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

Designed by macrovector / Freepik

目次

1. スパイ機関創設とサイバー戦争・監視社会化

1.1. 法と制度が変わる

日本政府は、インターネット上の私たちの通信情報の収集を可能にする新たな法制度や政府組織の創設を次々に進めてきました。現在政府が目指しているのは、

- 政府・自治体保有の個人情報を本人の同意なしにより広範囲にわたって利用できるような体制を構築すること
- 民間が保有している個人情報を政府も利用できるように、民間の通信事業者などに協力させること

などです。

憲法では通信の秘密の権利が保障され、検閲も禁じられていますし、私たちの基本的人権を保護する様々な法・制度も存在します。しかし残念ながら、こうした権利を骨抜きにする新たな法・制度が次々に導入されてきました。たとえば、2026 年の国会では、米国の CIA や NSA に匹敵するようなスパイ機関を目指す国家情報会議/情報局が設置され、同時に、本人の同意なしで個人情報の収集・利用を可能にする個人情報保護法の改悪も成立しました。国家安全保障を優先させる特定秘密保護法、働く人々の身元チェックのセキュリティ・クリアランス制度、マイナンバー/カードの利活用拡大なども実施されてきました。そしてまた、スマホによるキャッシュレス決済の普及から街中に張り巡らされた AI 搭載の監視カメラに至るまで、人々の日常行動の把握が格段に高度化されてきました。しかも、日本中に建設が進むデータセンターには世界中から膨大な個人情報が蓄積され、将来的にこうした情報が高度な監視社会や戦争の手段として利用される危険性も否定できません。

1.2. 情報収集・監視は身近にある

政府や民間企業は、私たちが日常利用している通信インフラから個人情報を収集します。メール、SNS、ネットショッピング、ウエッブ検索、天気や地図、動画の閲覧や配信など、日常生活に必須の活動が、同時に、私たちの動静を把握する手段にもなっています。ですから、こうしたネットの日常生活を見直し、情報を収集されない工夫をし、監視社会の被害者にも加害者にもならない取り組みが大切になります。

1.3. 自覚症状がない

私たち人間の五感では理解できない舞台裏を通じて、膨大なデータの収集が行なわれるために、実感できないという大きな問題があります。実感できないために、情報の意図せざる収集を阻止したり回避することも非常に困難なのです。実感に頼ってプライバシーや個人の権利を防衛することも容易ではありません。

まず私たちがすべきことは、情報収集を可視化することです。可視化することによって、望まない情報収集を遮断するために、どうしたらいいか、その具体的な手立ても導入できるようになります。

1.4. 副作用は生涯続く

収集された個々の情報は、些細で個人を特定できるとは限らないようなものであったりもするために、プライバシー情報として重視されない可能性があります。しかし様々な些細な情報が膨大に収集されることで個人が特定できたり、重要なプライバシー情報とも連携されて、私たちの生涯を監視するための基盤となったりもします。いったん収集された情報を取り戻すことは不可能です。収集された個人情報がもたらす副作用は生涯続くことにもなります。

1.5. このパンフについて

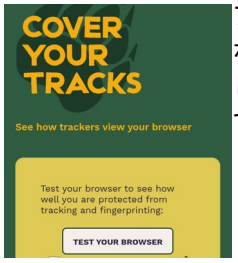
このパンフでは、まず最初に、どのようなデータが私たちの実感をすり抜けて気づかないうちに収集されているのかについて、可視化可能な方法を紹介します。その上で、どのような対策をとるべきなのか、どのような対抗手段があるのかなど、監視社会を生きる私たちが、萎縮せずに情報発信を継続するための基本的な考え方を示します。

このパンフでは情報窃取を回避し、人権やプライバシーをより重視した代替的なツールを紹介しています。ここで紹介しているツールの選択基準は以下です。

- オープンソース/フリーソフトウェアであること。技術の仕様を公開していない営利目的のサービスは原則紹介しません。
- 戦争に協力する企業のサービスに対する代替サービスの紹介。
- スマホやパソコンには様々な OS が用いられています。可能なかぎりどのようなデバイスを利用していても採用できるツールを紹介。(一部例外があります)

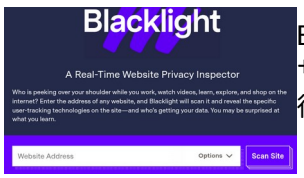
このパンフには技術的に難しい内容も含まれていますが、わからないところは読み飛ばして構いません。ページの順番通りでなくてもよいので、やれそうなことや関心のあるところから取り組んでください。

2. データ収集を実感する



ブラウザを使ってあなたがどこかのウエッブにアクセスするとします。このときに、あなた自身は実感できないのですが、相手のサイトがあなたについての様々な情報を取得します。その内容はびっくりするほど多いのです。どれほどのデータがブラウザを通じて相手に把握さているかは、下記のサイトで確認できます。

https://coveryourtracks.eff.org/



Blacklights のサイトは、アクセス先のサイトの URL をスキャンし、サイト上で使用されていユーザー追跡技術や、誰があなたのデータを取得しているかを明らかにしてくれます。

https://themarkup.org/blacklight

もし Gmail や Google のサービスを常用しているなら Google のプライバシーポリシーは必読です。最後まで読み切るにはかなりの努力が必要ですが、Google がどれほどの個人情報を収集しているのかが説明さ

れています。

https://policies.google.com/privacy?hl=ja

このプライバシーポリシーを読んで Google のサービスで最適なプライバシー対策をとることが困難だと判断した場合には、本パンフにあるような代替ツールに切り替えることを推奨します。

メールについては、普段は非表示になっている「メールヘッダ」を見ることで多くの情報が確認できます。ただしヘッダ情報は技術用語満載で理解が難しいので下記のサイトなどを参考にしてください。
日本データ通信協会「E メールヘッダ情報の確認方法」

https://www.dekyo.or.jp/soudan/contents/ihan/header.html

または、右の解説書を参考にしてみてください。増井敏克『メール技術の教科書』翔泳社。

3. 情報収集・情報操作の手段となっているのは何か

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(スマホ決済、SNS、メール、ウエッブ閲覧など)
- 政府・自治体が保有する個人データ(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)
- 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
- Wi-Fi ルーターや電力のスマートメーターなど物のインターネット(IOT)と呼ばれる機器

こうした情報収集・情報操作の入口は、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共有し、民間情報についても入手可能な法的・制度的な権限を獲得します。同時に SNS のインフルエンサーなどを動員して巧みな情報操作や扇動を組織したりもします。EU も含め多くの民主主義を標榜する国においてすら国家安全保障上の情報収集・情報操作については、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。

ここからわかるように、私たちが日常生活で最も頻繁に利用しているスマホやパソコンが、政府による情報収集・情報操作の最大の入口になる部分です。だからこそ、この情報収集・情報操作の入口を可能な限り塞ぐことが重要になります。

4. 何ができるか

メッセージを送受信する、サイトにログインするなどでは、ID とパスワードの組み合わせによって、なりすましや情報の窃取を防御しています。パスワード(パスフレーズ)は私たちの通信の秘密を防御する最も基本的な必須の条件です。

4.1. パスワード(パスフレーズ)の設定を見直す

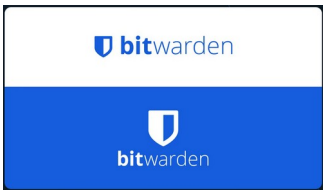
アカウントやログイン ID は第三者に知られる可能性があり、これを秘匿することは現実的ではありません。このアカウントや ID を保護する唯一の手段はパスワード(パスフレーズ)になります。パスフレーズは複数の単語を組み合わせたものを指します。以下本パンフではパスフレーズも含めた意味でパスワードと表記します。もし政府のスパイ機関などがアカウント(ID)とパスワードの組み合わせを把握した場合、メールの盗み読み、なりすまし、住所録などデータの窃取など何でもやれてしまいます。さらにはマルウェアを仕込むなど、深刻な攻撃にも晒されかねません。パスワードの管理は、必須の重要事項です。強固な暗号化サービスなどを利用している場合であってもパスワードの管理を怠れば、暗号化の効果はない、ということを十分に理解してください。

4.1.1. 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 など推測されやすいもの、辞書に掲載されている単語をそのまま使うことは避ける。
- 上記の条件を満たした上で、最低でも 18 文字は必要とされています。

4.1.2. パスワードの管理で困ったらどうするか

上記の条件を満たすパスワードを自分の記憶力だけを頼りに幾つも管理することはほぼ不可能です。信頼できるパスワード管理ソフトを利用することで、数多くの複雑なパスワードを使い回さずに容易に管理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。

管理ソフト	説明
 Bitwarden https://bitwarden.com/ja-jp/	下記に詳しい解説があります。 https://bitwarden.com/ja-jp/help/
 KeepassXC https://keepassxc.org/	下記に入門マニュアルの日本語訳があります。 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/keepassxc_gettingstarted/

4.1.3. 指紋認証、顔認証は使わない

パスワードの入力は面倒なので顔認証や指紋認証を利用したくなるかもしれません。しかし、これらは、本人の意思に反して利用される恐れがあるために推奨しません。捜査機関が裁判所の令状を取得してスマホの顔認証などを強制的に利用した実例[1]があります。

4.1.4. アナログな選択肢：工夫して紙に書く

安易なパスワードを使い回すくらいならパスワードのヒントを記載した紙を自分だけしか知らない場所にそれとなく隠しておく方が安全かもしれません。本当のパスワードを自分だけが決めたルールでちょっとした修正を加えたものを公然と貼っておくという手もありえます。パスワードの数が少ない場合、苦手なパスワード管理ソフトの使い方を四苦八苦して覚えるよりは、しっかり 18 文字のパスワードを使い回さないで管理するアナログなやり方の方がセキュリティは高くなるでしょう。こうした手法は不特定の人達の目につく場所ではお勧めしません。

1 （朝日）「強制的にスマホの顔認証」警察の捜査で新手法⬚「行きすぎ」懸念も 2026/8/12 https://digital.asahi.com/articles/ASV7Y34MQV7YPTIL014M.html

4.2. ブラウザ

4.2.1. 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 で動画を観たり、Gmail のメールを読んだりするのも、みなブラウザを使ってやっていることです。時には X や Instagram などの SNS や Zoom の会議もブラウザ経由でアクセスしている場合があります。この意味でブラウザは、ネットに繋いでコミュニケーションをとる際に必須の万能ツールといってもいい役割を担います。先に紹介したように、ブラウザを通じて実感を伴わない形で多くのデータが提供されてもいますから、プライバシーを重視して密かなトラッカー(追跡者)を阻止するなどの仕組みを重視しているブラウザを選択することは、とても重要なことになります。

4.2.2. http と https

ウエッブの URL には、http で始まっている場合と https で始まっている場合の二通りがあります。http のサイトにアクセスした場合、通信経路上のパスワードやクレジットカード番号などあらゆるデータが第三者に盗み見される危険性があります。他方で https の場合は、通信経路上のデータが暗号化されるために、盗み見の危険性は格段に低くなります。http で開設されているウエッブサイトの主宰者はできるかぎりサイトを https に移行する手続をとってください。

どうしても http のサイトにアクセスしなければならない場合は、常に通信内容を第三者に見張られていると考えて行動してください。

4.2.3. (とりあえずの対処)ブラウザの「設定」を見直すことで不必要なデータを相手に提供しないように工夫します。

ブラウザの「設定」画面を開きます。「設定」画面はブラウザの右上端の三本線や三つの点といったわかりにくいアイコンをクリックして、表示されるメニュー一覧のなかに見つかると思います。

1. 「設定」変更(その 1) Google や Bing などからプライバシー重視の検索エンジンに切り替えます。

   検索行為は、嘘をつくことができないため、Google のような検索サービスでは、検索行為から私たちの関心を把握しようとします。検索エンジンをプライバシー重視のものに切り替えることは最も簡単な情報収集への対抗手段になります。ブラウザの「設定」メニューから「検索」の項目を探し、「既定の検索エンジン」を以下のいずれかに変更します。

