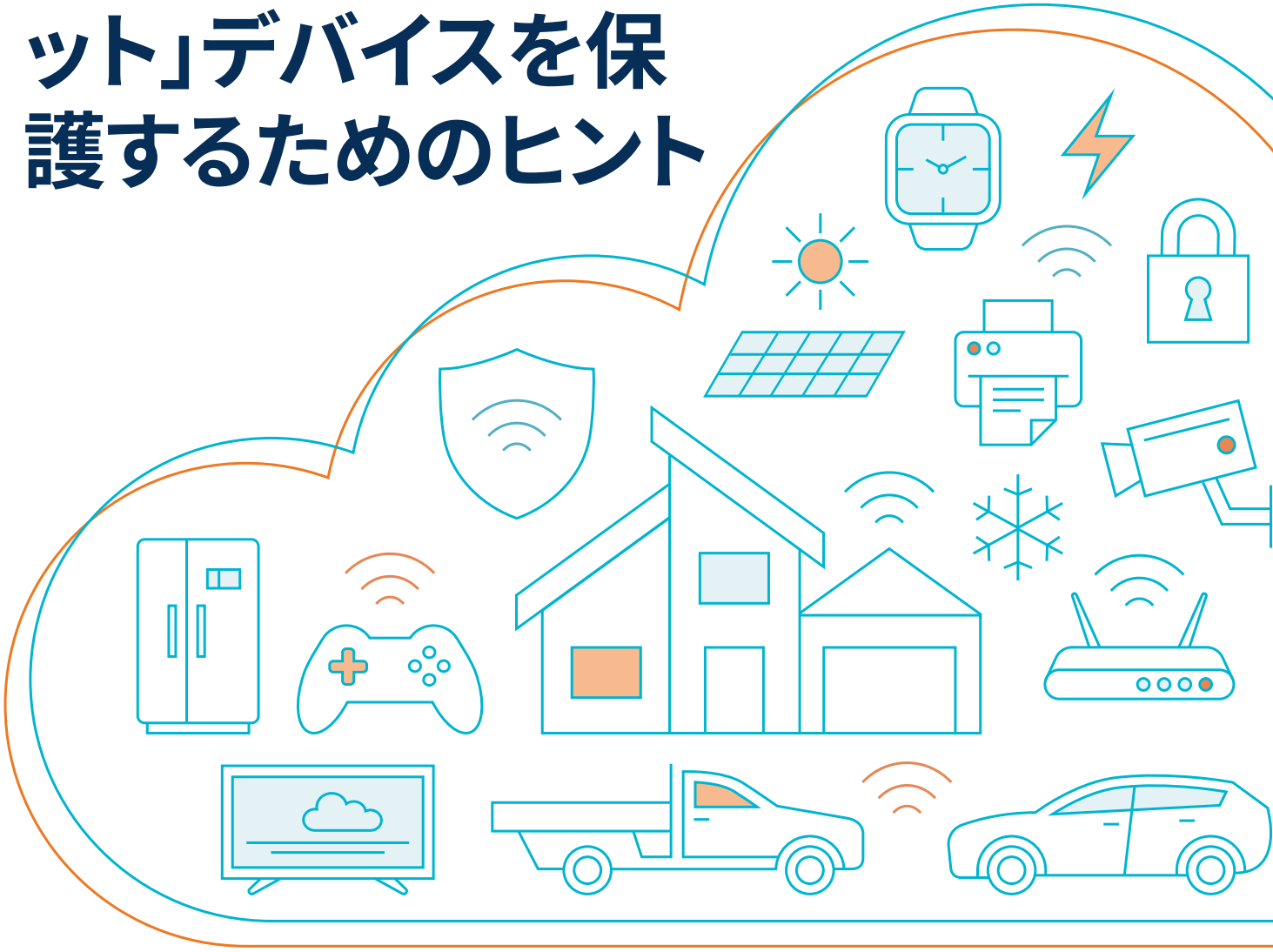
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

cyber.gov.au

# 「モノのインターネット」デバイスを保護するためのヒント



オーストラリア・サイバーセキュリティセンターは、コミュニティの皆様が「モノのインターネット（IoT）」デバイスを安全に購入し、利用できるよう支援するために、この情報を作成しました。IoTデバイスとは、日常的な製品にインターネット接続機能が追加されたものを指します。IoTデバイスの例としては、ベビーモニター、ドローン、防犯カメラ、スマートテレビ、ソーラーインバーターなどがあります。家庭や企業内のIoTデバイスは、一般的にWi-Fiのほか、4Gや5Gなどの携帯通信ネットワークを利用してインターネットに接続します。

オーストラリアの家庭や企業で一般的に見られる多くのIoTデバイスは、セキュリティを考慮して設計されていません。その結果として、デバイスはインターネット経由での侵害に脆弱になりました。こうしたインシデントにより、サイバー犯罪者が悪意のある目的で、あなたのデバイスや個人データに無断でアクセスする恐れがあります。

# IoTデバイスを購入する前に

メーカーによってセキュリティ対策のレベルが異なるため、購入前にデバイスの情報をしっかり調べることが重要です。デバイスを購入する前に、異なるメーカーから販売されている同種のデバイスを比較しましょう。検討すべきポイントには、以下が含まれます。

1. **そのデバイスは、信頼できる有名な企業によって製造され、信頼できる有名な店舗で販売されているものですか？** 信頼性の高い有名企業は、セキュリティを意識してデバイスを製造している可能性が高いです。よく知られた信頼性の高い店舗では、同様に信頼できる有名企業の製品のみを取り扱っている可能性が高く、メーカーの意図した状態で製品が手元に届くよう、より厳格なサプライチェーン管理が行われている傾向があります。

2. **パスワードを変更することは可能ですか？** パスワードは変更するのが望ましいです。特に、デバイスに脆弱な初期パスワードが設定されている場合は、パスワードの変更がより重要になります。セキュリティが優れたデバイスには、一意で予測困難かつ複雑で、推測が不可能なパスワードを設定するべきです。なぜなら、脆弱な初期パスワードはデバイスを攻撃する最も簡単な手段の一つだからです。

3. **メーカーはアップデートを提供していますか？** 企業が、発見されたデバイスの脆弱性を修正するためのアップデートを提供することは重要です。例えば、デバイス上のソフトウェアに既知の脆弱性が含まれている場合や、ハッカーが新たな侵害手法を開発した場合には、それらを修正するためのアップデートが必要です。

4. **デバイスはどのようなデータを収集し、そのデータは誰と共有されますか？** どのようなデータが収集され、どのように使用されるのかに関する情報は、メーカーのウェブサイトやプライバシーポリシーで容易に確認できるはずです。オンラインアプリやモバイルアプリが収集する情報について、常に注意を払うことが重要です。

5. **そのデバイスは、あなたが必要なことだけを実行しますか？** 必要以上の機能、特にインターネット接続機能を備えたデバイスを購入すると、セキュリティが低下する可能性があります。使用しない機能は、あなたにとって利益がないだけでなく、攻撃に対する脆弱性を高める原因となる場合があります。

# IoTデバイス

デバイスを設定する際には、ネットワークやデータのセキュリティを強化するために、いくつかの基本的なポイントを意識しましょう。

1. **そのデバイスはインターネットに接続する必要がありますか？** 接続可能であるからといって、必ずしも接続すべきとは限りません。インターネットに接続されていないデバイスは、侵害される可能性が大幅に低くなります。インターネット接続が必要な機能を使用しないのであれば、そのデバイスを本当にインターネットに接続する必要があるかを検討すべきです。

2. **そのデバイスは安全な場所に設置されていますか？** デバイスを安全でない場所に設置する必要がない場合は、安全な場所に設置することで物理的な侵害のリスクを低減できます。

3. **初期設定のユーザー名とパスワードは変更しましたか？** 強力なパスワードやパスフレーズを使用することが重要です。デバイスに一意で予測困難かつ複雑で推測不可能なパスワードが設定されていない場合、そのパスワードを変更する必要があります。初期設定のユーザー名やパスワードは収集され、オンラインで公開されることがあるため、デバイスが攻撃に対して脆弱な状態になります。

4. **私のWi-Fiネットワークは安全に設定されていて、強力なパスワードが設定されているでしょうか？** Wi-Fiネットワークとルーターをしっかり保護し、攻撃者がデバイスやネットワークに容易にアクセスできないようにしましょう。

### 一歩踏み込んだ対策を講じましょう

ルーターにIoTデバイス専用のWi-Fiネットワークを追加設定する。これは、Wi-Fiルーターで「ゲスト」ネットワークと呼ばれることがあります。IoTデバイス間の通信が不要であれば、「クライアントアイソレーション」機能を有効にしましょう。IoTデバイスを機密データから隔離しておくことで、仮にIoTデバイスが侵害されても、他のデバイスやデータへのアクセスを防ぐことができます。

5. **デバイスの不要な機能は無効にされていますか？** デバイスに不要な機能（カメラやマイクなど）がある場合は、可能な限り無効化しましょう。

### 一歩踏み込んだ対策を講じましょう

デバイスのウェブ管理インターフェースへのリモートアクセスをローカルLANやWAN／インターネット経由で有効にする設定がないか確認しましょう。リモートアクセスが必要な場合を除き、ローカルLANに設定されていることを確認してください。

