私たちのサイバーセキュリティを! 共謀罪で萎縮しないための実践セミナー

小倉利丸

2017 年 12 月 20 日

1 はじめに

共謀罪反対運動は、下記のような批判を共謀罪に投げかけてきました。

「普通の市民団体や組合が組織的犯罪集団に！！政府・法務省は、共謀罪はテロリスト集団や組織的犯罪集団が対象であり、普通の団体には適用されないといっていますが、これはウソです。法案には組織的犯罪集団とはどういう集団なのかなどの規定はありません。市民団体、組合、会社などの団体のメンバーが一度共謀したと判断されればその団体は組織的犯罪集団とされます。共謀罪は思想・意見・言論を処罰し、結社＝団体を規制する、現代の治安維持法です。(4 月 6 日 日比谷集会呼びかけ)」

わたしは、こうした反対運動が提起した共謀罪反対の危惧を、共謀罪推進側が言うような、単なるプロパガンダだとは考えていません。皆さんもまたそうだと思います。わたしたちが市民的な自由や人権のために闘えば闘うほどわたしたちは組織的犯罪集団とみなされることになる。そうした環境のなかにいるのだ、ということを冗談でも誇張でもなく受け止めて、闘い方に創意工夫をこらすことが必要になってきたのです。

1.1 わたしは何をやってきたか

共謀罪が成立して以降、上記のような危惧を抱いてわたし自身がやったことは下記です。(ネットやパソコンに関連して)

- パソコンのデータのセキュリティの強化。(ハードディクスの暗号化)
- クラウドサービスの見直し。(Dropbox から有料の Tresorit に変更)
- モバイル環境の見直し (タブレットの暗号化)
- 暗号化メールサーバのサービスの利用
- 匿名性を重視したブラウザの導入
- VPN の導入 (有料)
- 一部のメーリングリスト管理のサーバの引越しと利用頻度の低いメーリングリストの廃止
- 共謀罪を念頭にしたプライバシーの権利を具体的に防衛するツールの紹介サイトの開設
- プライバシーとセキュリティについての実践セミナーの開催

まだ取り組めていないこと

- まだ引越しできていないメーリングリストがある
- プロバイダーの見直し作業 (よりプライバシーの権利を重視するプロバイダーへの変更)
- 何年も使用していない古いパソコンや記憶媒体のデータの保護措置

まだまだ不十分なのですが、できるところから、ネットの情報を調べたり、セキュリティの本を読んだり、パソコンやネットの初歩的な技術を学んだりしながら、右往左往しながら取り組んできました。

こうしたことは反対運動に取り組んでこられた皆さんそれぞれがなさっていることと思います。本日の集会はこれまでの対抗的な取り組みの知恵を出し合い、知識を共有しながら更に強固な私たちのプライバシーの権利を防衛するための相談の集まりにしたいと思います。

1.2 チェックリストに記入してください

私たちは、共謀罪が成立してしまった結果として、普通の市民団体や組合が組織的犯罪集団とみられるようになってしまった、少なくとも、捜査機関はそうした疑いの目で、私たちに対する捜査を行なうことが正当化されてしまっているのだ、という認識に立たなければならないということになります。憲法に保障された表現の自由、集会・結社の自由、思想信条の自由、これらの権利を行使することが犯罪とされてしまったのです。しかし、いかに権力者が犯罪とみなそうと、私たちは、自らの権利の犯罪化に抵抗し、権利を防衛しなければなりません。共謀罪が廃止されるまで、私たちが萎縮しないためにも是非とも必要なことは、相談は続けるけれども、その内容への監視は権利侵害として断固として退ける！ということです。

そこでまず、お配りした「チェックリスト」の用紙をごらんください。話しを始める前に、このチェックリストに記入をしてみてください。

2 必須の取り組みベスト 3

2.1 名簿のプライバシーは運動の命である

共謀罪容疑での捜査は、なによりも人間関係の把握から始まります。ですから名簿の管理とセキュリティは何を置いても、お金をかけてでも実施すべきことです。企業の場合であれば、「顧客の個人情報」が外部に漏洩したら、企業の信用は喪失するように、わたしたちのとっては、会員名簿、集会参加者名簿、ニュースレターなどの郵送や電子メールのアドレス、会費やカンパの振込記録は、捜査当局にとっては共謀の容疑者名簿になりますから、そのセキュリティは共謀罪としての摘発を阻止する上で最も大切なことになります。

名簿のセキュリティを守る方法はただ一つしかありません。それは、名簿のデータを強固な暗号で守ることです。そして、こうしたデータの暗号化は今すぐにでも取り組める比較的簡単なものです。(無料で信頼性のあるソフトがウィンドウズでもマックでも入手可能です)

2.1.1 署名簿は必ず自己情報コントロール権を明示して提出すること

補足ですが、署名運動の際に、政府などに提出する署名簿は、デジタル化させない、複写させない、閲覧範囲を明確に指示するなどして、個人情報の二次利用をさせない工夫が必要です。もしこうした条件を先方が承諾しないときは提出すべきではないでしょう。

署名に書く名前と住所は、そのまま PDF ファイルなどでデータ化が可能ですし、文字情報に変換することも可能です。(こうした作業は外注するでしょうから役人たちの労力を使うことはないでしょう)1G で PDF

ファイル 3000 枚程度が収納できるとすれば、1 枚 5 人の署名用紙なら 15000 人分になります。100 万人分を 1T バイト程度、数千円のハードディクスに収めることができてしまう。これが文字データなら A4 で 40 万枚くらいは収納できる。数百円の記憶媒体で済むはなしです。いったんデータ化されればどのように共有されても私たちはそれを把握することはできません。署名運動は紙を前提にする時代ではない、という深刻なリスクを負うのだということを踏まえて署名運動を効果的に行なう作戦と知恵が必要です。

2.1.2 名前と住所だけで全ての個人情報が把握される危険性を理解すること

データ化された名前と住所さえあれば、そこからありとあらゆる個人情報を引き出すことは技術的に容易です。現在の法的な制約があっても、そのような制約が 5 年後、10 年後にどうなるかわからない。技術は急速に個人情報の大量収集と解析が可能な方向で「進歩」しています。こうした現実を見すえて、自己情報コントロールの権利をきちんと担保しないと、政府が「犯罪組織」とみなす可能性のあるわたしたちが提出する署名のデータは、逆手にとられかねない。これが共謀罪が成立してしまった現在のリスクです。

2.2 相談の権利を防衛する――メールとメーリングリストの管理

メールや SNS を使った相談は、共謀の容疑段階で捜査機関が様々な手法で監視し、情報を収集する対象になります。こうした監視のリスクがあるなかで自由な議論などはできないでしょう。自由闊達な議論をするためには、監視のリスクを排除してわたしたちのコミュニケーションのセキュリティを防衛しなければなりません。特に、メーリングリストは、その管理サイトに参加者全員のメールアドレスや個人情報が蓄積されており、それらをメーリングリストのサービス側は読むことができます。誰が相談に参加したのかが把握されて、捜査機関がこれを共謀の有力な証拠としてしまう危険性があるのです。こうした危険性を回避するには、以下のような取り組みが必要です。

- プライバシーの権利をきちんと保護するプロバイダーを選ぶ。
- メールサーバが暗号化されており、プロバイダーでも内容を読むことができない暗号化サービスを選択すること。
- メーリングリストの管理サーバを海外に移すこと。最低でも、管理名簿にはメールアドレス以外の余計な個人情報を残さないこと、投稿アーカイブは使わないこと。

2.3 ウエッブの匿名化

ネットで情報収集することはあたりまえになっています。ちょっとした調べ物をすることを「ググる」というように、Google は検索の代名詞になっています。しかし Google は膨大な個人情報を収集し、それを米国の諜報機関に提供していたことが知られています。

また、ネットのアクセス先 (政府のサイト、警察庁や自衛隊のサイト、民間企業など) は、わたしたちが何者であるのかをアクセス情報から最大限取得しようとします。こうした個人情報を収集することから私たちの身元をきちんと秘匿することは、わたしたちの重要なプライバシーの権利の防衛になります。たとえは以下のようなことが可能です。

- 使用しているブラウザ (インターネットイクスプローラなど) の設定をよりプライバシー強化の方向で修正する。(Javascript やクッキーの設定を見直す)

- Tor ブラウザを使う。(これが最も好ましい)

2.4 弁護士の事務所やパソコンのセキュリティの見直しを

共謀罪の導入によって、救援活動のありかたも見直しが迫られていると思います。弁護士の活動も従来以上にそのセキュリティの防衛に取り組む必要があります。

依頼者のセキュリティをきちんと保障できる技術的な前提を確保することが、弁護士にとっても人権を守るための基本条件になります。この点を踏まえて、日弁連や共謀罪対策弁護団あるいは刑事弁護に取り組む弁護士団体は組織として、セキュリティ防衛に取り組むことと、その取り組みを是非外部にもアピールしてほしいと思いますし、そうした取り組みを私たちもまた弁護士や弁護士団体に要請することが大切だと思います。(議員についても同様のセキュリティ対策が必要でしょう)

3 日本でも第二第三のスノーデンや内部告発者が登場できる環境を構築する

今回は概略を指摘するだけです。防戦一方ではなく、内部告発者が自分のプライバシーのリスクを負わないで汚職や腐敗、不正な企業の活動の情報を提供できる環境を整備することも大切です。New York Times や Gurdian など海外の主要なメディアが導入している SecureDrop という仕組が日本ではまだ導入されていません。こうした仕組の導入が是非とも必要でしょう。

4 いくつかの関連事項

4.1 共謀罪の何がリスク要因か

共謀罪は、残念ながら、安倍政権の強行突破によって、成立してしまった。共謀罪への危惧は、一言でいえば、実行行為とは関係なく、刑法で懲役 4 年以上の刑を定めた犯罪に関わる「計画」と捜査当局が判断した事柄を網羅的に罪に問うというものだ。物品や資金の調達だけでなく場所のなど捜査当局が「準備行為」とみなせば何でも含まれる。明日の行動のために今日やる準備といった短期的なことがらだけではなく、今は何ら犯罪とは関係ないと思われる言動も将来の様々な言動と関連づけられて、共謀罪の証拠の一部を構成することになるかもしれない。10 年、20 年後に実行されるかもしれないような大それた事案 (たとえば「内乱罪」などはその例かもしれない) も念頭に、権力者はその言動を子細に監視し、情報収集できる法的な枠組を獲得したのだ。

4.2 治安維持法の時代との違い

共謀罪は治安維持法の再来として批判されてきたが、実態は戦前とはかなり違ってきている。特に、インターネットなどのコンピュータを介したコミュニケーションが与える影響は戦前にはないものだ。実世界の私たちの行動にへばりついて、四六時中監視することはさほど意味のあることとは考えられない。私たちがどこにいるのかは、尾行しなくても常時持ち歩くスマホの GPS が教えてくれる。車に載れば N システムが追跡する。ネットのメールや SNS でのコミュニケーションは通信事業者のログでほぼ把握できる。ウエッブで内閣、

警察、自衛隊から企業までどこをチェックしても、必ず相手のサーバはこちらの行動を伺う技術を持っている。街中の監視カメラも次第に、ネットワーク化され、顔認証システムが搭載され、データベースと連動するようになっている。

膨大なデータを処理するのも人間ではなくコンピュータだ。たった 1 ギガのメモリに日本語 A4 で 40 万枚から 100 万枚もの文書が収録できる。8 ギガのメモリがたったの 1000 円程度である。しかも、政府やマスコミが警鐘を慣らす「サイバー攻撃」なるものの攻撃者になっているのは、どこの国でも政府、警察、軍隊であり、その攻撃の的は国内にいる反政府運動活動家や人権活動家なのだ。

4.3 個人情報の監視・盗聴リスクは飛躍的に大きくなっている

戦前も戦後も、日本であれ国外であれ、反政府運動 (ささやかな住民・市民の異議申し立てであれ全国規模の運動であれ) の参加者の個人情報を政府や捜査機関、諜報機関は収集しようとしてきた。データが紙で管理されていた時代と異なり、コンピュータがネットワーク化され、さらに膨大な個人情報が官民問わずデータベース化されている時代では、名前と住所のデータは、これを踏み台にして、住民票の取得やマイナンバーの取得などから、芋蔓式に大量の個人データを収集することが可能になっている。捜索・押収令状によって、パソコンがまるごと押収されることが当たり前になっている現状では、会員名簿やニュースレターの購読者名簿、集会参加者名簿などは、大量の情報収集を可能にする糸口となる。

日本の法体系では、プロバイダーへの捜査機関などの情報提供については、守秘義務の例外として幅広く捜査に協力し、ユーザのプライバシーの権利がきちんと守られないとしかいえないようなプライバシーポリシーを掲げているところも多い。私たちの知らないうちに、メールが盗み読みされたり、クラウドに保存されているデータが読まれているかもしれない。こうしたリスクにきちんと対応することが、憲法が保障しているわたしたちの言論、表現、結社の自由や検閲されない権利を防衛するために是非とも取り組まなければならないことである。

企業では、こうした個人情報 (企業ならさしずめ顧客データというだろうが) のセキュリティは何にもまして重要事項という認識があるが、プライバシーや反監視運動、共謀罪や秘密法に反対してきた市民運動など草の根の運動は、なかなかセキュリティを防衛するための具体的な方策をとれるところまで手がまわっていないところも多いと思う。弁護士や労働組合でもそうかもしれない。盗聴法、共謀罪、秘密保護法、これらの悪法に対抗するためには法律の廃止は必須だが、私たちの権利を防衛するための技術的な対抗手段が可能だということを是非知ってもらえればという思いを込めて、このサイトが作られている。

4.4 情報を渡さない!

このような時代に私たちが自由を獲得するためには、少なくとも彼らに情報を渡さないことが一番重要なことになる。ここでは技術的に詳細なことを書く余裕はないが、たとえば次のようなことを是非実践して欲しいと思う。

- ガサ入れされても「サイバー攻撃」されてもデータを読まれないために、重要なデータを暗号化すること。
- 情報収集のためのネットアクセスを追跡されないように、匿名でのネット利用を工夫すること。
- プロバイダーのメールサーバに蓄積されたメールは暗号化されていない。重要なメールのやりとりには、暗号化されたメールサーバのサービスを使うこと。

などだ。

4.5 世界中の人々が政府や企業から私たちの自由を防衛するために工夫しはじめている

上記のようなことは購入したパソコンをそのまま使うことでは実現できない。パソコンやスマホのログインパスワードは容易に解除できるので権力から私たちのセキュリティを防衛する手段にはならない。インターネットの回線もできれば、暗号化された回線サービスを使う方がいい。こうしたいくつかの工夫は、簡単なものからやや難易度が高いものまである。こうしたセキュリティ防衛手段は、とっくに企業などは実施しているあたりまえのことになっている。世界中で、人権弾圧の厳しい国では、こうしたノウハウを活動家、人権団体、弁護士たちが共有し、それをネットの技術者たちが支援するという体制が工夫されてもきている。スノーデンの内部告発以来監視問題への関心は高まったが更にトランプ政権成立以降、暗号化メールサービスを使う人たちが急増しているともいう。しかし、日本での取り組みはまだ十分ではない。

4.6 ant-surveilance のウエッブ紹介

https://antisurveillance.researchlab.jp
上記のサイトの目次の一部を紹介します。

4.6.1 共謀罪に対抗して私たちの自由を防衛するために (α版)

- ディスク暗号化/Cryptomator
- ディスク暗号化/Veracrypt
- ブラウザ/Tor
- メール/Protonmail
- メール/Protonmail/セキュリティ
- メール/メーリングリストのリスク回避
- 内部通報サイトの構築 (SecureDrop)
- 資料/Tor プロジェクト解説
- 資料/どのようにして Google を捨てるか
- 資料/なぜ ProtonMail は Gmail より安全か

4.6.2 セキュリティのための始めの一歩——米国電子フロンティア財団の文書の翻訳

- ソーシャルネットワークでの防衛策
- リスクを検証する
- 抗議行動に参加する (国際版)

問い合わせ先小倉利丸 070-5553-5495 ogr@nsknet.or.jp