スパイウェアから身を守る

最終更新日：**2026年10月15日**　所要時間の目安：**30分**

ACTIVIST CHECKLIST

このコピーは 2026年11月6日 に作成。 脅威が変化するにつれ、また自分の身を守るより良い方法が利用可能になるにつれ、ガイドを頻繁に更新します。最新バージョンはこちらから。 activistchecklist.org/ja/spyware/

自動翻訳: このページは自動翻訳されています。現時点で人によるチェックが済んでいるのはページの0%だけで、それ以外の部分には誤りがあるかもしれません。翻訳のチェックに協力する[1]。

ほとんどの活動家は、商用スパイウェアの標的にはなりません。導入には国家レベルの予算がかかるからです。あなた自身が著名な立場にいる場合や、そういう人と一緒に活動している場合、最も重要な対策は、パッチが公開されたその日にスマホをアップデートすること、ロックダウンモード（iPhone）または高度な保護機能（Android）をオンにすること、そして怪しいリンクを避けることです。何かおかしいと感じたら、Citizen LabやAccess Nowが無料でデバイスを検査してくれる場合があります。

スパイウェアとは、あなたのデバイスに感染し、知らないうちに、同意もなくあなたを監視してデータを盗むソフトウェアのことです。最も狙われやすいのはスマホです。詳細な位置情報や多要素認証（2FA）のコード、その他たくさんの個人情報が記録されているからです。ただし、ノートパソコンやその他のデバイスが狙われることもあります。

スパイウェアは、プライベートなメッセージを抜き取り（Signalのような暗号化メッセージアプリでも）、2FAコードにアクセスし、会話を監視し、位置情報をリアルタイムで追跡し、さらには気づかないうちにカメラやマイクをオンにすることさえできます。こうしたデータはすべて、スパイウェアを操る側に送り返されます。スマホを使っているあなたの肩越しに、誰かがずっと画面をのぞき込んでいるようなものです。

スパイウェアは民間企業によって作られ、政府に販売されています。そして犯罪者だけでなく、活動家、ジャーナリスト、弁護士に対しても使われています。最近では、ICE（移民・関税執行局）がスパイウェアツールへのアクセス権を購入しました[2]。

モバイル向けスパイウェアとして最もよく知られているのは、Pegasus（NSO Group製）とGraphite（Paragon Solutions製）の2つです。どちらの企業も、米国でいうNSAにあたるイスラエルの「8200部隊」の元幹部たちによって設立されました。でも、新しい[3]スパイウェア[4]は次々と見つかっています。しかもスパイウェアは、「マルウェア」や「ストーカーウェア」と呼ばれるもっと大きな世界のほんの一角にすぎません。こうしたツールは、抑圧的な政府や、パートナーに暴力をふるう人たちが、相手を黙らせるためにも使っています。スパイウェアは、クリックすらしなくても、ごく普通のオンライン広告を通じて送り込まれる[5]ことさえあります。

自分がスパイウェアの標的になる可能性はどのくらい？

政府はスパイウェアを犯罪者にしか使わないと主張していますが、政府が政治活動家、ジャーナリスト、弁護士に対して使った事例は数多く記録されています：

- 著名なオーガナイザーや活動家（カタルーニャ[6]）
- 人権派弁護士（メキシコ[7]）
- 調査報道ジャーナリスト（Forbidden Stories[8]とAmnesty International[9]を参照）
- 標的となった人の家族のデバイスがスパイウェアに感染していたケースも確認されています。（Citizen Lab[10] を参照）

PegasusやGraphiteのようなスパイウェアを使うには、政府にとっても**数万〜数十万ドル**のコストがかかります。**つまり、ほとんどのアクティビストはスパイウェアの標的にはならないので、他の脅威から身を守る[11]ことのほうが役に立ちます。**

まずはセキュリティの基本チェックリスト[11]から始めて、それからこのガイドに戻ってくるのがおすすめです。そのガイドは、位置情報の追跡や、警察がデバイスを押収した後に使うスマホのロック解除ソフトなど、もっと安く使える監視技術から身を守るのに役立ちます。