# IoTデバイスの維持管理

IoTデバイスが設定され、使用を開始した後も、覚えておくべき重要なポイントがいくつかあります。これらには、以下が含まれます。

1. **デバイスを定期的に再起動する。**IoTデバイスの動作が遅くなったり、操作できなくなったりした場合は、ウイルスに感染している可能性があります。ほとんどのマルウェアはメモリ内に保存されており、デバイスの再起動、つまり電源のオフ・オンによって簡単に削除できます。再起動後もデバイスの動作が遅い、または操作できない場合は、初期化（ファクトリーリセット）を試してみましょう。ただし、この操作を行うと、ユーザーデータや個人設定がすべて消去される可能性があるため注意が必要です。

2. **定期的にアップデートを適用する。**デバイスによっては、自動的にアップデートが適用されます。自動アップデートに対応していないデバイスの場合は、メーカーの情報を定期的に確認し、アップデートが提供されたら適用しましょう。お使いのデバイスへのアップデート提供が終了している場合は、アップデートが提供されている新しいデバイスへのアップグレードを検討しましょう。セキュリティアップデートが提供されないデバイスは、新たな脆弱性が発見された際に保護されず、ネットワークやプライバシー、データに対するリスクになりかねません。

3. **使用していないデバイスの電源は切りましょう。**使用しておらず監視もしていないデバイスの電源を入れたまま、長時間Wi-Fiネットワークに接続し続けると、デバイスが攻撃される可能性が高まります。これを自動的に実現する方法の一つとして、電源タイマー付きコンセントを使用し、指定した時間帯だけデバイスに電源を供給する方法があります。

4. **月々のインターネット使用量や請求額に大幅な増加がないか注意しましょう。**インターネット使用量や課金額が大幅に増加した場合、デバイスが侵害された可能性があります。社内のIT部門による調査が行われないのであれば、デバイスを初期化し（この際、ユーザーデータや個人設定がすべて消去される可能性があることにご注意ください）、その後パスワードを変更してください。

# IoTデバイスの処分

デバイスを処分したり売却したりすると、他人があなたの個人情報やデータに簡単にアクセスできてしまう可能性があります。
これを防ぐための方法としては、次のようなものがあります。

1. **すべてのデータと個人情報を消去する。**メーカーは、デバイス本体および関連アプリケーションからデータや個人情報を消去する方法を提供しているはずです。個人情報を消去しておけば、デバイスを処分した後に他人がその情報にアクセスすることがありません。IoTデバイスを使わなくなった場合、関連するオンラインアカウントも不要であれば削除してください。

2. **デバイスを初期化する。**初期化は、ローカルストレージに保存されたデータを消去し、パスワード、ユーザー名、設定を初期状態に戻すための機能です。初期化の方法については、デバイスの取扱説明書やメーカーのウェブサイトを確認してください。

3. **スマートフォンや他のデバイスとの関連づけを解除する。**他のデバイスやネットワーク、オンラインアカウントへのアクセス権を残したままデバイスを処分すると、第三者がそれらにアクセスする恐れがあります。他のデバイスを確認し、処分するデバイスとのペアリングがあれば必ず解除しておきましょう。不要になったモバイルアプリに付与した権限は解除しましょう。

4. **デバイスに接続されているUSBメモリやメモリーカードなどのリムーバブルメディアは、必ず取り外しておきましょう。**リムーバブルメディアには初期化では消去されない個人データが含まれている可能性があるため、物理的に取り外し、破壊した上でデバイスとは別に処分するようにしましょう。

# サポート

オーストラリア信号局のオーストラリア・サイバーセキュリティセンターへの連絡は、メールasd.assist@defence.gov.auまたは24時間対応のホットライン**1300 CYBER1 (1300 292 371)**をご利用ください。

サイバー犯罪は、以下のサイトからReportCyberに報告してください：
www.cyber.gov.au/report

個人情報の盗用被害に遭った場合は、以下のIDCAREのウェブサイトからご相談ください：
www.idcare.org

ご自身やご家族のサイバーセキュリティ対策に関するアドバイスは、以下のウェブサイトをご覧ください：www.cyber.gov.au。最新のオンライン脅威に関する情報を受け取るには、ACSCの無料アラートサービスにご登録ください。

オーストラリアを世界で最も安全にオンライン接続できる国にしましょう。

サイバーセキュリティに関するアドバイスは、以下のサイトをご覧ください：
www.cyber.gov.au

**免責事項**

このガイドブックの内容は一般的なものであり、特定の事情や緊急事態において法的な助言や依存すべき助言とみなされるべきものではありません。重要な事柄については、独立した専門家からご自身の状況に則した適切な助言を仰ぐべきです。

このガイドブックに含まれる情報に依存した結果生じた損害、損失や費用に対して豪連邦政府はいかなる責任も負いません。

**著作権**





**豪連邦政府紋章の使用について**



**さらに詳細な情報について、またはサイバーセキュリティ事件の報告は以下の連絡先まで:**

**cyber.gov.au** | 1300 CYBER1 (1300 292 371)

この電話番号はオーストラリア国内でのみご利用いただけます。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre