への転換を明言

膨大な顧客情報の活用へ踏み込みを宣言。顔識別カメラシステムの強化は不可避

ニ、商業施設、公的部門などの同システムの利用について

有識者検討会の対象は駅、空港などの準公共空間のみを対象で、

ⅱ、顔識別監視カメラシステム反対共同声明への賛同を

８月末が最終集約

以上です

4000 人のサイバー部隊と 2 万人のサイバー要員確保を目指す自衛隊

人員の確保は本当に可能か、不正アクセス禁止法の適用除外は、「外注化」は??

2023 年 7 月 30 日　横浜　木元茂夫

1.　22 年 3 月 17 日に発足した 3 つの部隊　陸海空に加えて領域横断作戦

1.1　自衛隊サイバー防衛隊(埼玉・朝霞)　隊司令は陸将補(少将)　約 540 人　23 年 3 月末 890 人

1.2　電子作戦隊発足　隊司令は 1 等陸佐(大佐)　約 180 人
　　隊本部(朝霞)
　　第 301 電子戦中隊(熊本・健軍駐屯地)　約 100 人　健軍、奄美、那覇
　　第 101 電子戦隊(朝霞)　約 60 人　留萌、相浦、知念

1.3　宇宙作戦群(東京・府中)　群司令は 1 等陸佐(大佐)　約 70 人
　　群本部
　　宇宙作戦指揮所運用隊
　　宇宙監視レーダー(山口県山陽小野田市海上自衛隊山陽受信所跡地)

2.　自衛隊サイバー部隊の法的根拠

2.1　　防衛省設置法

第 6 条　自衛官の定数

陸上自衛隊	150,500	
海上自衛隊	45,293	
航空自衛隊	46,994	
共同の部隊	1,588	←サイバー防衛隊は、ここに分類される。
統合幕僚監部	386	
情報本部	1,936	
内部部局	50	
防衛装備庁	407	

2.2　自衛隊法施行令

第四節　共同の部隊

(自衛隊情報保全隊)

第三十条の十六　陸上自衛隊、海上自衛隊及び航空自衛隊の共同の部隊として、自衛隊情報保全隊を置く。

2　自衛隊情報保全隊は、自衛隊情報保全隊本部及び中央情報保全隊その他防衛大臣の定める部隊をもって編成する。

(自衛隊情報保全隊司令)

第三十条の十七　自衛隊情報保全隊の長は、自衛隊情報保全隊司令とする。

２　自衛隊情報保全隊司令は、陸将補、海将補又は空将補をもって充てる。

（自衛隊サイバー防衛隊）

第三十条の十八　陸上自衛隊、海上自衛隊及び航空自衛隊の共同の部隊として、自衛隊サイバー防衛隊を置く。

２　自衛隊サイバー防衛隊は、自衛隊サイバー防衛隊本部及びネットワーク運用隊その他防衛大臣の定める部隊をもって編成する。

（自衛隊サイバー防衛隊司令）

第三十条の十九　自衛隊サイバー防衛隊の長は、自衛隊サイバー防衛隊司令とする。

２　自衛隊サイバー防衛隊司令は、陸将補、海将補又は空将補をもって充てる。

3.　ウクライナ戦争では??

「ロシアのサイバー部隊は、それ以前から続いていた政府機関や企業に対する DDoS(分散型サービス拒否)攻撃に加えて「ワイパー」と呼ばれる破壊的なマルウェアを使った攻撃を展開し、衛星通信網などのインフラを機能不全に陥れようとした」(小泉悠『ウクライナ戦争』)　ーそれほどの効果はなかった??

4.　ニコール・パーロース(「ニューヨークタイムス」女性記者)『サイバー戦争－終末のシナリオ』の指摘

「中国の国家安全部は社会的地位の高い標的に対する攻撃を、ますますアウトソーシングするようになったのだ。ダライ・ラマや、ウイグル族やチベット族など少数民族の反体制派、アメリカの有名な防衛関連産業に対するサイバー攻撃を、中国の大学やインターネット企業のフリーのハッカーに外注したのである」

「2015 年 9 月 25 日の朝は、入念な歓迎式典で始まった。ーーーー2 時間に及ぶ密室の会談で、オバマ大統領はアメリカ企業に対するサイバー攻撃をやめなければならない。もしこのままつづけるのであれば、アメリカは中国人ハッカーを再度起訴し、経済措置に踏み切る」- 米中は合意したが、中国は 2 年後に再開。

●ミサイル誘導システムの開発・製造を行っている三菱電機に対するサイバー攻撃は誰がやっているのか??

5.　安保 3 文書でのサイバー戦の位置づけ―建前としては防御が中心だが

■国家安全保障戦略

⑷　我が国を全方位でシームレスに守るための取組の強化 軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開され、グレーゾーン事態が恒常的に生起している現在の安全保障環境 において、サイバー空間・海

洋・宇宙空間、技術、情報、国内外の国民 の安全確保等の多岐にわたる分野において、政府横断的な政策を進め、我が国の国益を隙なく守る。 サイバー安全保障分野での対応能力の向上 サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の 安全等を確保するために、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。 具体的には、まずは、最新のサイバー脅威に常に対応できるように するため、政府機関のシステムを常時評価し、政府機関等の脅威対策 やシステムの脆弱性等を随時是正するための仕組みを構築する。その 一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、外交・防衛・情報の分 野を始めとする政府機関等のシステムの導入から廃棄までのライフサ イクルを通じた防御の強化、政府内外の人材の育成・活用の促進等を 引き続き図る。 その上で、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。 そのために、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。 また、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化する。 さらに、同盟国・同志国等と連携した形での情報収集・分析の強化、 攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために 引き続き取り組む。

■「防衛力整備計画」

(2)サイバー領域における能力

政府全体において、サイバー安全保障分野の政策が一元的に総合調整されることを踏まえ、防衛省・自衛隊においては、自らのサイバーセ キュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進することとする。

サイバー攻撃を受けている状況下において、指揮統制能力及び優先度 の高い装備品システムを保全し、自衛隊の任務遂行を保証できる態勢を確立するとともに、防衛産業のサイバー防衛を下支えできる態勢を構築する。

このため、最新のサイバー脅威を踏まえ、境界型セキュリティのみで ネットワーク内部を安全に保ち得るという従来の発想から脱却し、もは や安全なネットワークは存在しないとの前提に立ち、サイバー領域の能 力強化の取組を進める。この際、ゼロトラストの概念に基づくセキュリ ティ機能の導入を検討するとともに、常時継続的にリスクを管理する考 え方を基礎に、情報システムの運用開始後も継続的にリスクを分析・評 価し、適切に管理する「リスク管理枠組み（ＲＭＦ）」を導入する。さ らに、装備品システムや施設インフラシステムの防護態勢を強

化すると ともに、ネットワーク内部に脅威が既に侵入していることも想定し、当 該脅威を早期に検知するためのサイバー・スレット・ハンティング機能 を強化する。また、防衛関連企業に対するサイバーセキュリティ対策の強化を下支えするための取組を実施する。防衛省・自衛隊のサイバーセキュリティ態勢の強化のため、陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編し、サイ バー要員を育成する教育基盤を拡充する。さらに、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。

写真左

陸上自衛隊通信学校のある久里浜駐屯地。警察予備隊、保安大学校(防大の前身)以来の駐屯地。

これらの取組を行う組織全体としての能力を強化するため、2027 年度を目途に、自衛隊サイバー防衛隊等のサイバー関連部隊を約 4,000 人に拡充し、さらに、システム調達や維持運営等のサイバー関連業務に従事 する隊員に対する教育を実施する。これにより、2027 年度を目途に、サ イバー関連部隊の要員と合わせて防衛省・自衛隊のサイバー要員を約２ 万人体制とし、将来的には、更なる体制拡充を目指す。

⑶ 電磁波領域における能力

自衛隊の通信妨害やレーダー妨害能力の強化と併せて、電磁波の探知・識別能力の強化や電磁波を用いた欺まんの手段を獲得するなど電子 戦能力を向上させるとともに、レーザー等を活用した小型無人機（ＵＡ Ｖ）への対処等の電磁波の利用方法を拡大する。また、自衛隊の使用する電磁波の利用状況を適切に管理・調整する機能を強化する。このため、通信・レーダー妨害機能を有するネットワーク電子戦シス テム（ＮＥＷＳ）の整備、脅威圏外から通信妨害等を行うスタンド・オ フ電子戦機及び脅威圏内において各種電子妨害を行うスタンド・イン・ジャマー等の開発、電波探知器材の搭載による艦艇及び固定翼哨戒機の 信号探知・識別能力の向上、陸上からレーダー妨害を行う対空電子戦装 置の整備を行う。また、固定翼哨戒機等への電子妨害能力の付与につい て、試験的に検証し、必要な措置を講じる。加えて、小型無人機（ＵＡ Ｖ）に対処する車両搭載型レーザー装置の運用を開始するとともに、高出力レーザー、高出力マイクロ波（ＨＰＭ）等の指向性エネルギー技術 の早期装備化を図る。防衛省・自衛隊のシステムに電磁波の利用状況を 把握・管理するための機能を整備するとともに、関係省庁と緊密に連携 し、自衛隊の各種活動に必要な電波利用を確保していく

（朝日新聞社説）サイバー攻撃　危うさ伴う「能動防御」　2023 年 1 月 29 日

政府機関や重要インフラに対するサイバー攻撃は、国の安全保障や国民生活に対する重大な脅威である。対策を強化する必要性は理解できるが、通信の秘密など、憲法が保障する国民の権利が侵害される事態は避けねばならない。岸田政権が導入を宣言した「能動的サイバー防御（アクティブ・サイバー・ディフェンス）」には懸念がある。リスクを含めた十分な説明はまだなされておらず、拙速に突き進むことは許されない。昨年末に改定された安保３文書は、サイバー分野の対応能力を「欧米主要国と同等以上に向上させる」として、能動的サイバー防御の実施体制を整備すると明記した。被害を受けてから対処するのではなく、未然防止をめざす。２７年度をめどに、自衛隊のサイバー関連部隊を約４千人に拡充し、関連業務に従事する

要員と合わせ約２万人体制とする方針も打ち出した

現代の戦争は、従来の兵器に加え、サイバー攻撃や情報・心理戦などを組み合わせた「ハイブリッド戦」が主流となったと言われる。政府は中国、ロシア、北朝鮮がサイバー能力を向上させているとみており、受け身では守り切れないとの認識が背景にある。能動的サイバー防御は欧米ではすでに採用されており、平時からサイバー空間を監視し、システムやネットワークへの侵入、不審な通信を解析している。ただ、個人情報やプライバシーが侵される恐れが常に伴う。米国では、政府がテロ対策を名目に、米国市民の通信データを大量に収集したことが批判され、１５年に米国自由法を定めて活動に制限を加えた。日本では、憲法２１条が通信の秘密の保護を定め、「電気通信事業法」では、それを侵した事業者に罰則を科している。本人の承諾なしにデータにアクセスすることを禁じる「不正アクセス禁止法」もある。

政府・与党内には、自衛隊を不正アクセス禁止法などの対象外とするよう、法改正の検討を求める声があるが、権利の侵害に対する国民の懸念を払拭（ふっしょく）するのが先決である。安保３文書には、未然に攻撃者のサーバーに侵入して、無害化できるよう、政府に必要な権限を与えることも盛り込まれた。しかし、サイバー攻撃は犯罪か、テロか、武力攻撃か、主体が個人か、国か、にわかに判別が困難な場合が多い。何が武力攻撃にあたり、どこから反撃が認められるかも、国際的に定まっていない。対応を誤れば、国家間の深刻な対立や紛争につながる恐れがあることを直視すべきだ。

6.最近の国会での論戦

６月８日　外交防衛委員会、財政金融委員会　連合審査会
○宮崎勝君(公明党)　現状、民間企業におきましても御存じのとおりＩＴエンジニアは不足しており、二〇三〇年には七十九万人が不足すると言われております。そのような状況で優秀な人材を確保するのは容易ではありません。　その意味で、十分な処遇ができるよう体制を整える必要があると思いますけれども、防衛省の取組をお伺いしたいと思います。

○政府参考人（町田一仁君　防衛省人事教育局長）　お答えいたします。　サイバー攻撃が日々高度化、巧妙化する中、防衛省・自衛隊としては、サイバー防衛能力の強化を図る上で高度な技能を持つサイバー要員に対し適正な処遇を与えることが重要と考えており、必要な措置を行ってまいりました。　具体的には、例えば、自衛隊*サイバー防衛隊*において、**サイバー分野における専門性が極めて高い業務に従事する事務官等に対して月額約三万円程度の俸給の調整額を支給しております**。また、防衛力整備計画に基づき、専門的知見を持つ外部人材の活用を促進すべく、柔軟な働き方が可能となる新たな自衛官の人事制度の整備を検討しています。いずれにせよ、サイバー要員の大幅な拡充に伴う人材確保は重要な課題であり、**防衛省・自衛隊の人的基盤の強化に関する有識者検討会の提言**もいただきながら、鋭意検討を進めていく考えです。

●提言案「内部の養成基盤の充実強化に加え、新たな領域となるサイバー等の分野に従事する要員についても、部外派遣による教育機会も活用しつつ、各自衛隊の学校等での充実した教育による養成とその基盤が重要である」

○政府参考人（上田幸司君　**防衛大臣官房サイバーセキュリティ情報化審議官**）　サイバー攻撃への対処能力、こ

れは必ずしも要員の数のみで決まるものではなく、質といいますか、技術面、能力面、こういったものを重要と考えておりますので、我々としましては、現在八百九十名の体制を四千名に拡大しますとともに、この質も高めまして、二十四時間体制でサイバー攻撃への対処に当たる、このように対応してまいりたいと考えてございます。

2023 年 5 月 9 日　参議院　外交防衛委員会　　「維新」は自民よりも過激なのか??

〇音喜多駿君　日本維新の会の音喜多駿です。　この防衛三文書が発表され、能動的サイバー防御という言葉が初めて盛り込まれたことを受け、実効性を高めるためにも**不正アクセス禁止法、不正電磁的記録罪の要件を改正して、自衛隊への適用除外、これを認められるよう防衛省として課題を整理していくべきではないか**と考えますが、大臣の意気込みと現時点での見通し、見解をお伺いいたします。

〇国務大臣（浜田靖一君）　近年のサイバー空間における厳しい情勢を踏まえ、国家安全保障戦略においては、武力攻撃に至らないものの安全保障上の懸念を生じさせる重大なサイバー攻撃を可能な限り未然に排除し、発生してしまった場合には被害の拡大を防止するため、能動的サイバー防衛を導入する旨記述されました。　具体的な取組の内容については、**安全保障上の必要性と現行法令との関係等を総合的に勘案**しつつ、内閣官房が中心となって政府として検討を進めているところであります。防衛省・自衛隊としても、自らのサイバー防衛能力の抜本的な強化の取組を通じて、このようなサイバー安全保障分野に係る政府の取組に積極的に貢献していく所存であります。

見えないデジタルの落とし穴
デジタル監視社会はどこまで悪化したか！！
2023/7/30

小倉利丸
JCA-NET
toshi@jca.apc.org

デジタル/サイバー領域の「実感」

- 見える「敵」としか闘えていない
- 仕組みの難しさと便利さ
- デジタル/サイバー領域に焦点をあてた社会運動、人権運動の不在

監視社会化への政府・企業の基本戦略
- 「監視社会」批判を回避する迂回作戦が基本
- 法の抜け穴利用
- 「見えない」ところで進展(技術の悪用)
- 便利・無料による浸透
- メディア・情報操作(インフルエンサーの利用)
- 人権を逆手に取り、反論を封じる

NATO サイバー防衛演習ロックド・シールズ

参加組織の構成
- 自衛隊の各部隊
- 政府省庁：内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省、警察庁、情報処理推進機構（ＩＰＡ）、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」として民間からの参加

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 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 2 度目の参加
「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。」

演習では 5、500 の仮想システムに対し 8、000 以上の大規模なサイバー攻撃が行われ、重要インフラ等のシステムを攻撃から防護する技術的な対処やインシデントの報告のほか、法務、広報、情報活動に関する課題への対処

日本チームは官民や同志国との連携によりインシデント対応を演習し、日本国内の重要インフラ企業でサイバーセキュリティ戦略の実務を担う若手が参加

実空間での演習との違い

- 自衛隊・防衛省以外の政府省庁が正式参加
- 民間企業の多くが、私たちにとって馴染のある情報通信やインフラ企業である

こうした政府や企業は、私たちの動静を監視する様々な手段をもっている企業でもある。

- Microsoft はほとんどの PC の OS を供給している
- 総務省はマイナンバーを所管
- NTT など IT 企業はネットユーザのデータを網羅的に把握できる企業
- 警察庁の参加で、戦争と犯罪の境界が曖昧に

子どもの性的搾取や虐待の脅威

我々は、安全性及びセキュリティが優先されることや、各プラットフォームがそのプラットフォーム上で子どもの性的搾取や虐待の脅威に対処することを確保し、オンラインでの安全とプライバシーに対する子どもの権利を堅持しながら、テクノロジーの責任あるイノベーションと実装を推進する

Ｇ７広島首脳コミュニケ（２０２３年5月２０日）
「子どもの性的搾取や虐待の脅威」への対処は…「テクノロジーの責任あるイノベーションと実装」？

- 網羅的にデータを監視しなければ実現できない。
- 暗号化を弱体化させるような「イノベーション」を推進する
- 他の目的に転用可能な方法である。

参考：EU が提案した子どもの性的虐待をオンラインで闘うための規制の危険性に関する共同声明
https://www.jca.apc.org/jca-net/ja/node/265

「サイバー攻撃」「子どもの性的搾取」対策と称する監視社会戦略の共通点

- これが唯一の解決策であるかのように主張する
- 不安感や正義感を監視社会容認の世論形成に利用する
- 既存の市民運動などでの合意の未形成の隙を突く

私たちの課題

- 立法府への働きかけや集会、デモ、署名運動など、既存の「運動」には限界がある。
- 「運動」の領域を、デジタル/サイバーの領域に拡大させることが必要。
- 政府や企業に私たちのサイバーセキュリティを委ねることは、監視社会化の思う壺
  →民衆のサイバーセキュリティの確立

デジタル/サイバー領域を主課題とする運動体を作り出す
民衆のための技術開発も不在

カメラで追跡されるのはゴメンだ！
私たちはプライバシーを守りたい

顔識別カメラシステムに反対する市民団体共同声明

２０２３年5月３０日現在

呼びかけ団体（11）

共謀罪 NO！実行委員会
「秘密保護法」廃止へ！実行委員会
ビデオプレス
許すな！憲法改悪・市民連絡会
盗聴法に反対する市民連絡会
東京・地域ネットワーク
日本消費者連盟
憲法会議
平和を実現するキリスト者ネット
秘密法と共謀罪に反対する愛知の会
JCA−NET

賛同団体（３８）

ストップ秘密保護法かながわ
樹花舎
「憲法」を愛する女性ネット
北大生・宮澤弘幸「スパイ冤罪事件」の真相を広める会
大垣警察市民監視違憲訴訟の勝利をめざす「ものを言う」自由を守る会
秘密保護法廃止を求める岐阜の会
９条の会・おおがき
沖縄と連帯する会・岐阜
平和・人権・環境を守る岐阜県市民の声
「民主と自治の会」・鎌ヶ谷
ポレポレ佐倉
プライバシー・アクション　白石
ATTAC Japan(首都圏)
「平和への結集」をめざす市民の風
アジェンダ・プロジェクト
スーパーシティを考える会
緑の党グリーンズジャパン
あさひ九条の会
市民オンブズ西宮
秘密法廃止市民ネットとやま
秘密保護法と共謀罪を考える四日市の会
共通番号いらないネット
戦争あかん！ロックアクション
戦争させない・９条壊すな！岐阜総がかり行動実行委員会
婦人民主クラブ
日本山妙法寺
平和をつくり出す宗教者ネット
基地のない沖縄をめざす宗教者の集い
ふぇみん婦人民主クラブ
日本キリスト教団神奈川教区秘密法反対特別委員会
平和をつくる大和市民の会
秘密保護法対策団
共謀罪対策弁護団
破防法・組対法に反対する共同行動
秘密保護法を考える川崎市民の会
学校事務職員労働組合神奈川
バスストップから基地ストップの会
全国学校事務労働組合連絡会議

共同声明の賛同団体になってください

２０２３年3月２１日

顔識別カメラシステムに反対する市民団体共同声明への賛同
をお願いします。
賛同をいただける団体はネットか FAX でご返事ください。

■ネットからの申し込み
共謀罪 NO!実行委員会の HP の賛同ページ https://www.kyobozaino.com/sando
にアクセスし、団体名、メルアドをご記入して、クリックすれば OK です。

■FAX のばあい
顔識別カメラシステムに反対する市民団体共同声明に賛同します

団体名

メールアドレス

集約先 FAX 番号　０３−５１５５−４７６７

１、締切日について
第一次集約　４月２３日（日）　　第二次集約　５月末日
第三次集約　８月末日（最終集約）
２、市民団体共同声明の活用について
イ、呼びかけ・賛同団体一覧として可能な団体は HP などで発表します。記者会見をおこないます。また、国会議員に声明を配布します。
ロ、一回か二回、呼びかけ・賛同団体として院内集会を開き、国会議員への働きかけをおこないます。
ハ、顔識別カメラシステム、監視カメラ社会反対のｍｌをつくります。
ｍｌではこの問題に関する報告、情報交換などをおこないます。
※このｍｌでの投稿は顔識別カメラシステム、監視カメラ社会に関するものに限定となります。
ニ、市民団体共同声明の期間
呼びかけ・賛同団体のおこなう運動は、今通常国会、秋の臨時国会までの１年とします。１２月末日をもって ml は解散します。

問い合わせ先０８０−９４０８−０９６２（角田）

カメラで追跡されるのはゴメンだ！
私たちはプライバシーを守りたい
顔識別カメラシステムに反対する市民団体共同声明

２０２３年3月２１日

呼びかけ団体　（順不同　3月２８日現在　１１団体）
共謀罪 NO！実行委員会、「秘密保護法」廃止へ！実行委員会、ビデオプレス、許すな！憲法改悪・市民連絡会 、盗聴法に反対する市民連絡会 、東京・地域ネットワーク、日本消費者連盟、憲法会議 、平和を実現するキリスト者ネット、秘密法と共謀罪に反対する愛知の会 、JCA−NET

現在、駅、空港などの大規模空間における顔識別カメラシステム稼働の容認に向けての動きが急ピッチに進められています。

顔識別カメラシステムとは、照合用データベースに登録された人物の顔画像と、設置されたカメラに写る人物の顔画像が自動照合され、一致するとその人物を継続して追跡できるものです。そのネットワークにあるカメラの数が多く、広範であればあるほど、登録された人物の行動を詳しく追跡できます。従来の防犯カメラは、カメラに写る人物を「瞬間的」に撮影し、顔画像を一定期間保存し、その後、顔画像は削除されます。テレビドラマで捜査機関が事件現場などにあるカメラの一つ一つから犯人や逃走経路を探し出していくシーンがありますが、それが従来型の防犯カメラです。顔識別カメラシステム（以下 、「カメラシステム」と略）は、特定の人物の継続的な追跡能力をもつという点で、従来型の防犯カメラとは全く異なります。このカメラシステムがどういうものであり、いかに危険なのかはこのシステムを２０２１年７月導入したＪＲ東日本の例をみれば明らかです。