抑圧的な政治家たちがアメリカを権威主義へと押し進め続けるなか、高度なスパイウェアがアクティビストに対してより広く使われるようになると考えておくべきです。

良いニュース： スパイウェアやストーカーウェアから身を守るための対策は、あなたが実際に受ける可能性の高い他の種類の攻撃を防ぐことにも役立ちます。なので、どちらにしてもやっておく価値があります。

パニックにならないで： こうした高度なハッキングツールについて読むと、つい強い不安を感じてしまいがちです。ほとんどの活動家は、スパイウェアの標的にはなりません。権威主義者たちは、自分たちが全能で、私たちの行動をすべて見通せると思い込ませたいのです。いくつかの簡単なステップで、私たちを監視することを、彼らにとってコストが高く、政治的にもリスクの大きいものにできます。

基本の対策

すべての人　このセクションは、アクティビズムや権利擁護に関わるすべての人向けです。

☐ 「デジタルセキュリティの基本」チェックリストを完了しよう

このガイドでは、パスワード、アプリの位置情報の許可、ソフトウェアのアップデートなど、ドクシング対策として大切なその他のステップを紹介しています。

ドクシングが心配なら、「デジタルセキュリティの基本」チェックリスト →[11]にあるステップを済ませておくのがおすすめです。

ドクシングの標的になった場合、その多くが、あなたのアカウントやデバイスに誰かがアクセスしようとするのを防いでくれます。

「基本」チェックリストの中でも、特に大切なのは次の項目です：

- ほとんどのアプリで**位置情報の追跡をオフにする**
- パソコン、スマホ、アプリに**最新のソフトウェアアップデートをインストールする**
- **パスワードマネージャー**を使う
- 弱いパスワードや複数のサイトで使い回しているパスワードがあれば、**今使っているパスワードを変更する。**
- 重要なアカウントで**二要素認証**を有効にする
- **怪しいリンク**はクリックしない

☐ スマホ（とパソコン）のOSを常に最新バージョンにしておく

ハッカーやスパイウェア、警察が使うスマホのハッキングツールから身を守れます。

DO: 通知が来たらすぐにアップデートをインストールする　DO NOT: 「後でアップデート」ボタンを押し続ける

OSのアップデートが出るたびに、セキュリティホールが修正されています。インストールしていないアップデートが増えるほど、警察があなたのデバイスをハッキングできる手段も増えていきます。鍵のかかっていないドアがどんどん増えていく、大きな建物を想像してみてください。

OSが最新の状態でなければ、このガイドで紹介している他の対策の多くも、あなたのデータを守れません。

まずはスマホから始めましょう。リスクの高い活動をする場合は、すべてのデバイスをアップデートしておきましょう。

アップデートのやり方

セキュリティアップデートはとても大切なので、**手順を一つずつ案内するツールを作りました**。

スマホとパソコンのアップデートを確認する →

手動でアップデートする方法

手動でアップデートしたい場合は、デバイスごとに次の手順で行えます：

クリックして手動の手順を表示

iPhone

1. **デバイスがまだサポート対象か確認する：** お使いのiPhoneがまだサポートされているか確認する[1][2]
2. **オペレーティングシステム： 設定** → **一般** → **ソフトウェアアップデート**
3. **アプリ** は、デフォルトで自動アップデートされる設定になっています。確認するには、**設定** → **アプリ** → App Store を開き、**Appのアップデート** がオンになっていることを確かめましょう。

Mac

1. **デバイスがまだサポート対象か確認する：** お使いのMacがまだサポートされているか確認する[1][2]
2. **オペレーティングシステム：** Appleメニュー → **システム設定** → **一般** → **ソフトウェアアップデート**
3. **Mac App Storeからインストールしたアプリ：** これらのアプリは、デフォルトで自動アップデートされる設定になっています。確認するには、**App Store** を開いて App Store → **設定** に進み、**自動アップデート** がオンになっていることを確かめましょう。
4. **その他のアプリ：** 画面上部のメニューバー → アプリ名をクリック → **アップデートを確認** または [**アプリ名]について** をクリック でアップデートを確認するか、**設定...** の中を探してみてください。アップデートのオプションが見当たらない場合は、バックグラウンドで自動的にアップデートされる設定になっている可能性があります。

Android

1. **デバイスがまだサポート対象か確認する：** お使いのAndroidがまだサポートされているか確認する[1][2]
2. **オペレーティングシステム： 設定** → **システム** → **システム アップデート**（メーカーによって異なる場合があります）
3. Google Playストアの **アプリ** は、デフォルトで自動アップデートされる設定になっています。確認するには、**Playストア** を開いてプロフィールアイコンをタップし、**設定** → **ネットワーク設定** → **アプリの自動更新** に進みます。

Windows

1. **システムをアップデートする： スタート** → **設定** → **更新とセキュリティ** → **Windows Update**
2. **デバイスがまだサポート対象か確認する：** お使いのWindowsパソコンがまだサポートされているか確認する[1][2]
3. **Microsoft Store アプリ：** 自動更新[3]が有効になっていることを確認しましょう（デフォルトでオン）。
4. **その他のアプリ：** メニューバー → **ヘルプ** → **更新の確認** でアップデートを確認するか、アプリの設定で **アップデート** や **バージョン情報** を探してみてください。

☐ ロックダウンモード（iPhone）または高度な保護機能（Google・Android）を有効にする

スパイウェアは高度な攻撃の一種で、私たちのデバイスにある巧妙な脆弱性を悪用します。これに対抗するため、AppleとGoogleはスパイウェアへの防御を強化する高度なセキュリティモードを導入しています。

iPhoneでは**ロックダウンモード**[14]、Androidでは**高度な保護機能プログラム**[15]と呼ばれています。（Androidスマホを持っていなくても、Googleアカウントだけで高度な保護機能プログラムを有効にすることもできます。）

Appleのロックダウンモードをオンにしていたのにスパイウェアに感染した、という報告は**まったくありません**。Androidの高度な保護機能は比較的新しく、その効果はまだ実証されていません。

> **使い勝手とのトレードオフ：**どちらの機能も、一部の機能が使えなくなるなどの犠牲をともないます。トレードオフの一覧はこちら[16]。使っていて不便な問題が出てきたら、あとからいつでも機能をオフにできます。

IPHONEでロックダウンモードを有効にする方法

iPhone： 設定 → プライバシーとセキュリティ → ロックダウンモード → ロックダウンモードをオンにする

この機能はiOS 16以降で利用できます。

ANDROIDで高度な保護機能を有効にする方法

Android： 設定 → セキュリティとプライバシー → その他の設定 の下にある **高度な保護機能** をタップ

注：この設定の場所はAndroid端末によって異なる場合があるので、設定の検索バーで「高度な保護機能」と検索するのがおすすめです。

この機能はAndroid 16以降で利用できます。

☐ スマホとパソコンで広告をブロックする

ごく普通のネット広告を通じてスパイウェアが送り込まれた事例があります。クリックすら必要ありません。

Citizen Labの調査で[5]、日常的に使うアプリやウェブサイトに表示されるターゲティング広告を通じてスパイウェアが送り込まれていたことがわかりました。広告が読み込まれるだけでデバイスが感染してしまいます。広告を目にしていなくても、クリックしていなくても、です。

広告をブロックすれば、この侵入経路をふさげます。さらに、警察やデータブローカーが広告ネットワークを通じてあなたの位置情報を追跡する[17]のも難しくなります。

広告をブロックする方法

- ☐ **スマホに広告ブロック機能のある信頼できるVPN[17]をインストールして、常にオンにしておく。** ブラウザだけでなくアプリ内の広告もブロックできるので、これが一番大事なステップです。 IVPNでは、**AntiTracker**をオンにします。 Proton VPNでは、**NetShield**をオンにします（有料プランのみ）。 VPNの設定方法[17]を参照してください。
- ☐ **パソコンにも同じVPNをインストールして**、そちらでも広告ブロックをオンにする。
- ☐ **広告をブロックできるプライバシー重視のブラウザ[11]を使う。** たとえばBraveや、uBlock Origin[18]を入れたFirefoxなどです。ただし、守られるのはそのブラウザでの操作だけです。

VPNを使いたくない場合は、AdGuard[19]のような広告ブロック機能付きのDNSサービスを使えば、代わりにスマホ全体で広告をブロックできます。暗号化DNS[17]を参照してください。

☐ 広告ID（警察に位置情報を追跡されるおそれあり）を無効にする

ICEをはじめとする警察機関が位置追跡ツールを使っている[20]ことがわかっています。これらのツールは、スマホが発信する「広告ID」に部分的に依存しています。こうしたツールは、社会運動の弾圧によく使われています。

広告IDは、広告経由で送り込まれるスパイウェアの標的選びにも使われてきました[21]。

iPhoneでは、この機能はデフォルトで無効になっています。 Androidではデフォルトで有効になっているので、無効にする必要があります。

広告IDを無効にする方法

IPHONE

設定 → **プライバシーとセキュリティ** → **トラッキング** → **Appからのトラッキング要求を許可**をオフにする

iPhoneでは、この設定はデフォルトで無効になっています。でも、念のため確認しておきましょう。

ANDROID

設定 → 検索アイコンをタップして「広告」で検索 → **広告 ID を削除**をタップ

この設定の場所は機種によって違うので、検索するのがいちばん簡単です。

☐ iCloudの「高度なデータ保護」（iPhone）またはGoogleの「高度な保護機能プログラム」を有効にする

Apple、Googleなどのサービスは、アカウントやデータを狙った標的型攻撃から守るための追加のセキュリティ機能を提供しています。これらが守るのは各社のオンラインアカウントで、デバイスそのものではありません。

Appleの「高度なデータ保護」を使うと、ほとんどのコンテンツでエンドツーエンド暗号化が有効になります。

メール／クラウドアカウントで高度な保護を有効にする方法

データを守る：

- iCloudの「高度なデータ保護」[22] - iCloudに保存されているほぼすべてのデータでエンドツーエンド暗号化が有効になり、政府の裁判所命令から情報を守れます。復旧キーは必ずとても安全な場所（パスワードマネージャー[11]など）に保存しておきましょう。

アカウントを守る：

- Googleの「高度な保護機能プログラム」[23] - フィッシングや不正アクセスからアカウントを守るのに役立ちます。
- MicrosoftのAccount Guard[24]
- Proton Sentinel[25]

☐ 怪しいリンクはクリックしない

何をクリックするかに気をつけることで、スパイウェアから身を守れます

スパイウェア[21]は、あなたを狙って、つい開かずにはいられないように作り込まれたリンク付きのメッセージやメールで届くことがよくあります。これはただのスパムではありません。あなたにとって一番大切なものにつけ込む、あなたを狙い撃ちにした攻撃です。

怪しいリンクの見抜き方と対処法

迷ったら：リンクをクリックしない！

1. 代わりに、送り主（企業でも友人でも）に別の方法（電話する、別のアプリを使うなど）で連絡して、本当に送ったのか確認しましょう。確認に2分かけるほうが、クリックしてデバイスを乗っ取られるよりずっといい。
2. bit.lyやtinyurl.comのような短縮URLの場合は、ExpandURL.net[26]を使ってリンク先のページを確認できます。ただし、そのページがスパイウェアでないという保証にはなりません。本当のURLを確認できるので、信頼できるかどうかをより正しく判断できるようになるだけです。
3. リンクがすでに悪意のあるものとして報告されているかを確認したいときは、VirusTotal[27]（Google/Alphabet傘下）のようなフィッシング・マルウェアのデータベースにリンクを貼り付けて調べることができます。VirusTotalは誰でも検索できる公開データベースなので、送信するのは公開されていて個人情報を含まないリンクだけにしましょう。

要注意のサイン：

- **知らない番号からのメッセージ：** 連絡先に登録していないサービスからメッセージが届くことはよくあるので、本物かどうかを見分けるのは簡単ではありません。連絡先にない相手からなら、より慎重に対応しましょう。
- **焦りや恐怖をあおる**：「アカウントがロックされます」「緊急セキュリティ警告」「家族の緊急事態」
- **見慣れないドメイン名：** スパイウェアのメッセージは、`adsmetrics[.]co` のような変なドメインから届くことが多い
- **個人的すぎる**：あなたの活動、最近参加したイベント、知り合いなどに触れてくる。冷静な判断をさせないための手口
- **予想外のメッセージ**：知り合いから説明なしにリンクが届く、いつもと違う言い回し、変な時間帯に届く（相手のアカウントが乗っ取られているかも）
- **短縮URL**：`bit.ly`、`tinyurl.com` など、本当のリンク先を隠す短縮サービス
- **URLの微妙なスペル違い**：`google.com` ではなく `goog1e.com`

スパイウェアのメッセージは、特定の人を狙い撃ちにしていることがあります。 Pegasusスパイウェアが実際に使われた例をいくつか紹介します：

> 「カルメンへ　弟が事故で亡くなりました。とても辛いです。葬儀の情報を送ります。来てもらえたら嬉しいです：[スパイウェアのリンク]」（出典[28]）

> USEMBASSY.GOV/ あなたのビザに問題が見つかりました。至急大使館までお越しください。詳細を見る [スパイウェアのリンク]（出典[28]）

> LX 1955 BCN-ZRH 26Jun2020 - リンクをクリックしてモバイル搭乗券を受け取ってください [スパイウェアのリンク]（出典[29]）

注意： スパイウェアの中には、リンクをクリックしなくても感染させる攻撃（「ゼロクリック攻撃」）を使うものもあります。たとえば、WhatsAppの不在着信として現れることもあります。

さらに強化した対策

中程度の脅威 このセクションは、リーダー的な役割を担っている人や、国家や対立勢力から標的にされやすい運動分野に関わっている人向けです。

☐ スマホやデバイスからアプリをできるだけ削除する

泥棒に家へ侵入されにくくしたいなら、簡単な方法のひとつはドアの数を減らすこと。デバイスの中では、アプリひとつひとつが外の世界への「ドア」の役割を果たしていて、攻撃を受けるリスクを高めてしまいます。アプリにバグや脆弱性があると、デバイス全体が危険にさらされることがあります。

アプリの削除方法

1. **スマホに入っているアプリをすべて確認する。** パソコンも同じように確認しましょう。
2. **本当に必要かどうか判断する。** 多くのアプリは、代わりにウェブサイトから同じように利用できます。たいていは少し不便になりますが、その分プライバシーとセキュリティが高まります。
3. **できる限りアンインストールする。** 迷ったら、一週間アンインストールしてみて、なくてもやっていけるか試してみましょう。後からいつでも再インストールできます。

過去にスパイウェアに悪用されたアプリの例：

- Apple HomeKit + FindMy + iMessage[30]
- Apple カレンダー[31]

☐ SignalとWhatsAppのリンクプレビューをオフにする

メッセージにリンクを貼ると、多くの場合「リンクプレビュー」が自動で表示されます。目には見えなくても、実はあなたのデバイスがプレビュー画像を取得するために、そのウェブページにアクセスしています。そのウェブページが悪意のあるものだった場合、高度な攻撃者にあなたの位置情報を特定されたり、最悪の場合はスマホにスパイウェアを仕込まれたりするおそれがあります。

リンクプレビューをオフにする方法

- **Signal:** Signalを開く → プロフィール写真をタップ → **設定** → **チャット** → **「リンクプレビューを生成」をオフにする**
- **WhatsApp: 設定** → **プライバシー** → **詳細設定** → **リンクプレビューを無効にする**

☐ インカメラをふさぐ

すでにスパイウェアに感染している場合、カメラやマイクにアクセスされて、デバイスをリアルタイムで監視される可能性があります。監視する側に見られるものを減らすために、少なくともインカメラはふさいでおくのがおすすめです。

インカメラをふさぐ方法

1. 何度も貼り直せるくらい粘着力のあるシールを用意しましょう。または、SLNTのこのシールパック[32]を使うのもおすすめです。
2. スマホとノートパソコンに貼る
3. インカメラを使うときだけ一時的にはがして、使い終わったら忘れずに貼り直しましょう。

