市民組織のためのデジタル防衛マニュアル

Civil Society Organizations

數位防禦手冊

注重隱私與安全的開放原始碼工具

OpenCulture
Foundation_

Table of Contents

オープンカルチャー財団

2014年の設立以来、オープンカルチャー財団（OCF）は法人組織として台湾の40以上のオープンテクノロジーコミュニティを支援してきた。その過程で、オープンテクノロジーの概念を広めるだけでなく、政策提言にも参加し、人々のデジタル人権のために声を上げ、台湾におけるオープンテクノロジー発展の基盤を築いてきた。技術コミュニティや市民パートナーと連携し、参加形態が個人、コミュニティ、組織のいずれであれ、私たちは台湾のデジタル／ネットワーク環境をよりオープンで透明性が高く、市民参加型のものにするために共に努力している。

近年、OCFでは技術コミュニティと連携し、人材育成、ツールキット開発、イベント開催などを通じて、台湾の市民団体の情報セキュリティとデジタル能力向上に取り組んでいる。オープンテクノロジーの普及と分野横断的な協力を通じて、OCFは今後も台湾の技術コミュニティと他の公共／民間セクターを結びつけ、オープンな共創によるデジタル人権の保障、透明性と包摂性を支えるデジタル市民社会の実現を推進していく。

ウェブサイト ： https://ocf.tw メールアドレス ： hi@ocf.tw

画像出典 • Chrome、Safari、Microsoft Edge、Firefox、Firefox Focus、Brave、Librewolf、Tor 各ブラウザのアイコンはウィキメディア•コモンズ（Wikimedia Commons）サイトより取得した：https://commons.wikimedia.org/wiki/Main_ ページ • KeePassXC の画像は当該ソフトウェアの操作画面のスクリーンショットである。 • Nextcloudの画像は当該ソフトウェアの操作画面のスクリーンショットである。

1. 序論

1.1. デジタルセキュリティはなぜ重要なのか？

ほぼ全ての業務がインターネットに依存する時代において、世界中の市民社会組織（Civil Society Organization）[1]は、日常的な行政運営、内部•外部関係者との連絡調整、資金調達、記者会見や広報活動など、あらゆる業務プロセスでデジタルツールを活用することに慣れてきている。インターネットがなければ、市民組織の活動は困難を極めるだろう。

活動領域が物理空間からオンラインへ拡大するにつれ、市民組織の提言や行動の幅は広がる一方で、より多くのリスクや脅威に晒されるようになった。オープンカルチャー財団が2024年4月に公表した研究報告書[2]によれば、取材した35の人権•民主主義団体は、いずれも程度の差こそあれデジタル攻撃や脅威に遭ったことがある。各組織は公式サイトやSNSで頻繁に言葉による嫌がらせや脅迫を受けるだけでなく、半数以上がより深刻なデジタル攻撃に遭っている。監視、機密情報漏洩（寄付者データや支援対象者の所在情報など）、悪意あるネットワーク妨害、情報操作などが含まれ、中には独裁国家からの強圧的攻撃もあり、対応が困難だ！これらのデジタル攻撃は、組織が提唱し保護する価値観を損ない、組織の従業員、評判、資産に消えない損害をもたらしている。

提言活動において最も重要な資産は「人」と「声」である。「人」とは組織の提唱者を指し、「声」とは提唱活動の伝達経路や公式サイトに示される過去の成果を指す。『CSOs デジタル防衛マニュアル』は市民社会組織向けに書かれた、誰でも独学できるデジタルセキュリティ入門書だ。概念の構築、脅威の認識、より良い管理手法と防御ツールの理解を通じて、市民組織や人権活動家が基礎的な防衛知識を学び応用し、最も重要な資産を守る手助けをする。

デジタル攻撃は通常、ユーザーの「日常的なネット利用行動」を通じて侵入する。国際市民組織や独立系ジャーナリストを支援する非営利団体Internewsは、長年の支援経験から、組織と個人が基礎的な防御を徹底すれば、被害を大幅に軽減し、脅威を回避できる可能性があると指摘している。(2024年3月)[3]

本ハンドブックの主旨は、デジタルセキュリティ能力の基礎概念を固めることにある。市民組織の業務プロセスにおける四つの要素——ウェブ閲覧用ブラウザ、業務用アカウントのパスワード管理、データ管理とバックアップ、公式ウェブサイトの保護——をそれぞれ四つの章で解説する。概念から解決策、推奨ツールまでを網羅し、読者がデジタルセキュリティの概念を迅速に習得できるように構成した。さらに最後に、デジタル攻撃を受けた際の支援要請方法について注意を促す。

1.2. デジタルセキュリティ × オープンソース

オープンソースとは、ソースコードを公開し、誰もが閲覧•改善•監査できるようにすることを意味する。つまり、コードにはセキュリティ上の脆弱性が存在する可能性があるが、オープンソースは集団の知恵を結集し、迅速な修正を実現する利点を持つ。

コードはデジタル利用と密接に関わっている。全てのネットワークやデジタルサービスは、一連のコードの上に構築され、それによって動作方法(攻撃、データ収集、アドレス発見など)が決まる。私たちが知るネットやデジタルサービスの大半は民間企業に属し、これらは営利目的のためソースコードを公開しない。したがってユーザー、つまり私たちのデジタルプライバシーとセキュリティには一定の脆弱性とリスクが存在する。高リスクの人権活動家がソーシャルプラットフォームを利用すると一定の危険を招く理由もここにある——彼らは安全性の低いプラットフォームを使用することで、居場所や個人情報が漏洩し、組織活動の弱点となる可能性があるのだ。

本マニュアルで推奨するデジタルツールは、主にオープンソースのデジタルツールである。これらは世界中のオープンソース貢献者の知恵の結晶であるだけでなく、セキュリティ専門家や技術者からも認められ推奨されている。本マニュアルで言及するツールは全て三つの原則を満たしている。すなわち、インターネット上または信頼できるプラットフォームで公開され無料ダウンロードが可能、商業的利益による制約がほとんどない、開発過程でユーザーの安全とプライバシーをより重視している。これらのツールを通じて、市民組織活動家のデジタルセキュリティをさらに強化できる。

2. リスク評価

2.1. リスク評価

技術ツールの普及は、市民団体に新たな活動手法をもたらした。具体的にはより多様な決済連携手段を通じて支援者に働きかけ、資金調達を行うこと。また、オンライン会議やハイブリッド型のアプローチを通じて、現場での活動を行ったり、外部と連携したり、対象者へのサービスを提供したりすること、である。同時に、オンライン会議やハイブリッド方式の活用において、デジタル化に伴うリスクを直視し、管理方針を策定する必要がある。

ソーシャルメディアからクラウド上の仕事ファイル、寄付者データに至るまで、デジタル世界での私たちのあらゆる行動はデジタル足跡を残す。猫がトイレの後に砂をかき混ぜて匂いを隠すように敵に追跡されないことが大切だ。市民団体もまた、デジタルジャングルで自らを守る方法を理解する必要がある。

自己防衛の第一歩は、守るべき資産を特定することだ。そうして初めて潜在的な危険を分析し、対応するリスク管理メカニズムを策定できる。

これが「脅威モデリング」(Threat modeling)という概念だ。以下では、脅威モデリングの6つのステップを解説し、架空の組織A3を例に挙げて、組織のリスク評価やセキュリティポリシーの策定方法をわかりやすく説明する。

2.1.1. ステップ0 正しい認識を確立する

まず理解すべきは、「絶対的な安全」など存在しないということだ。 私たちにできるのは、相対的に安全な状態を可能な限り確保するプロセスを構築することである。家の資産を守るために、玄関ドアと鍵を設置し、鍵の所持者を管理することで、家に出入りできる者を制御するのと同じだ。 こうした対策は泥棒の侵入を完全に防げないかもしれないが、少なくとも一定の安全性は保証される。

組織 A[4] は、セキュリティポリシーを策定する前に、まず参加者全員に上記の考え方を周知し、誤った期待を避け、実行可能な方法の提案に集中させる。

2.1.2. ステップ1 保護すべき対象を明確化する

最も重要で保護すべき「資産」は何か？デジタル世界では、電子メール、連絡先リスト、寄付者情報、サービス対象者の個人情報、スケジュールや位置情報、さらには通信機器自体が資産となる。組織の資産を列挙し、 データの保存方法、保存場所、 データへのアクセス権限を持つ者、 データへのアクセスを制限する理由を明記する。[5]

組織Aは、政治難民支援団体として、資産には政治難民の現住所、連絡手段、移動経路などの情報が含まれる。これらのデータはGoogleドライブに保存され、全職員と外部協力者は共有アカウント「Staff」でアクセスする習慣がある。データ漏洩による政治難民の安全脅威を防ぐため、アクセス権限を制限すべきだと考える。

2.1.3. ステップ2 脅威の発生源を特定する

まず、リストアップした資産について、どの組織（企業、政府、民間団体）や個人がそれらを取得しようとするかを考える。彼らが「相手」だ。敵対者は競合他社、元上司、元従業員、ハッカー、あるいは過去の協力組織である可能性がある。もしあなたが独裁政権に対抗する人道支援者なら、政府、法執行機関、特定政権の代理人または団体が敵対者となり得る。注意すべきは、 この敵対者リスト自体が組織の重要な資産となり得る点だ。リスク評価完了後、このリストを破棄するかどうかを検討すべきである。

組織 Aの敵対者には、政治亡命者の母国政府機関、法執行機関、仲介組織（ロビー団体とハッカー）が含まれる。これらの敵対者は、政治亡命者を追跡するために我々の資産を入手しようとしている。

2.1.4. ステップ3 全ての脅威の潜在的な結果を可視化する

保護対象の資産が盗まれた場合、事態はどれほど深刻になるか？敵対者がどのような手段で私たちの組織の資産を入手できるか議論し記録する。可能性のある手段には、悪意のあるリンクをクリックさせる「フィッシング」――コンピュータにデータ窃取プログラムを仕込む[6]――が含まれる。敵対者は必ずしも高度な技術を用いるわけではなく、「ソーシャルエンジニアリング[7]」で信頼を得て情報を入手する可能性もある。

相手の能力を考慮することを忘れないようにしよう。例えば相手が政府機関なら、通信事業者から通信記録を入手する能力がある。さらに、相手が資産をどう利用するか？組織にどんな危険をもたらすか？を思考し書き留めよう。可能な限りあらゆる結果を書き出すことで、組織は想定される事態を想定しやすくなる。

組織Aのばあい、 敵対者は外部委託組織に潜入し、スタッフアカウントのパスワードを入手して政治難民の個人情報を取得し、その結果、政治難民の居場所が露見する可能性がある。

2.1.5. ステップ4 資産保護レベルの評価

次に、ステップ3で整理した悪事発生確率を評価する。私たちがどれだけの代償を払う覚悟があるのかについては主観的判断を伴う。例えば、市民団体が直面するシナリオは以下のように分類できる。

- 確率が低いが代償が高い：人権活動家が独裁国家に出張し、現地政府に逮捕される確率は低いものの、発生した場合、組織が人材を失う代償は大きい。
- 発生確率は高いが代償は低い：事務所に協力者の名刺が散らばっているが、名刺の情報は機密性が低く、たとえ漏洩しても重大な被害をもたらさない。

全ての脅威発生確率を個別に判断し、 どの脅威が厳重な警戒に値するか、あるいはあまりに稀で比較的無害ゆえに懸念不要かを議論する。

組織Aのばあい、ステップ3で推定した結果の発生確率が必ずしも高くない場合でも、一度発生すれば政治難民の生命の安全が脅かされ、代償が甚大であるため、資産を極力保護すべきと判断する。

2.1.6. ステップ 5 支払う意思のある保護コストの決定

現実的な安全戦略とは、利便性とコストのバランスを取ることにある。例えば、究極の安全を求めて自宅のドアに数十個の錠前を取り付け、さらに警備システムを導入した場合、毎月の警備費用は莫大なものとなる。結果として家族は帰宅時に鍵を開けるのに時間がかかり面倒だと感じ、毎日たった一つの錠だけをかけて出かけるようになる――明らかに不便で財政的負担の重い安全対策は、あなたには適していない。

脅威発生の確率を下げたり損失を軽減する方法を書き出せ。同時に、資金や注意力、能力といったリソースの制約を考慮し、組織メンバー全員が納得して実行できる方法を見つけ出せ。そうして初めて、セキュリティ戦略は真に実現されるのだ。

組織 Aのばあい、利便性を多少犠牲にし、全職員に個人アカウントの使用を義務付けることにした。同一のアカウント・パスワードの共有を禁止し、各データのアクセス権限を明確に管理するためだ。同時に権限階層制度を設け、プロジェクト関連職員のみにデータ使用権限を付与する。組織外メンバーは申請を経て承認された場合のみアクセス権を得る。この決定は全員の能力（全員がクラウド協業に精通している）に合致し、追加の財務負担も生じないため、実現可能だ。

2.1.7. ステップ6 相互支援の同盟を見つける

デジタルセキュリティ空間の構築は集団活動である。協力すれば力が強まるだけでなく、協力ネットワーク内のいずれかが攻撃されれば、最終的に自らが被害を受けることになるからだ。協力ネットワークの中から、自組織と類似の脅威に直面している、あるいは同じ資産を保護している団体や個人を探し始める。

類似の脅威に直面する団体（または個人）と相互支援協定を結ぶ方法がある。具体的には、情報共有（潜在的な敵対者や脅威の手法リストなど）、資源共有（セキュリティ講師の雇用費用を共同負担するなど）を通じて、相互のコスト削減、セキュリティ意識の向上、組織のレジリエンス 化を図ることができる。

組織Aは、組織Bとは政治難民に一時的な住居を提供しているため、密接に連携している。このため、組織Aは組織Bと敵対勢力及び潜在的な脅威のリストを共有することを決定した。これにより組織Bが脅威の源を把握し、安全対策方針を構築する手助けとなる。

2.1.8. ステップ7 リスクを定期的に再評価し、安全方針を頻繁に見直す

新たなリスクや脅威は常に発生し得る。また組織では新旧メンバーの交代により使用習慣が変化する可能性があるため、定期的にリスクを評価し、組織が現在保護すべき目標に対して適切な安全手順を策定していることを確認する必要がある。同時に、旧職員には安全方針を復習させ、新入社員には理解させることも重要だ。

組織Aは、新たなスタッフにはセキュリティポリシーの読了を義務付け、年末には全員でリスク評価プロセスを検証する。これにより、守るべき資産と許容できるコストについて共通認識を持つ。職員が懸念を表明することを奨励している。例えば、アカウントのパスワードを忘れることを恐れて付箋に記録し、パソコンに貼る者がいた。これは、頻繁に訪問者が訪れ、他の団体とオフィススペースを共有している組織にとって、データベースの鍵を放置しているに等しい。このため、セキュリティポリシーを修正し、このような行為を禁止する必要があると判断した。

3. 事例紹介

3.1. 事例

なぜリスクを重視し、脅威モデリングやデジタル防御の道を開くことが、どれほど重要なのか？本章では引き続き組織Aを例に、読者を組織Aの職員「小明」にみたてて、日常行動におけるデジタルリスクの所在を探ってみよう。

3.2. やられた、めちゃくちゃだ……

組織A はこの間、C政府に迫害された政治難民の救出を集中的に準備していた。他の団体と協力して救出ルートを手配し、 人々が台湾に到着した際の仮設住居も確保していた。必要な資金を調達するため、組織Aは独自にウェブサイトを立ち上げ、C政府の非道な人権侵害行為を暴露する報告書を発表した。これにより多くの市民の関心を集め、匿名で寄付する善意の人々も多数現れた。ところが、救援開始の前日、救援ルートに政府Cの執行機関が現れた。手配済みの仮住居は悪意のある落書きの被害に遭った。救援対象者は恐怖で姿を隠し、仮住居を提供していた団体は脅威を感じて協力を打ち切った。組織Aの救援任務は完全に失敗に終わった。さらに小明は通勤中に尾行されている気配を感じ、慌てて近くの派出所へ駆け込んだが、そこには尾行者が立ち去る姿しかなかった。

追い打ちをかけるように、ウェブサイトが「分散型サービス妨害（DDoS）」攻撃を受け、閲覧不能となった。実はC政府が支持者を動員し、組織Aのサイトに同時に大量接続させ、システムリソースを枯渇させていたのだ。小明は別の方法で報告書を公開しようと試みたが、サイト上の報告書が消えていることに気づいた！同僚とオンラインで共同作業した成果は跡形もなく消え、初版報告書を保存していたノートパソコンはクラッシュしてデータが復元不可能に。一方、寄付者からは組織Aに「個人情報が漏洩した」と抗議の電話が殺到し、政府Cは「C国で事業を行う家族に危害を加える」と脅迫してきた。組織Aは支援者の信頼を失っただけでなく、外部への発信手段も失い、苦労してまとめた報告書は水の泡となった。

小明と同僚は抱き合って泣いた。自身の安全を憂えるだけでなく、難民支援を完遂できなかったことに胸を痛めたのだ。彼は天に向かって叫んだ。「神様！一体どこが間違っていたんだ！？」その時、天から神が現れ、小明を過去へ連れ戻し、どこで誤りが生じたかを見せよう、と告げた。それが現在の組織危機に対処する助けになるかもしれないと。

3.3. 過去を振返る。どこで間違えたのか？

神の力によって、小明の視点は事件の1ヶ月前に戻った。

いつものように、小明は個人アカウントに紐づけたナビゲーションアプリ「Nono Map[8]」を開き、保存済みの自宅とオフィスの住所をタップして、システムにルートと接続するバス便の手配をさせた。組織Aのセキュリティポリシーを厳守する小明は、組織共有アカウント「Staff」を使用しない規定に従い、自身の業務用アカウントでNono Driveクラウドストレージにログインし、救助対象者の資料を閲覧した。

小明はNonoブラウザを開き、素早く万能パスワードを入力した。パスワードを忘れないように、組織Aの個人アカウントを仕事用アカウントとして設定し、CanvaやTrelloなどのアカウントも全て同じIDとパスワードで統一していた。無事にログインすると、小明は救援予定ルートを整理した。もちろん、同じアカウント情報で同僚のメイが無料サイト構築プラットフォームWoodlessで立ち上げたサイトの管理画面にもログインし、政府Cによる悪名高い迫害報告書の完

成を確認した。

この報告書作成過程を振り返ってみる。小明はノートパソコンを持って各地を奔走し、学者や迫害事件の目撃者、様々な利害関係者にインタビューを重ねた。数ヶ月を費やし、ようやくこの貴重な素材を整理し、論理的で充実した報告書にまとめた。その後、ノートパソコンからこの報告書をWoodlessの下書きエリアにアップロードし、同僚がオンラインで編集できるようにした。二週間、同僚と何度も修正を重ね、今日ようやく編集を終えて公開した。ほっと一息ついた小明は、Nonoブラウザで新しいタブを開き、Nono検索エンジンで無料小説サイトを探し、しばらく小説が紡ぐ幻想世界に浸って、 間の苦労を労おうと思った。

「まったく、ちょっと休みたいだけなのに、またあの国際人権団体の募金広告が？」この頃、フェイスブックをスクロールしてもネットショッピングをしていても、あの団体の広告が突然視界に飛び込んできて、小明はまるでずっと仕事から解放されていないような気分になり、精神的な疲労がどんどん蓄積していった。そして今、 広告がまた、小明が見つけた小説サイトを覆い隠してしまった。

しかし、別のことがすぐに小明の気を散らした。「おかしいな、なんで『安全でない接続』の警告が出るんだ？」URLバーの左にある鍵マークに赤い斜線が引かれているのを見て、小明は困惑した。考え直した。小説を読むだけだ、誰にも迷惑をかけない、大げさに騒ぐ必要はないだろう！彼は自分の万能アカウントとパスワードを使って のサイトでアカウントを作成し、会員限定の小説コンテンツを読んだ。次回より早くログインするために、彼はこのタブを「お気に入り」に追加し、Nonoブラウザにアカウントとパスワードを記憶させることに同意した。

「なんて人間味あふれる設計なんだ！」と小明は思った。 これでパスワード入力の手間も省ける、素晴らしい！」

午後、小明はNono Mapのルート計画に従い、救援対象者の台湾到着時の仮住居を提供する団体Bを訪問し、実際の空間配置と生活機能を確認した。面会の合間にスマホの通知を確認すると、同僚から「匿名寄付が数件入っている」と連絡があった。自分の使命が他人に支えられていると感じ、小明は深く感動した。人々の支援があれば、一ヶ月後の救援活動は必ず十分な資金を集め、計画通りに進み、これらの政治難民たちが安心して台湾で新たな生活を始める手助けができると確信した。

3.4. 神の目線：「相手」は一体どんな手を使ったのか？

「え？ これって、私の一日の日常のことだろ？何か間違ったことしたっけ？」小明は相変わらず困惑し、さらに慌てふためいた。

「お前の組織がリスク評価で議論した脅威の源、つまり『相手』のことを覚えているか？」神はしばらく沈黙した後、口を開いた。

「 もう一度お前を1ヶ月前に戻してやる。 おまえの相手が何をしたか見てこい。答えを見つける助けになるだろう。」

組織Aの救援活動を妨害するため、政府Cは自国市場に依存するNonoグループに対し、組織AのIPアドレスを特定し、組織Aの全デジタル足跡記録の提出を命じた。長期にわたる追跡と分析を通じ、政府Cは次第に政治難民と接触した職員を特定していった。小明もその一人だった。政府Cは、小明個人のアカウントと仕事用アカウントで閲覧した資料、地図検索履歴、移動軌跡などの情報を組み合わせた結果、小明のデジタルプロファイルが明確になり、通勤ルートを特定できるほどになった。

小明が無料小説サイトにアクセスし、Nonoブラウザにアカウントとパスワードを記憶させた時、政府Cは容易に彼の認証情報を入手し、その情報を使って政治難民を救出するための全資料を成功裏に取得した。さらに小明の地図検索記録を照合し、今回の救出作戦の連絡ルートと仮設住居を特定した。

組織Aの再起を阻むため、政府CはハッカーをDDoS攻撃を仕掛け、組織Aのサイトをダウンさせた。これにより市民は寄付ができなくなり、政府Cを告発する報告書も読めなくなった。組織AがWoodlessで構築したサイトに対し、ハッカーは無料プラグインの脆弱性を突いて堂々とサイト管理画面に侵入。告発文書を一掃し、全寄付者の情報を盗み出した。

3.5. 一からやり直すとして、どうすれば同じ過ちを繰り返さないか？

「今の惨事を防ぐには、一体どうすればいいんだ？」過去と全貌を見ても、小明にスーパーヒーローの能力はない。間違いをどう修正すればいいのか分からないのは当然だ。

「世界が破壊されるのを防ぐため、世界の平和を守るために…えへん！」神様が空から巻物を取り出し、小明に渡しながら慈悲深く言った。「この天の書をよく修練せよ。全ての秘訣を書き記した。お前たちに希望を授ける。この書をよく修練せよ。秘訣をすべて記してある。」

さあ、小明と共に学びの道へ踏み出そう！

4. 事前のテスト

小明と組織Aの物語に驚いただろうか？小明は不運ゆえに不幸に見舞われたと思うかもしれない。だが〈リスク評価〉の

章の例で言えば、普段から家のドアを開け放しにしておけば、そもそも悪党が侵入する確率が高くなる。だから小明の悲劇は単なる例外で、自分には起こらないと考えるべきではない。

この学習をより効果的にするため、小明が遭遇した様々な状況を以下の問題に分解した。紙とペンを用意し、自分の行動と選択を記録してほしい。普段通りの方法で回答すれば、 は、今後どの分野のデジタルセキュリティを強化すべきか理解する助けとなる。

4.1. ブラウザの使用習慣

4.1.1. 以下の記述のうち、あなたの使用習慣に当てはまるものはどれか？(複数選択可)

- [ ] 仕事とプライベートで同じパソコン、または同じスマートフォンを使っている。 (1点)
- [ ] 勤務時間内外を問わず、同じブラウザでネット検索をする習慣がある。 (1 点)
- [ ] 仕事用の事務処理に個人アカウントを使う習慣がある。(1点)
- [ ] 仕事用アカウントと個人用アカウントを明確に区別し、個人アカウントで仕事関連のメールを送受信しない。
- [ ] 同僚が素早く資料を入手できるように、会社の共有パソコンで文書を処理する際、通常は自分の仕事用アカウントからログアウトしない。 (1点)
- [ ] 外部の見知らぬコンピューターを使用する際は、シークレットモードを起動し、使用終了時には必ず自分のアカウントからログアウトする。

4.1.2. ブラウザを選ぶ際、以下の点を評価するだろうか？(複数選択可)

- [ ] ブラウザの性能を重視する。例えばインターフェースがシンプルで使いやすい、データの読み込みが速い、多くのタブを同時に開けることなどだ。(1点)
- [ ] 私はプライバシーをより保護できるブラウザを探す。例えば広告をブロックしたり、デジタル足跡を消去できるもの。
- [ ] クロスプラットフォーム同期機能は私にとって非常に重要だ。異なるデバイス間でブックマーク、パスワード、設定を同期する必要がある。(1 点)
- [ ] オープンソースのブラウザを好んで使う。ソースコードの透明性があるから安心できる。

4.1.3. 毎日多くのウェブページを閲覧し、マウスでスクロールしたりクリックしたり、指で画面をタップしたりする動作は、もはや無意識のものになっているかもしれない。ここで思い出してほしい。友人がLINEでウェブページを送ってきた時、会話画面を開いた後の次の行動は何だろうか？

- [ ] LINEの会話画面からURLをクリックし、そのウェブページにアクセスする。 (1 点)
- [ ] URLをコピーし、ブラウザを開いて貼り付けてページにアクセスする。

4.1.4. ページを開くと、URLバーの左側に鍵が×印で消されたアイコンが表示された。しかし、ウェブページは他の警告を表示せず、閲覧を続けることができる。次に何をしますか？

- [ ] 普段使っているブラウザでサイトを見る。 (1 点)
- [ ] シークレットモードを開くか、プライバシー保護に定評のあるサイトに切り替える。このサイト閲覧時は個人情報を入力せず、閲覧後はすぐに閉じるよう特に注意する。
- [ ] すぐにページを閉じて閲覧をやめる。

4.1.5. ウェブページを閲覧しようとした時、画面下部にメッセージが表示され視界を遮り、即座に選択を迫られる。さもないと閲覧を続けられない。どう選択する？

- [ ] クッキーって何？左側が白く光ってクリックしろって言ってるから、もちろん左を選ぶ！(1点)
- [ ] 右側をクリックし、数十秒かけてクッキーの管理方法を調べる。

「ブラウザの使用習慣」の項目で5点以上取ったなら、〈デジタル足跡の基本防御：オープンソースで安全なブラウザ〉の章をしっかり読んで、安全な使用習慣を身につけることを強く勧める。

4.2. パスワード管理

4.1.1. 個人用娯楽、ショッピング、仕事で使うソフトなど、どのサービスもアカウント設定が必要だ。これらのパスワードはどう管理しているか？ (複数選択可)

- [ ] 1つの汎用パスワードを全サービスで使い回している。新しいアカウントを作るたびにこのパスワードを使う。(1点)
- [ ] 手帳を持ち歩き、アカウントとパスワードを書き留める。昔ながらの方法だがロマンチックで、ハッカーによるパスワードの盗難も防げる。(1点)
- [ ] 付箋にパスワードを書いて、パソコンの画面やデスクに貼っておく。必要な時にちらっと見る。(1点)
- [ ] パスワードが多すぎて覚えきれないから、パスワードマネージャーに保存している。

☐ 常に「ログアウトしない」に設定している。もしそのサービスから強制ログアウトさせられても、「パスワードを忘れた」をクリックし、サービスが自動で割り当てるパスワードを使えばいい。（1点）
☐ 自分の記憶力には自信があるので、すべてのアカウントとパスワードを頭の中に記憶している。（1点）
☐ ブラウザは親切で、パスワード保存を聞いてくる。ブラウザに記憶させれば自動入力できる。（1点）

4.2.2．コンサートチケットを購入しようとしたところ、決済直前の最終段階で会員登録を求められた。基本情報を素早く入力した後、パスワードはどう設定する？

☐ もちろん万能パスワードを使う。どこでも使えるし、一生忘れないからな。（1点）
☐ 12文字以上の文字列を使う。意味のある単語を使っても構わないが、長さが十分であることが重要だ。

「パスワード管理」の項目で4点以上取ったなら、〈全てのパスワードを一元管理：パスワードマネージャー〉の章をしっかり読んで、安全な習慣を身につけることを強く勧める。

4.3．ウェブサイトの管理とメンテナンス

4.3.1．あなたの団体は自社でウェブサイトを運営しているか？あるいは外部に委託しているが、自分でメンテナンスしているサイトはあるか？通常、そのサイトをどのように利用・管理しているか？（複数選択可）

☐ 全従業員がサイト管理画面にアクセスでき、各自で掲載内容を更新できる。（ 2 点）
☐ ウェブサイトが受ける可能性のある攻撃については議論したが、対応方法が分からず、対策案は未だに策定されていない。（ 1 点 ）
☐ 定期的にウェブサイトのセキュリティをスキャンし、プログラムの脆弱性がないかチェックしている。
☐ これまでサイトが攻撃された経験がないため、対応策について議論したことがない。いざとなればその時に考えればいいと思っている。（2点）
☐ 信頼できるセキュリティ専門家のリストを収集しており、自社で解決できない問題が発生した際には彼らに支援を依頼できる。

4.3.2．利便性を高めるため、ウェブサイトには多かれ少なかれサードパーティ製のプラグインが導入されることがあります。あなたの団体では、プラグインを採用する際、以下の評価を行っていますか。（複数選択可）

☐ プラグインに関するセキュリティ上の問題が報告されていないかを確認する。
☐ 情報セキュリティの専門家に、そのプラグインが信頼できるかどうかを相談する。
☐ プラグインの更新頻度やメンテナンス履歴を確認する。
☐ 当団体の要件にはそのような規定がなく、機能が要件を満たしていれば使用する。（1点）
☐ セキュリティ評価を行う専門知識やリソースがないため、評価できない。（1点）

「ウェブサイト管理とメンテナンス」の項目で4点以上を獲得した場合、〈市民団体の自主運営ウェブサイトを安全に守る〉の章を熟読し、安全な使用習慣を確立することを強く推奨する。

4.4．データのバックアップ

4.4.1．重要なデータ（仕事用ファイルや個人写真など）のバックアップはどのくらいの頻度で取るか？

☐ 定期的にバックアップを取る習慣がある（例：毎週•毎月決まった日）。
☐ データ収集がある程度まとまった段階でバックアップする習慣がある（例：報告書の進行状況があるバージョンに達した時）。
☐ 思い出した時や時間がある時にバックアップする。（1点）
☐ データのバックアップ習慣がない。（2点）

4.4.2．主に使っているパソコンやスマホが突然故障した場合、大部分または全ての重要なデータを復元できるか？

☐ できる。最近バックアップを取っているので、最新のファイルに復元できる。
☐ 一部しか復元できない。バックアップデータが最新ではないからだ。（1点）
☐ できない。普段バックアップを取らないから。（ 2 点 ）

4.4.3．データバックアップを行う際、どのように進めるか？

もしバックアップをしたことがないなら、仮にバックアップするとしたらどうするか考えてみよう。

☐ データをパソコンの異なるフォルダに保存している。元のフォルダが開けなくなったら、別のフォルダからファイルを取り出す。（2点）
☐ ファイルはパソコンとクラウドストレージ（例：Google Drive、WordPress管理画面）にそれぞれ保存し、相互にバックアップする
。（1点）
☐ ファイルは自分のパソコンとUSBにそれぞれ保存し、万が一に備える。（1点）

- [ ] ファイルをパソコン、クラウドストレージ、USBまたは外付けハードディスクの3箇所に保存する。

「データバックアップ」の項目で1〜3点の場合は、基本的なバックアップ知識はあるが十分とは言えない状態だ。4点以上なら、〈バックアップ321を徹底してデータ損失を防ごう〉の章をしっかり読み、安全な使用習慣を身につけることを強く勧める。

5．デジタル足跡(デジタルフットプリント)の基本的な防御―オープンソースで安全なブラウザ

5.1．事例

小明がブラウザの使用習慣によって引き起こされたリスクは何だったか分かるだろうか？答えを考えてから、下で確認しよう！

答え：小明は仕事用アカウントと個人用アカウントを同じノートパソコン、同じブラウザで使い、ブラウザに検索履歴を記憶させない設定もしていなかった。そのため仕事中に調べた記録から、広告主は彼が人権問題に関心があると判断した。結果、小明がプライベートで買い物や娯楽を検索すると、仕事関連の広告が表示されるようになった。

- 上記の使用習慣から、小明は同じブラウザで開発されたナビゲーションサービスを利用している。そのため、同じネットグループが小明の毎日の通勤ルートや仕事の調査先を把握できる。
- 小明は無料小説サイトでアカウントを作成し、ブラウザにIDとパスワードを記憶させた。ブラウザ内にIDとパスワードを保存するのは安全な操作ではなく、情報が漏洩したり悪意を持って取得されたりする危険性がある。
- 無料小説サイトはHTTPS暗号化接続を採用していないため、閲覧や入力した内容（ログインページのパスワードを含む）は、ネットワーク伝送中に容易に傍受される危険性がある。

小明の事例から分かるように、生活でも仕事でも、ブラウザはパソコンやスマホで様々なサイトを訪れる際の交通手段だ。デジタルセキュリティは当然、ブラウザを評価する重要な項目となる。

5.2．概説

ブラウザはネット世界への「入り口」のようなものだ。私たちはブラウザを使ってネット上で情報を検索し、人と会話し、動画を見る。同時に、現代のウェブサイトは広告収益を得るために、可能な限りユーザー情報を収集しようとする。このユーザー情報の収集は長年続く商業マーケティングの基本機能であるだけでなく、一部の安全でない悪意のあるサイトは、ユーザーが入力した機密情報を傍受したり、ブラウザに保存された閲覧履歴やアカウントパスワードを盗み出したりして、デジタル攻撃を行うこともある。ラウザを利用する際に注意すべき脅威やリスクをいくつか挙げる。

5.2.1．クッキー(Cookie)、その背後には大きな懸念がある

クッキーとは何か？

ここでのクッキーとは、お菓子ではなく、そのウェブサイトにアクセスしたユーザーの情報を記録し、パソコンやスマートフォンのブラウザに保存する仕組みのことだ。

ウェブサイトがクッキーの有効化を尋ねる画面.png 図：ウェブサイトがクッキーの有効化を尋ねる画面

なぜほとんどのサイトでは、一度アカウントとパスワードを入力すれば、その後頻繁にログインしなくて済むのか？ユーザーが同じサイトにアクセスするたびに個人情報を再入力する手間を省くため、現在ほとんどのサイトがクッキー技術を利用している。初めてサイトを訪問すると、通常クッキーを有効にするか尋ねられる。同意した場合、そのサイトを利用する際、さまざまな情報が記録されることになる。

この技術は道端にクッキー（クッキー）の屑を撒いて足跡を記録するようなものだ。ユーザーのログイン情報、ショッピングカートのリスト、閲覧したウェブサイトの履歴、さらにはアップロードした画像や動画ファイルまで、全てブラウザソフトがコンピュータ内の特定のフォルダに一時保存する。

クッキーは非常に便利だが、悪用される可能性もある。例えば、あなたのウェブサイト閲覧履歴は、広告主があなたを理解するための根拠となる。最近どこに行ったか、何が必要か、どのネットサービスを利用したかなどが含まれる。例えば単に「Appleのパソコン」と一度検索しただけで、その後ウェブサイトで目にする広告のすべてが、「パソコンを買いたいのか」「周辺機器をもっと買わないか」と尋ねてくるようになるかもしれない。もしクッキーが暗号化されていなければ、ハッカーはあなたのクッキーを悪用して、簡単になりすましを行い、サービスにログインすることさえ可能だ。

5.2.2．デジタルフィンガープリント追跡技術（Browser fingerprinting）：会話を盗聴するスマホ、生活を覗き見るネット

何も入力していないのに、サイトはあなたの位置、言語、使用中のデバイスを既に把握している？

ブラウザを使うと、ブラウザは特定のデバイス情報、OS、ブラウザ、画面サイズ、タイムゾーン、フォント、言語など

を把握できる——。この一連の情報が各ユーザーのデジタルフィンガープリントとなる。多くの広告主はトラッカーを使ってウェブサイトのユーザーのデジタルフィンガープリントを収集する。デジタルフィンガープリント追跡技術はクッキーよりもさらにひどいもので、ユーザーの同意すら得ずに上記の情報を絶えず記録し続ける。

現在、多くのウェブサイトは同じ企業に属しているか、あるいは異なる企業が協力協定に基づいてユーザーデータを共有できる。例えば、FacebookとInstagramはどちらもMeta社に属し、Google検索エンジンとChromeブラウザも同じ企業に属している。閲覧したサイトが多ければ多いほど、トラッカーはあなたのデジタルフィンガープリント（特定のデバイスやブラウザの特徴）とクッキー（訪問したサイトや閲覧内容）を照合しやすくなり、広告主はあなたについてより多くの情報を得られるようになる。 こうした情報により、広告主はより説得力のある広告を正確に配信できる。政府や権威主義組織が公権力を使って反体制派のデジタルフィンガープリントなどの情報を入手すれば、彼らのネット上の身元を特定し、さらに実名や位置情報を推測することも可能になる。

5.2.3. HTTP 対 HTTPS — たった1文字の大きな違い

ウェブサイトを閲覧する際、サイトはクッキーやデジタルフィンガープリントで追跡する。しかし現在、大半のサイトは HTTPSだ。SはSecureの略で、サイトが暗号化保護されていることを示す。つまり閲覧先を知るのはサイト側だけで、ネット上の見知らぬ第三者には知られない。

一方、暗号化保護のないHTTPサイトに接続すると、それはまるで即座にウェブカメラをオンにし、マイクを最大音量にするようなものだ。ネット上で自分の行動や情報を放送し、デジタル上の姿を丸見えにしてしまう。このような暗号化保護のないサイトでは、ネット上で自分が晒される可能性がある。自分以外の誰もがデータを収集できるだけでなく、コンピュータへの侵入や生活の監視さえも許してしまうのだ。

このようなサイトをどう見分けるか？サイトを閲覧中に「安全でない接続」警告が表示されることがある。URL左側に鍵マークが×印で表示されるのだ。下図の通りだ。

図：HTTP非暗号化警告のイメージ図

これは、そのサイトとの接続が暗号化保護されていないことを示している。暗号化保護のないHTTPサイトに接続を続けると、サイト上での閲覧行動、入力内容、マウスの移動位置、入力したアカウントやパスワード、金融情報などが、ネット上の誰にでも丸見えになるのと同じだ。— 同じ会議室、教室、カフェ、空港で同じWi-Fiを利用している他の人々、特に悪意のある者がいれば、彼らは労せずしてあなたの情報を入手し、悪用する可能性がある。セキュリティとプライバシーを重視するユーザーは絶対にこのような状況を避けるべきだ。そのため、ブラウザ設定でHTTPS接続だけを許可し、通信過程を暗号化保護することが最善策である。そうすれば、一度の不注意で重要な情報が漏洩する事態を防げる。

5.2.4. 利用可能なツール

市場には多様なブラウザが存在し、自身のニーズに合致し、プライバシーとセキュリティを重視したブラウザを理解し選択することは非常に重要だ。自分に合ったブラウザの選び方を見ていこう。以下は台湾で一般的なブラウザの選択肢である。

Google Chrome	Safari	Microsoft Edge	Firefox
最も利用者の多いブラウザ	アップルに標準登載されているソフト	Windows内蔵ソフト	非営利団体が開発したソフト

小明の事例から見て、ブラウザの安全性を軽視すると、軽い場合は個人情報がサイトに収集されたり、ユーザーのデジタル足跡が漏洩したりする。重い場合はアカウントやパスワード、金融情報が盗まれたり、閲覧画面や送信中の会話内容が監視されたりする。

道路を走るクルマが速いから安全とは限らないのと同じで、最も利用者の多いブラウザが、セキュリティとプライバシーを重視すべき市民団体に適しているとは限らない。市民団体がブラウザの使用段階から基本的なデジタル防御能力を備え られるよう、本節では特にプライバシーとセキュリティを重視したブラウザを紹介する。これらは全てオープンソースの規範に準拠しており、全てのユーザーがプログラムの動作ルールを確認できる。これにより、誰もが動作上の脆弱性を検証できる一方、ユーザーは自身のニーズに応じて異なる機能のバージョンを改造することも可能だ。 特にFirefox、 LibreWolf、 Torは非営利団体やネットコミュニティのボランティアが開発•保守するソフトウェアだ。これらは広告収入に縛られず、ユーザーの安全保護に専念している。

また、 ChromiumはGoogleがChrome開発のために公開したオープンソースソフトウェアで、BSDライセンスなど複数のライセンスで提供されている。そのコアを開放し、他の企業がChromiumベースのブラウザを開発できるようにしている。

以下はプライバシーとセキュリティを重視したオープンソースブラウザの例だ：

Firefox	Brave	LibreWolf	Tor	Chromium
非営利団体が開発したソフトウェア	プライバシーを重視した商用ブラウザ	ボランティアによって開発•保守される非営利ソフトウェア	ボランティアによって開発•保守される非営利ソフトウェア	Google が Chrome公開したオープンソースソフトウェア

ブラウザ機能一覧

利便性とプライバシー保護のバランスをどう取るか？ 市民団体が情報の漏洩や悪意ある監視を望まないという基準で考えるなら、前述の通りブラウザの厳格な選択が極めて重要だ。以下は現在市場で知られているブラウザと、本マニュアルが推奨するブラウザの機能比較表である。これが皆がネット世界へ通じる門を選ぶ助けとなるだろう。

ブラウザ	クッキーを保護し、終了時に削除する	フィンガープリント追跡を厳格にブロックする	HTTPS暗号化を強制する	特徴
Firefox	あり	あり(自分で設定する必要あり)	あり	更新が早い。プライバシーとセキュリティ機能拡張を利用可能
Brave	あり	あり	あり	更新が早い。Chromiumのコア技術を使用。広告ブロック機能内蔵
Librewolf	あり	あり	あり	コミュニティ管理。広告追跡をブロックする各種プラグインを内蔵。
Tor	あり	あり	あり	非営利。米軍情報要員向けに開発され、暗号化が特に高い。追跡とユーザーの身元を完全に隠蔽。ほとんどのウェブページを閲覧できないため一般の日常生活での使用には適さない。
Mullvad Browser	あり	あり	あり	orブラウザを基盤としており、Mullvad独自のVPN[9]を使用できる。uBlock Origin[10]とNoScript[11]がプレインストール。
Chrome	なし。サードパーティクッキーのみブロック可能	なし	なし	最も多く使われていて、ハッカーの標的になりやすい。更新が速い。
Safari	なし。サードパーティクッキーのみブロック	あり	なし	組み込みのスマートトラッキング防止機能

注：本表の作成時期は2024年3月である。ブラウザは定期的に更新されるため、各ブラウザの詳細情報は公開情報をご参照ください。

5.2.5. ちょっとしたヒント

各ブラウザの使用方法はほぼ同じで、誰でも簡単に扱える。デジタル防御力を高める鍵は、ブラウザの内部設計と個人の使い方にある。以下に、ブラウザ使用の習慣を身につけ、ネット利用をより安全にするヒントをいくつか紹介する。

1. できるだけブラウザでウェブページを開き、コンピュータに直接ソフトウェアをインストールするのは避ける

   コンピュータでさまざまなウェブサイトにアクセスする際、Facebook Messenger、Slack、Discord、あるいはOutlookなどのメールソフトなど、仕事でよく使われるコミュニケーションソフトを別途ダウンロードして、コンピュータやスマートフォンにインストールするかどうかを尋ねられることがよくある。これらのコミュニケーションサービスをブラウザ経由で利用すれば、これらのソフトウェアがブラウザという枠組み内でのみ動作し、デバイスの他の機能を容易に危険にさらすことはない。逆に、デバイスに直接アプリをインストールし、このアプリに組込まれているブラウザ(アプリ内ブラウザと呼ぶ)を利用すると、画面の録画やフォルダ内容への直接アクセス、さらには他のインストール済みソフトウェアの操作権限まで与えてしまう可能性があり、安全な方法とは言えない。

2．スマートフォンやタブレットのSNSアプリ内で直接ウェブページを閲覧するのは避けるべきだ。

同様に、普段スマホやタブレットで各種SNSアプリを使う際、アプリ内のリンクをクリックしてアプリ内で直接閲覧することが多い。例えば、メッセージアプリで友達から送られてきたショッピングサイトのリンクを直接開いて、ここから購入するといった具合だ。しかしこの方法では、実はアプリがユーザーの入力内容を全て直接記録する機会を提供することになる。他のサービスのアカウントやパスワード、金融情報を入力すると、それらが直接アプリに取得されてしまう。したがって、SNS内のリンクをコピーした後、前述のオープンソースで安全なブラウザを使って閲覧することを推奨する。

3．自動でシークレットモードを有効化するブラウザ Firefox Focus

公共の場所や見知らぬPCでブラウザーのシークレットモードを使うと、閲覧の安全性が少し上がる。 スマートフォンやタブレットにダウンロードできる「 Firefox Focus」をお勧めする。これはFirefoxをベースにしたブラウザで、追跡をブロックするだけでなく、アプリを閉じるたびにクッキーや閲覧履歴を削除する。スマートフォンやタブレットでウェブページを開き、閲覧後にすぐに閉じる用途に最適で、ほとんどの追跡行為を負担なく回避できる。

4．パスワードをブラウザ管理に預けるな

あなたがどのブラウザを使っていても、アカウントとパスワードを入力する際に「ブラウザにパスワードを管理させるか」と尋ねられることがある。 そうすれば次回入力時にブラウザが自動で貼り付けてくれるからだ。セキュリティやプライバシーを重視する人は、このようなことはしない方がいい。ブラウザの防御ラインがハッカーに突破された場合、全てのアカウントとパスワードが一括で盗まれる可能性があるからだ。多数のアカウントとパスワードを管理する必要がある場合は、別途パスワード管理ソフトの使用を推奨する。本マニュアルで後述するKeePassXCやBitwardenを参照するとよい。

5．公式ダウンロードが最も安全だ

PCを使用する場合、前述のプライバシー重視のFirefox、Brave、LibreWolf、Torの4つのソフトウェアは、公式サイトからのみダウンロードすることを推奨する。スマートフォンやタブレットなどのモバイル端末を使用する場合、Android端末はGoogle Playストアから、iOS端末はApp Storeから直接ブラウザソフト名を検索し、ダウンロードしてインストールすることを推奨する。 公式管理のストアでは定期的にファイルの安全性をチェックしている。他の場所からファイルをダウンロードして端末に移すことは絶対に避けるべきだ（ ただし…いや、ただしはない！）。

6．リスク分散：2つのブラウザで公私を分ける

もちろん、時間をかければ前述の各ブラウザに拡張機能を追加し、保護機能を強化して万能ブラウザにすることも可能だ。しかし、娯楽•日常業務•機密通信など全てを同一ブラウザで行う場合、ハッカーに脆弱性を発見されれば全てを失うリスクが残る。

真にリスクを分散させる方法は、性質の異なる作業を異なるデジタルデバイスで処理することだ。しかし一般人は予算が限られているため、娯楽•日常業務•機密通信用に三つの異なる端末を購入するのは難しい。購入できたとしても、それらを持ち運ぶのは現実的ではない。

そこで私たちは折衷案を提案する——業務内容に応じて異なるブラウザを使用することだ。例えば、最も重要度の低い娯楽はブラウザＡで、日常業務はブラウザＢのみで処理し、機密通信が必要な時だけブラウザＣを起動する。そうすればネット上の足跡は簡単に分割でき、一つのブラウザに蓄積されることもない。複数のサイトを同時に監視するトラッカーが、娯楽用アカウント•仕事用アカウント•機密用アカウントを同一ユーザーと識別することも防げる。

簡単に言えば、卵を同じ籠に盛るな。ブラウザこそがその籠なのだ。

本記事の内容に疑問がある場合は、hi@ocf.tw オープンカルチャー財団まで連絡してもよい。

6．全てのパスワードを一元管理する

6.1．パスワードマネージャー

6.1.1．事例

小明はブラウザの重要性を理解し、自身のネット利用行動を見直したが、セキュリティ問題は解決しなかった。隣にいた技術者が巻物の第弐条を指さし、「パスワードが盗まれたからだ」と指摘した。小明の事例では、パスワード管理の不備がリスクだったのだろうか?答えを考えてから、下で確認しよう！

6.1.2．答え

- 小明は様々なサービスに同じアカウントとパスワードで登録していた。これは、どこかで情報が漏洩すれば、他の

アカウントの安全性も極めて高い確率で侵害されることを意味する。

-「リスク評価」の章で、組織Aでは従業員がパスワードを忘れるのを恐れ、付箋にアカウントとパスワードを書いて机に貼る事例があった。

- 小明はブラウザに自分のアカウントとパスワードを記憶させ、パスワードをブラウザに預けていた。もしブラウザから彼のアカウント情報が漏洩すれば、彼のデータも同時に晒されることになる。

6.1.3. 概説

またパスワードを忘れた？SNS、ショッピングサイト、ゲームで同じパスワードを使っている？それとも覚えきれないほどパスワードが多くて混乱している？デジタル時代において、パスワードは鍵のようなものだ。ソーシャルアカウント、購入履歴、ゲームデータを保護する。だからこそハッカーの狙いとなる。パスワードを入手すれば、なりすまし、クレジットカードの不正利用、オンラインゲーム内の仮想アイテム窃取が可能となり、被害者に様々な損害を与える。

さらに踏み込んで考えると、人権を守る市民団体にとって、電子メールボックス、会議文書、寄付者データは組織にとって重要な資産だ。もしアカウントとパスワードがハッカーに知られれば、組織スタッフの私生活が被害を受けるだけでなく、組織の名誉が傷つき、重要な活動情報が漏洩する可能性もある。さらに、組織スタッフや協力者が独裁国家に標的にされ、生命の危険にさらされる恐れさえある。

6.2. パスワードの記録方法にはどんなものがあるか？

今でも紙にパスワードを書いて引き出しに押し込んだり、付箋にアカウントとパスワードを書いてパソコンに貼ったりしているだろうか？紙はパスワードを記録する手段としては悪くないが、情報が露見しやすく、盗難や紛失のリスクもある。多くの人がウェブブラウザの自動保存機能で全てのパスワードを記録するようになった。しかし前述の通り、ウェブブラウザでの記録には懸念点がある。では紙やブラウザ以外に、より良い方法はあるのだろうか？

現在一般的なパスワード管理方法には、紙での記録、ブラウザの自動保存、パスワードマネージャー、セキュリティトークンなどがある。下表にそれぞれの長所と短所をまとめた。

管理方法	使用方法	長所	欠点
紙媒体での記録	紙とペンでパスワードを記録する。	いつでもどこでも記録でき、デバイスに直接貼れる。	物理的に盗まれたり、紛失したり、情報が漏洩しやすい。
ブラウザの自動保存	アカウントとパスワードをブラウザに記録し、自動入力する。	ログインする際、自動的にアカウントとパスワードが入力される。	ブラウザの脆弱性を悪用してアカウントとパスワードを盗まれる可能性がある。また、コンピュータのユーザー設定ファイルにアクセスできる者は誰でも、パスワードを見たり盗んだりできる。
パスワードマネージャー（ローカル保存版）KeePassXC、Bitwarden オフライン利用	パスワードをパスワードマネージャーに保存し、 ここからパスワードを取得する。	管理ツールを開くためのパスワードを一つ覚えておけば、全てのパスワードを管理できる。オフライン版は、ネットワーク環境が安全でない場合や接続していない状況で使用できる。	オフライン版のパスワードデータベースファイルを紛失すると全て消失し、PCとスマホ間で同期されない。
パスワードマネージャー（クラウド版）1Password、Bitwardenクラウド版	パスワードをパスワードマネージャーに保存し、 このマネージャーからパスワードを取得する。	• 一つのパスワードを覚えて管理ツールを開けば、全てのパスワードを管理できる。 • クラウド版は複数デバイス間でパスワードデータベースを同期できるため、アクセスが便利だ。	クラウド版のパスワードデータベースはサービスプロバイダーのサーバーに暗号化保存されるため、ハッカーによる侵入や盗難の可能性がある。
セキュリティトークン。例：YubiKey	物理的なセキュリティキーによる認証を使用する。	メインパスワード以外の保護手段を提供し、二段階認証は物理的な保護となる。	デバイスは別途購入が必要で、 紛失するとパスワード（ データベース）を開く手段がなくなる。

パスワードマネージャーの使用は重要でありながら軽視されがちな基本作業だ。KeePassXCやBitwarden以外にも、オープンソースや商用パスワードマネージャーが複数存在し、自身の使用習慣に合わせて選択できる。Privacy Guidesサイトが選定したパスワードマネージャー[12]も、選択時の参考になる。

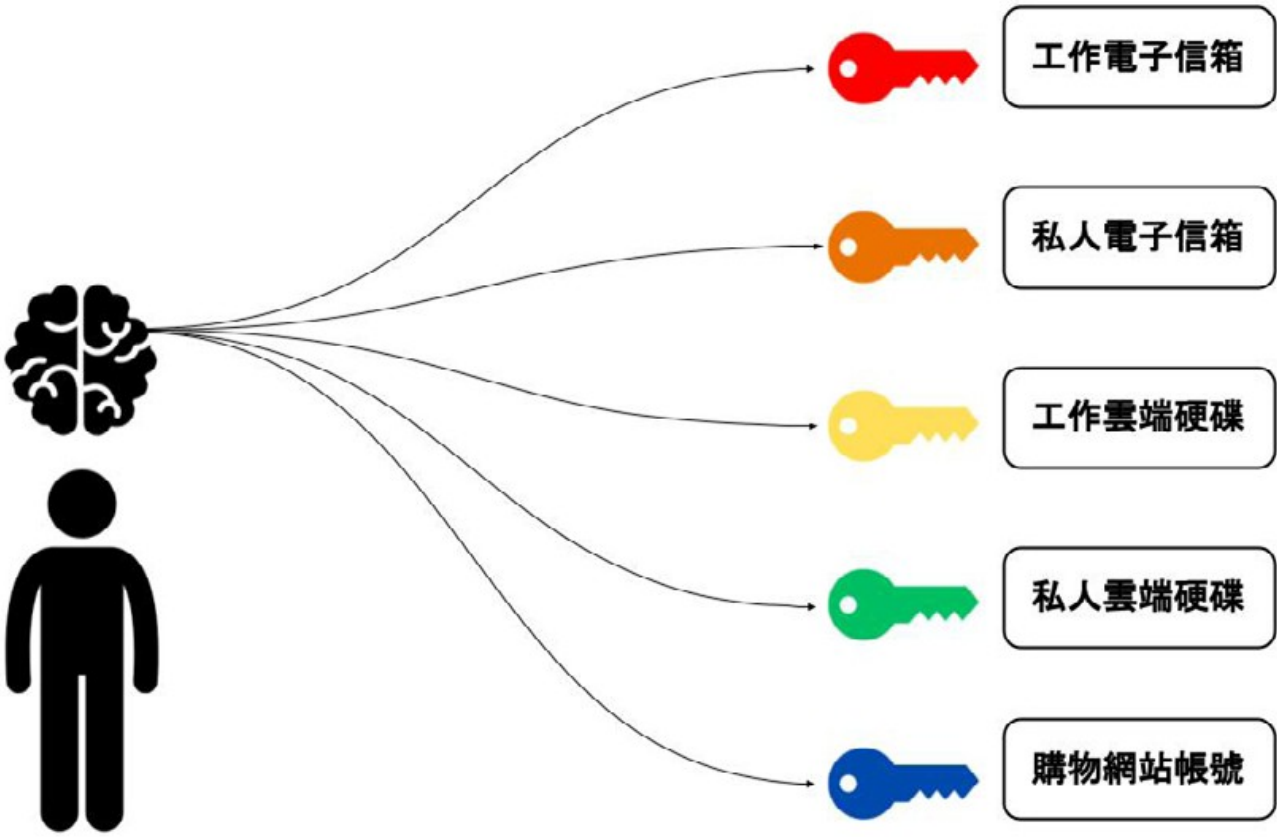
メインのパスワード以外に追加の保護措置を設け、たとえコンピュータ全体が盗まれても相手がパスワードデータベースを開けられないようにしたいなら、YubiKey[13]の使用を検討できる。これは物理的な保護手段として第二のロック（いわゆる「二段階認証」の概念）となり、USBメモリのような外観の物理的な鍵として機能する。こうすると、KeePassXCパスワードデータベースは、このデバイスをコンピュータに差し込んで認識させた場合にのみ、ロックが解

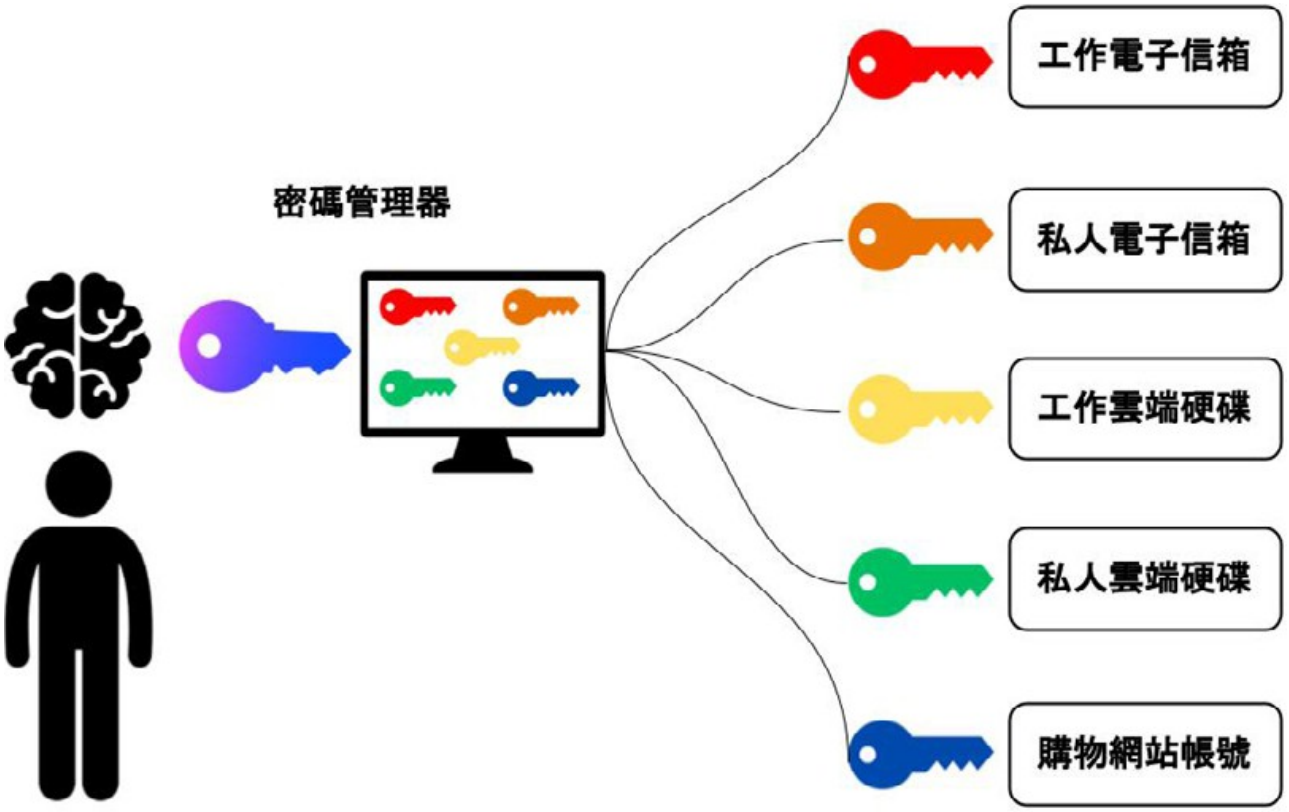
除される。ただし、ユーザーは本デバイスの購入費用を負担する必要があり、デバイスを紛失した場合、パスワードデータベースを開く手段は一切なくなる。

上記を踏まえて私たちは「1+1>2」のアプローチを推奨する。つまり、パスワードマネージャーと乱数パスワードを主要ツールとし、セキュリティトークンという物理キーを二段階認証の補助として活用し、パスワードをより強固に保護する、というものだ。

6.3. パスワード管理ツールはどんなものか

人間の記憶力には限界があり、複雑なパスワードに関してはなおさらだ。もし多くのパスワードを管理する必要がある場合、全てを1枚の紙に書き留めて金庫に保管することを考えたことがあるかもしれない。しかし、使用上の不便さと、紙を紛失した場合の深刻な結果を考え、結局やめたはずだ。パスワードマネージャーはまさにこのために生まれたものだ。複雑な思考と記憶作業をソフトウェアに任せ、「人間」が覚えるべきは最も重要なマスターパスワード（さらに二段階認証を追加することも可能）だけだ。これで多数のパスワードを保存•記憶するという困難な任務を完了できる。





図上：人間の脳が全てのパスワードを記憶する 図下：パスワードマネージャーによる管理

具体的には、パスワードマネージャーは左図のような「脳が異なるアカウントとパスワードを記憶する」状態から、「マネージャーの入口パスワードだけを覚え、どのアカウントがどのパスワードに対応するかをマネージャーに教えてもらう」状態へと改善する。どのアカウントでもパスワードの入力は、たった5ステップだ。

1. マネージャーを開き、パスワードを入力してデータベースを解除する。⇒ 2. ログインしたいアカウントを選択する。⇒ 3. パスワードをコピーする。⇒ 4. ログインしたいページにパスワードを貼り付ける。⇒ パスワードマネージャーを閉じる。

最初のステップで頭を使ってロックを解除するだけで、複雑なパスワードを記憶の奥底から呼び出す手間は不要だ。このマニュアル作成過程で、セキュリティ専門家やデジタル技術に深い関心をもつ人々と何度も議論した結果、最も使いやすく推奨されるのは、オープンソース技術を基盤とする2つのパスワードマネージャー：KeePassXC と Bitwarden であるという結論に至った。以下に、の2つの便利なパスワード管理ツールを紹介する。

6.3.1. KeePassXC

KeePassXCはオープンソースソフトウェアKeePassファミリーの一員だ。そのコードは透明性が高く、誰でも知ることができ検証可能である。ネットワークコミュニティのボランティアエンジニアによって共同開発•保守されているため、データを盗むための悪意のある機能を隠す可能性が低くなっている。

市販の商用パスワードマネージャーとは異なり、KeePassXCは無料で誰でも利用できるだけでなく、保護機能が営利目的で妥協されることもない。パスワードの保存と管理は商業企業が運営するサーバーではなく、ユーザー自身のコンピューターデバイス内で行われるため、パスワード漏洩のリスクやネットワーク切断による同期不能やダウンロード不能の危険性が大幅に低減される。

KeePassXCは多機能で、スマホやタブレットなど複数デバイス間で共有できる。ネット上には関連チュートリアルがあり、例えば「オープンソースパスワード管理ソフト：KeePass[14]」や「KeePassXC無料パスワード管理ソフト図解チュートリアル[15]」などがある。クレジットカード、ブラウザ、スマホへの入力も素早く行える。 ここでは詳細を割愛する。ただし、複数デバイスでの使用はパスワードデータベースの移動を意味し、クラウドストレージへのアップロードも必要になる。移動中のデータ損失や予期せぬ問題、パスワードデータベースを保管するネットワーク空間の盗難が懸念される場合は、クロスプラットフォーム機能の利用を慎重に検討すべきだ。[16]

KeePassXCを初めてインストールしてすぐに使いこなす方法を知りたいですか？〈付録二：KeePassXCの使用方法〉を参照してください。

6.3.2. Bitwarden

Bitwardenは自由でオープンソースのパスワード管理サービスだ。ソースコードが公開され検証可能で、ウェブ/コマンドラインインターフェース、デスクトップアプリ、ブラウザ拡張機能、モバイルアプリなど多様なクロスプラットフォームアプリケーションを提供する。Bitwardenはクラウドホスティングサービスを提供しているが、セキュリティ上の懸念やデータ保存の規制がある場合は、自分でパスワード保存サーバーを構築することもできる。この場合は、自分でパスワードを管理しながら、異なるデバイス間でパスワードを同期する利便性を維持できる。

Bitwardenは主に「Personal」と「Business」の2プランに分かれる。個人プランはさらに「Free」、「Premium」、そして「Families」の3種類に分かれている。複数人で同じパスワードライブラリにアクセスする必要がある場合は、マルチユーザー機能を備えた「Families」プランを選択する必要がある。個人利用の場合は「Free」で十分だ。無料版と有料版の機能差は大きくなく、主な違いは一部の高度な機能に限られる。一般ユーザーにとっては、無料プランでも無制限のパスワード保存数、全デバイスでの同期、パスワード生成ツールなど、ほとんどの作業を十分にこなせる。

KeePassXCとBitwardenは他のパスワードマネージャーと同様に使えるが、より安全だ。複数のアカウントとパスワードを簡単に管理したり、乱数で自動生成された破られにくいパスワードを使ったりできる。これで新しいパスワードを考えるのに頭を悩ませる必要はなくなる。

6.3.3. ちょっとしたヒント

1. ブラウザにパスワードを記憶させるのではなく、独立して動作するパスワードマネージャーを使うことだ

   ブラウザ自体にはユーザーの閲覧履歴や使用習慣が多く蓄積されており、ハッカーの標的になりやすい。そのため、パスワードは独立して動作するパスワード管理ソフトにのみ預け、ブラウザと直接関連付けないことを推奨する。異なる機能を別々のブラウザで処理する分離原則と同様に、リスクを一箇所に集中させないためだ。独立したパスワード管理ツールを使うのは不便かもしれないが、しかしパスワード管理ソフトの多くは、アカウント名やパスワードを直接コピーする機能を提供している。これによりユーザーが手動で入力する手間を省ける。さらにパスワード管理ソフトは、Windows、MacOS、Linuxといった主要なOSや、Android、iOS搭載のスマートフォン•タブレットなど、様々なデバイスで利用できる。これによりデバイスを跨いだパスワード管理が可能になる。

2. 異なるアカウントとパスワードを使用することで、重要な情報をより適切に保護できる。

   ほとんどの人は、忘れないようにするために、異なるネットサービスやアカウントで同じか似たパスワードを使っている。しかし、同じパスワードを使うということは、あるネットサービス事業者がデータを盗まれた場合、悪意のある人物が一度の漏洩事件で入手したパスワードだけで、あなたのすべての異なるサービスのアカウントを盗めることを意味する。例えば、個人情報の漏洩を検知するオンラインサービス「Have I Been Pwned」や「Firefox Monitor(日本語サイト)」は、定期的にDropboxやフィットネスサービス、オンラインデザインソフトCanvaなどの有名サービスの漏洩事故を発表している。利用したサービスの一つがハッキングされれば、他のアカウントも被害に遭い、損害範囲が拡大する可能性がある。

   基本的なアカウント利用の安全性を確保するため、複雑なパスワードの設定、定期的な変更、同一パスワードの複数サービスでの使用回避は周知の対策だが、実際の運用は極めて困難だ。複雑なパスワードを考案するたびに、記憶に時間と労力を要する上、全てのアカウントのパスワードを即座に変更できるとは限らない。パスワード管理のコストは業務内容の機密性に応じて増加する。だからこそ本章で特にパスワード管理ツールに焦点を絞って紹介した理由もここにある。一つのシステムが分散したアカウント情報を記憶してくれるため、忘れる心配がなく、アカウント漏洩の可能性も低減できるのだ。

3. 組織全体で同じパスワードを使うのは怠慢だ

   組織全体で同じパスワードを共有するのは良くない。組織内の全員がパスワードを適切に保護しているとは限らないため、万が一漏洩した場合、原因を特定できず、対策の改善やセキュリティ強化も困難になる。組織は同じアカウントを共有すべきでないだけでなく、業務の必要性に応じてメンバーに異なる権限のアカウントを割り当てることで、全体のセキュリティレベルを向上させるべきだ。

4. 「良いパスワード」の設定
   - 十分な長さ：通常は12文字以上が推奨される。[訳注：16文字以上を推奨]
   - 複雑性：パスワードには大文字、小文字、数字、記号など異なる種類の文字を含めるべきだ。あるいは覚えやすいが推測されにくい文を選ぶか、複数の単語を組み合わせてより長いパスワードを作成する。推測されやすい一般的な単語や単純な数字の並びは避けるべきだ。
   - 推測されにくく、ソーシャルエンジニアリング攻撃に耐える：個人情報に関連する単語、日付、その他の推測しやすいパターンは避けるべきだ。そのようなパスワードは、ソーシャルエンジニアリング攻撃や解読のリスクが高い。ランダムに生成されたパスワードを採用するのが望ましい。
   - 再利用しない：各アカウントには固有のパスワードを使用し、複数のアカウントで同じパスワードを共有しないこと。
   - 定期的な更新：パスワードは定期的に変更し、解読リスクを低減すべきだ。3〜6ヶ月ごとの変更が推奨される。[訳注：頻繁に更新するよりも、長めのパスワードを設定する方が好ましい、という考え方もある]

   本記事の内容について疑問がある場合は、過去記事「ハウツー：KeePassXCの使用」[17]を参照するか、hi@ocf.tw オープンカルチャー財団に問い合わせること。

7．市民団体の自主運営ウェブサイトの安全確保

7.1．事例

パスワードを設定した後も、サイトはまだ復旧していなかった……彼は再び巻物を取り出し、どうすべきか前後を読み返して確認した。前の事例紹介の章で、サイトセキュリティ／サイト管理に関連する内容を覚えているだろうか？

7.2．答え

- 同僚の小美がWoodlessとネットで拾った無料プラグインで組織Aのサイトを自作したが、コードのセキュリティホールを点検する能力がなく、ハッカー攻撃に対応できなかった。
- ウェブサイトが分散型サービス妨害攻撃（DDoS）を受けた際、組織Aには防御手段がなかった。

市民団体は第一線の活動に追われ、自前で構築したウェブサイトの維持管理に時間やリソースを割く余裕がなく、ましてや関連技術の向上など到底無理な話だ。しかし残念ながら、事例研究で描かれた状況は現実世界では珍しくない。まず、デジタル時代において、ウェブサイトを構築して提言活動を行うことは、効率的にリーチを広げられるだけでなく、組織の長期的な活動の基盤となる。ウェブサイト上に記録された資料や成果は、提言活動の長期的な展開に役立つのだ。

市民団体には自前のウェブサイトが必要だ。しかし、市民団体と対立する勢力からの脅威も存在する。政府資金を受けた敵対的なハッカー（例として挙げると、この種のハッカーは標的を絞った攻撃能力と持続的な攻撃能力を持つ）は、こうした自主運営サイトを攻撃・侵入するのは容易だ。軽度ならサイトを機能停止させる（繰り返し言及されるDDoS攻撃など）ことで情報伝達を阻害し、深刻な場合には悪意のあるプラグインを埋め込み、利用者の重要情報を盗み出す。

市民団体がサイバー攻撃を受ける時代に、私たちはまず何を優先すべきなのか？脅威モデリング、つまりリスク評価の観点から、「何を保護すべきか、なぜ保護すべきか、脅威やリスクはどこから来るのか、その形態は何か」という順序で思考することで明確にできる。

7.3．概説

以下にいくつかの脅威の形態を紹介する。 これらの説明は詳細には触れず、簡単な用語解説と想定されるリスクの結果を提供するものである。

7.3.1．DoS & DDoS

DoS & DDoS サービス拒否（DoS）攻撃は、システムのリソースを枯渇させ、正当なサービス要求に応答できなくすることを目的としている。分散型サービス拒否（DDoS）攻撃も同様だが、DDoSは複数のシステムが単一のシステムに対して行う攻撃であり、一対一のDoSに比べて規模が大きな場合が多い。いずれも標的となるシステムの処理能力を消耗させ、被害を受けたウェブサイトがユーザーにサービスを提供できないようにしようとするもので、その結果、被害を受けたウェブサイトが完全に停止してしまうことがよくある。さらに、ウェブサイトが停止して再起動する過程で、他の攻撃による被害を受ける可能性もある。

7.3.2．ドメインネームシステム（DNS）関連の攻撃

DNSは電話帳のようなもので、人間が読めるドメイン名（例：ocf.tw）を数値で表されるインターネットプロトコル（IP）アドレス（例：132.68.1.1）に照合•変換する。ここでは DNS 攻撃の技術的詳細には触れないが、DNS を標的とした攻撃は、ウェブサイトの停止、サイトアクセス時の不正なリダイレクト（粗悪なページや悪意のあるサイトへの誘導）、データ漏洩を引き起こす可能性があることを認識すべきだ。組織の評判や運営に損害を与えるだけでなく、ユーザーを傷つけ、法的責任を問われる事態にもなり得る。

7.3.3．HTTPS暗号化されていない危険なウェブサイト

HTTPSプロトコルで暗号化されていないサイトは、サイト上でやり取りされるデータをすべて日光の下に晒して閲覧される状態に等しい。サイト運営者がデータ漏洩の危険に晒されるだけでなく、サイトを閲覧するユーザーも同時にリスクに晒されることになる。

7.3.4．総当たり攻撃

文字通り、力ずくの攻撃、暴力的な攻撃、あるいはブルートフォース攻撃と呼ばれるものだ。ハッカーは、標的となるウェブサイトに対し、サイト管理者のアカウントとパスワードにアクセスできる可能性があると判断した候補リストを用意し、ボット（プログラム）にそれらを一つずつ試させ、サイト管理画面への侵入に成功するまで続ける。これにより、情報漏洩や、サイトの乗っ取り、削除などが引き起こされる可能性がある。

7.4．専門的なことは専門家に任せる

しかし、潜在的なリスクを理由にデジタル世界での活動に躊躇してはいけない！端的に言えば、現実世界と同じで、自身の安全に注意し、オフィスに見知らぬ人が侵入したり盗聴•盗撮したりしないようにする必要がある。デジタル世界の維持•運営にもコストがかかる。もし そのコストが金銭や時間でないなら、代償はあなたの安全やプライバシーかもしれない。では、十分な技術力を持たない市民団体や活動家は、どう自分を守ればいいのか？

簡単だ。専門家に任せることだ！

世界には市民団体や人権活動家を支援する非営利組織や企業が数多く存在し、情報セキュリティ関連のサービスを提供している。以下では、eQualitieが提供するDeflectとeQPressのウェブサイト保護サービス、およびCloudflareが公益団体のウェブサイト向けに提供するGalileoプログラムを紹介する。申請により、対象サイトはCloudflareの保護を受けることができる。これらの選択肢は現在、申請後に無料で提供されており、市民／公益団体の支援に焦点を当てている。中には中国語のカスタマーサポートを提供するサービスもある。本マニュアルの読者がウェブサイトの脅威に対処するのに適した選択肢だと考えている。

7.5. 自らの責任を軽んじてはいけない

外部からの脅威に対処する際には、多くの基本的な概念や行動を自ら理解し、内面化し、実践する必要がある。例えば、業務用アカウントの管理権限を階層化すること、 多段階認証を導入すること、強固なパスワードを設定すること、エンドツーエンド暗号化ソフトウェアやVPNを活用することなどは、 自身のセキュリティ体制を強化し、リスク露出を効果的に低減できる。個人や組織内部で潜在的なリスクにどう対応するか、専門家とどう連携するかは、自ら向き合う必要がある。個人としての規律や組織としてのルールを確立することが、より良い実践方法だ。具体的には：

- 暗号化意識を持ち、暗号化通信を多用する
- フィッシングメールへの警戒心
- 権限管理の階層化
- 強固なパスワード
- 多段階、二段階認証

要するに、技術的に高度な情報セキュリティ対策は専門家に任せた後でも、個人や組織にはまだ改善すべき点や努力すべき点がたくさんある。 知識や行動面での改善は、個人や組織の情報セキュリティを大きく助け、リスクを大幅に減らす。例えば、ドアに何重もの錠や生体認証を備えたとしても、家族が開けっ放しの通用口を使いつづけていては、玄関に取り付けた二要素認証の最新施錠システムの意味がない。

7.6. 利用可能なツール

> 以下に二種類のサービスを紹介する: ひとつは Deflect と eQPress、他方は Galileo project である。

7.6.1. Deflect と eQPress

カナダに本拠を置くeQualitieは、市民団体が無料で申請できる保護措置を提供している。eQualitie[18]は、デジタル世界における言論の自由の向上、検閲回避、匿名化、監視回避といった基本的人権の保護を目的とする公益企業であり、多国籍•多分野のメンバーと共に世界中でサービスを展開している。

本稿では、同社のウェブサイト保護サービス「Deflect」と、市民団体向けに無料で提供されるWordPressシステム運用サービス「eQPress」を紹介する。市民団体は攻撃リスクが高く、技術チームを欠く場合が多いため、サイト更新やプラグインの不備によるセキュリティ脆弱性が生じやすい。eQualitieチームはこうした課題を解決するため、DeflectとeQPressを開発した。

市民団体は専門チームが管理するスペースにウェブサイトを設置すれば、特定の攻撃侵入の確率を下げられる。例えば2016年、ウクライナの独立メディアサイトはこの仕組みにより、ロシアやベトナムなど国外からのDDoS攻撃[19]を回避し、サイトが中断することなく政府の不正を暴露し続けられた。人権擁護を目的とする市民団体、例えば独立メディアや人権活動支援団体は、利用規約に同意しプライバシー規範を受け入れた上で、ウェブサイト保護サービスの支援を申請できる。[20]

1. どのような場合に利用するか

   以下の二つの状況に該当する場合、活動の安全性と持続性を確保するため、DeflectとeQPressの利用を真剣に検討してほしい。

   1. あなたのウェブサイトが攻撃される恐れがある

      市民団体がネット上で発信する内容は、既得権益者（通常は政府やハッカーを雇える有力者）の反感を買うことが多く、悪意のある攻撃を招くことがある。もしハッカーがあなたの意見をネット上から消し去ろうとしたり、社会的信頼を損なおうとした場合、いわゆるDDoS攻撃（トラフィック過負荷攻撃）でサイトを機能停止させる可能性がある。攻撃者は短時間で数百万もの読み取り要求を発生させ、サイトが置かれたサーバーが他の訪問者に対応できる帯域幅を失わせるものだ。

      また、市民団体のウェブサイトは反体制派にとってプライバシー侵害の標的となりやすい場所である。独裁

国家がハッカーを通じてサイト利用者の安全を脅かす場合、市民団体のサイトを監視し、ネットワーク通信の過程で関係者の個人情報を傍受•識別•窃取する。

2. WordPressシステムを使用してサイトを構築している、または構築しようとしている場合

   WordPressは一般的なウェブサイト構築ソフトウェアであり、世界の40%以上のサイトがこのシステムを使用している。同時に、ソフトウェアが無料で使いやすく、ソースコードがオープンソースとして公開されているため、市民団体は社会とのコミュニケーションのために、独自にドメインやサーバーをレンタルし、WordPressで自らネットプラットフォームを構築することが多い。特にWordPressは様々なプラグインのインストールが容易で、寄付、購読、チャリティー商品の購入機能を提供できる。

   しかし、柔軟性が高くユーザーに自主性を与え、ウェブサイト構築業者に縛られない一方で、専門技術チームによるメンテナンスがない場合、自作のWordPressサイトには多くのセキュリティ上の脆弱性が生じる可能性がある。WordPressで運営しているサイト、あるいはWordPressでのサイト構築を検討している場合、eQPressプラットフォームによるサイト保守サービスを申請できる。専門技術チームが管理を行うことで、攻撃を受けてもサイトは堅牢に維持され、継続的な啓発活動が可能となる。さらに、すべてのデータ転送プロセスを暗号化し、ユーザーのプライバシーと安全を確保する。Deflectによる保護に加え、本サービスには以下の機能がある。

   - ウイルス対策
   - リモートバックアップ
   - テーマとプラグインの編集インターフェースを提供し、顧客が自ら操作できるようにする
   - カスタマーサポート技術支援
   - WordPress および Deflect の詳細なオプションとサービス

   WordPress以外のシステムで運営しているウェブサイトの場合、Deflectサービスのみを申し込むことで、サイトへの攻撃を防ぐことができる。

   これらのサービスの利用を希望する場合は、以下の文章を読み続け、サービスの利用方法や申請手続きについて確認してほしい。関連する技術情報の意味が分からない場合は、組織内で適切な担当者と相談するか、コンサルタントの支援を求めることをお勧めする。

2. 利用開始前に

   組織でウェブサイトを構築する必要があり、かつハッカーの攻撃標的となる可能性がある場合は、WordPress と eQPress のサービスを組み合わせるという選択肢がある。簡単に言えば、Deflect サービスはウェブサイトを保護するものであり、WordPress で構築されたウェブサイトであれば、eQPress フレームワークを追加することで、より安全になる。

   もし組織のウェブサイトがWordPressシステムでない場合、Deflectの保護機能だけで十分なら、申請プロセスの段落に直接進んで読み進めてください。

   WordPressはオープンソースのウェブサイトシステムだ。ユーザーは外観やコンテンツをカスタマイズでき、様々なプラグイン機能を追加できる。WordPressでサイトを構築しeQPressのサービスと組み合わせることは、ネット上でオフィスを借りて活動を開始するイメージだ。おおまかに三つのステップに分けられる。

   1 ドメイン名の決定とレンタル

   URLの名称を決める。例えば「https：//サイト名.tw」 という形式で、誰もが覚えやすく見つけられるようにする。ドメイン名を決めたら、Gandi、Cloudflare、GoDaddy、 などのドメイン登録サービスを探す。これらはショッピングプラットフォームのように様々なドメインをまとめて提供している。組織の年間予算に応じて、異なるドメイン末尾を選択できる。決定後、あなたのドメインは のようにネット上に登録される。

   2 適切なスペースを借りる

   現実のオフィスには住所だけでなく、具体的な建物スペースが必要だ。デジタル世界におけるウェブサイトの「建物スペース」とは、サイトデータを保管するサーバーホスティングを指す。これは建物の大きさや仕様に相当し、サイトにアクセスできる訪問者数や行動制限に影響を与える。eQPressはサーバーホストとして機能し、WordPressサイト に健全かつ柔軟な保護を提供する。サイトにアクセスしようとする訪問者は、必ずeQPressのサーバーを経由してサイトに入る必要がある。

   3 ウェブページの外観デザイン

   提案の必要性に応じて、WordPressのソフトウェアシステムを使ってウェブサイトの見た目、機能、コンテンツを設定できる。ただし、ウェブデザインはeQPressの保証範囲外だから、自分で見た目の良いウェブページを選んだりデザインしたりする必要がある。もちろん、プロのウェブデザイナーに外注して、その成果物をeQPressに移行することも可能だ。

3. 申請手順

eQPressはDeflectを基盤とした無料サービスであり、コンピュータへのソフトウェアのダウンロードやインストールは不要だ。オンライン申請により、Deflectのウェブサイト保護とeQPressのサイト保守サービスを利用できる。 上記の項目のサービスを申請する組織は、以下の条件を満たす必要がある。

- 人権の擁護；市民団体；独立系または非営利のメディアの運営；人権活動家への支援。
- 活動内容が『世界人権宣言』の原則に違反しないこと。
- 活動過程において、ヘイトスピーチを助長したり、差別を奨励したりしないこと。
- 利用規約に同意し、受け入れること[21]

上記の条件を満たし、規約に同意する場合は、https://deflect.ca/non-profits/ で登録申請を行う。

申請前に以下の準備が必要。

- ウェブサイトのURL（ドメイン名とサーバーのIPアドレス）、連絡担当者のメールアドレス。
- eQPressでWordPressサイトを管理する必要がない場合、この手順ではDeflectのサイト保護機能のみを申請すればよい。

申請プロセスで問題があれば、カスタマーサポートに連絡できる。

申請が承認されたら、Deflectダッシュボードの選択画面（Hostingタブ）で利用するeQPressプランを決めることができる。プランは3種類ある。

1 空のWordPressサイトを作成する

サイト構築が初めての場合や、サイトを再構築したい場合はこのプランを選択し、WordPressの管理ツールでサイトコンテンツを設計できる。始め方が分からない場合は、「WordPress」「テーマ」などのキーワードで検索すると、サイト設計のプロセスを解説した記事が多数見つかる。本記事では詳細な説明は省略する。

2 空白のWordPressを作成し指定テーマをプリロードする

既に選定済みでデザインが完了したウェブサイトテーマがある場合、そのデザイン済みサイトをロードできる。

3 既存の WordPress サイトを eQPress プラットフォームへ移行する

既に他の場所で WordPress を使用してサイトを構築しており、既存のサイトコンテンツをそのまま移行したい場合は、以前のサイト管理を支援したサーバープロバイダーに連絡し、WordPress のオリジナルファイル、コード、データベースのバックアップファイルを提供してもらい、eQPress の技術担当者に渡すように依頼してほしい。

Deflectアカウントを登録した後、IT関連の技術者でなくとも、WordPressのソフトウェアやドメインレンタルプロセスに詳しくなくても問題ない。使用フローに関する疑問やサイト運営中のその他の問題については、https://support.deflect.ca/ からアカウントにログインし、カスタマーサポートに問い合わせることができる。アカウント未登録の場合は、公式サイトのフォーム（ https://deflect.ca/contact-us/ ）から申請できる。eQualitieチームは、世界中の市民団体がデジタル世界に適応し、 能力を身につけるための支援を目的として設立された。組織の活動目標が公平性、自由、人権の促進である限り、彼らは喜んで支援する。

7.6.2. Galileoプロジェクト

芸術、人権、市民社会、ジャーナリズム、民主主義活動に従事する組織は、申請[22]を通過すれば、組織のウェブサイトがGalileoプロジェクトに参加する機会を得られる。これにより、Cloudflareのビジネスレベル顧客向けサービスサポートを受けられる。Cloudflareは米国に本拠を置く企業で、CDN（コンテンツ配信ネットワーク）、クラウドセキュリティ、DDoS対策、ドメイン登録サービスを提供している。2022年時点で、世界のインターネットユーザーの20% 以上がCloudflareのサービスを利用している。 つまり、Cloudflareのユーザーコミュニティは相当な規模に達しており、そのサービスには一定の信頼性がある。Galileoプログラムは保護対象サイトに多くのサービスを提供しており、前述の一般的な攻撃に対応するため、以下の重点項目を抽出する。

- DDoS防御：DDoS攻撃の検知と警告を提供し、ウェブサイトやアプリケーションを保護する。同時に正当なトラフィックのパフォーマンスを損なわないようにする。
- DNS：CloudflareのDNSサービスを提供し、DNSに対するDDoS攻撃を緩和する能力を持つ。また DNSSEC機能を備えており、DNSの完全性と真正性を確保し、DNSへの攻撃を軽減する。
- ユニバーサルSSL証明書：既存のSSL設定と互換性がある。ウェブサイトはSSL証明書を必要とする。これによりユーザーデータの安全性を確保し、サイトの所有権を検証し、攻撃者が偽のサイトを作成するのを防ぎ、ユーザーの信頼を得る。現在SSLを使用していない場合でも、追加操作なしでCloudflareがSSL機能を提供する。SSL証明書は、ウェブサイトを構築しHTTPS接続を確立する際に必要な暗号化証明書ファイルである。
- ボット対策：ブルートフォース攻撃の影響を効果的に軽減する。
- Webアプリケーションファイアウォール（WAF）：WAFでは、サイトを保護するように設計されたルールエンジンと脅威インテリジェンスに対してリクエストが検査される。不審と判断されたリクエストはブロックするか、質問を送り返すか、または記録するかをユーザーのニーズに応じて選択できる。

Galileoプロジェクトが提供する数多くのサービスには、Cloudflare自体のパフォーマンス向上やリスク低減を目的とした改善サービスも含まれる。例えばCloudflare Gateway、CloudflareのDNS、CDN、キャッシュ効率化や完全クリアなどだ。 これらのサービスはすべて、Cloudflareの巨大なユーザーコミュニティに依存している。情報セキュリティを例にとれば、巨大なユーザーコミュニティは柔軟で豊富な脅威インテリジェンスを意味し、それゆえCloudflareは攻撃の緩和と阻止を効果的に運営できる条件を備えている。

Galileoプロジェクトの申請書記入完了後、相手から返信がある。コミュニケーションプロセスは非定型となる可能性があり、本マニュアルでは予測や詳細な説明は行わない。要望や疑問がある場合は、オープンカルチャー財団まで連絡を歓迎する。

7.6.3. ちょっとしたヒント

私たちが以前に作成したデジタルセキュリティ関連コンテンツに加え、台湾のCivil Society Cyber Shield (CSCS) セキュリティコミュニティが翻訳した教材[23]には、パスワード関連や二段階認証についての解説がある。セキュリティ概念やツールについてさらに学びたい場合は、Surveillance Self-Defenseウェブサイト[24]も強く推奨する。同サイトにはジャーナリストの出張や抗議活動参加といったシナリオ例も掲載されており、非常に分かりやすい。以下はDeflect / eQPressの公式説明文書(訳注：いずれも英文)だ。

- eQPress — Deflectによるセキュアホスティングサービス（https://equalit.ie/eqpress-secure-hosting-with-deflect/）
- 非営利団体向けDeflect / eQPressサービスと申請方法の概要：Deflect$_{\text{eQPressIntrozhTWMay8.pdf}}$（https://drive.google.com/file/d/1ciHbLpKA34HxRv811-E8KqdzXs2-qt3e/view）

この紹介内容について疑問がある場合は、hi@ocf.tw オープンカルチャー財団まで問い合わせることができる。

8. バックアップを確実に行う「321ルール」： データ消失の心配がなくなる事例

8.1. 事例

サイトが再開したのを見て、小明は思わずほっとした。レポートを再アップロードしようとした時、ふと気づいた。

「しまった！データが全部消えた…」。今後のデータをどうするか考えていると、風が巻物を巻き上げ、第4章が開いた。この事例で、小明がどのような行動を取った結果、ファイルを失いバックアップもない窮地に陥ったか分かるか？答えを考えてから、下で確認しよう！

8.2. 答え

小明は全ての報告資料（インタビュー記録、研究資料）と初稿ファイルを自身のノートPCに保存していた。これらのデータはPC以外の場所にバックアップされていなかった。もしPCを紛失したりウイルスに感染したりすれば、組織Aが数ヶ月かけて注いだ努力が水の泡となる。

小明は同僚とのオンライン共同作業のために、初稿をWoodlessにアップロードした。しかし、修正過程の各バージョンや公開前の最終版ファイルは、Woodlessシステム上にしか存在しなかった。オンラインファイルが失われると、この期間の編集進捗も消えてしまう。

「自分のノートパソコンで作業し、チームで議論が必要な時にクラウドにアップロードする」というのは多くの人に馴染み深い作業スタイルだ。Googleドキュメントならバージョン管理が容易で、特定の編集時点に遡れる。中にはバージョンごとに別ファイルを作成し、細やかに分類•保管する慎重な人もいる。しかし、最後の句点を打った後、皆が覚えているのはレポートの完成やプロジェクト終了のお祝いだけで、ファイルをバックアップすることなど忘れている。つまり、あなたも私も、小明と組織Aの悲劇に遭遇する可能性があるのだ。

8.3. 概説

8.3.1. データが予期せず消える確率は想像以上に高い

組織Aが遭遇した状況は例外ではない。データ保護ベンダーVeeamが発表した『2023年データ保護トレンドレポート[25]』によると、調査対象の4200組織のうち85%が2022年に少なくとも1回のランサムウェア攻撃を受けており、そのうち33%の組織では現用データが攻撃で暗号化されたり破壊された。被害者は影響を受けたデータの平均55%しか復旧できなかった。

たとえ組織がハッカーの標的にならなくても、人的ミスや機械故障、自然災害などの理由でデータを失う可能性がある。人的要因では、仕事が忙しい時にミスが起きやすい。例えばファイルを誤削除したり、うっかりフォーマットしたり、PC再インストール前にバックアップを取らなかったり、事故後にファイルを上書きしてしまうと復元がさらに困難になる場合がある。USBやCD、 NAS[26]などのストレージ装置が故障することもある。地震や洪水などの自然災害で装置

が損傷する可能性もある。あるいは組織Aのケースのように、オフィスと復旧拠点の両方が露見した場合、敵対者にデータを盗まれるリスクが大幅に高まる。

8.3.2. なぜバックアップが必要なのか？失う悲しみを経験しないためだ！

2021年に起きた高校生の学習履歴ファイル消失事件[27]は、まさに警鐘となる事例だ。政府が委託した業者が新データセンターへの移行作業中、誤った設定テンプレートを適用した上、スケジュールが逼迫していたためバックアップ体制が不十分だった結果、 期間にアップロードされたファイルが全て消失し、復旧の余地がなかった。 この件は計81校に影響し、 7854名の生徒が精魂込めて制作した作品を消し去った。業者にとっては、協力機関の信頼を失い、データ救出に追加で費やした金銭と時間のコストという代償は甚大だった。

市民団体にとっては、プロジェクト文書、サービス対象者の個人情報、寄付者情報など、あらゆるファイルが組織が守るべき価値に関わるものであり、組織の運営基盤そのものだ。万全なデータバックアップ体制を構築すれば、いかなる緊急事態に直面しても、組織の中核資産と運営能力が致命的な打撃を受けることはない。 組織が継続的に提言活動を推進し、個別の支援ケースに取り組む上で、これは極めて重要だ。

8.3.3. どうすれば完璧なデータバックアップ体制を構築できるか？「321」を覚えよう

データをいくつかの場所に保存しておけばいいのだろうか？それとも、パソコンやNASに「お守り」をいくつか置いて、データが失われないよう祈るべきだろうか？「卵を同じかごに盛るな」と言われるが、卵をどこに分散させれば最も安全なのか？IT業界の「バックアップ321」という仕組みこそが、これらの疑問に対する答えだ。

- データを少なくとも3か所に分散保存する。
- 少なくとも2つのファイルは異なる媒体に保存する。例えばパソコンに1部、USBや外付けHDDなどの外部ストレージに1部、あるいはクラウドに保存する。少なくとも1つのファイルはオフライン状態にしておく。これにより、ウイルス攻撃やセキュリティホールなどのリスクによるデータ損失を防げる。クラウドバックアップを利用する際は、そのクラウドストレージサービスが十分に安全か、クラウドからのデータ漏洩リスクがないかを考慮すること。[28]
- 少なくとも1つのファイルについて、オフサイトバックアップを行う。つまり、そのファイルを前述の2つのファイルとは異なる場所に保管する。例えば、そのファイルを保存した外付けハードディスクを銀行の貸金庫や、オフィス以外の場所に置くといった方法がある。これにより、すべてのオフラインファイルを同じ場所に保管することを避けられる。万が一、ある保管場所で盗難や自然災害などの不測の事態が発生しても、他の場所に保存されたデータがバックアップとして機能する。

「バックアップ321」は実は難しくない。例えば、文書のバージョンが完成するたびに、オフィスのパソコン、USB、クラウドストレージにそれぞれ1部ずつ保存する。USBはオフライン状態を保ち、別の場所に保管する（ただし、組織のデータを外部に流出させないよう制限する方法については、別の検討課題となる）。このようにすれば、バックアップ321の原則を満たすことになる。もしオフィスで事故が起きたり、オンラインバックアップが人為的ミスで失われたりしても、オフラインで別の場所に保管したUSB内のファイルを復元して使える。

ただし、同じコンピュータ内の異なるハードディスクやフォルダに保存するのは、「異なる媒体にファイルを保存する」原則に合致しない。考えてみてほしい。もし1台のコンピュータがウイルス感染や事故で損傷したら、これらのデータも消えてしまう。この状況では、卵は依然として同じ籠に入っている。リスクは分散されていないのだ。

バックアップ時には、ファイルが開けるかどうかを確認することを忘れないでほしい。必要な時に正しく復元できることを保証するためだ。バージョン管理ができればなおよい。小明のケースで言えば、レポート内容を修正するたびにファイルを保存•バックアップしておけば、特定の時点のレポートバージョンを復元できる。万が一に備えるためだ。

8.4. 利用可能なツール

8.4.1. 一般的な外部ストレージデバイス

実践は難しくなく、最も難しいのはこの良い習慣を維持することだ。以下に一般的な外付けストレージを紹介する。読者がニーズに最も合ったバックアップデバイスを選ぶ際の参考になるだろう。

ストレージデバイス／性能	CD	DVD	USB	NAS	外付けハードディスク
容量	700 MB	4.7 ～ 17GB	2GB ～ 2TB	CPU アーキテクチャによって異なり、最大数TBに達する	500 GB ～ 8TB
耐久性	低い	低い	中	高い	高い
携帯性	高い	高い	高い	低	中

ストレージデバイス／性能	CD	DVD	USB	NAS	外付けハードディスク
データ転送速度[29]	低	低	高	高	高
取得原価	低	低	低	高	中
故障警報	なし。通常、傷や保管環境の温度•湿度の変化が原因で、ユーザーが事前に察知するのは難しい	なし。通常、傷や保管環境の温度•湿度の変化が原因で、ユーザーが事前に察知するのは難しい	なし。頻繁な読み取りエラーや転送速度の低下などの兆候から故障の可能性を推測できる。	あり。ハードディスクの自己監視•分析•報告機能により、故障の兆候をリアルタイムで把握できる。	
推奨用途	小さなファイル、音楽	大容量ファイル、動画	外出時の予備用ファイル	オフィス集中 バックアップファイル	数も多く、大きいファイル

8.5. クラウドバックアップの選択肢

組織がクラウドをバックアップの選択肢とする場合、組織のリソースとセキュリティを考慮して適切なクラウドストレージを探すことができる。一般的なクラウドストレージサービスにはGoogle Drive、Microsoft OneDrive、Dropboxなどがあり、いずれも無料ストレージ容量を提供している。組織は予算やチームの作業習慣などを評価し、最も適したサービスプロバイダーを選択できる。 これらのプロバイダーは詳細な利用ガイドを提供しているため、本マニュアルでは改めて説明しない。

もし組織Aのように、特定のデータが極力保護すべき資産と判断される場合、クラウドバックアップベンダーを選ぶ際には「データの自律性」を考慮に入れるべきだ。クラウドにデータをアップロードするとは、自らのデータをネットワーク経由で送信し、他人のコンピュータに保存することを意味する。データにアクセスする際には、再びネットワーク接続を通じて利用することになる――― ここで が示すデータ保管場所（つまりデータセンター）の所在国は、法執行機関にサーバーの差し押さえやファイルの押収を命じる権限を持つ可能性がある。事例で政府CがNonoグループに組織Aのデジタル足跡記録の提出を命じたように。

したがって、データを重視する市民団体にとっては、クラウドに保存したデータが誰によって管理され、誰がアクセス権限を持つのかを十分に理解することが最善である。ただし、「リスク評価」の章で指摘したように、自らが負担可能なセキュリティ対策を選択することが最も重要だ。下表の通り、オープンソースソリューションの利点はデータの管理権限が大きく、データの流れを監視しプライバシーを守りやすい点にある。一方で、自社での技術的構築にはハードルがある。技術力がない場合や、専門チームにオープンソースのクラウドバックアップ構築•保守を委託できない場合は、保守不足によるセキュリティリスクを避けるため、非オープンソースソリューションも選択肢として残る。

クラウドバックアップ	オープンソースソリューション	非オープンソースソリューション
データ自律性	高い。データの保存場所やアクセス権限を管理できるため、セキュリティとプライバシーがより高い。	低い。サプライヤーが提供する選択肢の中からしか選べない。
サービスの安全性	可視性が高い。誰もがソフトウェアの動作をソースコードで確認し、セキュリティ上の脆弱性がないか確認できる。	可視性が低い。プロバイダーの管理に依存する。
コスト	構築および維持管理コスト。サーバーの購入、サーバールームの賃貸、あるいは運用・保守の外部委託にかかる費用を含む	月額サブスクリプション費用がかかる。

オープンソースソリューションには多くのデータバックアップサービスがあるが、本マニュアルではNextcloudのみを紹介する。このスイートのインターフェースはGoogle Driveと非常に似ており、使いやすく、移行ツールのコストが低いためだ。まずNextcloudの使用方法を見てみよう。操作が比較的簡単だと感じたら、次にセットアップ方法を確認し、オープンソースソリューションでクラウドバックアップを行うべきか評価する。

Nextcloudには3つの利用方法がある。

1. ウェブ経由でバックアップする

図：Nextcloudログイン画面

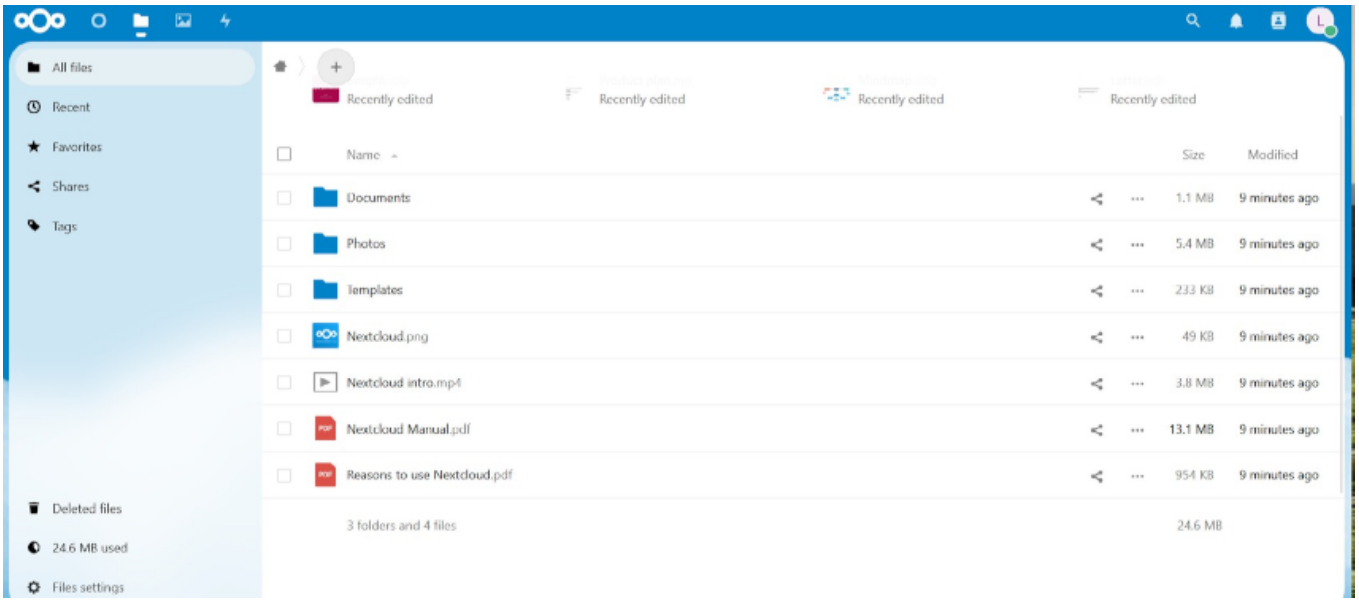
ブラウザを開き、 設定済みの NextcloudのURLをアドレスバーに入力する。ログイン画面に入り、自分のアカウントとパスワードを入力する。

1. PCのファイル同期機能を使う

Nextcloudの公式サイトからプログラムをダウンロードしてインストールする（ https://nextcloud.com/install/ ）。次に、最初の方法と同様に、既に設定済みのNextcloudのURLを入力し、アカウントにログインすれば、パソコン内のファイルと自動同期される。

1. スマートフォンやタブレットのアプリを使用する

iPhoneを使用している場合は、App StoreでNextcloudを検索する（ https://apps.apple.com/us/app/nextcloud/ id1125420102 ） 。 Androidを使用している場合は、Google PlayでNextcloudを検索する（ https://play.google.com/store/apps/details?id=com.nextcloud.client ）。Nextcloudアプリをインストールしたら、最初の方法と同じ手順でクラウドストレージのインターフェースにアクセスできる。



図：Nextcloudの操作画面

NextcloudのインターフェースがGoogle Driveと似ていて、操作に問題がないと感じるなら、以下の設定方法を参考

に、組織がNextcloudをクラウドバックアップソリューションとして利用できるかどうかを検討してみてもいいだろう。

1. ストレージの構築方法：二通りある。

- サーバーとして自前のコンピュータを購入する。利点はセキュリティが高く、ファイルの保存場所を完全に管理できること。欠点は、コンピュータの購入•保守費用や、サーバーを設置するデータセンターの賃料などの費用を負担する必要があることだ。
- サーバーとコンピュータ室のレンタルをサービスプロバイダーに委託する方法。利点は手軽さだが、データの自律性が低下する欠点がある。そのため、サービスプロバイダーが顧客の安全とプライバシーを最優先目標としていることを再三確認することを推奨する。
  1. クラウドストレージのURLを決める

Google Driveが独自のURL（ https://drive.google.com/ ）を持つように、構築するNextcloudにもURLが必要だ。ドメインをレンタルする必要がある。例えば次のようなURL

https：//nextcloud.組織名.tw/

を作成する。組織が既に独自ドメインを持っている場合は、そのまま流用できる。

設定プロセスが組織の技術能力を超える場合、あるいは専門チームによるクラウド空間のセキュリティ維持や外部攻撃の防止を希望する場合は、ネットワークホスティングプロバイダーのGreenhost[30]、GreenNet[31]に相談するか、オープンカルチャー財団（hi@ocf.tw ）に連絡して関連する助言を求めることができる。

8.6. ちょっとしたヒント

データのバックアップは重要でありながら、しばしば見落とされる基礎作業だ。運動の姿勢やテクニックには注意を払うが、運動後のクールダウンを忘れがちで、筋肉をリラックスさせ、スポーツ障害を防ぐ必要がある。そうすることで、より安全に、長く運動を続けられるのだ。同様に、データのバックアップを日常業務の必須要素と捉え、組織が危機的状況に対応する強靭性を構築する必要がある。

読者は〈リスク評価〉の章を参照し、組織がいろんなデータをどの程度保護でき、どの程度のコストを負担できるかを検討し、組織メンバーが実際に実行できるバックアップ体制を確立することを推奨する。定期的なバックアップの習慣を身につけるためには、まずいくつかのチェックポイント（例：レポートがある程度進んだ時点、プロジェクトが終了してアーカイブする前など）を設定し、 重要なステップを見落とさないようにすることから始めるといいだろう。

本稿の内容に疑問がある場合は、hi@ocf.tw オープンカルチャー財団まで問い合わせることができる。

9. 事後検証

大失敗からたくさんのことを学んだ小明のケースをもとに、デジタル・セキュリティの良い習慣は仕事にも生活にも安全をもたらすことを理解されたと思う。小明が授かった巻物の末尾にはチェックリストがついていたので、これを参考にして繰り返し確認するとよい。神が残した忠告も小明は決して忘れないだろう。良いデジタルセキュリティ習慣は一朝一夕で身につくものではなく、継続的な努力が必要なのだという。最初から全てを完璧になどと思わずに定期的に見直し、一歩ずつ改善していくことを忘れないようにしたい。

	チェック項目	実施状況
ブラウザ管理	ウェブサイトからクッキーの受け入れを求められた場合、拒否するか、追跡項目を最小限に抑える。 ブラウザのクッキーと履歴を定期的に削除し、情報漏洩のリスクを減らす。 ほとんどの場合、暗号化されていないHTTPサイトは閲覧しない。やむを得ず利用する際は、個人情報の入力を避け、HTTPページは暗号化されていないため改ざんのリスクがあることを念頭に、ページの内容を再確認し検証する。 個人用と仕事用のブラウザは分けて使用する。 ブラウザを選ぶ際は、プライバシー保護とセキュリティを最優先に考慮する。 ブラウザをインストールする際は、公式サイトからのみインストーラーをダウンロードし、出所不明の場所からのダウンロードは避ける。 ブラウザは最新のバージョンに更新し、セキュリティホール(抜け穴)の発生を防ぐ。	
パスワード	全てのアカウントには、12文字以上で英数字と特殊記号を含む高 度のパスワードを設定してい	

	チェック項目	実施状況
管理	る。 パスワードの再利用は避け、各アカウントごとに異なるパスワードを設定する。 二段階認証に対応しているアカウントについては、全て二段階認証を有効にしている（ 例：Google、Facebook、 LINEなどのサービス ） パスワードマネージャーを使って全てのパスワードを生成•保存•管理している。	
ウェブサイト管理とメンテナンス	自分で構築したウェブサイトでは、データ転送の安全性を保護するためにHTTPSを使用している。 ウェブサーバーとプラットフォームは定期的に更新し、重大なセキュリティ情報の発出に注意を払っている。 団体では権限階層制度を設定し、クラウドストレージへのアクセス権やサイト管理画面へのアクセス権を厳格に管理している。これにより、従業員間や協力チームのデータ取得権限を区別している。 団体は以下のいずれかのウェブサイト管理措置を採用している。(1)ウェブサイトホスティングサービス（本マニュアルで紹介するeQPressなど）を利用し、積極的にサイトを保護する。(2)自社で雇用するか、信頼できる外部セキュリティ専門家を委託し、ウェブサイトと全てのサードパーティ製プラグインを定期的にスキャンし、セキュリティ上の脆弱性がないことを確認する。	
データバックアップ	データバックアップの321ルールに従い、重要な文書やデータを少なくとも3か所に定期的にバックアップする。 バックアップデータが使用可能な状態にあるかどうかを定期的に確認する。	
全体	団体はリスク評価（脅威モデリング）のプロセスに基づき、独自の組織セキュリティポリシーを策定している。 全スタッフに組織セキュリティポリシーを周知する。組織の重要データなどの資産に外部の作業チームなどのアクセスを許可する場合は、作業チームに組織のデータ保護方針などを伝える。外部のアクセスに関するセキュリティ・ポリシーを適用する。 団体は定期的に組織セキュリティポリシーを見直し、最新の状況に対応できるよう調整する。	

日付 ：

記入者：

10. 危機が来た時、どうする？[32]

デジタルセキュリティ防御は脅威の発生を予防するものだが、実際にデジタル攻撃が起きた時に慌てふためけば、かえって努力が水の泡になる。これまでの章で 多くのリスクと対応方法を学んだ今、みなさんには十分な基礎的なセキュリティ知識と防御ツールが備わっている。しかし、デジタル攻撃が発生したその瞬間、どうすれば即座に対応して被害を最小限に抑え、大切な人や物、使命を守れるだろうか？

答えは――「緊急対応メカニズム」を構築する必要があるということだ。

「ああ！また緊急対応『体制』を作らなきゃいけないのか。面倒くさいし、疲れるよ！」 そんな考えが浮かんだんじゃないか？「緊急対応体制」って言葉は重くて複雑に聞こえるけれど、形としては短い文書（電子ファイルかその他の形式）に、関連情報や手順をまとめたものになる。これが緊急事態に直面した時の指針となり、素早く対応する助けになる。以下、三つの側面から説明する。ガイドライン、緊急対応計画の策定、情報セキュリティ支援リソースだ。これらが「緊急対応メカニズム」構築の助けとなる。

10.1. ガイドライン

デジタル攻撃に直面した時、恐怖を感じても「積極的な報告」と「安全最優先」 という二つの原則を貫かねばならない。デジタル攻撃を「積極的に報告」することは、組織全体が早期に発見•介入できるだけでなく、組織とスタッフの安全を確保する。同時に、情報セキュリティ上の損失（携帯電話の盗難、フィッシング詐欺被害、SNSアカウントの乗っ取りなど）に対して共感を持ち、組織や個人が叱責や責任追及を恐れて被害を隠蔽する事態を防ぐ。さらに重要なのは、報奨制度を通じて「安全最優先」の風土を醸成し、情報セキュリティを重視する文化を根底から築くことだ。

10.2. 緊急対応計画の策定

緊急対応計画は危機発生時に「行動」を起こすためのものだ。リスク評価が組織や個人によって異なるように、緊急対応計画も自組織の状況やリソースを総合的に考慮してカスタマイズする必要がある。結局のところ、規模の異なる組織が危機に対処できるリソースは異なり、性質の異なる組織が受けるデジタル攻撃の種類や頻度は大きく異なるからだ。> 個人であれ組織であれ、自らが行動主体となるので、計画策定の適任者なのだ。もちろん、セキュリティ専門家が監修すれば、計画はより完璧になる。

どこから始めればよいか分からない場合、以下に最も一般的な情報セキュリティ緊急事態をいくつか挙げる。まず以下の問題から緊急対応策を考え始めよう。ここで注意しておきたいのは、情報セキュリティインシデントが発生した場合、必要なのは技術やセキュリティ専門家だけでなく、法律の専門家、警察、心理カウンセリング、その他の市民団体などのリソースも必要になる可能性があるということだ。

アカウントやウェブサイトがハッカーに攻撃されたら、どうすればいいか？

- > フィッシングメールをクリックした場合や、その人の端末に不審な動作が見られる(深夜にデータを送信したり大量のファイルをダウンロードするなど)場合、どう対応すべきか？
- 組織のメールや最も機密性の高いファイルが盗まれたり漏洩したりしたら、どうすればいい？
- 組織のメンバーが身体的安全の危険に直面したり逮捕されたりした場合、どうすればよいのか？
- 組織メンバーが身体的安全の危険や逮捕の脅威に直面し、ストレスや不安を感じている場合、どうすればよいか

？

- 組織の事務所が自然災害で被害を受けた場合、どうすればよいか？
- 組織メンバーのパソコンや携帯電話などの端末が紛失または盗難に遭った場合、どうすればよいのか？ これらの質問を通じて、頭の中にリソース連絡先リストと対応策が浮かんだはずだ！ これらの情報を「緊急対応」手順書に書き込む際、 記載したリソースが「連絡可能」であることを確認し、支援要請の連絡手順を順序立てて記載する必要がある。数回の訓練（あるいは実際の使用！）と実行上の障害の排除を経て、定期的な点検と演習を組み合わせることで、効果的な情報セキュリティ対応体制が構築される。

10.3. 情報セキュリティ支援リソース

情報セキュリティ攻撃による被害は、オンライン上で発生するだけでなく、オフラインに波及することもある。攻撃発生時に個人の生命や資産の安全が直接脅かされる場合、生命の安全を最優先の保護概念とし、次に資産の保護を考えること。

台湾において、現地の警察署や病院が信頼できる状況であれば、113（医療救急専用ダイヤル）または110（警察専用ダイヤル）に連絡し、最優先で保護を受けるのが最善策だ。事前に医療•人身安全リソースのリストを準備し、組織内の全員が保管場所を把握しておくこと。デジタル空間における被害、例えばアカウントのハッキング、データ窃取、ネットワーク遮断、ウェブサイト乗っ取りなどについては、現時点では身体的安全に目に見える危機がないとはいえ、直ちに情報セキュリティの専門家に支援を求めなければならない。どのような攻撃なのか、損害をどう食い止めるか、その後の対応と防御策をどう取るかを確認し、被害がさらに拡大したり、現実生活における身体や資産の安全を脅かしたりしないようにするためである。

国際的には、緊急のサイバーセキュリティ状況に対応するため、AccessNowのヘルプライン[33]が24時間体制で緊急対応サービスを提供している。多言語サービスを提供しているが、現時点で中国語は対応しておらず、台湾人が支援を求める場合は英語での通報が主流だ。台湾では、支援を求める者は直接Civil Society Cyber Shield（CSCS）に連絡することを推奨する。CSCSは「技術者と市民社会の架け橋となり、市民団体の情報技術利用の安全性を高める」ことを目標とする情報セキュリティコミュニティである。情報技術やセキュリティ分野のボランティアで構成され、公式連絡先メールcontact@cscs.asiaを通じて以下の支援を依頼できる。

1 情報セキュリティ研修：組織の担当者を対象に、情報セキュリティに関する知識（基礎概念、ネットワークの仕組み、コンピュータセキュリティ、モバイルセキュリティ、オンラインアカウントのセキュリティなど）を研修する。また、各団体の実際のニーズに応じて、カスタマイズされた高度なテーマを提供することも可能だ。例えば、CSCSは過去に「ハッカーによるネットワーク監視技術の実演」を企画・提供したことがある。研修とセキュリティ診断は併せて実施することを推奨する。そうしなければ、効果は限定的となる。

2 機器のセキュリティチェック：講師が組織の担当者を指導し、パソコン、スマートフォン、組織の共用機器（Wi-Fiアクセスポイント、プリンター、ネットワークストレージなど）のセキュリティ設定を確認し、調整の提案や指導を行う。

3 情報セキュリティインシデントに関する相談：ウェブサイトの不正アクセスやアカウントの乗っ取りなど、緊急・非緊急を問わずインシデントへの対応策を提案する。ただし、運用・保守管理のサービスは提供しない。これらは組織が独自に対応するか、専門の外部業者に委託する必要がある。

CSCSはボランティア団体であり、緊急度に応じて1〜2週間以内に回答する。より緊急の支援やその他の支援が必要な場合は、本書の著者であるオープンカルチャー財団（hi@ocf.tw ）に直接連絡し、支援者と利用可能なリソースをつなぐ窓口として活用してほしい。

11. 結語

> 本マニュアルの内容を振り返ってみよう。まずはデジタルセキュリティの理解に始まり、リスク評価のあとには、ブラウザ選択、パスワード管理、ウェブサイトセキュリティ、バックアップについて説明した。デジタルセキュリティの緊急対応メカニズム策定にも重点を置いた。本マニュアルで提唱した概念と提言は、デジタルセキュリティの技術知識や基礎概念に加え、組織メンバー間のコミュニケーションと定期的なトレーニングを繰り返すことが強調されている。デジタルの安全は組織の全員で確保するものだ。屋根の瓦を想像してもよいだろう。最高級の瓦材でなくても風雨は防げるが、もし1枚でも欠けていれば雨水が漏れてくる。組織もたった1人の不注意から安全が脅かされる。

最後に、六つの重要なポイントをまとめ、読者のための最終確認としたい。

1 デジタルセキュリティが守るのは、ウェブサイトやデータ、評判だけではない。組織の中の「人」と使命そのものを守るのだ。

2 デジタルセキュリティの防御と対応に臨むにあたり、まず組織や個人が主に守りたいものは何かを理解する必要がある。

3 デジタルセキュリティの日常ルール4項目と、緊急対応計画とを組織で策定する。

- ブラウザ選択、パスワード管理、ウェブサイトセキュリティ、バックアップ321の4点について、組織と個人の日常業務で改善できる事項を収集し、文書に記録する。
- 起こりうる事象について集団で議論し、事象発生前に「発生時／事後」の対応策を準備しておく。
- 対応策を文書化し、緊急連絡先リストと共に記録する（同一ファイルでも別ファイルでも構わない）。

4 定期的に見直すこと。しかし、より重要なのは頻繁にトレーニングを行うことだ。

5 メンバー全員が、事象発生後の組織の連絡方法と、各役割の行動内容を確実に理解しておく。

6 緊急連絡先リストとは、デジタルセキュリティに関するリソースや身の安全に関するリソースに加え、法律、メンタルヘルス、社会的支援などのリソースも含まれるリストのことだ。

12. 付録1：オープンソースブラウザのダウンロード／インストール手順

パソコンを使用する場合、前述のプライバシー重視のソフトウェアである Firefox、 Brave、 LibreWolf、 Torの4種類は、いずれも公式サイトからのみダウンロードすることを推奨する。すなわち

https://www.mozilla.org/zh-TW/firefox/new/

https://brave.com/zh/download/

https://librewolf.net/installation/

https://www.torproject.org/

自分のOS（Windows、MacOS）に合ったバージョンを選んでダウンロードし、クリックするだけでインストールが始まる。絶対に無料ソフト紹介サイトからダウンロードしてはいけない。公式サイト以外のインストールファイルの安全性は保証できないからだ。

スマートフォンやタブレットなどのモバイル端末を使用している場合、Android端末はGoogle Playストアから、iOS端末はApp Storeから直接ブラウザソフト名を検索してダウンロード•インストールすることを推奨する。公式管理のストアでは定期的にファイルの安全性が確認されているため、他の場所からインストールファイルをダウンロードして端末に持ち込むことは絶対に避けるべきだ。

上記で紹介したオープンソースで安全なブラウザは、いずれも繁体字中国語版が利用可能だ。ただし各ブラウザの公式サポートプラットフォームにおける中国語対応の程度は異なる。例えば Firefoxは中国語対応の歴史が長く、公式サポートプラットフォームで様々な質問に対応する中国語ボランティアが比較的豊富にいる。とはいえ自動翻訳機能は日々進歩しており、プライバシーとセキュリティ保護機能を備えた他のブラウザも安心して試せる。

ブラウザ	サポートプラットフォーム	対応言語
Firefox	https://support.mozilla.org/zh-TW/products/firefox	繁体字中国語
Brave	https://support.brave.com/hc/en-us/	英語
LibreWolf	https://librewolf.net/docs/faq/	英語
Tor	https://support.torproject.org/zh-CN/	簡体字中国語

13. 付録2:KeePassXCの使用方法

KeePassXCは厳重に暗号化されたパスワードマネージャーで、繁体字中国語版がある。ユーザーは簡単に使いこなせる。5分でできるので、設定する手順を一緒に進めよう！

13.1. ダウンロード／インストール手順⬚パソコンへのインストール

注意：ツールをダウンロードする際は必ず公式サイトから行うこと。出所不明のソフトウェアやバックドアが仕込まれたソフトをダウンロードするリスクを避けるためだ。KeePassXCの公式サイト（https://keepassxc.org/ ）にアクセスし、トップページにあるダウンロードリンクから、お使いのOSに対応したバージョンをダウンロードすればよい。覚えておいてほしいのは、KeePassXCは他の商用パスワードマネージャーとは異なり、無料で提供されているということだ。もし登録や支払いを求められたら、間違ったソフトウェアをダウンロードしたことになる。

図：KeePassXCのダウンロード

図：KeePassXCのダウンロード

ダウンロード後、インストールファイルを直接クリックし、ソフトウェアの指示に従って順を追って進めればよい。インストールが完了すれば、使用を開始できる。

スマートフォンやタブレットへのインストール

AndroidやiOS（アップル）版をインストールしたい場合、それらの名称はPC版とは異なる。公式サイトのガイド（https://keepassxc.org/docs/ ）では、AndroidではKeePassDX[34]とKeePass2Android[35]を、iOSではStrongbox[36]と KeePassium[37]の使用を推奨している。これらは全てKeePassファミリーのメンバーであり、互換性があり、パスワード管理の方法も似ている。本稿では主にPC版KeePassXCについて説明する。

13.1.1. 初期設定

KeePassXC は、このソフトウェアを通じて「データベース」（拡張子は .kdbx）と呼ばれる暗号化されたファイルを作成し、ユーザーが設定したマスターパスワードでのみロックを解除できる仕組みになっている。初めて起動すると、ソフトウェアは「新しいデータベースを作成する」か「既存のデータベースを開く」か、あるいは他のパスワードマネージャーからデータベースをインポートするかを尋ねてくる。初めて使用する場合、まだアカウント情報やパスワードを保存していない場合、あるいは別のアカウント情報を保存したい場合は、以下の「新しいデータベースを作成」の手順に従う。

1. 新しいパスワードデータベースに名前を付ける。内容を忘れないように、説明を追加してもよい。

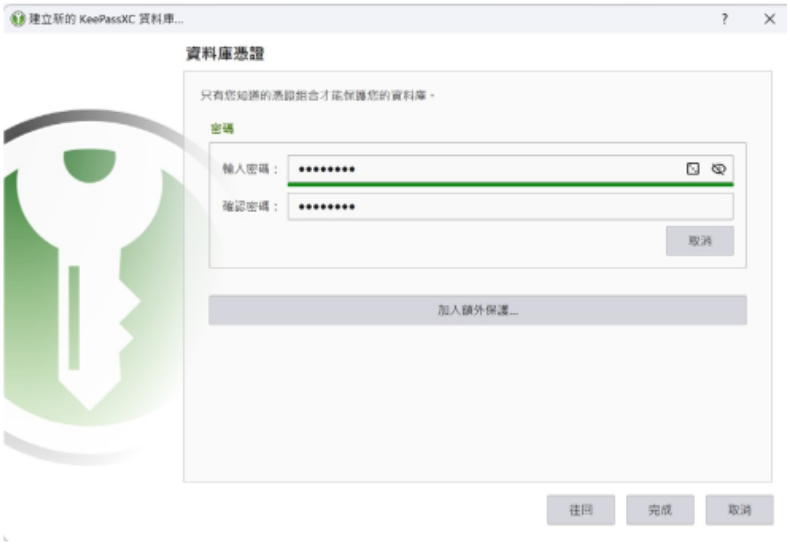
図：新しいKeePassXCデータベースの作成

1. データベースの暗号化レベルを設定できる。レベルを上げておけば、データベースファイルが攻撃者の手に渡ったときに攻撃者が解読してしまうまで時間が長くなる。（その間にパスワードを全部変えてしまえば新たな攻撃をかわすことができる。）

図：新しいKeePassXCデータベースの暗号化設定

図：新しいKeePassXCデータベースの暗号化設定

1. データベースに「マスターパスワード」を設定することは、最も重要な作業だ。マスターパスワードを忘れると、中のデータは二度と取り出せなくなる。



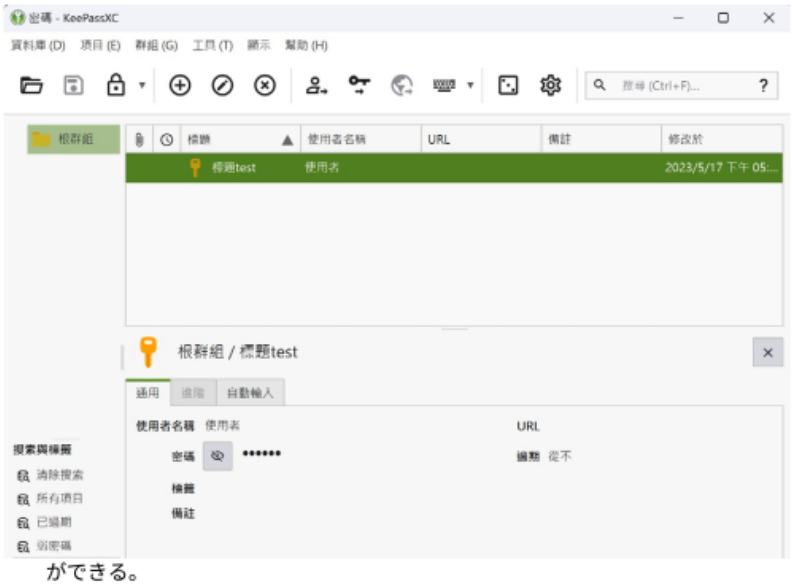
図：新しいKeePassXCデータベースへのマスターパスワード設定

図：新しいKeePassXCデータベースへのマスターパスワード設定

13.1.2. 使用してみる

KeePassXCを起動するたびに、マスターパスワードでデータベースをロック解除する必要がある。ロック解除後は以下の操作が可能だ。

1. ホーム画面には各アカウントの管理項目が一覧表示される。パスワードを使うアカウントをクリックすると、パスワードの閲覧やコピー＆ペーストの準備ができる。

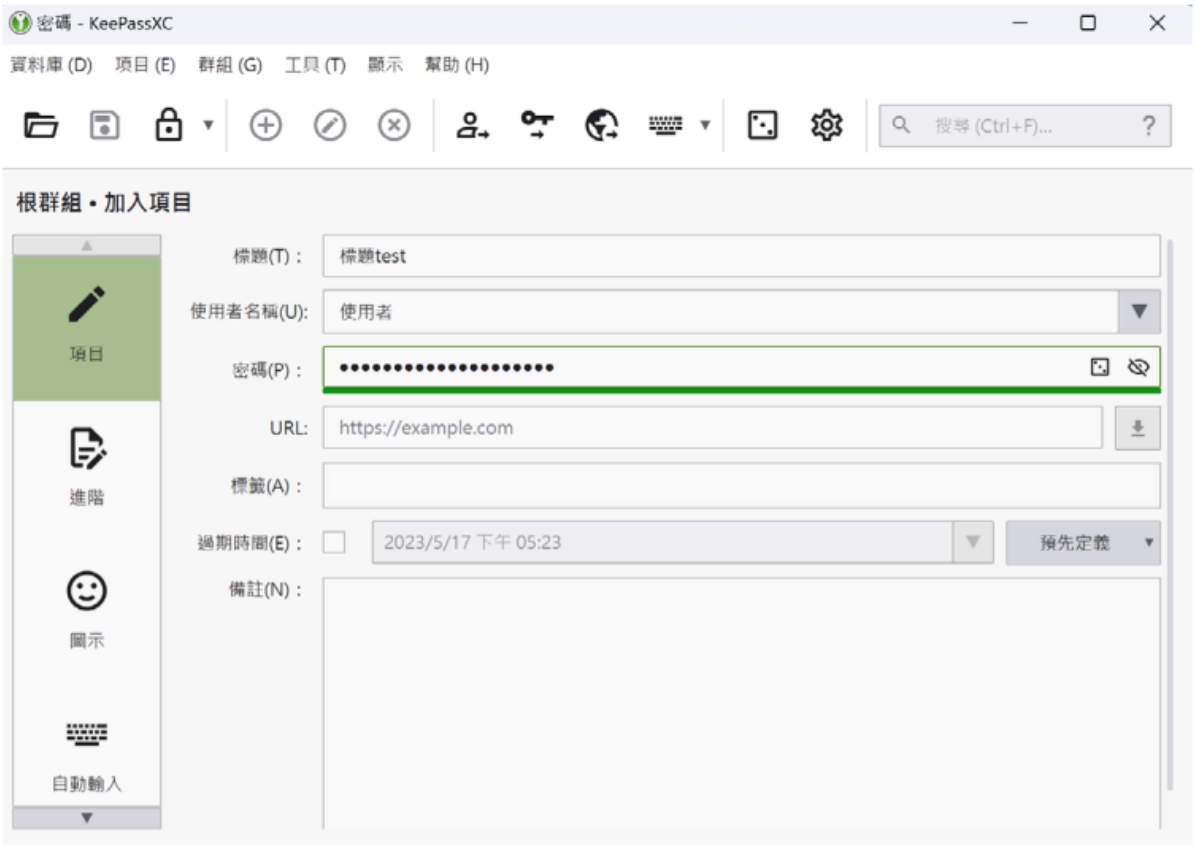


ができる。

図：KeePassXCデータベースでアカウントパスワードを検索

図：KeePassXCデータベースでアカウントパスワードを検索

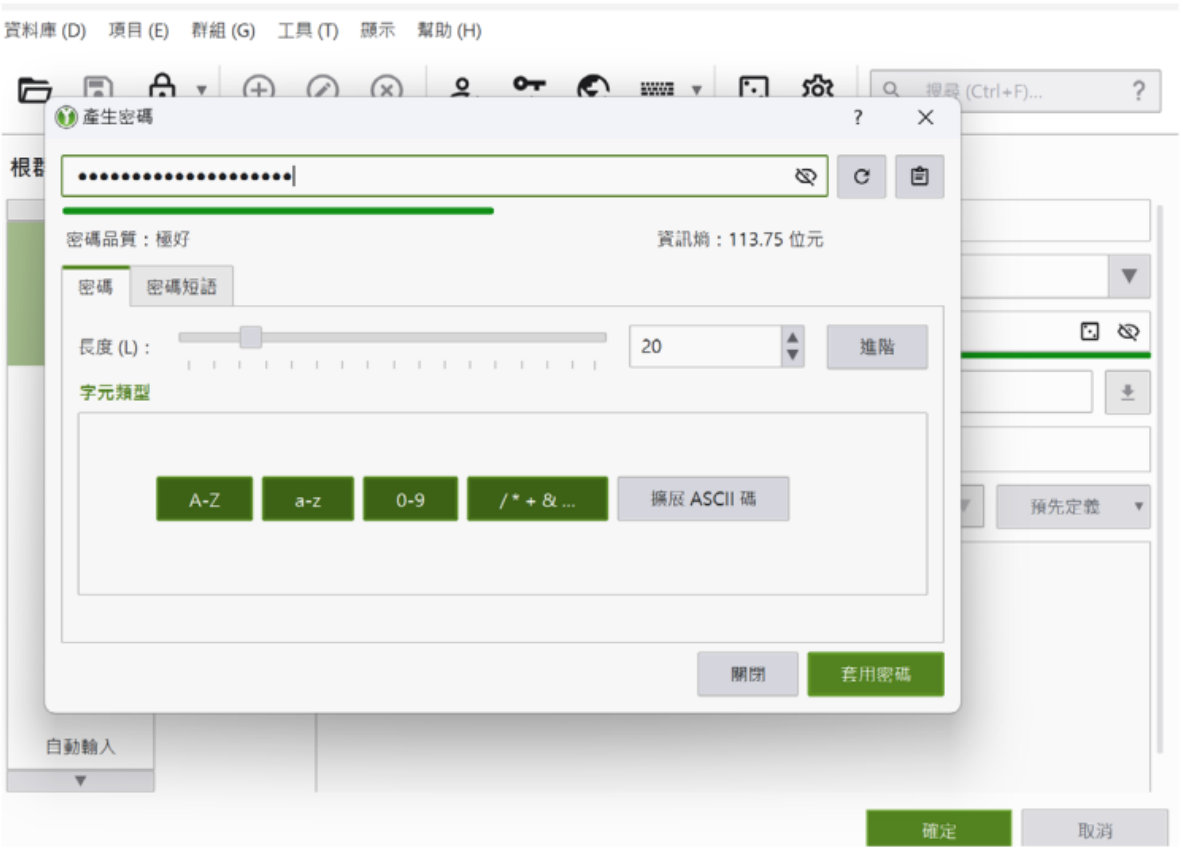
1. 特定のウェブサイトやサービスのアカウントとパスワードを追加するには、ツールバーの「新規項目」を選択する。



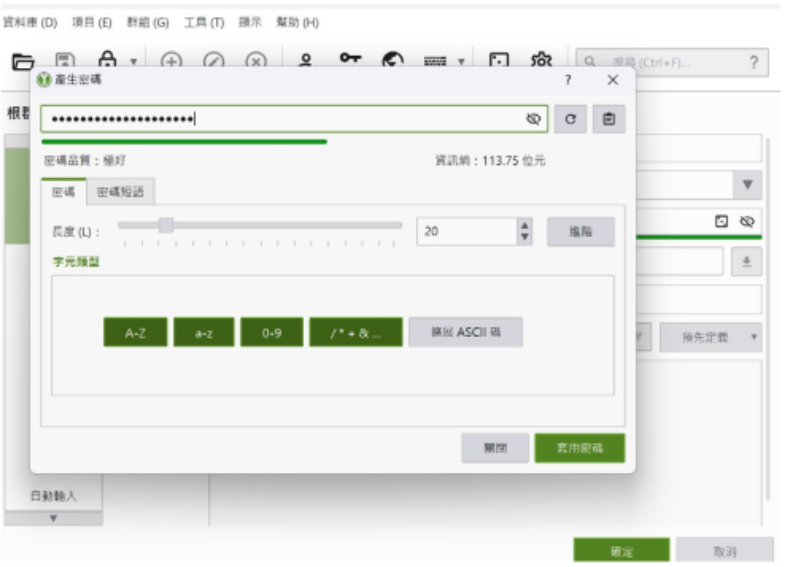
a．タイトルを入力する（例：某ショッピングサイト）

b．ユーザー名（そのサービスに登録したアカウント名）

c．新しいパスワードを生成する。自分で入力してもいいし、ランダムに生成してもいい。



図：KeePassXCデータベースでアカウントパスワードを追加する



図：KeePassXCデータベースでランダムなパスワードを生成する

図：KeePassXCデータベースでランダムなパスワードを生成する

1. ツールバーの「項目編集」：項目のタイトル、ユーザー名、パスワードを変更できる。
2. ツールバーの「項目削除」：選択した項目を削除できる。
3. KeePassXCの設定を変更する必要がある場合、ツールバーの最後にある「設定」で行う：
4. 例えば「一般」では、パソコン起動時にKeePassXCを自動起動。
5. あるいは「セキュリティ」では、> パスワードをコピーしてから貼付けるまでの有効時間を設定できる。もしパス

ワードがコピーされたままになっていて、貼り付けた先が公開のチャットだったら、ゾッとするだけでは済まないだろう。
6. ブラウザで直接パスワードマネージャーに接続したい場合、「ブラウザ統合」からFirefox、Google Chrome、Brave、Edgeなどの主要ブラウザ向けに拡張機能をダウンロードしてインストールできる。これによりブラウザ内で直接パスワードをコピー＆ペーストできるようになる。

前述の1〜4の手順を使えば、パスワード管理ツールの主な機能はマスターできる。これで生活も仕事もより楽に、より安全になる。

13.1.3. 新しいパソコンや他のデバイスでの設定

1. 新しいコンピューターに切り替えても KeePassXC を使い続けるには、データベースを新しいコンピューターに移す必要がある。つまり、拡張子が.kdbx ファイルを新しいコンピューターに移しておく。
2. 新しいコンピューターにKeePassXCをインストール後、初回起動時に「既存のデータベースを開く」を選択する。
3. > 元からデータベース用に設定してあったマスターパスワードを入力すれば、すぐに使用できる。

パスワードマネージャーを使えば、全てのサービスのアカウントとパスワードを覚える必要はなくなる。ただし、KeePassXCのマスターパスワードを絶対に忘れず、コンピュータ内のパスワードデータベースファイル（つまり.kdbx ファイル）を厳重に保管すること。別の場所にバックアップを取ったり、前述のAndroidやiOS版のKeePassファミリーで開き直したりできる。

マスターパスワードを忘れたりデータベースファイルを紛失したりすると、全てのパスワードが失われる。細心の注意を払うことを忘れないでほしい！

奥付

市民組織 デジタル防御マニュアル — プライバシーとセキュリティを重視したオープンソースツール

著者：財団法人オープンカルチャー財団

編集：林倚安

デザイン：張文蘊

発行元：財団法人オープンカルチャー財団

メール：hi@ocf.tw URL：https://ocf.tw/p/csodefense/

2023年5月 初版

2024年7月 第二版第一刷

ISBN : 37838G35708G2

Footnotes:

[1] (訳注)原著では「市民社会組織(Civil Society Organization)」とあるが、日本では、市民社会組織というばあい、いわゆるNPOなどが自称としてこの用語を用いる一方で、労働組合や草の根の市民運動や社会運動は自らの組織を市民社会組織とは呼ばない場合がある。本マニュアルでは、便宜的に市民団体とした。

[2] https://ocf.tw/p/defendhrd/

[3] https://internews.org/resource/global-trends-in-digital-security-civil-society-and-media/

[4] 組織 Aは、読者が本マニュアルの応用方法を理解するための架空の組織であり、実在する事例ではない。

[5] 「脅威モデリング」は物理世界の資産保護にも適用される。例えば組織が従業員の身体的安全を重要資産と判断した場合、最高速度制限の設定や運転安全教育の実施といった規則を策定する。本マニュアルは市民団体がデジタル世界のリスクに対応する体制構築を支援することを目的としているため、脅威モデリングではデジタル世界で一般的な脅威と防御手段を主に取り扱う。

[6] (訳注) 「「フィッシングとは、捏造・偽装した電子メールやWebサイトなどを用いて利用者を騙し、重要な情報を入力させて盗み取ったりマルウェアに感染させる攻撃」 IT用語辞典 https://e-words.jp/w/%E3%83%95%E3%82%A3%E3%83%83%E3%82%B7%E3%83%B3%E3%82%B0.html

[7] ソーシャルエンジニアリング：ソーシャルエンジニアリングとは、情報セキュリティにおいて人間の心理を操作し、行動を起こさせたり機密情報を漏洩させたりする手法を指す。リスク評価

[8] 物語の都合上、本編で使用されるデジタルサービスは全て架空のものである。

[9] VPNは仮想プライベートネットワークであり、ネットワークトラフィックを暗号化しIPアドレスを隠蔽することで、第三者による監視やデータ収集を防ぐ。

[10] uBlock Originは、自由でオープンソースのクロスプラットフォーム対応コンテンツフィルタリングブラウザ拡張機能だ。広告やウェブサイトの追跡を削除し、ユーザー自身がフィルタリング設定を実装できるオプションを提供する。

[11] NoScriptは、JavaScript、Java、Flash、Silverlight、その他のプラグインやスクリプトコンテンツをホワイトリストで選択的に実行できる、自由でオープンソースのブラウザ拡張機能だ。

[12] パスワードマネージャー紹介：https://www.privacyguides.org/zh-Hant/passwords/

[13] YubiKey：https://www.yubico.com/products/yubikey-5-overview/

[14] オープンソースパスワード管理ソフト：KeePass：https://ithelp.ithome.com.tw/articles/1022G300

[15] KeePassXC 無料パスワード管理ソフト図解チュートリアル：クレジットカード•ブラウザ•スマホから素早く入力： https://www.playpcesor.com/2020/07/keepassxc.html

[16] (訳注) スマホ用はkeepassxc.orgに記載がない。Apple StoreやGoogle PlayからKeepass互換のソフト(KeePass2AndroidあるいはKeePassiumなど)をインストールすることになる。

[17] ハウツー：KeePassXCの使用方法 https://ocftw.github.io/ssd.eff.org/zh_TW/module/how-use-keepassx.html

[18] https://equalit.ie/values/

[19] https://www.vice.com/en/article/qv5xwq/the-activists-on-the-forefront-of-ukraines-cyberwar

[20] https://deflect.ca/non-profits/

[21] https://deflect.ca/privacy-notice/

[22] https://www.cloudflare.com/zh-tw/galileo/

[23] https://ocf.tw/p/cscs/SEC%20%EG%35%B4%E4%BD%B5%E7%83%88_+%E3%A0%81%E7%A2%BC.pdf

[24] https://ssd.eff.org/

[25] https://www.veeam.com/blog/air-gap-vs-immutable-backups-key-differences.html

[26] NASの正式名称はNetwork Attached Storage（ネットワーク接続ストレージ）である。ユーザーはIPアドレス設定、FTP、ネットワーク共有などを通じてNAS内のファイルにアクセスできる。多くの組織がオフィス内のデータ共有•保存•バックアップ場所としてNASを利用している。

[27] https://www.ithome.com.tw/news/147155

[28] 〈リスク評価〉の章で述べたように、100%の安全は存在しない。クラウドバックアップを利用すれば、物理的なバックアップが故障や盗難で失われるリスクを低減できるほか、共同作業の利便性といったメリットもある。しかし同時に情報セキュリティ上のリスクも伴う。組織は脅威モデリングのプロセスを用いて、保護すべきデータの価値や許容できるコストを特定し、組織の経済力で実行可能な最適のバックアップ方法を見つけることが推奨される。

[29] データ転送速度は、バックアップと復元時の効率に関わる。具体的には、ファイルをコンピュータからストレージデバイスへコピーする（書き込み速度）時間と、ストレージデバイスからファイルをアクセスまたはコンピュータへ復元する（読み取り速度）時間を指す。速度が速ければ速いほど、バックアップと復元の完了時間が短縮される。 これは、大量のデータを頻繁にバックアップする必要があるユーザーにとって特に重要だ。

[30] https://greenhost.net/

[31] https://www.greennet.org.uk/

[32] 参考資料： https://www.ndi.org/sites/default/files/%5BEnglish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf

[33] AccessNow セキュリティ相談窓口（Digital Security Helpline）: https://www.accessnow.org/help/

[34] https://play.google.com/store/apps/details?id=com.kunzisoft.keepass.free

[35] https://play.google.com/store/apps/details?id=keepass2android.keepass2android

[36] https://apps.apple.com/us/app/strongbox-password-manager/id837283731

[37] https://apps.apple.com/us/app/keepassium-keepass-passwords/id1435127111

Author: toshi
Created: 2026-08-22 土 12:05
Validate