Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# インターネットを安全に使うには

## 高齢者向けガイド

cyber.gov.au

# はじめに

**インターネットを使うと友人や家族と連絡を取り合ったり、さまざまなことについて学んだりすることができますし、ゲームもできます。**

車を運転するときにシートベルトをまず締めるように、インターネットを使う時もまず安全を確認しなければいけません。

豪州サイバーセキュリティセンター(ACSC)はインターネットを使うすべての人の安全を確保したいと考えています。この文書には、インターネットを使う時に自分を守るために実践できる基本的なサイバーセキュリティ対策がまとめられています。


豪州通信電子総局(ASD)の一部である豪州サイバーセキュリティセンター(ACSC)はオーストラリアに対するサイバー脅威の防止・検知と修復のためのアドバイス・援助や運用上の対応を行っています。ACSCの目標は、オーストラリアを最も安心してインターネットを使える国にすることです。

**サイバーセキュリティのさらに詳しい情報やガイド、アドバイスについてはホームページcyber.gov.auから**





# 高齢者向けサイバーセキュリティ

## ヒントその1：デバイスのアップデートする

**ソフトウェアをアップデートするのはクルマを定期点検に出すようなものです。デバイスの性能を向上させ、より安全にします。**

サイバー犯罪者はデバイスに不正侵入する新しい方法を常に探しています。デバイスが自動的にアップデートをインストールするよう設定することでソフトウェアに潜む脆弱性を解消し不正侵入を防ぐことができます。

**さらに詳細な情報はホームページcyber.gov.auから「Updates」を検索してください。**



### ご存知でしたか：

アップデートを行うと新しい性能がデバイスに追加されたりより速く作動するようになったりすることもあるのです。

## ヒントその2：多要素認証の使用

**アカウントのログインに多要素認証を使うのは自宅に防犯用のドアや網戸を設けるようなものです。犯罪者の不正侵入から自分を守ります。**

多要素認証を使うと、アカウントにログインする際に2種類以上の情報を提供しないとアクセスできません。例えば、ソーシャルメディアのプロフィール画面にログインする場合にパスワードに加えてテキストメッセージに送付されてきたコードも入力するなどです。

多層的な仕組みを使うことによりサイバー犯罪者が不正侵入を行いにくくなります。たとえ犯罪者が例えばパスワードを推測できても、それ以外の認証要素がなければアカウントにはアクセスできません。

**さらに詳細な情報については ホームページcyber.gov.auから「Multi-factor authentication」または「MFA」を 検索してください。**



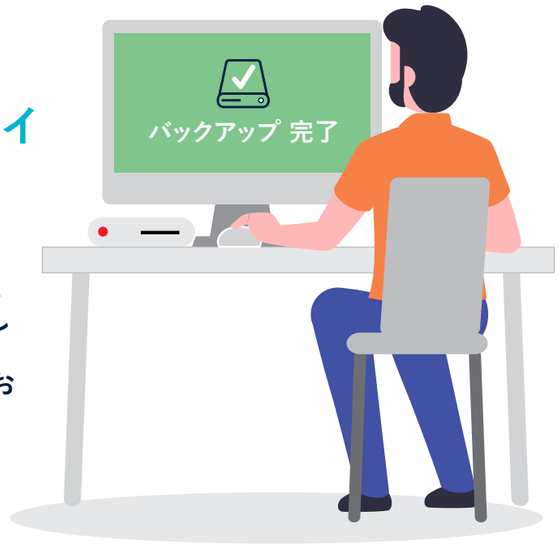
**忘れないで：**

**多要素認証の設定方法がよくわからない場合は友人や家族に手伝ってもらいましょう。**





## ヒントその3：デバイスのバックアップ




**「バックアップ」を行うというのは大切なファイルのコピーを作ってそれをどこか安全な場所に保管しておくことを指します。大切な写真が万が一紛失した時のためにコピーをとって金庫に入れておくようなものです。**

パソコン、スマートフォンやタブレット型コンピュータをバックアップする場合には、ファイルのコピーがオンラインに保存されるか別の記憶装置に保存されます。大切なファイルや大事な写真のバックアップがあれば安心です。

万が一デバイスに不測の事態が起きたり、サイバー犯罪者による不法侵入があってもバックアップを使って簡単にファイルを復旧できます。

**さらに詳しい情報についてはホームページcyber.gov.auから「Backups」を検索してください。**


**ご存知でしたか：**

定期的にデバイスをバックアップしておけば **常に最新のファイルにアクセスできます。**

## ヒントその4：パスフレーズの使用

**パスワードがアカウントにかかった南京錠ならパスフレーズは本格的なセキュリティシステムです！パスフレーズはより強固で安全なパスワードのようなものです。**


MFAが使えない場合にはパスフレーズを使ってアカウントをセキュアにしましょう。パスフレーズとは、4つ以上の単語を無作為に組み合わせた長文のパスワードを指します。サイバー犯罪者による推測が困難になる一方ユーザーには覚えやすいのです。

パスフレーズを考える時には次の点に留意しましょう：

- **長いもの**長いほど安全です。最低でも14文字の長さを目標にしましょう。4つ以上の単語の無作為な組み合わせで覚えられるものを。例えば、'purple duck potato boat'など。
- **推測しにくいもの**推測しにくければしにくいほど良いのです。普通の文章はパスフレーズにしやすいですが、簡単に推測されてしまいます。4つ以上の単語を無作為に組み合わせた方がパスフレーズとしては強固です。
- **固有性の高いもの**一回使ったパスフレーズは再使用してはいけません。アカウントごとに別のパスフレーズを設けましょう。たくさんのパスフレーズを覚えるのが大変な場合は、パスワードマネージャー・プログラムを使うことを考えましょう。このプログラムを使えば、パスワードは一つ覚えておけばあとはパスワードマネージャーにお任せです。詳しいアドバイスはホームページcyber.gov.auから「password manager」を検索してください。

**安全なパスフレーズの作り方についてさらに知りたい方はホームページcyber.gov.auから「Passphrases」を検索してください。**





## ヒントその5：詐欺を見つけたら通報

**迅速に通報すればするほど取り締まりも素早くできます。**

誰かがインターネットを使って自分に詐欺をはたらこうとしているのではと思ったら被害が起きるまで待たずに積極的に行動しましょう。

話がうますぎると思う話はふつう本当ではありません。あなたが賞金を獲得したとかあなたのパソコンにウイルスが侵入したとかというメッセージがきてもそれはあなただけに送られたものではありません。

詐欺犯罪者からのメッセージがあなたに付け込もうとしているだけかもしれません。

詐欺犯罪者は、信用できる個人や団体組織のフリをしてくることが多いのを忘れずに。信用できる人物からメッセージを受け取っても、電話番号、メルアドやソーシャルメディア・プロフィールが新しくなっている場合は特に用心が必要です。そうしたメッセージに返信する前に、信頼できる方法でその人や団体組織に連絡をとってメッセージを送ってきた相手が本当に本人やその組織かどうか確認しましょう。例えば、お子様の一人からきたように見えるテキストメッセージが知らない番号から発信されていたら返信してはいけません。ソーシャルメディアを使って直接メッセージを送り、本当に電話番号を変えたのか確認しましょう。

### ご存知でしたか：

**サイバー犯罪者は巧妙でよく知っている名前やメルアドを使ってくるかもしれません。次のような場合は要注意です：**

- **至急支払いを求められている。**
- **パスワードやその他詳細の変更を求められている。**
- **リンクをクリックしたり添付ファイルを開けるよう求められている。**

## 結論

さて、インターネットをより安全に利用するための知識がつきましたので、これで安心してネットをブラウズし、オンライン生活を引き続き楽しむことができます。

ただし、サイバー犯罪者は常に新しい方法でユーザーを狙っていることを忘れずに。

サイバーセキュリティについてのノウハウを随時アップデートしインターネット上で安全を保つ新しい方法を身につけましょう。

# ボーナスヒント

## インターネットを安全に使う方法を他にも知りたいですか？以下のヒントも参考にしましょう。

**インターネットに投稿する内容には注意。**

インターネット上で共有する情報内容と、誰がそれを見ることになるか注意して考えてみましょう。実生活で知っている人以外からの友達申請には応じてはいけません。

**新たなサイバー脅威についての警報をゲット。**

無料警報サービスに申し込みましょう。新種のサイバー脅威が発見されるたびに通知があります。

サイバー攻撃があった場合にどうしたら良いのかについてのアドバイスも提供します。

**家族や友人とサイバーセキュリティについて話し合う。**

サイバーセキュリティについて知識アップができたら、家族や友人と学んだ知識を共有しましょう。あなたが学んだことがいつか家族や友人の役に立つかもしれません！

**公共Wi-Fiネットワークを使って オンラインバンキングやショッピングを行わない。**

ビデオを観たりウェブサイトを見るだけなら公共Wi-Fiネットワークも良いのですが、金銭取引に関係することは自宅のインターネットで行いましょう。公共Wi-Fiネットワークにはリスクが伴います。

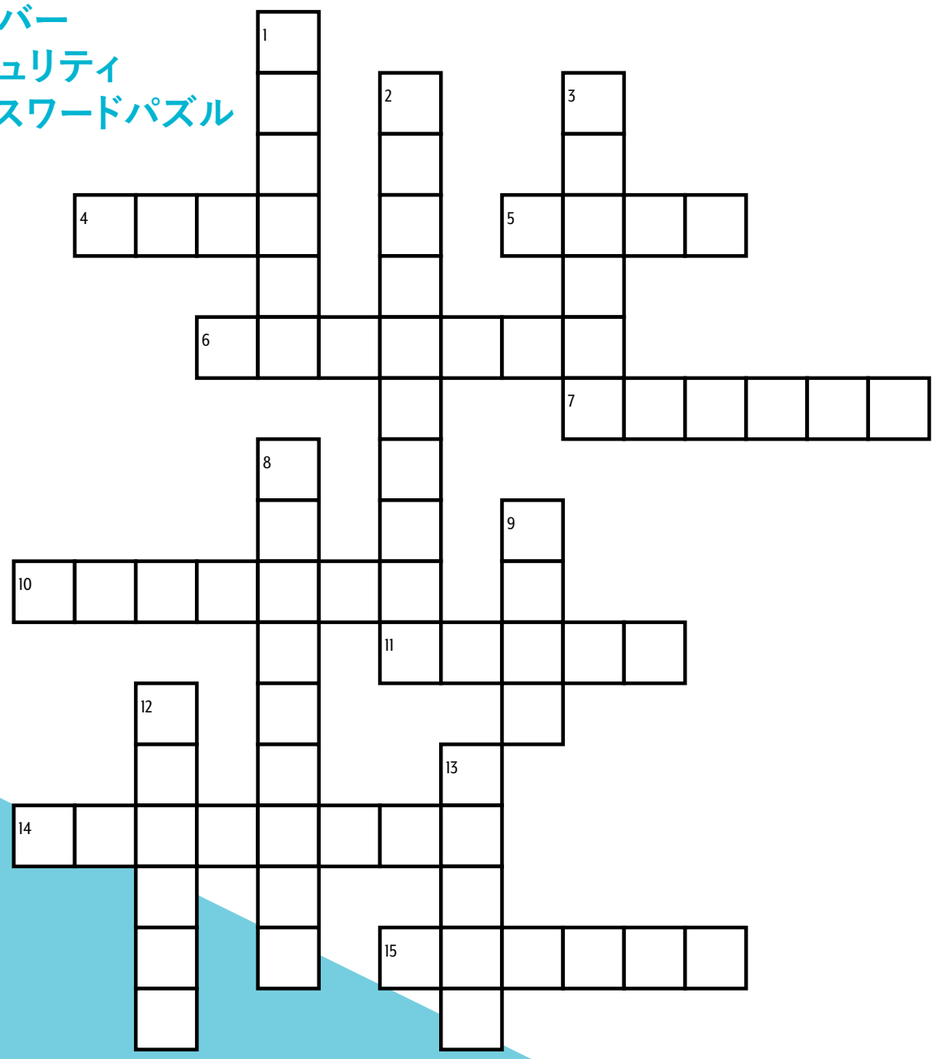
**サイバー犯罪や事件を通報し、オーストラリアをセキュアに保つ。**

サイバー犯罪の犠牲になったと思ったら、速やかに行動を取りましょう。ホームページcyber.gov.auでさらにアドバイスを提供しています。





## サイバー セキュリティ クロスワードパズル



### タテのカギ

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

### ヨコのカギ

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

## 補足ガイド

さらに詳細な情報については「Personal Cyber Security」シリーズをご参照ください。一般の国民がサイバーセキュリティの基本を理解し、よくあるサイバー脅威から自分を守るためには何をしたら良いのかを説明したガイドブック、全三冊。




三冊とも **ホームページcyber.gov.au**から入手できます。

## クロスワードパズルの解答：

1. online, 2. passphrase, 3. hacker, 4.Wi-Fi, 5.ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device





# メモ

**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は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。



**豪連邦政府紋章の使用について**
豪連邦政府紋章の使用が許される条件については総理大臣内閣省ホームページ(www.pmc.gov.au/government/commonwealth-coat-arms)に詳述があります。

## 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通報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。

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre