

이 문서는 일본어 원문을 바탕으로 번역된 것이다. 기계 번역(DeepL)을 사용하여 번역되었으므로 부정확한 부분이 포함되어 있을 수 있다.

스파이 및 감시에 대응하기 위해

혼자서 할 수 있는 일부터 동료들과 함께 할 수 있는
일까지

JCA-NET jca.apc.org



Designed by [macrovector](#) / [Freepik](#)

목차

1.		2
1.1.		2
1.2.		2
1.3.		3

1.4.		3
1.5.		3
2.		3
3.		4
4.		4
4.1.	비밀번호(, 패스프레이즈) 설정을 재검토한다.....	4
4.2.		6
4.3.		9
4.4.	SNS의 위험성 파악하기.....	9
4.5.	VPN.....	10
4.6.	지도 Google Maps에서 OpenStreetMap으로.....	11
4.7.		11
4.8.		13
4.9.	온라인 회의 시스템: Jitsi-meet.....	14
4.10.	메일링 리스트를 Google Groups에서 Frama Groups로 전환.....	14
5.		14
5.1.		14
5.2.	Windows를 보이콧하는 것은 어렵더라도, 할 수 있는 일이 있다.....	15
6.		15
7.		15
7.1.		15
7.2.		15
7.3.		16
7.4.		16
7.5.		16

1. 첩보 기관 창설과 사이버 전쟁·감시 사회화

1.1. 법과 제도가 바뀐다

일본 정부는 인터넷상의 우리 통신 정보를 수집할 수 있게 하는 새로운 법 제도와 정부 조직의 창설을 잇달아 추진해 왔습니다. 현재 정부가 목표로 하고 있는 것은,

- 정부 및 지자체가 보유한 개인정보를 본인의 동의 없이 광범위하게 이용할 수 있는 체제를 구축하는 것
- 민간이 보유하고 있는 개인정보를 정부도 이용할 수 있도록, 민간 통신 사업자 등으로부터 협력을 이끌어내는 것

등입니다.

헌법에서는 통신 비밀의 권리가 보장되고 검열도 금지되어 있으며, 우리의 기본적 인권을 보호하는 다양한 법과 제도도 존재합니다. 그러나 안타깝게도 이러한 권리를 무력화시키는 새로운 법과 제도가 잇달아 도입되어 왔습니다. 예를 들어, 2026년 국회에서는 미국의 CIA나 NSA에 필적하는 첩보 기관을 목표로 하는 국가정보회의/정보국이 설치되었으며, 동시에 본인의 동의 없이 개인정보를 수집·이용할 수 있도록 하는 개인정보보호법 개악안도 통과되었습니다. 국가 안보를 우선시하는 특정비밀보호법, 근로자들의 신원 확인을 위한 보안 심사 제도, 마이넘버/카드의 활용 확대 등도 시행되어 왔습니다. 또한, 스마트폰을 통한 무현금 결제의 보급부터 거리 곳곳에 설치된 AI 탑재 감시 카메라에 이르기까지, 사람들의 일상 행동을 파악하는 기술이 비약적으로 고도화되었습니다. 게다가 일본 전역에 건설이 진행 중인 데이터 센터에는 전 세계에서 방대한 양의 개인정보가 축적되고 있으며, 장래에 이러한 정보가 고도화된 감시 사회나 전쟁의 수단으로 이용될 위험성도 부정할 수 없습니다.

1.2. 정보 수집·감시는 우리 주변에 있다

정부와 민간 기업은 우리가 일상적으로 이용하는 통신 인프라를 통해 개인정보를 수집합니다. 이메일,

SNS, 온라인 쇼핑, 웹 검색, 날씨 및 지도, 동영상 시청 및 공유 등 일상생활에 필수적인 활동들이 동시에 우리의 동향을 파악하는 수단이 되고 있습니다. 따라서 이러한 온라인 일상생활을 재검토하고, 정보가 수집되지 않도록 대책을 마련하며, 감시 사회의 피해자나 가해자가 되지 않도록 노력하는 것이 중요합니다.

1.3. 자각 증상이 없다

우리 인간의 오감으로는 이해할 수 없는 이면에서 방대한 데이터 수집이 이루어지기 때문에, 이를 실감할 수 없다는 큰 문제가 있습니다. 실감할 수 없기 때문에, 의도치 않은 정보 수집을 저지하거나 회피하는 것도 매우 어렵습니다. 실감에만 의존해 사생활이나 개인의 권리를 지키는 것도 쉽지 않습니다.

우선 우리가 해야 할 일은 정보 수집을 가시화하는 것입니다. 가시화함으로써 원치 않는 정보 수집을 차단하기 위해 어떻게 해야 할지, 그 구체적인 방안도 도입할 수 있게 됩니다.

1.4. 부작용은 평생 지속된다

수집된 개별 정보는 사소하고 개인을 특정할 수 있다고 단정할 수 없는 것일 수도 있기 때문에, 개인정보로서 중요하게 여겨지지 않을 가능성이 있습니다. 그러나 다양한 사소한 정보가 방대하게 수집됨으로써 개인을 특정할 수 있게 되거나, 중요한 개인정보와 연계되어 우리의 일생을 감시하기 위한 기반이 되기도 합니다. 일단 수집된 정보를 되찾는 것은 불가능합니다. 수집된 개인정보가 초래하는 부작용은 평생 지속될 수도 있습니다.

1.5. 이 팸플릿에 대하여

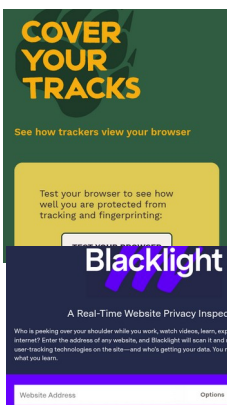
이 팸플릿에서는 우선, 어떤 데이터가 우리의 실감을 비껴가 눈치채지 못하는 사이에 수집되고 있는지에 대해 시각화할 수 있는 방법을 소개합니다. 그 후, 어떤 대책을 세워야 하는지, 어떤 대응 수단이 있는지 등, 감시 사회에서 살아가는 우리가 위축되지 않고 정보 발신을 지속하기 위한 기본적인 사고방식을 제시합니다.

이 팸플릿에서는 정보 도용을 피하고, 인권과 사생활을 더욱 중시하는 대안적인 도구를 소개합니다. 여기서 소개하는 도구의 선정 기준은 다음과 같습니다.

- 오픈소스/자유 소프트웨어여야 합니다. 기술 사양을 공개하지 않는 영리 목적의 서비스는 원칙적으로 소개하지 않습니다.
- 전쟁에 협력하는 기업의 서비스에 대한 대체 서비스 소개.
- 스마트폰이나 컴퓨터에는 다양한 OS가 사용되고 있습니다. 가능한 한 어떤 기기를 사용하더라도 활용할 수 있는 도구를 소개합니다. (일부 예외가 있습니다)

이 팸플릿에는 기술적으로 어려운 내용도 포함되어 있지만, 이해하기 어려운 부분은 건너뛰어도 괜찮습니다. 페이지 순서대로 읽을 필요는 없으니, 할 수 있을 것 같은 부분이나 관심 있는 부분부터 시작해 보세요.

2. 데이터 수집을 실감해 보기



브라우저를 사용하여 여러분이 어떤 웹사이트에 접속한다고 가정해 봅시다. 이때, 여러분 스스로는 실감하지 못하지만, 상대방 사이트가 여러분에 대한 다양한 정보를 수집합니다. 그 내용은 놀라울 정도로 많습니다. 어느 정도 어떤 데이터가 브라우저를 통해 상대방에게 파악되고 있는지는 아래 사이트에서 확인할 수 있습니다.

<https://coveryourtracks.eff.org/>



Blacklights 사이트는 접속한 사이트의 URL 을 스캔하여, 해당 사이트에서 사용되고 있는 사용자 추적 기술과 누가 여러분의 데이터를



수집하고 있는지 밝혀줍니다.

<https://themarkup.org/blacklight>

Gmail이나 Google 서비스를 자주 이용하신다면 Google의 개인정보 처리방침은 꼭 읽어보셔야 합니다. 끝까지 다 읽으려면 상당한 노력이 필요하지만, Google이 얼마나 많은 개인정보를 수집하고 있는지 설명되어 있습니다.

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

이 개인정보 처리방침을 읽고 Google 서비스에서 최적의 개인정보 보호 조치를 취하기 어렵다고 판단되는 경우에는, 본 팸플릿에 소개된 대체 도구로 전환하는 것을 권장합니다.

이메일의 경우, 평소에는 숨겨져 있는 ‘이메일 헤더’를 확인하면 많은 정보를 알 수 있습니다. 다만 헤더 정보는 기술 용어가 많아 이해하기 어려우므로 아래 사이트 등을 참고하시기 바랍니다. 일본 데이터 통신 협회 ‘이메일 헤더 정보 확인 방법’

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

또는 오른쪽의 해설서를 참고해 보시기 바랍니다. 마스이 토시카츠 『이메일 기술 교과서』 쇼에이샤.



3. 정보 수집 및 정보 조작의 수단이 되는 것은 무엇인가

우리의 데이터를 수집하기 위한 수단은 다음 중 어느 것입니까?

- 스마트폰이나 컴퓨터를 이용한 통신(스마트폰 결제, SNS, 이메일, 웹 검색 등)
- 정부·지자체가 보유한 개인 데이터(마이넘버와 연동된 데이터, 운전면허증, 범죄 이력, 민간 기업에서 취득한 개인 데이터 등)
- 금융기관이나 의료기관이 보유한 개인 데이터
- 거리 곳곳에 설치된 감시 카메라
- Wi-Fi 라우터나 전력 스마트 미터 등 사물인터넷(IoT)이라 불리는 기기

이러한 정보 수집 및 정보 조작의 통로는 정부 정보기관도 활용합니다. 첩보 기관은 정부가 보유한 정보를 공유하고, 민간 정보에 대해서도 입수할 수 있는 법적·제도적 권한을 확보합니다. 동시에 SNS 인플루언서 등을 동원해 교묘한 정보 조작이나 선동을 조직하기도 합니다. EU를 포함해 많은 민주주의를 표방하는 국가들에서도 국가 안보상의 정보 수집 및 정보 조작에 대해서는 사생활 보호권 등 인권 보호가 미치지 않는 예외로 간주되는 경우가 일반적입니다.

이것에서 알 수 있듯이, 우리가 일상생활에서 가장 빈번하게 사용하는 스마트폰이나 컴퓨터가 정부에 의한 정보 수집 및 정보 조작의 최대 진입점이 됩니다. 그렇기 때문에 이 정보 수집 및 정보 조작의 진입점을 가능한 한 차단하는 것이 중요합니다.

4. 무엇을 할 수 있을까

메시지를 주고받거나 사이트에 로그인할 때는 ID와 비밀번호의 조합을 통해 사칭이나 정보 도용을 방어하고 있습니다. 비밀번호(패스프레이즈)는 우리의 통신 비밀을 보호하는 가장 기본적이고 필수적인 조건입니다.

4.1. 비밀번호(패스프레이즈) 설정을 재검토하기

계정이나 로그인 ID는 제3자에게 알려질 가능성이 있어 이를 비밀로 유지하는 것은 현실적으로 어렵습니다. 이 계정이나 ID를 보호하는 유일한 수단은 비밀번호(패스프레이즈)입니다. 패스프레이즈는 여러 단어를 조합한 것을 말합니다. 본 팸플릿에서는 패스프레이즈를 포함한 의미로 ‘비밀번호’라고 표기합니다. 만약 정부 정보기관 등이 계정(ID)과 비밀번호의 조합을 파악하게 되면, 이메일 도청, 사칭, 주소록 등 데이터 탈취 등 무엇이든 할 수 있게 됩니다. 나아가 악성코드를 심는 등 심각한 공격에 노출될 위험도 있습니다. 비밀번호 관리는 필수적인 중요 사항입니다. 강력한 암호화 서비스 등을 이용하고 있는 경우라도 비밀번호 관리를 소홀히 하면 암호화의 효과가 없다는 점을 충분히 이해해 주십시오.

4.1.1. 비밀번호 설정 시 반드시 다음 규칙을 준수해 주십시오

- 같은 비밀번호를 여러 곳에 재사용하지 마십시오.
- 본인의 이름, 생년월일, 전화번호, 주소, 혹은 1234 나 abcd 등 추측하기 쉬운 것, 사전에 수록된 단어를 그대로 사용하는 것은 피하십시오.
- 위의 조건을 충족한 상태에서, 최소 18자 이상이어야 합니다.

4.1.2. 비밀번호 관리에 어려움을 겪을 때 어떻게 해야 할까요?

위의 조건을 충족하는 비밀번호를 자신의 기억력에만 의존하여 여러 개를 관리하는 것은 거의 불가능합니다. 신뢰할 수 있는 비밀번호 관리 소프트웨어를 이용하면, 수많은 복잡한 비밀번호를 중복 사용하지 않고도 쉽게 관리할 수 있습니다. 정평이 나 있는 소프트웨어로는 다음과 같은 것들이 있습니다.

관리 소프트웨어	설명
 Bitwarden https://bitwarden.com/ja-jp/	자세한 설명은 아래를 참조하십시오. https://bitwarden.com/ja-jp/help/
 KeePassXC https://keepassxc.org/	아래에 입문 매뉴얼의 일본어 번역본이 있습니다. https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/keepassxc_gettingstarted/

4.1.3. 지문 인증, 얼굴 인증은 사용하지 마세요

비밀번호 입력이 번거로워서 얼굴 인식이나 지문 인식을 사용하고 싶을 수도 있습니다. 하지만 이러한 방식은 본인의 의사에 반하여 이용될 우려가 있으므로 권장하지 않습니다. 수사 기관이 법원의 영장을 발부받아 스마트폰의 얼굴 인식 등을 강제로 이용한 실제 사례¹가 있습니다.

4.1.4. “아날로그적인” 대안: “요령을 발휘해 종이에 적기”

무분별하게 비밀번호를 재사용하는 것보다는, 비밀번호 힌트를 적어둔 종이를 자신만 아는 곳에 은근슬쩍 숨겨두는 편이 더 안전할 수 있습니다. 진짜 비밀번호를 자신만의 규칙에 따라 약간 수정해 공개적으로 붙여두는 방법도 있습니다. 비밀번호 수가 적은 경우, 다루기 힘든 비밀번호 관리 소프트웨어 사용법을 애써 익히는 것보다, 18자 비밀번호를 중복 사용하지 않고 철저히 관리하는 아날로그 방식이 보안상 더 효과적일 것입니다. 이러한 방법은 불특정 다수가 볼 수 있는 장소에서는 권장하지 않습니다.

¹(아사히) “강제적인 스마트폰 얼굴 인식” 경찰 수사의 새로운 기법… “과도하다”는 우려도 2026년 8월 12일
<https://digital.asahi.com/articles/ASV7Y34MQV7YPTIL014M.html>

4.2. 브라우저

4.2.1. 브라우저란, 그 역할은 무엇인가

인터넷상의 다양한 웹 페이지에 접속하기 위해 필수적인 소프트웨어는 일반적으로 ‘브라우저’라고 통칭되며, 여러 종류가 있습니다. 예를 들어, Google Chrome, Microsoft Edge, Firefox, Safari 등이 있습니다. Google에서 검색하거나 Amazon에서 쇼핑을 하거나, Yahoo에서 뉴스를 읽거나, YouTube에서 동영상을 보거나, Gmail 이메일을 확인하는 것도 모두 브라우저를 통해 이루어지는 일입니다. 때로는 X나 인스타그램 같은 SNS나 줌(Zoom) 회의도 브라우저를 통해 접속하는 경우가 있습니다. 이런 의미에서 브라우저는 인터넷에 연결하여 소통할 때 필수적인 만능 도구라고 할 수 있는 역할을 담당합니다. 앞서 소개한 것처럼, 브라우저를 통해 실감이 나지 않는 형태로 많은 데이터가 제공되기도 하므로, 개인정보 보호를 중시하여 은밀한 트래커(추적자)를 차단하는 등의 기능을 갖춘 브라우저를 선택하는 것은 매우 중요한 일이 됩니다.

4.2.2. http와 https

웹 URL에는 http로 시작하는 경우와 https로 시작하는 경우 두 가지가 있습니다. http 사이트에 접속할 경우, 통신 경로상의 비밀번호나 신용카드 번호 등 모든 데이터가 제3자에게 도청될 위험이 있습니다. 반면 https의 경우, 통신 경로상의 데이터가 암호화되므로 도청 위험은 현저히 낮아집니다. http로 개설된 웹사이트 운영자는 가능한 한 사이트를 https로 전환하는 절차를 밟아 주십시오.

어쩔 수 없이 http 사이트에 접속해야 하는 경우에는, 항상 통신 내용이 제3자에게 감시당하고 있다고 생각하고 행동해 주십시오.

4.2.3. (당장 취할 수 있는 조치) 브라우저의 ‘설정’을 재점검하여 불필요한 데이터를 상대방에게 제공하지 않도록 주의하십시오.

브라우저의 ‘설정’ 화면을 엽니다. ‘설정’ 화면은 브라우저 우측 상단의 세 줄이나 세 개의 점과 같은 알아보기 어려운 아이콘을 클릭하면 표시되는 메뉴 목록에서 찾을 수 있습니다.

1. ‘설정’ 변경(1) Google이나 Bing 등에서 개인정보 보호를 중시하는 검색 엔진으로 전환합니다. .

검색 행위는 거짓말을 할 수 없기 때문에, Google과 같은 검색 서비스는 검색 행위를 통해 우리의 관심사를 파악하려고 합니다. 검색 엔진을 개인정보 보호를 중시하는 것으로 바꾸는 것은 정보 수집에 대항하는 가장 간단한 방법이 됩니다. 브라우저의 ‘설정’ 메뉴에서 ‘검색’ 항목을 찾아 ‘기본 검색 엔진’을 다음 중 하나로 변경합니다.



DuckDuckGo <https://duckduckgo.com/>



ecosia <https://www.ecosia.org/>



Startpage <https://www.startpage.com/>

2. ‘설정’ 변경(2) 추적 방지를 강화합니다.

‘설정’ 화면에서 개인정보 보호 및 보안 설정을 변경할 수 있는 항목을 찾습니다. 그리고 평소보다 더 엄격한 설정으로 변경합니다. 예를 들어, Firefox의 경우

- ‘강화된 추적 방지 기능’을 ‘표준’ ⇒ ‘엄격’으로 변경합니다.
- Firefox를 종료할 때 쿠키와 사이트 데이터를 삭제하도록 설정을 변경합니다.

3. ‘설정’ 변경(3) 광고나 추적을 차단하는 확장 기능을 추가합니다.

어떤 브라우저든 기능을 추가할 수 있는 시스템이 마련되어 있습니다. 이를 ‘확장 기능’이라고 부릅니다. 브라우저 우측 상단의 설정 아이콘(세 줄 또는 세 점 아이콘)을 클릭하고 ‘확장 기능’ 항목에서 다양한 확장 기능을 설치할 수 있습니다.

확장 기능 중, 웹에 접속했을 때 광고를 숨기거나 추적 행위를 차단하는 등의 기능(아래에서 소개)을 추가합니다. 사용자의 위치 정보 등을 파악하는 상업용 광고를 통해 수집된 데이터를 정부가 확보하여 사용자 감시에 활용하는 사례가 미국에서 보고되고 있습니다.² 일본에서도 민관 협력 체제가 정비됨에 따라, 광고 관련 사용자 추적 기능의 위험성은 높아지고 있습니다.

이러한 악용을 방지하려면 브라우저에 uBlock Origin과 Privacy Badger 확장 기능을 추가합니다. uBlock Origin은 주로 광고를 차단하고, Privacy Badger는 인터넷상의 행동을 추적하는 행위를 차단하는 확장 기능으로 정평이 나 있습니다. 이들에 더해 NoScript라는 확장 기능을 도입함으로써 웹에 접속한 사용자의 컴퓨터가 해킹당하는 것을 방지하는 효과를 높일 수 있습니다.

설치 방법

Firefox 계열(Firefox, LibreWolf, Mullvad)에서는 아래 사이트에서 위 확장 기능의 이름으로 검색하여 설치할 수 있습니다.



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

또는 설정 아이콘 ⇒ ‘확장 기능 및 테마’에서 ‘애드온 찾기’ 검색창을 통해 확장 기능을 찾을 수도 있습니다.

Chrome 계열(Vivaldi)에서는 Google Chrome 웹 스토어에서 확장 기능을 설치 합니다.

<https://chromewebstore.google.com/>



다만, uBlock Origin은 Google의 정책에 따라 Google Chrome에서는 이 기능을 충분히 이용할 수 없습니다. 아래에서 권장하는 바와 같이, Google Chrome 계열 이외의 브라우저로 전환하는 것을 권장합니다.

uBlock Origin ‘빠른 가이드: 팝업 사용자 인터페이스’ https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/ublock-origin_quick-guide-popup-user-interface_jp/



(EFF) 온라인 추적은 감당하기 힘든 상황—Privacy Badger가 반격을

지원



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/

4.2.4. 개인정보 보호에 더 중점을 둔 브라우저로 변경하기

Google Chrome이나 Microsoft Edge에서 아래의 브라우저로 전환하는 것을 권장합니다. 브라우저로서의 기본 기능은 비슷하지만, 개인정보 보호에 중점을 둔 기능을 제공합니다. PC의 경우, 아래 공식 웹사이트 URL에서 설치할 수 있습니다. 스마트폰의 경우, Android라면 Google Play에서,

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

iPhone 이라면 Apple Store에서 앱을 설치합니다.

어떤 것을 선택해야 할지 망설여진다면, 우선 Firefox를 설치해 보세요.



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/>

Windows나 Mac 사용자, 스마트폰의 Android나 iPhone 사용자라면 DuckDuckGo 브라우저를 이용할 수 있습니다. (Linux용 버전은 없습니다)



<https://duckduckgo.com/>

Chrome에서 Firefox로 옮길 경우, 지금까지 사용하던 Chrome의 데이터(북마크나 검색 기록 등)를 Firefox에서도 사용할 수 있습니다. 아래 설명을 참고해 주세요.

Chrome에서 Firefox로 전환하기

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



4.2.5. 아날로그적인 선택지: 도서관!!

정보를 찾는 방법으로 도서관 이용을 추천합니다. 도서관의 장점은 사서로부터 전문적인 조언이나 검색 지원을 받을 수 있다는 점입니다. 개방형 서고라면, 원하는 자료뿐만 아니라 뜻밖의 흥미로운 자료를 우연히 발견하는 행운을 누릴 수도 있습니다. 책 한 권을 통째로 읽으며 얻는 경험은 인터넷에서는 맛볼 수 없습니다. 물론, 인터넷이 존재하지 않았던 시대에 종이로만 보존된 자료도 있습니다. 도서관은 정보의 보물창고라는 사실을 기억합시다. 국회도서관의 자료도 디지털화되어 온라인으로 접근 가능한 자료가 늘어나고 있습니다. <https://www.ndl.go.jp/>



4.3. 스마트폰 보안 재점검

4.3.1. 이용 시 비밀번호 입력을 필수로 설정합니다

스마트폰 화면을 터치하면 바로 사용할 수 있는 것은 편리하지만, 누구나 이용할 수 있게 됩니다. 도난이나 분실의 위험을 염두에 두고, 사용할 때 비밀번호 입력이 필요하도록 설정합니다.

4.3.2. 스마트폰 ‘설정’의 개인정보 보호 및 보안 설정을 더 엄격하게 변경합니다.

- 위치 정보는 끕니다. 꼭 필요한 경우에만 켭니다.
- 주소록에 접근할 수 있는 앱을 제한합니다.
- 카메라와 마이크는 사용하지 않을 때는 끕니다. 카메라에 커버를 씌웁니다.
- 개인정보 보호를 중시하는 브라우저로 변경합니다.
- 사용하지 않는 앱이나 어떤 앱인지 알 수 없는 것은 삭제합니다.

스마트폰 설정은 복잡하고 이해하기 어려운 경우가 많아 당황스러울 수 있습니다. 다음 내용을 참고해 보시기 바랍니다.

(EFF) Android의 개인정보 보호 및 보안 설정 방법



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) iPhone의 개인정보 보호 및 보안 설정 방법

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



and-

4.4. SNS의 위험성 알아보기

4.4.1. 앱 내 브라우저는 사용하지 마세요

SNS 메시지 내에 링크가 포함되어 있는 경우, 웹 사이트에 접속할 때 SNS 내의 브라우저가 사용됩니다. 기본 브라우저의 개인정보 보호 설정 등을 엄격하게 설정하더라도, SNS 내의 브라우저에는 적용되지 않아 의도하지 않은 개인정보 유출을 초래할 수 있습니다. 번거롭더라도 SNS 내의 링크는 일단 복사한 후 기본 브라우저를 열어 접속해 주십시오.

4.4.2. 확산 알고리즘

SNS를 통한 확산은 시민 운동이나 사회 운동에 있어 중요한 홍보 수단입니다. 하지만 확산은 SNS의 알고리즘에 의존하며, 영리 목적의 서비스에 의해 제공되는 것임을 잊지 마십시오. 거리에서 전단지들을 나눠주어도 대부분의 사람은 받아주지 않습니다. 이것이 진정한 확산의 실력입니다.

다만, 모든 SNS가 영리 목적의 알고리즘에 의해 운영되는 것은 아닙니다. 예를 들어, 다음과 같이 비영리이며, 광고가 없고, 자의적인 알고리즘이나 혐오 발언의 확산 등이 적은 몇몇 SNS의 예시입니다. 아래의 SNS들은 서로 연동되어 있습니다. 예를 들어, 마스토돈(Mastodon)에 게시한 내용을 프렌디카(Friendica)에서 읽거나 팔로우할 수 있습니다.



마스토돈(Mastodon) <https://joinmastodon.org/ja> X의 대안으로.





Friendica <https://friendi.ca/> 장문의 게시물을 올릴 수 있습니다.



Pixelfed <https://pixelfed.org/> 인스타그램의 대안으로.



PeerTube <https://joinpeertube.org/> YouTube 의 대안으로.

4.4.3. 팔로워라는 ‘인질’

광고나 혐오 발언, 가짜 정보 게시물에 지쳐 있더라도 팔로워가 많은 SNS 와 결별하는 것은 쉽지 않습니다. 주류 SNS 는 팔로워를 인질로 삼아 다른 SNS 로의 이동을 방해합니다. 하지만 위에서 소개한 대안 SNS 를 통해 정보를 공유하는 것부터 시작해, 장기적인 계획으로 SNS 이전을 검토해 보시기 바랍니다.

4.4.4. 집단학살이나 혐오 발언에 가담하는 기업의 서비스는 가능한 한 이용하지 마세요

X, 페이스북, 인스타그램 등 대형 SNS 는 전쟁을 부추기는 선전 수단이 되고 있습니다. 또한, 가자 지구에서 벌어지고 있는 집단학살 사태에서는 이스라엘 내 팔레스타인계 주민들의 게시물에 대한 검열이나 확산 억제 조치 등이 빈번하게 발생하고 있습니다. 구글, 아마존, 마이크로소프트 등 대형 빅테크 기업들은 집단학살을 가능하게 한 공습 등의 공격 인프라를 제공해 왔습니다. 이들 모두 우리 생활에 필수적인 서비스를 제공하는 기업인 만큼, 가능한 한 대체 서비스로 전환하는 것이 중요한 의지 표명이 됩니다.

4.5. VPN

인터넷에 접속해 서비스를 이용할 때, 인터넷 서비스 제공업체는 이용자에게 IP 주소를 할당합니다. 사용자가 어떤 웹사이트에 접속했는지 등을 모두 기록할 수도 있어, 온라인 활동을 추적하는 수단이 될 수도 있습니다. VPN(가상 사설망)은 이 IP 주소를 인터넷 서비스 제공업체로부터 숨길 수 있는 서비스입니다. 그중 두 가지만 소개하겠습니다.



ProtonVPN <https://protonvpn.com/ja>



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

MullvadVPN 은 유료 서비스만 제공합니다. 월 5유로이며, 월별 결제가 가능하고 자동 갱신이 없으므로, 요금을 납부하지 않으면 다음 달에 계약이 해지됩니다. 한번 사용해 볼 만한 가치가 있습니다. ProtonVPN 은 무료 버전도 있지만, 회선이 혼잡할 수 있습니다.

VPN 을 사용하면 계약한 인터넷 서비스 제공업체로부터 접속 정보 등을 숨길 수 있지만, VPN 업체는 접속처를 파악할 수 있습니다. 이용자의 개인정보 보호를 최우선으로 하는 신뢰할 수 있는 업체를 선택해야 합니다.

VPN 사용법에서 어려운 점은 거의 없습니다. 앱을 설치하기만 하면 사용할 수 있습니다. 접속 지점을

자신의 거주지와 다른 곳으로 설정하는 것만으로도 위치를 숨기는 효과가 있습니다.

4.5.1. 아날로그적인 선택지: 의외로 안전한 봉투 우편

디지털화가 사회의 추세인 현재에도, 계약한 인터넷 서비스 제공업체에 비밀번호 재발급을 요청하는 경우 등에서는 봉투에 담은 비밀번호 발송이 사용되기도 합니다. 관공서나 금융기관의 중요한 서류도 우편 발송이 일반적일 것입니다. 봉투에 개인정보를 담아 우편으로 보내는 방법은 현재에도 온라인 통신에는 없는 기밀성을 가지고 있습니다. 시간과 비용이 들지만, 필요에 따라 우편이라는 수단도 선택지 중 하나라는 점을 염두에 두시기 바랍니다. 전서비둘기도 좋은 선택지가 될지 모르겠네요.

4.6. 지도 Google Maps 에서 OpenStreetMap 으로

스마트폰의 GPS 를 켜고, 구글 지도에서 경로 정보를 확인하며 목적지로 향하는 방법이 가장 일반적일 것입니다. 하지만 우수한 오픈소스 지도인 OpenStreetMap 을 이용하는 것을 권장합니다. 기능이 뛰어나며 직접 지도를 편집할 수도 있습니다. 익숙해지는 데 시간이 조금 걸릴 수도 있지만, 구글에 추적당하지 않는다는 점을 생각하면 그 노력은 보람 있을 것입니다.

아래에 사용법 입문 설명이 있습니다.



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

4.6.1. 아날로그적인 선택지: 종이 지도와 나침반

종이 지도와 나침반을 사용하는 것은 인류가 오랫동안 익혀온 능력인데, 디지털 기기의 보급으로 인해 이를 희생해서는 안 될 것입니다. 종이 지도와 나침반에는 디지털에는 없는 장점이 있다는 점도 발견해 보시기 바랍니다. M.R. 오코너의 『길을 찾는 힘—인류는 내비게이션을 통해 진화했다』(우메다 토모요 번역, 인터시프트)도 꼭 참고해 보시기 바랍니다.

4.7. 암호화 서비스

4.7.1. 암호화 이메일 서비스: Proton 과 tuta

일본 정부는 통신 사업자의 협력을 이끌어내어 통신 정보를 제공하도록 하는 체제를 갖추고 있습니다. 이메일은 통신 회선 상에서는 암호화되어 있어 도청이 어렵지만, 사업자의 서버 상에서는 데이터가 암호화되지 않은 채로 보관되는 경우가 대부분입니다. 자신이 계약한 통신 사업자가 사용자의 사생활이나 통신 비밀의 권리보다 정부에 대한 협력을 우선시할 가능성이 있습니다.

통신 사업자가 정부에 통신 정보를 제공하는 것을 피하는 방법 중 하나로, 암호화 이메일 서비스를 이용하는 방법이 있습니다. 정부와 통신 사업자 모두 암호화된 데이터에만 접근할 수 있을 뿐, 암호를 해독할 수는 없습니다.



proton: 스위스에 본사를 두고 있습니다. 이메일 외에도 캘린더, 클라우드 서비스, VPN(앞서 4.5 항 참조) 등 다양한 암호화 서비스를 제공합니다. <https://proton.me/ja>



tuta: 독일에 본사를 두고 있습니다. 이메일 외에도 캘린더 암호화 서비스도 제공합니다. <https://tuta.com/ja>

암호화된 이메일에도 단점이 있습니다. 같은 서비스를 사용하지 않으면 암호화를 통한 양방향 통신

(엔드투엔드 암호화)이 불가능합니다. 상대방이 Gmail 등 암호화되지 않은 이메일 서비스를 사용하는 경우, Proton이나 tuta에서 보낸 이메일은 상대방의 수신함에 암호화되지 않은 상태로 저장됩니다. 하지만 상대방이 보낸 이메일은 암호화된 상태로 Proton이나 tuta의 수신함에 저장됩니다. 수신한 상대방의 이메일이 보호된다는 것만으로도 큰 장점입니다. 또한 Proton의 경우 PGP 암호화나 비밀번호 보호 기능을 사용하면 외부와도 암호화된 이메일을 주고받을 수 있습니다. tuta에도 비밀번호 보호 기능이 있습니다. Proton Mail에서 PGP를 사용하는 방법

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



Tuta Mail에서 무료로 암호화된 이메일을 보내는 방법

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



4.7.2. 암호화 메시지 서비스: Signal

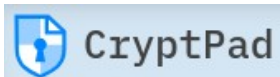
일본에서 사용자 수가 가장 많은 LINE의 경우, 2025년 하반기 수사 기관 등으로부터의 사용자 정보 공개 요청이 약 7,000건에 달했으며, 법원의 영장에 근거하지 않은 수사 관련 사항 조회를 통한 정보 공개가 급증하고 있습니다.³ Signal은 그룹 채팅, 화상 회의, 전화 기능 등 LINE과 거의 동일한 서비스를 제공하며, 사용법도 비슷하고, 메시지 암호화 서비스로서 가장 정평이 나 있는 서비스입니다.



<https://signal.org/ja/>

4.7.3. 클라우드 데이터 암호화: CryptPad

CryptPad는 문서 작성, 스프레드시트, 일정 관리 등 다양한 작업을 암호화하여 보관할 수 있습니다. Google Docs에서 수행하던 작업의 대부분을 CryptPad에서도 처리할 수 있습니다. 공동 작업도 가능합니다. CryptPad는 오픈 소스이므로, 자신의 서버에 설치하여 서비스를 제공할 수 있어 전 세계에 제공 사이트가 있습니다.



<https://cryptpad.fr/index.html> 개발팀이 호스팅합니다.

<https://cryptpad.org/instances/> 공개되어 있는 사용 가능한 CryptPad 목록.

4.7.4. 이 서비스들을 사용하지 않으면 암호화가 불가능한가요?

그렇지 않습니다. 암호화 방법에는 여러 가지가 있습니다. 자신의 컴퓨터에 있는 문서를 직접 암호화할 수 있는 소프트웨어도 있습니다. 혹은 컴퓨터 하드디스크 전체를 암호화할 수도 있습니다. 암호화의 원리도 다양합니다. 암호에 대해 자세히 알고 싶다면 아래 소책자를 읽어보시기 바랍니다.

글렌콜라 볼라다일 『반대파를 방어하다——사회 운동의 디지털 탄압과 암호를 통한 방』

[https://www.jca.apc.org/jca-net/sites/default/files/2021-11/反对派を防御する\(통합판\).pdf](https://www.jca.apc.org/jca-net/sites/default/files/2021-11/反对派を防御する(통합판).pdf)



기술적인 지식이 없어도 암호화의 혜택을 누릴 수 있는 방법으로 앞서 소개한 것과 같은 암호화 서비스를 이용하는 것이 가장 손쉬운 방법이라고 할 수 있습니다.

4.7.5. 이러한 암호화로 정말 정부의 감시 활동에 대항할 수 있을까?

가능합니다. 암호화 기술은 순수하게 수학적 이론으로 구성되어 있습니다. 신뢰할 수 있는 암호화 기술은

³ <https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/reports/2025h2/>

해당 기술의 사양을 공개하여 누구나 검증할 수 있도록 하고 있습니다. 만약 “당사의 암호화 기술은 기업 비밀이므로 공개하지 않습니다” 라는 식의 홍보 문구로 판매를 시도하는 암호화 서비스가 있다면, 절대로 사용하지 마십시오. 제 3자의 검증을 받을 수 없는 서비스는 신뢰성이 떨어지기 때문입니다. 위에서 소개한 Proton, Tuta, CryptPad 등은 모두 기술 사양을 공개하는 오픈소스입니다.

4.7.6. 암호화에서 주의해야 할 점은 역시 비밀번호입니다!

데이터를 암호화하거나 암호화된 데이터를 복원(복호화라고 합니다)할 때는 비밀번호를 입력해야 합니다. 비밀번호 설정 규칙을 준수하고 철저히 관리하는 것이 필수적인 전제 조건입니다. 아무리 강력한 암호를 사용하더라도, 허술한 비밀번호를 설정해 두면 전혀 효과가 없습니다.

4.7.7. 암호화가 정부의 스파이 활동에 이토록 효과적이라면, 정부의 스파이 활동은 그리 큰 위협이 아닐까요?

이 팸플릿 서두에서 언급했듯이, 우리가 자각하지 못하는 메커니즘을 통해 우리의 정보가 도용되고 있습니다. 이 점에 대한 위협은 자각할 수 없기 때문에 매우 심각합니다. 이 사실을 이해한 뒤, 암호화 등의 조치를 가능한 한 취하는 것이 중요합니다. 암호화된 데이터는 아무리 방대하게 수집되어도 해독할 수 없어 쓸모가 없습니다. 그 때문에 일본 정부는 미국이나 호주 등과 함께, 우리가 암호를 이용하는 것 자체를 규제하려고까지 하고 있습니다. 아동 포르노, 테러리즘, 해킹 방지 등 다양한 이유를 내세워 암호화 서비스를 법적으로 금지하거나, 사용할 수 있는 암호의 강도를 약화시키는 등 법적 권한의 확대를 꾀하고 있습니다. 이러한 움직임은 EU에서도 구체적인 조치로 나타나고 있습니다.

암호화는 우리 사생활 보호 권리 그 자체입니다. 암호화 이용을 법적으로 범죄로 규정하려는 움직임에는 단호히 반대해야 합니다.

4.8. 익명성

선거는 익명 투표이며, 현금으로 물건을 살 때도 익명입니다. 내부 고발 제도로도 익명의 권리로 보호받아야 합니다. 시위나 집회에 참여할 때도 익명이 기본입니다. 익명이기에 권력을 고발하거나 다수의 의견에 이의를 제기할 용기를 얻을 수 있습니다.

그러나 방대한 데이터를 수집하여 사소한 정보의 파편을 직소 퍼즐처럼 맞춰 나감으로써, 익명권이 침해될 수 있는 시대가 되었습니다. 정보 기관이 정부에 이의를 제기하는 사람들을 감시해 온 역사를 고려할 때, 가능한 한 익명으로 행동할 수 있는 방안을 마련하는 것도 중요합니다. 특히 이메일은 계정을 통해 누구의 이메일인지 특정되기 쉬운 편입니다. 이러한 이메일의 취약점을 보완해 주는 이메일 익명화 서비스를 DuckDuckGo 등이 제공하고 있습니다. 정부 부처에서 제공하는 이메일 뉴스레터 서비스나 쇼핑 사이트의 등록 이메일 주소에 익명화 이메일 서비스를 활용하면, 상대방에게 자신의 실제 이메일 주소를 알리지 않을 수 있습니다.

(DuckDuckGo mail) 메일함을 보호하자: DuckDuckGo Email Protection 의 베타 버전이 모든 사용자에게 공개되었다!



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. 아날로그적인 선택: 쇼핑은 현금으로

모바일 지갑이든 신용카드든 현금 이외의 결제 수단은 결제 관련 데이터가 확실히 기록됩니다. 디지털 공간에서 현금의 익명성에 필적하는 개인정보 보호를 실현하는 것은 매우 어렵습니다. 익명성을 중시하고 싶다면, 쇼핑은 원칙적으로 현금으로 한다는 습관을 들이는 것도 중요합니다.

4.8.2. 아날로그적인 선택: 마이나 카드, 마이나 건강보험증 사용 중단

마이넘버 카드는 소유자의 카드 이용 동향을 파악하는 수단이 됩니다. 마이넘버 건강보험증도 의료 행위의 범위를 넘어선 의료 정보를 수집하는 수단이 됩니다. 수집된 정보가 장래에 어떻게 이용될지는 법과 제도에 달려 있지만, 그 범위가 확대되는 경향이 뚜렷합니다. 또한, 관공서에 가지 않고도 주민 서비스를 처리할

수 있다는 점은 편리하지만, 행정 기관을 직접 방문하여 관공서의 실태를 파악하는 것은 민주주의의 기본입니다. 관공서에서 절차를 밟는 것은 중요한 권리 행사이기도 합니다. 마이넘버 카드를 반납하고, 마이넘버 건강보험증 대신 자격확인서와 약품 수첩을 활용합니다. 자세한 내용은 [‘공통번호\(마이넘버\) 필요 없는 네트워크 블로그’](#) <https://www.jca.apc.org/activist/> 를 꼭 확인해 주십시오.



4.9. 온라인 회의 시스템: Jitsi-meet

Jitsi-meet 는 ZOOM을 대체할 수 있는 온라인 회의 시스템입니다. 20~30 명 정도의 회의라면 충분히 원활하게 작동하며, 발언자를 제외한 참가자들이 카메라를 끈 상태라면 50 명을 넘어도 사용할 수 있습니다. Zoom 과 달리, 회의실을 운영하는 서버는 독립되어 있으며, 서버 운영 주체도 다양합니다. 신뢰할 수 있는 서버를 선택하는 것이 중요합니다. 다음 서버를 권장합니다.

개발자 사이트

<https://meet.jit.si/>



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



Framatalk <https://authent.framatalk.org/>



Jitsi-meet 사용법에 대해서는 아래 JCA-NET 매뉴얼을 참고해 주십시오.
<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. 메일링 리스트를 Google Groups 에서 Frama Groups 로 전환하기

메일링 리스트 서비스의 대표 주자로 꼽히는 Google Groups 외에도, 개인정보 보호에 중점을 둔 우수한 메일링 리스트 서비스가 있습니다. 예를 들어, Frama Groups 는 ‘구글 탈피’ 를 주창하며 활동하고 있는 프랑스 기반의 Framasoft 가 제공하는 서비스입니다.



[Framagroupeshttps://framagroupes.org/abc/en/](https://framagroupes.org/abc/en/)



5. 전쟁에 협력하지 말고, 민간 협력의 정보 수집에 맞서자

5.1. 국가의 첩보 활동은 전쟁의 일환이기도 하다

이스라엘의 가자 전쟁은 새로운 사이버 전쟁이기도 합니다. 우리 주변에서 인터넷을 통해 일상 필수품이라 할 수 있는 서비스를 제공하는 대형 IT 기업들이 가자에서 벌어지는 이스라엘의 집단학살에 깊이 가담하고 있음이 밝혀졌습니다.

예를 들어, 구글, 아마존, 마이크로소프트 등은 가자에서 수많은 일반 시민의 살해를 초래한 공습이나 드론 공격을 가능하게 하는 정보와 시스템을 제공함으로써, 집단학살에 가담하는 전쟁 범죄 기업이라고 할 수 있습니다.

한편, X, 페이스북, 인스타그램 등의 SNS 기업들은 이용자 데이터를 수집해 감시와 탄압에 활용하고 있습니다. 팔레스타인 사람들의 목소리를 검열하고 정보 확산을 억제하는 반면, 이스라엘의 집단학살을 부추기는 게시물이나 팔레스타인 사람들을 향한 혐오 발언을 묵인하는 정책을 취해 왔습니다.

정보통신 관련 기업의 전쟁 가담은 미국의 글로벌 기업에만 국한되지 않습니다. 예를 들어 일본의

라쿠텐은 독일의 무기 산업체 ‘헬싱’ 과의 제휴를 발표⁴ 했으며, 이를 우려하는 기업들이 라쿠텐 입점을 보이콧하고 있습니다. 전쟁에 가담하는 기업의 서비스를 지금까지처럼 이용하는 것은, 정부의 전쟁이나 스파이 활동에 가담하고 인권을 침해하는 기업의 범죄를 사실상 묵인하는 것이 됩니다. 전쟁이나 감시 사회에 가담하는 기업의 서비스를 이용하지 않는 것은, 오늘부터라도 할 수 있는 일입니다.

5.2. 윈도우를 보이콧하는 것은 어렵더라도, 할 수 있는 일이 있습니다

구글이나 아마존과 달리, 마이크로소프트사는 윈도우라는 컴퓨터의 기본 소프트웨어(OS)를 제공하고 있어, 윈도우 자체를 보이콧하는 것은 어려울 수 있습니다. 하지만 업무에서 표준으로 사용되는 마이크로소프트사의 워드, 엑셀, 파워포인트 등 ‘오피스 스위트’ 라고 불리는 대표적인 소프트웨어 사용을 중단하고, 예를 들어 리브레오피스로 전환하는 것이라면 불가능한 일은 아닙니다.



<https://ja.libreoffice.org/>

또한, CryptPad(앞서 언급한 ‘암호화 서비스 이용하기’ 참조)로 전환하는 방법도 있습니다.

6. 동료 만들기가 가장 중요, 우선 토론부터

정부의 첩보 기관인 국가정보회의/정보국의 창설을 통해 민관 협력이 강화되고, 포괄적이며 강력한 정보 수집 체제가 구축될 계획입니다. 이러한 전례 없는 상황에 대해 시민 운동 등에 참여하고 계신 여러분은 우선 동료들과 이 상황에 대해 토론하고, 스스로 할 수 있는 일을 함께 실천하며, 소통 환경과 관련된 운동의 문화를 바꾸는 것이 중요합니다.

이를 위해서는 정부의 첩보 기관이 관민 협력을 통해, 또한 미국 등 해외 정부와도 연계하여 우리의 정보를 어떻게 수집하려 하고 있는지에 대해 공통된 인식을 갖는 것이 중요합니다. 스마트폰이나 컴퓨터의 보안 설정, 비밀번호 설정 등은 번거로운 일이지만 매우 중요한 일이므로, 모두 함께 논의하며 이 까다로운 과제에 도전해 주시기 바랍니다. 이용 중인 서비스를 재검토하고, 가능한 부분부터 사생활을 배려하며 정보 도난에 취약하지 않은 것으로 변경해야 합니다. 또한, 스마트폰이나 컴퓨터 조작에 서툰 동지들을 지원하는 것이 매우 중요합니다.

7. 자주 묻는 질문

7.1. 정부의 권력이 막강하니 무엇을 해도 소용없는 것 아닌가?

헛된 일이 아닙니다. 인터넷 환경 속에서는 정부가 할 수 없는 일이 많이 있습니다. 예를 들어, 전 세계를 아우르는 인터넷 회선 케이블이나 전파는 현재 대부분 암호화되어 있어 내용을 파악할 수 없는 구조로 되어 있습니다. 그 때문에 정부는 민간 통신 사업자의 협력을 얻어 데이터를 확보하는 것 외에는 선택지가 없습니다. 서버나 스마트폰, 컴퓨터의 데이터를 암호화하는 것은 이러한 정부의 정보 수집에 대한 효과적인 대응 수단입니다.

7.2. 누구나 이 정도만 해두면 만전이라고 할 수 있는 방어 방법은 무엇일까요?

반드시 해야 할 일로는, 예를 들어 비밀번호 관리가 있습니다. 이는 누구나 해야 할 대책입니다. 하지만 이것만으로는 만전을 기할 수 없습니다. 우선, 자신에게 무엇이 가장 큰 위험이 되는지 판단해야 합니다. 그 위에서 어떤 방어책을 취할 수 있는지 알아봐야 합니다. 이 위험의 우선순위는 각자가 처한 상황에 따라 다르기 때문에, 모든 사람에게 통용되는 만능 대책은 없습니다.

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

7.3. 비밀번호나 개인정보 보호 같은 사소한 조치를 취한다고 해서 정부의 막강한 감시 권력에 효과가 있을까?

분명히 효과는 있습니다. 이러한 조치를 취함으로써, 당신에 대한 정보 수집량은 확실히 줄어들고, 결과적으로 당신과 연결된 사람들에 대한 정보 수집량도 줄어듭니다. 만약 당신이 선거에 투표하러 간다면, 단 한 표로 세상을 바꿀 수는 없는데도 왜 투표하러 가는지에 대해, 당신 나름의 답이 있을 것입니다. 그 답이 여기에도 적용됩니다. 수십 명, 수백 명이 참여하는 시위에 참가해 본 적이 있다면, 그런 작은 시위로 정부가 태도를 바꿀 리 없다는 것을 알면서도 행동하는 데에는 나름의 이유가 있을 것입니다. 그 이유가 여기에도 적용됩니다. 그리고 무엇보다, 한 사람 한 사람은 수많은 사회적 연결망 속에서 생활하고 있으며, 자신의 정보를 지키는 것은 자신과 연결된 사람들의 정보도 지키는 것으로 이어진다는 점을 기억해 주십시오.

7.4. 인터넷이나 컴퓨터에 대해 잘 모르기 때문에, 이에 나서기를 주저한다.

지금까지 시민 운동이나 다양한 사회 운동은 기술적으로도 매우 복잡한 문제에 정면으로 맞서온 실적이 있습니다. 예를 들어, 원전이나 핵무기 문제에 대해 핵물리학 등의 전문가가 아니더라도 많은 사람들이 반대해 왔습니다. 농약이나 화학 비료의 유해성, 의약품 피해 등 전문적인 지식이 없으면 그 메커니즘의 세부 사항을 이해할 수 없는 문제에서도 사람들은 과감하게 도전하고 싸워왔습니다.

전문적인 지식이나 기술적 구조의 세부 사항을 이해하지 못하더라도, 문제의 본질을 파악하고 위기감을 가지고 싸우는 것은 가능합니다. 이는 사이버 영역에도 마찬가지로 적용됩니다. ‘모르는’ 문제라 할지라도, 반드시 맞서 싸워야 할 심각한 문제라는 점을 이해할 수 있습니다.

7.5. 주변에 인터넷이나 컴퓨터에 밝은 사람이 없다. 스스로도 잘 모르는 부분이 많다. 어떻게 해야 할까?

만약 시민 운동 등의 동료들 사이에서도 이러한 문제에 직면해 있다면, 꼭 JCA-NET에 상담해 보시기 바랍니다.

JCA-NET은 여러분의 인터넷 및 컴퓨터 보안 등에 대한 활동을 지원합니다. 우선, 두세 명이라도 괜찮으니 부담 없이 모임을 가져 봅시다. 그곳에 JCA-NET 회원도 함께하여, 여러분이 가지고 있는 의문을 공유하고 가능한 해결책을 논의합니다.

이 팸플릿의 PDF 버전은 아래에서 다운로드할 수 있습니다. 또한 이 페이지에는 팸플릿에 기재할 수 없었던 추가 정보나 해설 등도 순차적으로 게재할 예정입니다. 꼭 활용해 주시기 바랍니다.

<https://jca.apc.org/jca-netの取り組み/スパイ・감시와 대항하기 위해—혼자서도 할 수 있는/>



저자 JCA-NET 발행 2026년 9월 20일

무료. 마음에 드신다면 꼭 후원금을 보내 주시기 바랍니다. 이 팸플릿은 JCA-NET 회원의 회비와 여러분의 후원금으로 제작되었습니다.

우편 이체 계좌 JCA-NET (제이씨에이-넷)

기호 번호: 00190-3-417584 유초은행 019 점 417584

※통신란에 ‘기부금’ 이라고 기재해 주십시오.

비영리 목적이라면 전재 및 복제가 자유롭습니다.

JCA-NET 담당 담당자 토시마루 070-5553-5495 toshi@jca.apc.org



... ..