

為防範間諜活動與監控

從個人能做的事到與他人共同能做的事

JCA-NET jca.apc.org



設計：[macrovector](#) / [Freepik](#)

目錄

1. 情報機構的成立、網路戰與監控社會的崛起.....	2
1.1. 法律與制度的變遷.....	2
1.2. 資訊蒐集與監控無所不在.....	3
1.3. 公眾對其影響的認知不足.....	3
1.4. 終身難消的副作用.....	3
1.5. 關於本小冊子.....	4
2. 理解資料蒐集.....	4
3. 哪些手段被用來蒐集與操縱資訊？.....	5
4. 我們能做些什麼？.....	5

4.1.	檢視您的密碼（密語）設定.....	5
4.2.	瀏覽器.....	7
4.3.	檢視智慧型手機的安全性.....	10
4.4.	了解社群媒體的風險.....	11
4.5.	VPN.....	12
4.6.	地圖：從 Google 地圖到 OpenStreetMap.....	13
4.7.	加密服務.....	13
4.8.	匿名性.....	16
4.9.	線上會議系統：Jitsi-meet.....	17
4.10.	將郵件列表從 Google 群組遷移至 Frama Groups.....	17
5.	拒絕配合戰爭；反對政府與私營部門的資訊蒐集.....	18
5.1.	國家間諜活動也是戰爭的一部分.....	18
5.2.	即使抵制 Windows 很困難，仍有你能做的事.....	18
6.	建立社群至關重要——讓我們展開討論.....	18
7.	常見問題.....	19
7.1.	政府的權力如此龐大，似乎做任何事都毫無意義。.....	19
7.2.	有什麼適合所有人的防禦策略——只要照做，就能確保自己獲得全面保護？.....	19
7.3.	面對政府龐大的監控能力，注意密碼和隱私等細微細節真的會有任何效果嗎？.....	19
7.4.	我對網路或電腦了解不多，因此不願參與其中。.....	20
7.5.	你身邊可能沒有人熟悉網際網路或電腦。你自己可能也有許多不完全理解的地方。你該怎麼辦？.....	20

1. 情報機構的成立、網路戰與監控社會的崛起

1.1. 法律與制度的變革

日本政府一直穩步推進建立新的法律框架和政府組織，以便收集我們的線上通訊資料。政府目前的目標是：

- 建立一套機制，使政府及地方當局得以在未經個人同意的情况下，廣泛使用其持有的個人資料
- 透過確保獲得私營電信業者及其他實體的合作，以確保政府能夠取得私營部門所持有之個人資料

以及其他類似措施。

《憲法》保障通訊隱私權並禁止審查，且現有各項法律與制度皆旨在保護我們的基本人權。然而，遺憾的是，一項項損害這些權利的新法律與制度卻接連被引入。例如，在 2026 年的國會會期中，成立了國家情報委員會／情報局——其目標是成為與美國中情局（CIA）及國家安全局（NSA）同級的間諜機構。與此同時，《個人資料保護法》的修訂案亦獲通過，允許在未經當事人同意的情况下蒐集及使用個人資料。其他已實施的措施還包括：將國家安全置於首位的《特定機密保護法》；用於對勞工進行背景調查的安全審查制度；以及擴大使用「我的編號」系統與「我的編號卡」。此外，從透過智慧型手機普及的無現金支付，到如今遍布各城市的配備人工智慧的監視攝影機，追蹤民眾日常活動的能力已變得更加精細。此外，目前日本各地正在興建的資料中心，正累積來自世界各地的海量個人資料，我們無法排除這些資訊未來可能被用作高度監控型社會的工具，或被用於戰爭的風險。

1.2. 資訊蒐集與監控無所不在

政府與私營企業透過我們日常使用的通訊基礎設施蒐集個人資料。電子郵件、社群媒體、網路購物、網頁搜尋、天氣與地圖服務，以及觀看或串流影片等日常生活不可或缺的活動，也成為追蹤我們行蹤的手段。因此，重新評估我們的日常網路習慣、採取措施防止資訊被蒐集，並努力確保我們在監控社會中既不會成為受害者，也不會成為加害者，至關重要。

1.3. 缺乏對影響的認知

一個主要問題在於，由於海量數據是在幕後、超出我們五感所能觸及的範圍內被蒐集的，因此我們無法真正掌握這個現實。正因我們無法感知，要防止或避免個人資訊被無意間蒐集，便極為困難。此外，僅憑主觀感知來捍衛我們的隱私與個人權利，也絕非易事。

我們首先必須讓資料蒐集變得可見。透過使其可見，我們才能找出具體措施來阻斷不必要的資料蒐集。

1.4. 副作用將伴隨終生

由於單一的被蒐集資訊看似微不足道，且未必能與特定個人對應，因此可能不會被視為重要的隱私資料。然而，當大量此類看似微不足道的資訊被蒐集後，便可能被用來識別個人身分，或與關鍵的隱私資料相互關聯，從而成為監控我們生活的基礎。一旦資訊被蒐集，便無法撤回。被蒐集的個人資訊所造成的副作用，可能伴隨終生。

1.5. 關於本小冊子

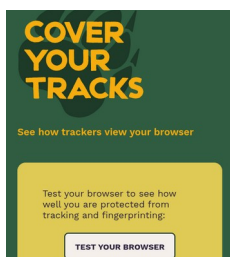
本小冊子首先介紹實用方法，讓讀者能具體了解哪些數據正在我們渾然不覺的情況下被蒐集，並從我們的意識中悄然溜走。在此基礎上，小冊子闡述了身為監控社會中的一員，我們應遵循哪些基本原則，才能在持續分享資訊的同時不感到受脅迫，其中包含應採取的預防措施以及可用的對策。

本手冊介紹了有助於避免資訊竊取、並更重視人權與隱私的替代工具。此處介紹的工具篩選標準如下：

- 這些工具必須是開源軟體或免費軟體。原則上，我們不會介紹那些未公開技術規格的營利性服務。
- 我們介紹了可替代那些支持戰爭行動之企業所提供服務的替代方案。
- 智慧型手機和電腦使用各種不同的作業系統。我們介紹的工具幾乎可在任何裝置上使用（部分例外情況除外）。

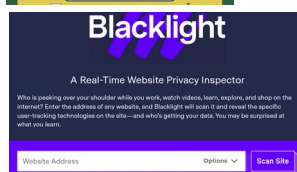
本手冊包含部分技術性較高的內容，但若您對某些部分不理解，請隨意跳過。您無需依頁碼順序閱讀——請從您覺得容易上手或最感興趣的部分開始。

2. 了解資料蒐集



假設您使用瀏覽器存取某個網站。在那一瞬間，儘管您可能沒有察覺，該網站正在蒐集關於您的各種資訊。資料量之龐大令人驚訝。若要確切了解 哪些資料正透過您的瀏覽器被追蹤，請造訪以下網站。

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



Blacklights 網站會掃描您正在瀏覽的網站網址，並揭露該網站所使用的的使用者追蹤技術，以及誰正在蒐集您的資料。

<https://themarkup.org/blacklight>



若您經常使用 Gmail 或其他 Google 服務，Google 的《隱私權政策》絕對是必讀內容。雖然要從頭到尾讀完這份文件需要花費不少心力，但其中詳細說明了 Google 究竟會蒐集多少個人資訊。

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

若您在閱讀本隱私權政策後，認為在使用 Google 服務時難以實施最佳的隱私保護措施，我們建議您改用其他替代工具，例如本手冊中列出的那些工具。



談到電子郵件，您可以透過檢視通常被隱藏的「電子郵件標頭」來驗證大量資訊。然而，由於標頭資訊充斥著技術術語，可能難以理解，請參閱以下網站：日本數據通訊協會，《如何檢查電子郵件標頭資訊》



此外，亦可參考右側的指南：增井俊勝所著《電子郵件技術教科書》（日文版），秀英社出版。

3. 目前採用何種方式進行資訊蒐集與處理？

以下是被用來蒐集我們資料的手段。

- 透過智慧型手機與電腦進行的通訊（行動支付、社群媒體、電子郵件、瀏覽網頁等）
- 政府及地方當局持有的個人資料（與「My Number」相關的資料、駕駛執照、犯罪紀錄、從民間企業取得的個人資料等）
- 金融機構及醫療機構所持有之個人資料
- 安裝於市區街道的監視攝影機
- 俗稱「物聯網」（IoT）的裝置，例如 Wi-Fi 路由器和智慧電表

政府情報機構亦利用這些管道進行資訊蒐集與操縱。情報機構不僅共享政府持有的資訊，更取得存取私人資訊的法律與制度授權。與此同時，它們動員社群媒體影響者及其他人士，組織精巧的資訊操縱與煽動行動。即使在許多自稱民主的國家——包括歐盟在內——基於國家安全目的的情資蒐集與資訊操縱，通常被視為對人權（例如隱私權）保護的例外情形。

由此可見，我們日常生活中最常使用的智慧型手機和電腦，正是政府進行情報蒐集與操縱的主要入口。正因如此，盡可能封鎖這些入口至關重要。

4. 我們能做些什麼？

在傳送或接收訊息，或是登入網站時，我們會透過使用者名稱與密碼的組合來防範身分盜用與資訊竊取。密碼（或密語）是保障通訊機密性的最基本且不可或缺的條件。

4.1. 檢視您的密碼（密語）設定

帳號和登入 ID 可能被第三方發現，要將其完全保密並不現實。保護這些帳號和 ID 的唯一方法就是使用密碼（密語）。所謂密語，是指由多個單字組合而成的詞組。在本手冊中，「密碼」一詞將同時涵蓋密語。若政府情報機構或類似單位取得您的帳號（ID）與密碼的組合，他們便能夠所欲為——從閱讀您的電子郵件、冒充您的身分，到竊取通訊錄等資料。此外，您還可能面臨嚴重的攻擊，例如裝置被植入惡意軟體。密碼管理是一項至關重要且不可忽視的事項。請務必充分理解：即使您使用強加密服務，若疏於妥善管理密碼，加密措施也將形同虛設。

4.1.1. 設定密碼時，請務必遵循以下規則

- 請勿重複使用相同的密碼。
- 請避免使用您的姓名、出生日期、電話號碼、地址，或「1234」、「abcd」等容易被猜中的序列，以及字典中的單字。
- 密碼必須符合上述條件，且長度至少為 18 個字元。

4.1.2. 若您在管理密碼時遇到困難，該怎麼辦

僅憑記憶來管理多個符合上述條件的密碼，幾乎是不可能的。透過使用可靠的密碼管理軟體，您便能輕鬆管理大量複雜的密碼，且無需重複使用。以下是一些廣受好評的選項：

密碼管理軟體	說明
--------	----

   Bitwarden https://bitwarden.com/ja-jp/	以下將提供詳細說明。 https://bitwarden.com/ja-jp/help/ 
   KeePassXC https://keepassxc.org/	以下提供新手指南的日文譯本。 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/keepassxc_gettingstarted/ 

4.1.3. 請勿使用指紋或臉部辨識

由於輸入密碼可能相當麻煩，您可能會想使用臉部或指紋辨識功能。然而，我們不建議使用這些方法，因為存在這些功能可能在您不知情的情況下被濫用的風險。實際上曾發生過一樁案例，執法機關取得法院搜查令後，利用臉部辨識功能強行存取智慧型手機：¹。

4.1.4. 「傳統」的替代方案：發揮創意，將密碼寫在紙上

既然你還是會重複使用簡單的密碼，不如將寫有密碼提示的紙條悄悄藏在只有你才知道的地方，這樣可能更安全。另一種選擇是，根據你自己制定的規則，將實際密碼稍作修改後，公開發布該版本。若您只有少數幾個密碼，採用類比方式——例如謹慎管理 18 個字元的密碼且不重複使用——很可能比費力學習如何使用您不熟悉的密碼管理軟體更能提供更高的安全性。我們不建議在可能被公眾看見的地方使用這些方法。

4.2. 瀏覽器

4.2.1. 瀏覽器的功能是什麼？

用於存取網際網路上各類網頁的軟體通常稱為「瀏覽器」，其種類繁多。例如 Google Chrome、Microsoft Edge、Firefox 以及 Safari。無論是使用 Google 搜尋、在 Amazon 購物、於 Yahoo 閱讀新聞、在 YouTube 觀看影片，還是查看 Gmail，這些操作都是透過瀏覽器進行的。有時，您也可能透過瀏覽器存取 X 或 Instagram 等社群媒體平台，或是參加 Zoom 會議。從這個角度來看，瀏覽器是連接網路與進行溝通不可或缺的萬用工具。如前所述，由於瀏覽器會以不易察覺的方式傳送大量資料，因此選擇一款重視隱私並具備阻擋隱藏追蹤器功能的瀏覽器至關重要。

4.2.2. HTTP 與 HTTPS

網頁網址可以以「http」或「https」開頭。當您存取「http」網站時，透過該連線傳輸的所有資料（例如密碼和信用卡號碼）都有可能被第三方攔截。另一方面，使用「https」時，透過該連線傳輸的資料會經過加密，大幅降低了遭攔截的風險。若您目前營運的網站仍使用「http」，請盡快採取必要措施，將其遷移至「https」。

若您確實必須存取 HTTP 網站，請始終假設您的通訊正受到第三方監控而行事。

¹(朝日新聞)「強制智慧型手機人臉辨識：警方調查的新技術——對權力過度的擔憂(日文)」2026年8月12日
<https://digital.asahi.com/articles/ASV7Y34MQV7YPTIL014M.html>

4.2.3. （臨時措施）請檢視瀏覽器的「設定」，確保您不會無意間向他人提供不必要的數據。

開啟瀏覽器的「設定」畫面。通常可透過點擊瀏覽器右上角難以辨識的圖示（例如三條橫線或三個點），來開啟「設定」畫面；點擊後會顯示一個選單，您可從中選擇「設定」。

1. 設定變更（第一部分）：將搜尋引擎從 Google 或 Bing 切換至注重隱私的搜尋引擎，例如 DuckDuckGo。

由於搜尋行為無法偽造，Google 等搜尋服務會根據我們的搜尋內容來推斷我們的興趣。切換至注重隱私的搜尋引擎，是抵禦這種資料蒐集的最簡單方法。請在瀏覽器的「設定」選單中找到「搜尋」區段，並將「預設搜尋引擎」變更為以下其中一個：



DuckDuckGo <https://duckduckgo.com/>



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



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

2. 設定變更（第二部分）：強化追蹤防護。

在「設定」畫面中尋找可變更隱私權與安全性設定的區塊。接著，將設定調整為比預設值更嚴格。例如，在 Firefox 中，

- 將「增強型追蹤防護」從「標準」調整為「嚴格」。
- 將 Firefox 設定為在關閉瀏覽器時刪除 Cookie 和網站資料。

3. 設定變更（第 3 部分）：安裝擴充功能以阻擋廣告與追蹤。

每個瀏覽器都內建了可新增功能的機制，這些功能稱為「擴充功能」。點擊瀏覽器右上角的設定圖示（三條橫線或三個點），並從「擴充功能」區段安裝各種擴充功能。

在瀏覽器擴充功能中，有些能在您瀏覽網站時隱藏廣告，或阻擋追蹤行為（如下所述）。在美國，曾有報導指出政府取得商業廣告所蒐集的資料——這些資料會追蹤使用者的位置及其他資訊——並利用這些資料監控使用者。² 隨著日本也開始建立公私合作夥伴關係，透過廣告進行使用者追蹤所帶來的風險正日益增加。

為防止此類濫用行為，請在瀏覽器中安裝 uBlock Origin 和 Privacy Badger 擴充功能。uBlock Origin 以阻擋廣告聞名，而 Privacy Badger 則以阻擋線上追蹤著稱。此外，安裝 NoScript 擴充功能還能進一步加強防護，避免您在瀏覽網頁時電腦遭到劫持。

安裝方法

針對基於 Firefox 的瀏覽器（Firefox、LibreWolf、Mullvad），您可在下方網站搜尋上述擴充功能的名稱並進行安裝。

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



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

此外，您也可以點擊設定圖示 ⇒ 「擴充功能與主題」，並使用「尋找附加元件」搜尋欄來尋找該擴充功能。

針對基於 Chrome 的瀏覽器（如 Vivaldi），請從 Google Chrome 網路商店安裝此擴充功能：

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



然而，由於 Google 的政策限制，uBlock Origin 在 Google Chrome 中無法提供完整功能。我們建議您改用 Google Chrome 系列以外的瀏覽器，具體建議如下。

uBlock Origin「快速指南：彈出式使用者介面」
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/ublock-origin-quick-guide-popup-user-interface_jp/



（EFF）線上追蹤已失控——Privacy Badger 助您反擊



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. 切換至重視隱私的瀏覽器

我們建議您從 Google Chrome 或 Microsoft Edge 切換至以下列出的瀏覽器之一。雖然它們具備相似的核心瀏覽器功能，但這些瀏覽器提供了專為保障隱私而設計的功能。若您使用電腦，可從下方列出的官方網站網址進行安裝；若您使用智慧型手機，請從 Google Play（Android 系統）或 Apple Store（iPhone）安裝應用程式。

如果您不確定該選擇哪一款，不妨先安裝 Firefox。



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/>

如果您是 Windows 或 Mac 使用者，或是使用 Android 或 iPhone 智慧型手機，您可以使用 DuckDuckGo 瀏覽器。（目前尚無 Linux 版本。）



<https://duckduckgo.com/>

當您從 Chrome 切換至 Firefox 時，可將現有的 Chrome 資料（例如書籤和瀏覽紀錄）轉移至 Firefox。請參閱以下說明。

從 Chrome 遷移至 Firefox

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



4.2.5. 「類比」選項：圖書館！！

我們建議您利用圖書館進行研究。圖書館的優勢在於，您可以向館員尋求專業建議與檢索協助。在開放式書架的圖書館中，您不僅可能幸運地找到所需的資料，還可能意外發現有趣的讀物。完整閱讀一本書的體驗，是線上無法獲得的。當然，也有一些資料僅以紙本形式存在，其歷史甚至可追溯至網際網路尚未問世之前。讓我們記住，圖書館是資訊的寶庫。國會圖書館越來越多的資料已數位化，現在可透過網路查閱。<https://www.ndl.go.jp/>



4.3. 檢視智慧型手機的安全性

4.3.1. 設定密碼才能存取

雖然只需輕觸螢幕就能使用智慧型手機非常方便，但這也意味著任何人都能使用它。為防範遭竊或遺失的風險，請將裝置設定為使用時必須輸入密碼。

4.3.2. 請在智慧型手機的「設定」中，將隱私權與安全性設定調整為更嚴格的模式。

- 關閉定位服務。僅在絕對必要時才開啟。
- 限制哪些應用程式可以存取您的聯絡人。
- 不使用時請關閉相機和麥克風。並用布遮蓋相機鏡頭。
- 切換至注重隱私的瀏覽器。
- 刪除您不使用或不認識的應用程式。

智慧型手機的設定往往複雜且令人困惑，可能會讓人不知所措。請參考以下指引。

（EFF）如何在 Android 上設定隱私與安全設定



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）如何在 iPhone 上設定隱私與安全

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. 了解社群媒體的風險

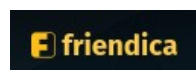
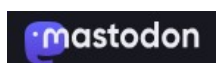
4.4.1. 避免使用應用程式內建瀏覽器

若社群媒體訊息中包含連結，系統將透過該平台的內建瀏覽器開啟網站。即使您在預設瀏覽器上設定了嚴格的隱私權設定，這些設定並不適用於社群媒體平台的瀏覽器，這可能導致個人資訊在不知不覺間遭竊。即使稍顯麻煩，也請從社群媒體平台複製連結，並在您的預設瀏覽器中開啟。

4.4.2. 病毒式分享背後的演算法

社群媒體上的病毒式分享，是公民運動與社會運動的重要宣傳手段。然而，請記住：這種分享仰賴社群媒體演算法，並由營利服務所驅動。若您在街頭發放傳單，多數人並不會接受。這正是病毒式分享的真正力量。

值得注意的是，並非所有社群媒體平台都由以營利為目的的演算法所運作。例如，以下列舉了幾個非營利且無廣告的社群媒體平台，這些平台具有較少的任意演算法，且仇恨言論較少。這些平台彼此互聯。舉例來說，您可以透過 Friendica 閱讀或追蹤在 Mastodon 上發布的貼文。



Mastodon <https://joinmastodon.org/ja> X 的替代平台。

Friendica <https://friendi.ca/> 支援長篇貼文。



Pixelfed <https://pixelfed.org/> Instagram 的替代方案。



PeerTube <https://joinpeertube.org/> YouTube 的替代方案。



4.4.3. 將追蹤者當作「人質」

即使你對廣告、仇恨言論和不實資訊感到厭倦，要脫離擁有大量追蹤者的社群媒體平台也並非易事。主流社群媒體平台會將你的追蹤者當作「人質」，以阻止你轉向其他平台。然而，不妨先從在上述這類替代平台上分享內容開始，並將轉移至新的社群媒體平台納入長期計畫中。

4.4.4. 盡可能避免使用那些涉及種族滅絕和仇恨言論的公司所提供的服務

像 X、Facebook 和 Instagram 這樣的主要社群媒體平台，已淪為煽動戰爭的宣傳工具。此外，在加薩種族滅絕期間，屢屢發生審查及壓制以色列境內巴勒斯坦居民貼文傳播的行為。Google、Amazon 和 Microsoft 等大型科技公司，則提供了使種族滅絕得以實施的基礎設施——例如空襲行動。正因為這些公司提供的服務對我們的日常生活至關重要，因此在可能的情況下轉用替代服務，是表明我們立場的重要方式。

4.5. VPN

當您連線至網際網路以使用各項服務時，您的網際網路服務供應商（ISP）會為您指派一個 IP 位址。ISP 可以記錄所有資料，包括您造訪的網站，這些資料可被用來追蹤您的線上活動。VPN（虛擬私人網路）是一項能向您的 ISP 隱藏此 IP 位址的服務。以下是兩個範例。



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



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

MullvadVPN 僅提供付費服務，每月費用為 5 歐元。您可以選擇按月支付，且由於沒有自動續約機制，若未於次月繳費，訂閱服務將自動取消。值得一試。ProtonVPN 雖提供免費版本，但網路有時可能會出現擁塞。

雖然 VPN 能隱藏您向網路服務供應商傳送的連線資訊，但 VPN 服務商本身仍可追蹤您的連線目的地。因此，選擇一家將用戶隱私置於首位的值得信賴的服務商至關重要。

使用 VPN 通常非常簡單。只需安裝應用程式，即可開始使用。即使只是將連線地點設定為與您居住地不同的位置，也能幫助隱藏您的位置。

4.5.1. 一種「類比」選項：出乎意料地安全的平信寄送

即使在當今數位化已成社會主流趨勢的時代，透過密封郵件寄送密碼的做法仍偶有使用——例如向服務供應商申請重設密碼時。政府機關和金融機構透過普通郵件寄送重要文件的情況也相當常見。透過密封郵件傳送私人資訊，仍能提供線上通訊所缺乏的保密程度。雖然這需要時間且會產生費用，但請記住，在必要時，郵政郵件依然是一個可行的選擇。說不定連信鴿也是一個不錯的選擇。

4.6. 地圖：從 Google 地圖到 OpenStreetMap

最常見的方法大概是開啟智慧型手機的 GPS，並在 Google 地圖上查看路線以導航至目的地。不過，我建議使用 OpenStreetMap，這是一項出色的開源地圖服務。它功能豐富，甚至允許您親自編輯地圖。雖然可能需要一點時間來適應，但考慮到您不會被 Google 追蹤，這份努力是值得的。

以下是一份關於如何使用它的初學者指南。



OpenStreetMap



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

4.6.1. 「類比」選項：紙本地圖與指南針

我們不該僅因數位裝置的普及，就犧牲使用紙本地圖與指南針這項技能——這可是人類歷經漫長歲月才掌握的技能。試著發掘紙本地圖與指南針所具備、而數位工具所缺乏的獨特優勢。我也極力推薦閱讀 M.R. O'Connor 的著作《Wayfinding: The Science and Mystery of How Humans Navigate the World》。

4.7. 加密服務

4.7.1. 加密電子郵件服務：Proton 與 Tuta

日本政府正在建立一套機制，迫使電信業者配合並交出通訊資料。雖然電子郵件在傳輸過程中經過加密，難以被攔截，但資料幾乎總是以未加密的形式儲存於電信業者的伺服器上。您的電信業者有可能會將配合政府的要求置於用戶的隱私權及通訊保密性之上。

防止電信業者向政府提供通訊資料的一種方法，是使用加密電子郵件服務。除非資料被解密，否則無論是政府還是電信業者本身都無法存取該資料，而他們也無法解密這些資料。



Proton：總部位於瑞士。除了電子郵件外，還提供各種加密服務，例如行事曆、雲端服務和 VPN（參見上文第 4.5 節）。<https://proton.me/>



tuta：總部位於德國。除了電子郵件外，還提供加密行事曆服務。<https://tuta.com/>

加密電子郵件也有其缺點。除非雙方都使用相同服務，否則無法實現雙向安全通訊（端對端加密）。若收件者使用 Gmail 等未加密的電子郵件服務，從 Proton 或 Tuta 發送的電子郵件將以未加密形式儲存於收件者的收件匣中。然而，收件者發送的電子郵件則會被加密，並儲存於您的 Proton 或 Tuta 收件匣中。您收到的來自對方之電子郵件受到保護，這本身就是一項顯著的優勢。此外，透過 Proton，您可以利用 PGP 加密或密碼保護功能，與外部對象交換加密電子郵件。Tuta 亦提供密碼保護功能。如何在 Proton Mail 中使用 PGP

<https://www.alt-movements.org/no-more-capitalism/hankanshi-info/knowledge-base/proton-mail-how-to-use-pgp/>



如何使用 Tuta Mail 免費發送加密電子郵件

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



4.7.2. 加密通訊服務：Signal

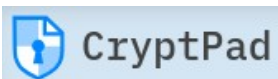
以在日本擁有最大用戶群的 LINE 為例，2025 年下半年共收到來自執法機關及其他單位約 7,000 筆用戶資訊揭露請求，其中非基於法院搜查令的調查詢問所導致的資訊揭露數量更出現急遽增加。³ Signal 提供與 LINE 幾乎相同的服務，例如群組聊天、視訊會議和電話通話，其使用情況也與 LINE 相似；它是備受推崇的訊息加密服務。



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

4.7.3. 雲端資料加密：CryptPad

CryptPad 讓您能在確保資料加密與安全的前提下，建立文件、處理試算表、管理行程，並執行各種其他任務。您可以使用 CryptPad 處理許多與 Google Docs 相同的任務，同時也支援協作功能。由於 CryptPad 屬於開源軟體，您可以將其安裝在自己的伺服器上來託管服務，這也是為何全球各地都有託管網站的原因。



<https://cryptpad.fr/index.html> 由開發團隊託管。

<https://cryptpad.org/instances/>：公開可用的 CryptPad 實例清單。

4.7.4. 如果不使用這些服務，就無法進行加密嗎？

絕非如此。加密方法多種多樣。有軟體可讓您在自己的電腦上加密文件。此外，您也可以加密整台電腦的硬碟。加密機制也各不相同。若您想進一步了解加密，請閱讀以下小冊子。

Glencora Boradale, 《捍衛異議：社會運動的數位壓制與加密防禦》



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

<https://open.oregonstate.education/defenddissent/>

對於缺乏技術知識的人來說，使用如上所述的加密服務，是享受加密帶來好處的最快速方式。

4.7.5. 這種加密方式真的能抵禦政府的監控嗎？

是的，可以。加密技術完全建立在數學理論之上。值得信賴的加密技術會公開其技術規格，以便任何人都能進行驗證。若您遇到某項加密服務試圖以「我們的加密技術屬於商業機密，因此不予公開」這類標語來推銷，務必避免使用。無法經第三方驗證的服務缺乏可信度。上述介紹的服務——例如 Proton、Tuta 和 CryptPad——皆為開源軟體，並公開其技術規格。

4.7.6. 談到加密，最需要留意的是——當然就是您的密碼！

在加密資料或還原（解密）加密資料時，您都需要輸入密碼。嚴格遵守密碼政策並妥善管理密碼，是不可或缺的先決條件。無論加密強度多高，若使用弱密碼，加密將完全失效。

4.7.7. 如果加密對政府間諜活動如此有效，是否意味著政府間諜活動其實並非真正的威脅？

正如本手冊開頭所述，我們的資訊正透過我們渾然不知的機制被竊取。正因為我們對此毫不知情，所帶來的威脅才格外嚴重。理解這一點並盡可能採取加密等措施至關重要。即使收集了大量加密資料，若無法解密，這些資料也毫無用處。正因如此，日本政府正與美國、澳洲等國聯手，甚至試圖對我們使用加密技術本身進行規範。他們以兒童色情、恐怖主義及打擊有組織犯罪等各種理由為藉口，策劃透過法律禁止加密服務或削弱現有加密強度，藉此擴大其法律權限。此類舉措在歐盟也已開始具體化。

加密技術正是我們隱私權的本質所在。我們必須堅決反對任何將加密技術的使用刑事化的企圖。

4.8. 匿名性

投票是匿名的，用現金購物也是匿名的。舉報機制也應受到匿名權的保護。在參與示威和集會時，匿名性至關重要。正因為有匿名性，我們才敢於譴責當權者，或對主流意見表達異議。

然而，我們如今所處的時代，匿名權可能因海量資料的蒐集，以及像拼圖般將瑣碎資訊片段拼湊起來而受到侵害。鑒於情報機構過去曾監控反對政府人士的歷史，採取措施以盡可能匿名的方式行事至關重要。尤其是電子郵件，僅憑帳號便能輕易識別寄件者身分。DuckDuckGo 等服務提供電子郵件匿名化功能，以解決此一漏洞。當您訂閱政府機關的電子報或在購物網站註冊時，若使用電子郵件匿名化服務，即可確保收件者無法得知您的真實電子郵件地址。

（DuckDuckGo Mail）保護您的收件匣：DuckDuckGo 電子郵件保護（☐）的測試版現已向所有使用者開放！



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. 一種「類比」選項：使用現金支付

無論您使用行動錢包還是信用卡，任何非現金的支付方式都不可避免地會留下交易紀錄。在數位領域中，要達到與現金匿名性相當的隱私保護程度，極為困難。如果您重視匿名性，務必養成在可能的情況下盡量使用現金支付的習慣。

4.8.2. 一種「類比」選擇：停止使用「個人編號卡」與「個人編號健康保險卡」

「個人編號卡」是追蹤持卡人使用模式的工具。「個人編號健保卡」則用於蒐集超出醫療範圍的醫療資訊。未來這些蒐集到的資訊將如何被運用，雖取決於法律法規，但其用途擴大的趨勢已然明朗。此外，雖然無需親赴市政府即可辦理居民服務十分便利，但親臨政府機關並了解其實際運作，是民主制度的根本所在。前往市政府辦理手續，亦是行使您權利的重要實踐。讓我們歸還「個人編號卡」，並改用資格驗證證明書及用藥

紀錄，取代「個人編號健康保險卡」。更多詳情，請瀏覽「[我們不需要統一編號（個人編號）網絡部落格](https://www.jca.apc.org/activist/)」：<https://www.jca.apc.org/activist/>。

4.9. 線上會議系統：Jitsi-meet



Jitsi Meet 是一款可作為 Zoom 替代方案的線上會議系統。它非常適合約 20 至 30 人的會議，只要除發言者以外的所有人關閉鏡頭，即可容納超過 50 位參與者。與 Zoom 不同，託管會議室的伺服器是獨立的，且由各家機構營運。選擇值得信賴的伺服器至關重要。我們推薦以下伺服器。

開發者網站

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



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



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



有關如何使用 Jitsi Meet 的說明，請參閱下方的 JCA-NET 手冊。

<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. 將郵件列表從 Google Groups 遷移至 Frama Groups

雖然 Google Groups 已成為郵件列表服務的標準，但仍有其他優秀的替代方案更重視隱私。例如，Frama Groups 是由 Framasoft 提供的服務，該組織總部位於法國，致力於倡導擺脫對 Google 的依賴。



<https://framagroupes.org/abc/en/>



5. 拒絕與戰爭合作；反對政府與私營部門的資訊蒐集

5.1. 國家間的情報活動也是戰爭的一部分

以色列在加薩的戰爭也是一種新型態的網路戰。如今已很清楚，那些融入我們日常生活、並提供已成為線上不可或缺服務的主要 IT 公司，其實是以色列在加薩實施種族滅絕的深度共犯。

舉例來說，Google、Amazon 和 Microsoft 等公司可被視為涉入種族滅絕的戰爭罪企業，因為它們提供的資訊與系統，使空襲和無人機攻擊得以實施，導致加薩地區無數人喪生。

與此同時，X、Facebook 和 Instagram 等社群媒體公司則收集用戶資料，並將其用於監控與鎮壓。這些公司一方面審查巴勒斯坦人民的声音並壓制資訊傳播，另一方面卻維持著默許煽動以色列種族滅絕及針對巴勒斯坦人民仇恨言論的貼文的政策。

資訊與通訊科技公司參與戰爭的現象，並不限於美國跨國企業。例如，日本的樂天（Rakuten）宣布與德國軍火製造商「Helsing」⁴ 建立合作關係，此舉促使關注此議題的企業抵制在樂天平台上開設商店。繼續使用與戰爭同流合污的企業所提供的服務，實質上等同於默許其罪行——包括參與政府主導的戰爭與間諜活動，以及侵犯人權的行為。拒絕使用與戰爭及監控國家同流合污的企業所提供的服務，是您今天就能開始做的事。

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

5.2. 即使抵制 Windows 相當困難，您仍有其他可以採取的行動

與 Google 和 Amazon 不同，微軟提供個人電腦的作業系統（OS）Windows，因此要抵制 Windows 本身可能相當困難。然而，停止使用微軟的「Office 套裝軟體」——例如在職場中普遍使用的 Word、Excel 和 PowerPoint 等標準軟體——並改用 LibreOffice，這並非不可能。



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

另一種選擇是改用 CryptPad（參見上文「使用加密服務」）。

6. 建立社群至關重要——讓我們展開討論

隨著國家情報委員會（National Intelligence Council）和國家情報局（National Intelligence Agency）等政府情報機構的成立，當局已規劃強化公私部門合作，並建立一套全面且強大的情報蒐集系統。面對這前所未有的局勢，參與公民運動及類似倡議的人士，務必先與同儕討論現況、共同商議可採取的行動，並改變圍繞通訊環境的社會運動文化。

為此，我們必須建立共識，了解政府情報機構——透過與私營部門及美國等外國政府合作——打算如何蒐集我們的資訊。雖然為智慧型手機和電腦設定安全措施（包括設定密碼）可能相當麻煩，但這卻至關重要。請透過彼此討論這些議題，共同承擔這項艱鉅的任務。重新評估您所使用的服務，並在可行範圍內，轉用那些優先保障隱私且較不易遭竊取資料的選項。此外，支持那些不擅長科技操作的夥伴，更是至關重要。

7. 常見問題

7.1. 政府的權力如此龐大，似乎做任何事都毫無意義。

這絕非徒勞。在網路環境中，仍有許多事情是政府無法做到的。舉例來說，縱貫全球的網際網路電纜與無線電波如今幾乎全都經過加密，使得政府根本無法監控其內容。因此，政府別無選擇，只能仰賴私人電信供應商的配合來取得資料。對伺服器、智慧型手機及電腦上的資料進行加密，是對抗政府資訊蒐集行為的有效對策。

7.2. 究竟有什麼防禦策略能適用於所有人——只需做到這一點，就能確保你獲得全面保護？

有一件事你絕對必須做到，那就是妥善管理你的密碼。這是每個人都應該採取的預防措施。然而，僅靠這一點並不能保證完全的保護。首先，你需要評估什麼對你個人構成最大的風險。然後，你應該研究可以採取哪些防禦措施。由於這些風險的優先順序會因個人情況而異，因此沒有放諸四海皆準的解決方案。

7.3. 在面對政府龐大的監控能力時，留意密碼和隱私等細微細節真的會有任何效果嗎？

當然有。透過採取這些步驟，你必定能減少關於你的資訊被蒐集的數量，進而也將減少關於你周遭相關人士的資訊被蒐集的數量。如果你前往投票站投票，即使一票根本無法改變世界，你必定有自己這麼做的理由。同樣的道理也適用於此。如果你曾經參加過數十或數百人規模的示威活動，你大概也有自己採取行動的理由——即使你知道像那樣的小型示威不太可能改變政府的立場。同樣的道理在此也適用。最重要的是，請記住，我們每個人都生活在社會人際網絡之中，保護自己的資訊也有助於保護與你相關的人的資訊。

7.4. 我對網路或電腦了解不多，因此頗為猶豫是否該參與其中。

人民運動與各類社會運動，向來有直面處理極其複雜技術問題的實績。例如，許多人儘管並非核物理或相關領域的專家，卻仍反對核電廠與核武器。即使是像農藥與化學肥料造成的危害，或是藥品的不良反應這類議題——若沒有專業知識便難以掌握其詳細機制——人們依然大膽地迎接這些挑戰，並為改變而奮鬥。

即使不了解專業知識或技術機制的細節，我們仍能掌握問題的本質，並懷抱緊迫感投入抗爭。這一點同樣適用於網路空間。即使我們「不理解」某些事物，仍能認清這是一個必須面對的嚴峻問題。

7.5. 您身邊或許沒有熟悉網路或電腦的人，您自己可能也有許多不完全理解的地方。這時該怎麼辦呢？

若您或您在人民運動中的夥伴正面臨此類問題，歡迎隨時向 JCA-NET 諮詢。

JCA-NET 支持各位在網路與電腦安全方面的努力。首先，讓我們來一場輕鬆的聚會——即使只有兩三個人也沒關係。JCA-NET 的成員將會與各位一同分享疑問，並討論可能的解決方案。

您可從下方連結下載本手冊的 PDF 版本。此外，我們也將逐步在此頁面發布手冊中未能收錄的補充資訊與說明：。請善用此資源。



<https://jca.apc.org/jca-netの取り組み/スパイ・To Monitor and Resist—What One Person Can Do/>

作者：JCA-NET | 發佈日期：2026 年 9 月 20 日

免費。若您覺得這份資料有幫助，請考慮捐款支持。本小冊子係運用 JCA-NET 會員會費及公眾捐款製作而成。

郵政轉帳帳戶：JCA-NET (J-C-A-NET)

帳號：00190-3-417584，日本郵政銀行第 019 分行，帳號 417584

*請在備註欄註明「捐款」。

允許為非商業目的進行轉載及複製。

JCA-NET 聯絡方式：，Toshimaru 070-5553-5495 toshi@jca.apc.org



<https://jca.apc.org>