データベースへの登録は無限定

同カメラシステムの問題は、第一に事業者の判断で対象者を無限定に照合用データベースに登録し、特定の人物を追跡できるということです。

ＪＲ東日本は、同カメラシステムのデータベースに指名手配犯、同社の管内で事件をおこした出所者・仮出所者 、「不審者」の顔画像を登録しました。メディアなどから、出所者・仮出所者を登録したことについて、これはいわゆる「前科」という機微情報（要配慮個人情報）にあたるのではないかと批判され、登録からはずしました。しかし、指名手配犯 、「不審者」の登録はそのままにし、同カメラシステムを稼働し続けています。重要なことは、個人情報保護委員会が同システムの導入にあたって、ＪＲ東日本から相談を受けた際に、 OK をだしていたことです。

本人は何も知ることができない

同カメラシステムの問題は、第二に本人がデータベースに登録されていることを知ることができないことです。その端的な例が、 ＪＲ東日本の「不審者」の登録です。そもそも「不審者」の概念が曖昧です。そのため、駅構内で落とし物を探している人や乗り換えのホームを探している人などが「不審者」とされかねません。そもそも「不審者」とされた人は、何か法律に違反する行為をしたわけではなく 、「容疑者」でもありません。にもかかわらず、どの駅から乗り、どの駅で乗り換え、どの駅で降

りるかまで行動を追跡されます。ＪＲ東日本の管内は広く、一日の利用客は膨大です。誰が、いつ「不審者」とされ、行動を追跡されるかもわかりません。また、本人は登録されていることを知らないため、抗議も是正も求めることはできません。これを重大なプライバシー、個人情報の侵害といわずなんというのでしょうか。

設置場所での掲示が義務付けられていない

同カメラシステムの問題は、第三にカメラは犯罪の予防、公共の安全の確保のために必要としながら、その設置場所に「防犯カメラ稼働中」などの告知、掲示が義務付けられていないことです。つまり、告知、掲示は事業者の努力目標にすぎません。多くの事業者がこの点を利用し、カメラ設置場所での告知、掲示をしていません。

こうした状況のなかで、市民のプライバシー、個人情報の侵害度の強い顔識別カメラシステムが導入されようとしているのです。設置場所に目立つように「防犯カメラ作動中」の告知、掲示があって、はじめて犯罪の予防や公共の安全に役立つといえます。それがないなら、その目的は「防犯カメラ」ではなく「監視カメラ」との批判を受けることになります。

市民のプライバシー、個人情報保護のために、個人情報保護法を改正し、カメラ活用にあたっては、防犯カメラ、顔識別カメラシステムを問わず、設置場所にカメラ作動中などの告知、掲示を義務付けるべきです。

共同利用の行く先は

同システムの問題は、第四にある事業者とほかの事業者との顔画像の共同利用が可能になるということです。これは、個人情報保護法において、個人情報（この場合、顔画像）を取得した事業者は、本人の同意がなければ、それを第三者に提供できないとされていますが、共同利用はその例外とされているからです。

これを活用すれば、全国窃盗団対策としてＪＲ関係各社、私鉄などすべての交通機関の共同利用が可能となり、文字通り、全国的な顔識別カメラシステムのネットワークが可能となってしまいます。

国会での議論がない

同カメラシステムの問題は、第五に国会で一度も議論されることなく、容認されようとしていることです。この問題を担当している個人情報保護委員会は、なぜ国会に対して駅や空港などでの同システムの稼働の是非、是とする場合、顔画像をシステムに登録する際の要件、保存期間、チェック体制、違反した場合の処罰などについて法律で決めることをもとめないのでしょうか。現在、日本は世界有数のカメラ保有国です。至る所にカメラが設置されているといって過言ではありません。

プライバシー、個人情報の侵害度の強い顔識別監視カメラシステムについて、国会での議論が必要です。欧米では、駅、空港などでの同システムの導入について、規制の動きがあります。日本では、この問題についてもっと慎重な議論が必要です。

私たちは、問題の多い顔識別カメラシステムの稼働に反対します。