DuckDuckGo https://duckduckgo.com/

ecosia https://www.ecosia.org/

Startpage https://www.startpage.com/

2. 「設定」変更(その2) 追跡防止を強化します。

「設定」画面のなかからプライバシーやセキュリティの設定を変更できる箇所を探します。そして、通常よりも厳格な設定に変更にします。たとえば、Firefoxの場合であれば

- 「強化型トラッキング防止機能」を「標準」⇒「厳格」に変更します。
- Firefoxを終了したときに Cookie とサイトデータを削除する設定に変更します。

3. 「設定」変更(その3)広告や追跡をブロックする拡張機能を追加します。

どのブラウザでも、機能を追加する仕組みが備わっています。これを「拡張機能」と呼びます。ブラウザ右上端の設定アイコン(三本線か三点アイコン)をクリックし「拡張機能」の項目から様々な拡張機能を導入できます。

拡張機能のなかで、ウエッブにアクセスしたときの広告を非表示にしたり追跡行為を阻止するなどの機能(下記で紹介)を追加します。ユーザーの位置情報などを把握する商用広告によって収集されたデータを政府が取得してユーザーの監視に利用するケースが米国では報告されています。[2]日本でも官民連携体制が整備されることから、広告関連のユーザー追跡機能のリスクは高まっています。

こうした悪用を防ぐには、ブラウザーに uBlock Origin と Privacy Badger の拡張機能を追加します。uBlock Origin は主に広告をブロックし、Privacy Badger はネット上の行動を追跡する行為をブロックする拡張機能として定評があります。これらに加えて NoScript という拡張機能を導入することでウエッブにアクセスしたユーザーのコンピュータが乗っ取られることを防ぐ効果を高めることができます。

導入方法

Firefox系(Firefox、Librewolf、Mullvad)では下記のサイトから上記の拡張機能の名称で検索してインストールできます。

https://addons.mozilla.org/ja/firefox/

あるいは、設定アイコン⇒「拡張機能とテーマ」から「アドオンを探す」の検索窓で拡張機能を探すこともできます。

Chrome系(Vivaldi)では、Google Chrome ウエッブストアから拡張機能をインストールします。

https://chromewebstore.google.com/

ただし、uBlock Origin は、Google社の方針によって、Google Chrome ではこの機能が十分には利用できません。以下で推奨するように、Google Chrome系以外のブラウザに切り替えることを推奨します。

uBlock Origin「クイックガイド：ポップアップユーザーインターフェース」

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/ublock-origin_quick-guide-popup-user-interface_jp/

(EFF)オンライン追跡は手に負えない状況—Privacy Badger が反撃を支援

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_online-tracking-out-control-privacy-badger-can-help-you-fight-back_jp/

2 https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/

4.2.4. 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

Google Chrome や Microsoft Edge から下記のブラウザへの切り替えを推奨します。ブラウザとしての機能は共通していますが、プライバシーを重視した機能を供えています。パソコンの場合は、下記の公式 web の URL からインストールできます。スマホの場合は、Android であれば、Google Play、iPhone であれば Apple Store からアプリをインストールします。

どれを選択したらいいか迷う場合は、Firefox をとりあえずインストールしてください。

Firefox https://www.firefox.com/ja/

Vivaldi https://vivaldi.com/ja/download/

LibreWolf https://librewolf.net/

Mullvad https://mullvad.net/ja/browser

Tor https://www.torproject.org/

Windows や Mac のユーザー、スマホの Android や iPhone のユーザーであれば、DuckDuckGo ブラウザが利用できます。(Linux ユーザー版はありません)

https://duckduckgo.com/

Chrome から Firefox に引越しするばあい、これまで利用していた Chrome のデータ(ブックマークや閲覧履歴など)を Firefox でも利用できます。下記の解説を参考にしてください。

Chrome から Firefox への移行

https://support.mozilla.org/ja/kb/switching-chrome-firefox

4.2.5. アナログな選択肢：図書館！！

調べ物をする方法として図書館の利用をお勧めします。図書館のメリットは、司書による専門的なアドバイスや検索のサポートが得られること。開架式の書庫であれば、目的の資料だけでなく、思いもかけない興味深い資料に偶然遭遇するというラッキーな体験ができます。本を一冊丸ごと読んで得られる経験はネットでは味わえません。もちろん、ネットなど存在しなかった時代の紙でしか保存されていない資料もあります。図書館は情報の宝庫であることを思い出しましょう。国会図書館の資料もデジタル化されオンラインでアクセス可能な資料が増えています。https://www.ndl.go.jp/

4.3. スマホのセキュリティの見直し

4.3.1. 利用に際してはパスワード入力を必須にします

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ます。

4.3.2. 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ます。

- 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。
- 住所録にアクセスできるアプリを制限する。
- カメラ、マイクは使わないときには off にする。カメラにカバーをする。
- 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。

スマホの設定は複雑でわかりにくいことが多く戸惑います。以下を参考にしてみてください。

(EFF)Android のプライバシーとセキュリティの設定方法

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/eff_android-how-to-get-to-know-android-privacy-and-security-settings/

(EFF)iPhone のプライバシーおよびセキュリティの設定方法

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/effiphone-how-to-get-to-know-iphone-privacy-and-security-settings_jp/

4.4. SNS のリスクを知る

4.4.1. アプリ内ブラウザは使わない

SNS のメッセージ内にリンクが貼られている場合、ウエッブへのアクセスは SNS 内のブラウザが用いられてしまいます。既定のブラウザのプライバシー設定などを厳格にしても、SNS 内のブラウザには適用されず、意図しない個人情報窃取をまねきます。面倒でも SNS 内のリンクはいったんコピーして既定のブラウザを開いてアクセスしてください。

4.4.2. 拡散のアルゴリズム

SNS での拡散は、市民運動や社会運動にとって重要な宣伝手段です。しかし、拡散は SNS のアルゴリズムに依存しており、営利目的のサービスによって与えられたものであることを忘れないでください。街頭でチラシを配ってもほとんどの人は受け取ってくれません。これが本当の拡散の実力です。

なお、SNS がすべて営利目的のアルゴリズムによって運営されているわけではありません。たとえば以下のように非営利で、広告なし、恣意的なアルゴリズムやヘイトの拡散などが少ないいくつかの SNS の一例です。以下の SNS は相互に連携しています。たとえば mastodon に投稿したものを friendica で読んだりフォローすることができます。

mastodon https://joinmastodon.org/ja　X の代替として。

Friendica https://friendi.ca/ 長文の投稿ができます。

Pixelfed https://pixelfed.org/ Instagram の代替として。

PeerTube https://joinpeertube.org/ YouTube の代替として。

4.4.3. フォロワーという「人質」

広告やヘイト、偽情報の投稿にうんざりしていても、フォロワーが多くいる SNS から決別することは容易ではありません。主流の SNS はフォロワーを人質にとって他の SNS への移行を妨害します。しかし、上で紹介したような代替的な SNS でも情報発信することから始めて長期計画で SNS の移行を検討してください。

4.4.4. ジェノサイドやヘイトスピーチに加担する企業のサービスを可能な限り使わない

X、Facebook、Instagram など大手の SNS は、戦争を煽る宣伝の手段になっています。また、ガザのジェノサイドでは、イスラエル国内のパレスチナ系住民の投稿への検閲や拡散抑制措置などが頻発しています。Google、Amazon、Microsoft など大手ビッグテックはジェノサイドを可能にした空爆などの攻撃インフラを提供してきました。いずれも私たちの生活に必須のサービスを提供している企業だからこそ可能な限り代替サービスに切り替えることが大切な意思表示になります。

4.5. VPN

インターネットに接続してサービスを利用するとき、プロバイダーは IP アドレスを利用者に割り当てます。ユーザーがどのような Web サイトにアクセスしたのかなどをすべて記録することも可能で、オンラインでの活動を追跡する手段にもなりえます。VPN(バーチャル・プライベート・ネットワーク)は、この IP アドレスをプロバイダーから隠すことができるサービスです。二つだけ紹介します。

ProtonVPN https://protonvpn.com/ja

MullvadVPN https://mullvad.net/ja/vpn

Mullvadvpn は有料のみ。月 5 ユーロ。月払いが可能で、契約の自動継続はないので、支払わなければ翌月は契約解除になります。試しに使ってみる価値はあります。ProtonVPN は無料もありますが、回線が混みあうことがあります。