- [ ] **活動用にサブのスマホや使い捨てのバーナーフォンを用意することも検討しよう**

自分の活動スタイルに合うなら、リスクの高い活動専用に別のスマホやパソコンを用意することも検討してみてください。

詳しくはサブのスマホのチェックリスト[33]をチェックしてください。

その場合でも、すべてのデバイスでセキュリティ対策を忘れずに行いましょう。機密性の高いやりとりやデータが入っているのが片方のデバイスだけでも、どちらのデバイスもスパイウェアの標的になる可能性があります。どちらからも、あなたの位置情報など、攻撃者が狙う個人情報がわかってしまうからです。 **GrapheneOS[34]**に対応したスマホを選ぶのもひとつの手です。 GrapheneOSは、Google Pixelで動作する、セキュリティとプライバシーを重視したAndroidベースのOSです。

- [ ] **デバイスを定期的に再起動する**

ほとんどのスパイウェアは、デバイスにファイルを一切書き込まないことで痕跡を隠そうとします。そのため、デバイスを再起動すれば、スパイウェアはひとまず消える可能性が高いです。とはいえ、まだ標的にされている場合は、相手がすぐにまたスマホを感染させようとしてくる可能性が高いです。感染の中には、リンクをクリックする（または何らかの操作をする）ことで起こるものもあれば、ユーザーが何も操作しなくても起こるものもあります。つまり、スマホをこまめに再起動すれば攻撃者にとって手間を増やすことはできますが、それでスパイウェアから確実に逃れられるわけではありません。

デバイスの検査

iPhone を使っているなら、iMazing[35] でスパイウェアの分析ができます。無料で利用できます（「購入」ボタンはクリックしないでください）。技術に詳しい人は、Mobile Verification Toolkit (MVT)[36] を使って、本人の同意のもとで詳しいデバイスのフォレンジック調査を行うこともできます。

ただし、デバイス上のスパイウェアを検出するのは簡単なことではありません。誰にでもスマホの調査を任せていいわけではありません。世界中の市民社会のメンバーが、以下の機関に頼って、専門家のサポートのもとでスマホを調べ、詳しい分析を行ってきました：

- Citizen Lab[37] - スパイウェア分析の第一線の専門家
- Access Now[38]
- Amnesty Security Lab[39]
- Constitutional Communications[40] - 活動家コミュニティのより多くの人がスパイウェア分析を受けられるよう支援している団体

- Electronic Frontier Foundation[41] - 米国在住の人向け

団体ごとに独自の審査プロセスがあり、先方で確認を進める間、返事が来るまでに時間がかかることもあります。

感染しているかもしれないサインに気づくには

スパイウェアは通常、目立った症状がなく、**気づかれないうちに**感染します。ただし、これまでスパイウェアの標的になった人たちからよく報告されている症状には、次のようなものがあります：

- スマホのバッテリーが急に減る
- 特定のアプリの動作がおかしい
- データ通信量が異常に多い
- 怪しいリンクや添付ファイルが届く

> こうした症状があったとしても、必ずしもデバイスがスパイウェアでハッキングされているとは限りません。上でリンクした団体のいずれかに連絡して、デバイスを検査してもらうことをおすすめします。

> スパイウェアは非常に高度なマルウェアで、一般的なウイルス対策ソフトでは**検出できません**。デバイスに（過去または現在の）侵害の兆候があるかどうかを判断するには、信頼できる専門団体にサポートを求めることをおすすめします。

現在、**Apple**と**WhatsApp**は、傭兵型スパイウェアの標的にされた疑いのあるユーザーに定期的に通知を送っています。詳しくはAppleの脅威通知[42]とWhatsAppの脅威通知[43]をご覧ください。

もっと詳しく

- Citizen Lab は、Pegasus による作戦を45か国[44]で確認しています
- Forensic Architecture は、それらの作戦がもたらした人的被害を、自身のサイト Digital Violence[45] でマッピングしています

関連情報：アメリカ政府がインターネットのセキュリティを損なってきた歴史：

- Microsoft handed the NSA access to encrypted messages（Microsoft が暗号化されたメッセージへのアクセスを NSA に提供）[46] - The Guardian、2013年
- Revealed: how US and UK spy agencies defeat internet privacy and security（暴露：米英の諜報機関はいかにしてインターネットのプライバシーとセキュリティを破っているか）[47] - The Guardian、2013年
- N.S.A. Able to Foil Basic Safeguards of Privacy on Web（NSA、ウェブ上のプライバシーの基本的な保護を突破可能）[48] - The New York Times、2013年
- NSA infected 50,000 computer networks with malicious software（NSA、5万のコンピューターネットワークをマルウェアに感染させる）[49] - NRC、2013年
- Secret contract tied NSA and security industry pioneer（秘密契約が NSA とセキュリティ業界の先駆者を結びつけていた）[50] - Reuters、2013年
- N.S.A. Devises Radio Pathway Into Computers（NSA、無線経由でコンピューターに侵入する手段を考案）[51] - The New York Times、2014年

- How the NSA Plans to Infect 'Millions' of Computers with Malware（NSA は「数百万台」のコンピューターをいかにマルウェアに感染させようとしているか）[52] - The Intercept、2014年
- Prying Eyes: Inside the NSA's War on Internet Security（詮索の目：NSA によるインターネットセキュリティへの戦争の内幕）[53] - Der Spiegel、2014年
- New Discovery Around Juniper Backdoor Raises More Questions About the Company（Juniper のバックドアをめぐる新発見で、同社への疑問がさらに深まる）[54] - Wired、2016年
- The NSA Leak Is Real, Snowden Documents Confirm（NSA のリークは本物、スノーデン文書が裏付け）[55] - The Intercept、2016年

関連ガイドでさらに学ぼう

ドクシング対策
ドクシングやネット上のハラスメントから身を守ろう。

緊急時への備え
拘束されたり脅威にさらされたときに備え、緊急時の支援ネットワークをつくろう。

「警察が家に来たら」ポスター [56]

リンク

1. activistchecklist.org/ja/contribute/
2. 404media.co/were-suing-ice-for-its-2-million-spyware-contract/
3. unwall.app/www.wired.com/story/coruna-iphone-hacking-toolkit-us-government/
4. unwall.app/www.wired.com/story/hundreds-of-millions-of-iphones-can-be-hacked-with-a-new-tool-found-in-the-wild/
5. citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/
6. citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
7. citizenlab.ca/research/lawyers-murdered-women-nso-group/
8. forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
9. securitylab.amnesty.org/case-study-the-pegasus-project
10. citizenlab.ca/research/reckless-exploit-mexico-nso/
11. activistchecklist.org/ja/essentials/
12. activistchecklist.org/ja/updates/
13. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
14. support.apple.com/en-us/105120
15. landing.google.com/intl/en_us/advancedprotection/
16. activistchecklist.org/ja/lockdown/
17. activistchecklist.org/ja/vpn/
18. ublockorigin.com
19. adguard.com/en/welcome.html
20. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
21. activistchecklist.org/ja/spyware/
22. support.apple.com/en-us/108756
23. landing.google.com/advancedprotection/
24. accountguard.microsoft.com
25. proton.me/support/proton-sentinel
26. expandurl.net
27. virustotal.com/gui/home/url
28. citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
29. citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
30. citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/
31. citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/
32. slnt.com/products/webcam-cover
33. activistchecklist.org/ja/secondary/
34. grapheneos.org
35. imazing.com/spyware-analyzer
36. github.com/mvt-project/mvt
37. citizenlab.ca/spyware-outreach/
38. accessnow.org/help/
39. securitylab.amnesty.org/get-help/
40. constitutionalcommunications.org
41. eff.org/about/contact
42. support.apple.com/en-us/102174
43. faq.whatsapp.com/641700318302674
44. citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
45. digitalviolence.org
46. theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
47. theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
48. unwall.app/archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
49. nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487
50. reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
51. unwall.app/www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html
52. theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/
53. spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
54. unwall.app/www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/
55. theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/
56. activistchecklist.org/ja/police/