日本政府によるスパイ・監視と対抗するために――一人でもできることから仲間と一緒にできることまで

JCA-NET jca.apc.org

2026 年4 月

目次

1．スパイ機関創設とサイバー戦争・監視社会化の核心

日本政府はスパイ機関の創設を目指して、2026 年通常国会で様々な法案を通過させつつ、官民一体となった情報収集と監視・取り締まり強化の制度を作り上げようとしています。

これまでも日本にはスパイ機関と呼べるような組織がいくつかありましたが、高市政権が目指しているのは、より大規模で軍事安全保障から国内の治安監視体制までを網羅した監視国家を目指すものになります。

私たちは、こうした傾向に対して、スパイ機関を合法化するいかなる法制度にも反対し、また政府組織体制に対しても明確に反対します。これまで幾度となく繰り返されてきた悪法に対する反対運動同様、法案への反対、組織や制度の創設への反対を強く訴えていきます。

同時に、サイバー領域におけるスパイ関連の法律や制度については、以下のように、従来の法・制度と根本的に異なる課題があることにも注目する必要があります。

- スパイ機関は、自らの行動を秘匿して活動します。たとえ違法行為がなされたとしても、そのこと自体が公然化されることはありません。
- サイバー領域での日本政府のスパイ活動(以下サイバースパイと呼びます)は、私たちの通信環境それ自体に対するスパイ活動にならざるをえません。これは実空間でのスパイ活動とは全く異なる性質をもちます。
- サイバースパイは、サイバー攻撃の性質を併せもつものであり、しかも、実空間での武力攻撃と密接に連動します。
- サイバースパイは、偽情報の拡散や情報の攪乱、戦争の扇動やヘイトスピーチなど、いわゆる「情報戦」とも連動するために、国内外を問わず行なわれ、深刻な人権侵害の元凶となり、私たちの情報環境を大きく歪めます。
- 日本政府のサイバースパイ活動は民間企業との連携なしには不可能です。この意味において、スパイ機関の創設は官民連携を必須とし、私たちの日常生活全体への監視に繋がります。
- 同時に、サイバー領域はグローバルなネットワークでもあり、いわゆる「同盟国」のスパイ・情報機関との連携や、米国などの巨大 IT 企業のノウハウ、AI 技術などを駆使したものになり、これまでにない監視国家体制となります。

このパンフレットでは、サイバースパイによる監視や情報収集、情報操作に対して私たちにできる対抗手段について説明します。法律や制度への反対運動は必須ですが、他の軍事・安全保障の問題とは違って、もっと身近なところから、些細にみえる取り組みを通じて対抗することが可能です。

例えば、投票で一票を投じるという些細な行動が大きな政治を動かしたり、地域の人びとが協力して、政府や企業に頼らずに自立した相互扶助や連帯の取り組みをすることで生活や労働の場を変えるのと同じことを、サイバー空間で実践することなのだと考えてみてください。

実空間にある軍事・安全保障の制度や組織を阻止することは容易ではありませんが、私たちを狙うサイバースパイを阻止することは、実は、決して不可能ではありません。以下、そのいくつかの方法について、一人でもできることから、仲間と一緒に取り組めることまで、紹介します。

2．サイバースパイはどうやって情報を収集するのか

サイバー領域とは、主にわたしたちのスマホやパソコンなどを使った通信環境になります。[1]サイバースパイは、私たちが利用するスマホやパソコンやこれらが繋がっているインターネットの仕組みを通じて、私たちの動静を監視し情報を収集し、時にはサイバー攻撃にも利用します。

たとえば、自分が今どこにいるのかは、スマホの GPS 機能で把握できてしまいます。メールのやりとりや通話の記録は、契約しているプロバイダーや Gmail のようなメールサービス事業者に把握されます。ウエッブにアクセスして買い物したり動画を閲覧すれば、アクセス先の企業や関連する広告主などが情報を把握できます。政府のサイバースパイでは、通信事業者やネットのサービス事業者に協力させて、こうした様々な断片的なデータを網羅的に収集することも活動の重要な一環になります。スパイ行為には、違法にネットやあなたの通信機器に侵入して情報を密かに収集する行為も含まれます。

私たちがメールでやりとりしたり、オンラインショッピングしたりしたときに、どれだけ多くの情報のやりとりをしているのかは直感的には理解できません。メールの内容や送受信に関するデータが通信事業者に把握され、捜査機関などにも提供可能であることはよく知られています。ウエッブの利用に際しては、「クッキー」の仕組みを悪用して第三者が私たちの行動を追跡できるという問題についても、知られるようになりました。

このほかに「フィンガープリント(指紋)」と呼ばれる問題にも関心が高まっています。ウエッブにアクセスすると、あなたがいる地域、パソコンを使ったアクセスかスマホか、使用しているソフトウェアの種類、使用言語など非常に多くの情報が相手に提供されます。こうした情報を「フィンガープリント(指紋)」と呼びます。これら断片的なデータのひとつひとつは些細ですが、膨大に収集されることによって、私たちひとりひとりが何者であるのかを把握できるようなデータが生成できます。だから「フィンガープリント」と呼ばれるのです。[2]

政府のサイバースパイは、ネットでの私たちの動静に関する情報を民間事業者に協力させて収集するとともに、自治体や警察を含めて政府全体が保有している個人情報(マイナンバーによって紐付けされた情報やそれ以外の様々な情報)が加わることに

1　このほかに、Wi-Fi ルーターやスマートメーターなど、いわゆるモノのインターネット(IoT)もサイバースパイ・サイバー攻撃では重要になりますが、本パンフレットでは扱いません。下記を参照してください。JCA-NET セミナー資料「Wi-Fi のセキュリティとプライバシー――現状と対策」https://pilot.jca.apc.org/nextcloud/index.php/s/yBH2Y4fR5ZQkcG7 同「政府の情報収集はどこまで進んでいるのか――NOTICE による侵入調査とは」https://pilot.jca.apc.org/nextcloud/index.php/s/i4KxpsCoXe8bcde

2　自分が使っているブラウザのフィンガープリントは下記の電子フロンティア財団(EFF)のサイトで調べることができます。https://coveryourtracks.eff.org/ このサイトにアクセスして TEST YOUR BROWSER というボタンをクリックしてください。詳細なデータ(英語)が表示され、説明も付されています。使い方の日本語訳が下記にあります。https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_fingerprint_check/

よって詳細な個人別のデータ(プロファイル)を構築することができます。日本政府が敵国とみなす外国に対しては、より強引な手法として、相手国内でのハッキングやマルウェアのインストールなどによって情報を収集することになります。

政府であれ民間であれ、営利目的であれ政治目的であれ、あるいは犯罪目的であれ、わたしたちのデータを収集するための手段は次のどれかです。

- スマホやパソコンを使った通信関連データ。(スマホ決済、SNS、メール、ウエッブ閲覧、GPS の位置情報、画像や音声情報、住所録など)
- 政府が保有する個人データ(戸籍や住民票、社会保障関連など様々なデータのほかマイナンバーと紐付けされたデータ、運転免許証、犯罪歴、民間企業から取得した個人データなど) [3]。
- 金融機関や医療機関が保有する個人データ。
- 街頭に設置されている監視カメラに記録されているデータ。
- Wifi ルーターや電力のスマートメーターなどモノのインターネット(IoT)と呼ばれる機器のデータ。

こうした情報収集の入口を政府のスパイ機関も利用します。スパイ機関は、政府が保有する情報を利用するとともに、民間情報も入手可能な法的・制度的な権限を獲得することになるでしょう。EU も含め多くの国では、国家安全保障上の情報収集については、プライバシーの権利など人権の保護が及ばない例外とされる場合が一般的です。

とはいえ、サイバー領域の情報収集の選択肢は決して多くはないのです。たぶん私たちの日常生活で最も頻繁に利用しているのはスマホやパソコンを使った通信でしょう。これらを利用した情報収集を阻止するだけでも、私たちの動静のかなりの部分をスパイ活動から防御することが可能です。

3. 何ができるか

私たちが、上で列挙した情報収集の入口を塞げば、情報は収集できません。街頭の監視カメラのデータや自分の手許で保管されていない個人データを防御することは難しくても、私たちの日々の動静をリアルタイムで記録しているスマホやパソコンのデータ提供は自分で工夫することで阻止することは可能です。路上で私たちを尾行する政府のスパイをまくのと同じことをサイバー領域で行うようなことだと考えてみてください。ここでは、いくつかの防御の方法を紹介します。

3.1. パスワード

3.1.1. パスワード設定では必ず以下のルールを守ってください

- 同じパスワードを使い回さないこと。
- 自分の名前、生年月日、電話番号、住所、あるいは 1234 とか abcd など推測さ

3 政府が保有する個人情報については、下記に省庁別に保有個人情報に関する開示請求窓口の一覧があります。https://personal-info.e-gov.go.jp/contents/disclosure/ 利用ガイドはこちら。https://personal-info.e-gov.go.jp/contents/help/guide

れやすいものは使わないこと。

- 上記の条件を満たした上で、最低でも 15 字は必要です。

3.1.2. なぜパスワードは大切か

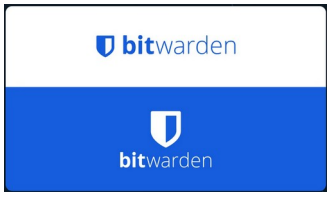
パスワードの窃取は、ハッキングや不正アクセスを狙う者たちの常套手段です。

メールなど個人のデータはアカウント(登録名など)とパスワードの組み合わせで保護されています。アカウントは公開され誰もが知ることになります。政府のスパイ機関などがアカウント名とパスワードの組み合わせを把握した場合、メールの盗み読み、なりすまし、データの窃取など何でもできてしまいます。 最近ではパスワードだけでなく多要素認証(あるいは多段階認証)[4]も普及してきましたが、だからといってパスワードを軽視してはいけません。パスワードのルールをきちんと守った上で多要素認証などを採用することが必要です。

3.1.3. パスワードの管理で困ったらどうするか

上記 3.1.1 の条件を満たすパスワードを幾つも管理することはかなり困難です。信頼できるパスワード管理ソフトを利用することで管理を容易にすることができます。定評のあるソフトとして以下があります。

Bitwarden https://bitwarden.com/ja-jp/ KeepassXC https://keepassxc.org/



3.2. ブラウザ

3.2.1. ブラウザとは、その役割は何か

インターネット上の様々なウエッブページにアクセスするために利用する必須のソフトウェアは、一般に「ブラウザ」と総称され様々な種類があります。 たとえば、Google Chrome、Microsoft Edge、Firefox、Safari などです。Google で検索したり Amazon で買い物をしたり、Yahoo でニュースを読んだり、Youtube の動画を観たりするのも、みなブラウザを使ってやっていることです。

ブラウザは、あなたがウエッブにアクセスしてどのような行動をとっているのかを最もよく把握できます。Google はこうした仕組みを利用して、膨大なユーザーの挙動データを収集して収益に繋げています。こうしたデータ収集を可能な限り阻止します。

3.2.2. ブラウザの「設定」を見直します

- 設定画面でプライバシーとセキュリティの設定をより厳格にします。たとえば、

4 多要素認証(多段階認証)については情報処理推進機構の下記の記事を参照。https://www.ipa.go.jp/security/anshin/measures/account_security.html#3_2stepsevs

サードパーティ Coockie[5] はすべて不許可にする、ブラウザの「設定」で広告ブロック機能があれば、ブロックするように選択します。(3.2.3 も参照)

- 検索エンジンを変更します。プライバシー重視の検索エンジンに切り替えます。ブラウザの「設定」メニューからブラウザの項目を探し以下のいずれかに変更します。DuckDuckGo、ecosia、Satarpage。

3.2.3. わたしたちの行動にひそかにつきまとう「追跡者」(トラッカーと呼びます)などを排除する拡張機能を追加

私たちがブラウザを使うたびにつきまとい、私たちの好みなどを把握しようとするトラッカーという仕組みが組み込まれている場合があります。トラッカーを送り込んできた事業者はこのような情報を広告主に販売しているのです。ブラウザには追加で様々な機能を導入する仕組み「拡張機能」があります。この「拡張機能」を使ってトラッカーを阻止することができます。「設定」メニューから「拡張機能」を選ぶなどして、拡張機能の提供サイトからインストールします。たとえば、以下のような拡張機能の導入を検討してみてください。

- uBlock Origin 広告ブロッカーとして定評があります。
- Privacy Badger 第三者のトラッカーを阻止します。

3.2.4. ブラウザをよりプライバシーを重視したものに変更する

もし Google Chrome や Microsoft Edge を利用しているなら下記のブラウザへの切り替えを推奨します。

Firefox https://www.firefox.com/ja/ Brave https://brave.com/ja/download/

Vivaldi https://vivaldi.com/ja/download/ Librewolf https://librewolf.net/

Tor https://www.torproject.org/

5 アクセス先のサイトに掲載されている広告などをサードパーティと呼びます。広告主がアクセスしてきた者を追跡などの目的で Cookie と呼ばれる仕組みを利用(悪用)する場合があります。

3.3. スマホのセキュリティの見直し

3.3.1. 利用に際してはパスワード入力を必須にする

スマホの画面をタッチしてすぐ使えるのは便利ですが、誰でも利用できてしまいます。盗難や紛失のリスクを念頭に、使用する際にはパスワード入力が必要になるように設定してください。

3.3.2. スマホの「設定」のプライバシーやセキュリティをより厳格な設定に変更してください。

- 位置情報は off にする。どうしても必要なときだけ on にする。
- 住所録にアクセスを許可しているアプリを制限する。
- カメラにレンズカバーをつけ、使うときだけ外す。
- プライバシーを重視したブラウザに変更する。
- 使わないアプリや何のアプリか不明なものは削除する。

3.4. 暗号化

スパイ機関は多くの国で、国家安全保障を口実に超法規的な活動が容認されていたり、司法のチェックが効かない特権を享受している場合がみられます。また民間企業がこうしたスパイ機関と協力することもよくみられます。

インターネットを用いた私たちのコミュニケーションの多くは、ネットの回線上では暗号化されておりスパイ機関でも容易に内容を解読できません。これに対して、プロバイダーやクラウドサービス業者のサーバーなどに保管されているデータは暗号化されていないのが普通です。このために、サイバースパイはプロバイダーなどのサーバーでの情報収集を試みます。これに対して私たちがとれる手段があります。

3.4.1. 暗号化サービスを使う

メールやファイルを暗号化して提供するサービスがあります。たとえサイバースパイがサーバーに侵入してもデータを解読できませんし、通信事業者自身も暗号化されたデータを解読できません。こうしたサービスとして以下がよく知られています。

- proton メールやファイルの暗号化サービス。スイスに拠点がある。
  https://proton.me/ja

Proton

- tuta メールの暗号化サービス。ドイツに拠点がある。 https://tuta.com/ja

tuta

- Cryptpad 文書の作成、表計算など様々な作業を暗号化して保管できる。フランスに拠点がある。https://cryptpad.fr/index.html

3.4.2. これらのサービスを使わないと暗号化は無理なのか

そんなことはありません。暗号化の方法はさまざまあります。自分のパソコンの書類を自分で暗号化するためのソフトもあります。あるいは、パソコンのハードディスクをまるごと暗号化することもできます。暗号化の仕組みも様々です。もし暗号について詳しく知りたいばあいは、下記のブックレットをお読みください。

グレンコラ・ボラダイル『反対派を防衛する――社会運動のデジタル弾圧と暗号による防御』
https://www.jca.apc.org/jca-net/sites/default/files/2021-11/反対派を防衛する(統合版).pdf

技術的な知識がなくても暗号化の恩恵を受ける方法として前述(3.4.1)のような暗号化サービスを使うのが最も手っ取り早いといえます。

3.4.3. このような暗号化で本当に政府のスパイ活動に対抗できるのか？

できます。暗号技術は純粋に数学的な理論で組み立てられています。信頼できる暗号技術は、その技術の仕様を公開し、誰でも検証できるようにしています。もし「我が社の暗号技術は企業秘密なので公開していない」といった謳い文句で売り込みを図る暗号サービスがあれば、絶対に使わないでください。第三者の検証が得られないサービスは信頼に欠けるからです。上で紹介した proton、tuta、Cryptpad はいずれもオープンソースと呼ばれる技術の仕様を公開するものになっています。

3.4.4. 暗号化で注意すべきことは、やっぱりパスワード!

暗号化されたデータを復元(復号と呼びます)する場合には、パスワードを入力することになります。パスワードの管理をきちんとすること、つまり、上述(3.1.1)したようなパスワードの条件を守ることが必須です。いかに強固な暗号を用いても、復号パスワードを安直なものに設定していたら、暗号化は全く効果をもちません。

3.4.5. 暗号化が政府のスパイ活動にこれほど効果があるとすれば、政府のスパイ活動はさほど脅威ではないのでは？

政府のスパイが膨大なデータを収集しても、その大半が暗号化さていては使い物になりません。そこで日本政府は米国やオーストラリアなどとともに、私たちが暗号を利用することそのものを規制する措置をとろうとしています。[6]児童ポルノとかテロリ

6 下記の声明を参照「暗号規制に反対します―日本政府は「エンドツーエンド暗号化及び公共の安全に関するインターナショナル・ステートメント」から撤退を!!」https://jca.apc.org/jca-net の

ズムなど様々な理由をつけて、暗号化サービスを法的に禁止したり、利用できる暗号の強度を弱めたるなど様々な法的な権限の利用を画策しようとしています。こうした動きは、EU でも具体的になっています。

暗号化は私たちのプライバシーの権利そのものです。暗号利用を法的に犯罪化するような動きにははっきり反対していく必要があります。

3.5. 匿名性

選挙は匿名投票ですし、現金で買い物をするときも匿名です。内部通報制度も匿名の権利で保護されるべきだとさています。[7]デモや集会に参加するときも匿名が基本です。匿名だからこそ権力を告発したり、多数の意見への異論を述べる勇気を与えられます。

しかし、膨大なデータを収集して、些細な情報の断片をジグゾーパズルのように組み立てることで、匿名の権利が侵害されうる時代になっています。外国のスパイ機関は、伝統的に、政府に異論を唱える人たちを監視してきました。ネットの監視では、パソコンやスマホにマルウェアを仕掛けるなど違法な行動をとることもあります。

いつも使うメールアドレスは容易にそのユーザーを特定可能です。オンラインの買い物やオンラインアンケートなどでメールアドレスの記入を要求されたときに、自分がいつも使っているメールアドレスを使わずに、ダミーのメールアドレスで対処する方法があります。たとえば、DuckDuckGo のメール保護機能を使うと、「Duck アドレス」を使ってあなたの実際のメールアドレスを隠してくれます。

3.6. 政府のスパイ活動は大手民間 IT 関連企業の協力が不可欠。しかし、私たちには対抗手段があります

3.6.1. 国家のスパイ活動は戦争の一環でもある

イスラエルのガザでの戦争は、新たなサイバー戦争でもあります。私たちの身近にあってネットで日常必需品ともいえるサービスを提供している大手の IT 企業が、ガザにおけるイスラエルのジェノサイドに深く加担していることが明かになっています。

たとえば、Google、Amazon、Microsoft などは、ガザで多数の一般市民の殺害を引き起した空爆やドローン攻撃を可能にする情報やシステムを提供しており、ジェノサイドに直接加担する加害企業といえます。

他方で、X、Facebook、Instagram などの SNS 企業は、これらのサービスの利用者データを収集し、監視や弾圧に利用しています。パレスチナの人びとの声を検閲し、情報の拡散を抑える一方で、イスラエルのジェノサイドを煽るような投稿やパレスチナの人びとへのヘイトスピーチを黙認するようなポリシーをとってきました。

私たちが、こうした企業のサービスを今まで通り利用することは、政府のスパイ活動を容易にするだけでなく、こうした戦争に加担し人権を侵害する企業の犯罪を事実上黙認することになります。私たちにはいくつもの対抗手段があります。なによりも、

取り組み/暗号規制に反対します―日本政府は「エンドツー/

7 消費者庁「事業者における通報対応に関する Q&A」https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/faq/faq_009/#q2

一人でもできることとして、こうした企業のサービスを使わない、ということは、今日からでもできることです。

3.6.2. 一人でもできるボイコット

すぐにでもできることがいくつかあります。

- Google 検索をしない。⇒ DuckDuckGo などに切り替える。(3.2.2 の「ブラウザの「設定」を見直します」を参照)
- ブラウザを Google Chrome や Microsoft Edge から別のものに切り替える。(前述 3.2.4「ブラウザをよりプライバシーを重視したものに変更する」を参照)
- Microsoft の Word、Excel、PowerPoint など「オフィススイート」と呼ばれる定番ソフトを使うことをやめて、たとえば、LibreOffice に切り替えます。 ⇒ https://ja.libreoffice.org/

3.6.3. 共同作業を切り替える

事務作業の共同化では Google Docs や Google Groups が定番となっていますが、有力な代替策があります。

- OnlyOffice に切り替える。OnlyOffice は、クラウドでの利用が可能で、データを暗号化して保管することもできます。⇒ https://www.onlyoffice.com/ja
- CryptPad に切り替える。上述 7 ページの「暗号化サービスを使う」を参照してください。
- メーリングリストの GoogleGroups の代替として FramaGroup があります。⇒ https://framagroupes.org/abc/en/

4. 仲間作りが最も大切 まず議論を

政府のスパイ機関創設は、これまで以上に網羅的で強力な情報収集の体制を確立することを意味しています。そうでなければ、スパイ機関を創設する意味はないでしょう。こうしたこれまでにない状況について、市民運動などに関わる私たちとしては、まず仲間とこの状況について議論し、自分たちでできることに一緒に取り組み、コミュニケーション環境に関わる運動の文化を変えることが大切です。

そのためには、政府のスパイ機関がネットをどのように駆使し、私たちの情報をどのように収集するのかについて、共通の認識を持つことが大切です。スマホやパソコンのセキュリティやパスワードの設定などを皆で検討しあう、利用するサービスを検討し、プライバシーに配慮し情報収集に利用されにくいものに変更することです。そして、スマホやパソコンの操作が苦手な仲間をサポートすることがとても大切になります。

5．よくある質問

5.1．政府の権力は強大なので何をやっても無駄ではないか。

無駄ではありません。ネットの環境のなかで政府にできないことがたくさんあります。インターネット回線のケーブルや電波は、現在では、ほとんどが暗号化されているために、政府は民間の通信事業者のサーバーを盗聴したり個人のスマホやパソコンを押収してデータを取得する以外になくなっています。サーバやスマホ、パソコンのデータを暗号化することで政府の情報収集をかなりの程度まで防御することが現状では可能といえます。しかし、残念ながら多くの人たちは、こうした防御をとっていません。

5.2．スノーデンの内部告発で米国が世界規模でのスパイ行為をやっているのは知られているが、他の国でも政府がサイバースパイのような行為をすることが可能なのか。

2021 年に EU 各国政府が「Pegasus」というスパイウエアによるスパイ活動をしていたことが発覚しました。欧州議会調査サービスのレポートに次のような記述があります。

> 「2021 年、メディア各社は、EU 加盟国および非加盟国の複数の政府が、政治的、さらには犯罪的な目的で、欧州議会議員（MEP）、ジャーナリスト、政治家、外交官、法執行官、弁護士、実業家、市民社会活動家らに対して、商用スパイウェア「Pegasus」を使用していたというスクープを報じた。Pegasus は、携帯電話に侵入し、テキストメッセージ、通話傍受、パスワード、位置情報、マイクやカメラの録音、インストールされたアプリからの情報など、標的システムで処理される膨大な量のデータを抽出するように設計されていた。」[8]

Pegasus のようにマルウェアを仕込んでのスパイについても、防御の方法をアムネスティなどが提供しており、対抗手段はあるのです。[9]

5.3．誰もがこれだけやっておけば万全といえる防御の方法は何か

必ずやるべきこととして、パスワードの管理があります。これは誰もがすべき対策です。しかし、これで万全なわけではありません。リスクは人それぞれで、置かれている状況で変わります。まず、自分にとって何が最も大きなリスクになるのかを判断することです。その上で、どのような防御策がとれるかを調べることです。このリスクの優先順位は人それぞれが置かれている状況で異なります。

---

8 EPRS ¦ European Parliamentary Research Service, *Setting spyware standards after the Pegasus scandal,* Author: Hendrik Mildebrath, 2024 https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766262/EPRS_BRI(2024)766262_EN.pdf

9 https://www.amnesty.org/en/latest/news/2024/06/amnesty-international-introduce-digital-safety-tools/ また様々な対抗策については、下記を参照してください。Kaspersky 「Pegasus、Chrysaor など APT 関連のマルウェアからモバイルデバイスを守るために」https://blog.kaspersky.co.jp/how-to-protect-from-pegasus-spyware/32437/、 Mobile Verification Toolkit（MVT）https://docs.mvt.re/en/latest/

5.4. パスワードとかプライバシーとか些細なことをして、政府の大きな監視権力に効果があるのか？

効果は確実にあります。こうした対処をとることで、確実に政府の情報収集量は減り、結果として、あなたと繋がっている人たちについての情報収集量も減ります。

たった１票で世界を変えられるはずもないのに、なぜ投票に行くのか、あなたなりの答えがあるはずです。その答えがここにもあてはまります。

数十人、数百人のデモで政府が態度を変えるはずがないとわかっていても、参加するのにはそれなりの理由があるはずです。その理由が、ここにもあてはまります。

そして、何よりも、一人一人の人間は多くの社会的な繋りのなかで生活しており、自分の情報を守るということは、自分との繋りのある人たちの情報を守ることにも繋がる、ということを思い出してください。

5.5. ネットやパソコンのことはよくわからないので、取り組むことに躊躇がある。

これまで市民運動や様々な社会運動は、技術的にも非常に複雑な問題に真正面から取り組んできた実績があります。たとえば、原発や核兵器の問題について、核物理学などの専門家でなくても、多くの人びとが反対してきました。農薬や化学肥料の害や薬害など専門的な知識がなければ、そのメカニズムの詳細を理解できない問題でも、人びとは果敢に挑戦し闘ってきました。

専門的な知識や技術的な仕組みの詳細が理解できなくても、問題の本質を理解し、危機感をもって闘うことは可能です。同じことは、サイバー領域についてもあてはまります。「わからない」ことであっても、闘わなければならない深刻な問題であることを理解することができます。

5.6. ネットやコンピュータに詳しい人が周りにいない。自分でもよくわからないことが多い。どうしたらいいか。

もし、市民運動などの仲間の間でも、このような問題に直面しているようであれば、ぜひ JCA-NET に相談してみてください。

JCA-NET は皆さんのネットやコンピュータのセキュリティなどへの取り組みをサポートします。まず、少人数で気軽な集まりをもちましょう。そこに JCA-NET のメンバーも加わり、皆さんがかかえている疑問を共有して、可能な解決策を議論します。

発行日 2026 年 4 月 1 日 著作・発行 JCA-NET 担当者連絡先 としまる 070-5553-5495 toshi@jca.apc.org 無料 非営利であれば転載複製自由	是非余裕のある方はカンパをご検討ください。 郵便振替口座 ＪＣＡ－ＮＥＴ （ジ゛ェイシーエイーネット ） 記号番号：00190-3-417584 ゆうちょ銀行〇一九店 417584 ※通信欄に「カンパ」とお書きください。