VPN によって契約プロバイダーからアクセス先情報などを隠すことができますが、VPN の業者はアクセス先を把握可能です。利用者のプライバシーを最優先とする信頼できる業者を選ぶ必要があります。

VPN の使い方で難しいことはほとんどありません。アプリをインストールすれば使えるようになります。アクセスポイントを自分の居住地とは別の場所にするだけでも居場所を隠す効果はあります。

4.5.1. アナログな選択肢：意外にセキュアな封書での郵送

デジタル化が社会の趨勢になっている現在でも、契約しているプロバイダーにパスワードの再発行を依頼する場合などでは、封書によるパスワード送付が用いられることがあります。役所や金融機関の重要な書類も郵送が一般的でしょう。封書でプライバシー情報を郵送するという方法は、現在でも、オンライン通信にはない秘匿性があります。時間とコストがかかりますが、必要に応じて郵便という手段も選択肢としてあることを念頭に置きましょう。伝書鳩もよい選択肢かもしれませんね。

4.6. 地図 Google Maps から OpenStreetMap へ

スマホの GPS をオンにして、Google Maps で経路情報を表示させながら目的地を目指す、という方法が最も一般的でしょう。しかし、オープンソースの優れた地図 OpenStreetMap を利用することを推奨します。高機能で自分で地図を編集することも可能です。慣れるのにちょっと時間がかかるかもしれませんが、Google に追跡されないことを考えれば、努力は報われるでしょう。

下記に使い方の入門解説があります。

OpenStreetMap

https://learnosm.org/ja/beginner/

4.6.1. アナログな選択肢：紙の地図と方位磁石

紙の地図と方位磁石を使うという人類が長いこと習得してきた能力をデジタル機械の普及によって犠牲にすべきではないでしょう。紙の地図と方位磁石にはデジタルにはない良さがあることも発見してみてください。M.R.オコナー『道を見つける力―人類はナビゲーションで進化した』(梅田智世訳、インターシフト)も是非参考にしてみてください。

4.7. 暗号化サービス

4.7.1. 暗号化メールサービス:Proton と tuta

日本政府は通信事業者に協力させて、通信情報を提供させる体制を整えつつあります。電子メールは、通信回線上では暗号化されていて盗聴が困難ですが、事業者のサーバー上ではデータが暗号化されないまま保管される場合がほとんどです。自分が契約している通信事業者が、ユーザーのプライバシーや通信の秘密の権利よりも政府への協力を優先させる可能性があります。

通信事業者による政府への通信情報の提供を回避する方法として、暗号化メールサービスを利用する、という方法があります。政府も通信事業者自身も暗号化されたデータにしかアクセスできず、暗号を解読することもできません。

Proton Mail

proton スイスに拠点。メールのほか、カレンダー、クラウドサービスや VPN(前述 4.5 参照)など様々な暗号化サービスを提供。 https://proton.me/ja

tuta

tuta ドイツに拠点。メールのほかカレンダーの暗号化サービスも提供。https://tuta.com/ja

暗号化メールにもデメリットがあります。同じサービスを使っていないと暗号化による双方向の通信(エンド・ツー・エンド暗号化)ができません。相手が Gmail など暗号化されていないメールサービスの場合、

Proton や tuta から送ったメールは相手の受信箱に暗号化されずに保管されます。しかし、相手からのメールは暗号化されて Proton や tuta の受信箱に保管されます。受信した相手のメールが保護されるだけでも大きなメリットです。更に Proton の場合は PGP 暗号やパスワード保護機能を使えば外部とも暗号化されたメールのやりとりが可能です。tuta にもパスワード保護機能があります。Proton Mail で PGP を使用する方法

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/proton-mail_how-to-use-pgp/

Tuta Mail で暗号化メールを無料で送信する方法

https://tuta.com/ja/blog/email-encryption-guide-how-send-encrypted-email

4.7.2. 暗号化メッセージサービス：Signal

日本で最もユーザーが多い LINE の場合、2025 年下半期捜査機関等からのユーザー情報開示要請が約 7000 件あり、裁判所の令状に基かない捜査関係事項照会による情報開示が急増しています。[3]Signal は、グループチャット、ビデオ会議、電話機能など、ほぼ LINE と同様のサービスを提供し、使い方も似ており、メッセージの暗号化サービスとして最も定評の高いものです。

https://signal.org/ja/

4.7.3. クラウドデータの暗号化:CryptPad

CryptPad は、文書の作成、表計算、スケジュール管理など様々な作業を暗号化して保管できます。Google Docs で行なっていた作業の多くを CryptPad でもこなすことができます。共同作業も可能です。CryptPad は オープンソースであるため、自分のサーバーにインストールしてサービスを提供できるので、提供サイトが世界中にあります。

https://cryptpad.fr/index.html 開発チームがホスト。

https://cryptpad.org/instances/ 公開されている利用可能な CryptPad の一覧。

4.7.4. 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上で紹介した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 https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/reports/2025h2/

4.7.5. 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などはいずれも技術の仕様を公開するオープンソースです。

4.7.6. 暗号化で注意すべきことは、やっぱりパスワード！

データを暗号化したり、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。パスワード設定のルールを守りをきちんと管理することが必須の大前提です。いかに強固な暗号を用いても、安易なパスワードを設定していたら、全く効果はありません。

4.7.7. 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？

本パンフの冒頭で述べたように、私たちの自覚できない仕組みを通じて私たちの情報が窃取されています。この点の脅威は自覚できないために非常に深刻です。このことを理解した上で、暗号化などの措置を可能な限りとることが大切です。暗号化されたデータは、膨大に収集されても解読できず使い物になりません。そのために、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自体を規制しようとさえしています。児童ポルノ、テロリズム、匿流対策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させるなど、法的な権限の拡大を画策しようとしています。こうした動きは、EUでも具体的な動きになっています。

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断固として反対していく必要があります。

4.8. 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ものです。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。スパイ機関が政府に異論を唱える人たちを監視してきた歴史を踏まえたとき、可能な限り匿名で行動できる手立てを講じることも大切です。とくにメールはアカウントから誰のメールなのかが特定されやすいものです。このメールの弱点をカバーするメールの匿名化サービスをDuckDuckGoなどが提供しています。政府の省庁が提供しているメールマガジンのサービスとかショッピングサイトの登録メールアドレスに匿名化メールサービスを利用することで、自分の本当のメールアドレスを相手に知られない工夫が可能です。

(DuckDuckGo mail)メールボックスを保護しよう：DuckDuckGo Email Protectionのベータ版が、すべてのユーザーに公開された！

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/duckduckgo-mail_protect-your-inbox-with-duckduckgo-email-protection_jp/

4.8.1. アナログな選択肢：買い物は現金で

お財布携帯であれクレジットカードであれ現金以外の支払い方法は、確実に支払い関連データが記録されます。デジタル空間で現金の匿名性に匹敵するプライバシー防御を実現するのは非常に困難です。匿名性に配慮したいのであれば、買い物は原則現金で、という習慣を身につけることも大切です。

4.8.2. アナログな選択肢：マイナカード、マイナ保険証をやめる

マイナンバーカードは所有者のカード利用動向を把握する手段になります。マイナ保険証も医療行為の範囲を越えた医療情報の収集手段になります。収集された情報が将来どのように利用されるのかは法・制度次第ですが、拡大される傾向が顕著です。また、住民サービスを役所に行かずに済ませられるのは便利ですが、行政機関に出むき、役所の実態を知ることは民主主義の基本です。役所で手続をすることは大切な権利行使でもあります。マイナカードを返納し、マイナ保険証ではなく資格確認書とお薬手帳を活用しましょう。詳しくは「共通番号（マイナンバー）いらないネットブログ」 https://www.jca.apc.org/activist/ をぜひごらんください。

4.9. オンライン会議システム：Jitsi-meet

Jitsi-meet は、ZOOM に代替するオンライン会議システムです。20〜30 名程度の会議であれば十分機能しますし、発言者を除いて参加者がカメラを切った状態であれば 50 名を越えても使えます。Zoom とは違い、会議室を設置しているサーバーは独立しており、サーバーの運営主体も様々です。信頼できるサーバーを選択することが重要です。以下のサーバーを推奨します。

開発者サイト
https://meet.jit.si/

JCA-NET https://jitsi-01.jca.apc.org/

Framatalk https://authent.framatalk.org/

Jitsi-meet の使い方については下記の JCA-NET のマニュアルを参考にしてください。
https://jca.apc.org/jca-net サービスについて/オンライン会議システム jitsi-meet マニュアル/

4.10. メーリングリストを Google Groups から Frama Groups に切り替える

メーリングリストサービスの定番になっているのが Google Groups ですが、プライバシーに配慮した優れたメーリングリストサービスがあります。たとえば Frama Groups は脱 Google を提唱して活動しているフランスに拠点を起く Framasoft が提供しているサービスです。

Framagroupeshttps://framagroupes.org/abc/en/

5. 戦争に協力しない、官民連携の情報収集に対抗しよう

5.1. 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らかになっています。

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するジェノサイドに加担する戦争犯罪企業といえます。

他方で、X、Facebook、Instagram などの SNS 企業は、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ポリシーをとってきました。

情報通信関連企業の戦争への加担は米国のグローバル企業に限りません。たとえば日本の楽天はドイツの兵器産業「ヘルシング」との提携を発表[4]し、憂慮する企業が楽天への出店をボイコットしています。戦争に加担する企業のサービスを、今まで通り利用することは、政府の戦争やスパイ活動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。戦争や監視社会に加担する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。

5.2. Windows をボイコットするのは難しくても、できることがある

Google や Amazon と違って、Microsoft 社は Windows というパソコンの基本ソフト(OS)を提供しており、Windows そのものをボイコットするのは大変かもしれません。しかし、仕事で標準的に用いられている Microsoft 社の 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 に切り替えることなら不可能ではありません。

https://ja.libreoffice.org/

また、CryptPad(上述の「暗号化サービスを使う」を参照)に切り替えるという選択肢もあります。

6. 仲間作りが最も大切　まず議論を

政府のスパイ機関=国家情報会議/情報局の創設では、官民連携が強化され、網羅的で強力な情報収集の体制がとられることが計画されています。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皆さんは、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を一緒に取り組み、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官民連携しつつ、また米国など海外の政府とも連携して、私たちの情報をどのように収集しようとしているのかについて、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の設定、パスワードの設定など、面倒なことですが、とても大切なことなので、皆で検討しあうことで、この厄介な取り組みにチャレンジしてください。利用するサービスを再検討し、可能なところから、プライバシーに配慮し情報窃取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。

7. よくある質問

7.1. 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。たとえば、世界中を網羅している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、内容を把握できない仕組みになっています。そのために、政府は民間の通信事業者に協力させてデータを取得する以外に選択肢がなくなっています。サーバやスマホ、パソコンのデータを暗号化することは、こうしたで政府の情報収集への有効な対抗手段です。

7.2. 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、たとえば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。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

4 https://jp.reuters.com/economy/ZKGNP2C7YNI53EI7HUU7FZGFBE-2026-08-17/

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るので、万人向けのオールマイティな対策はありません。

7.3. 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、確実にあなたについて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。もしあなたが選挙で投票に行くのであれば、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、数百人のデモに参加したことがあるのであれば、そんな小さな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、行動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も守ることに繋がる、ということを思い出してください。

7.4. 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。

7.5. 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、二三人でも構わないの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。

このパンフの PDF 版は下記からダウンロードできます。またこのページには、パンフに記載できなかった追加情報や解説なども順次掲載します。ぜひご活用ください。

https://jca.apc.org/jca-net の取り組み/スパイ・監視と対抗するために―一人でもできる/

著作者 JCA-NET　発行 2026 年 9 月 20 日

無料。気に入ればぜひカンパをお寄せください。このパンフレットは JCA-NET の会員の会費とみなさんのカンパで作成されています。

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。

JCA-NET 担当者 としまる 070-5553-5495 toshi@jca.apc.org

https://jca.apc.org