Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

個人のサイバーセキュリティガイド

最初のステップ

cyber.gov.au

個人のサイバーセキュリティガイドシリーズ

個人のサイバーセキュリティガイドシリーズ

「個人のサイバーセキュリティガイド：最初のステップ」 は、一般の国民の方々にサイバーセキュリティの基本を理解していただくために作成された三冊あるガイドブックの第一巻です。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です。

最初のステップ

次のステップ

上級ステップ

目次

はじめに

個人のサイバーセキュリティとは何か？

テクノロジー主導がますます進んでいく世界で、私たちはサイバー脅威に弱いデバイスやアカウントを毎日使っています。

- このようなデバイスにはパソコン、携帯電話、タブレット型コンピュータやその他のインターネットに接続された機器が含まれます。
- オンラインアカウントには電子メール、バンキング、ショッピング、ソーシャルメディア、ゲームなどが含まれます。

個人のサイバーセキュリティとは、あなたのアカウントやデバイスをサイバー脅威から守るために継続的に実施できるステップを指します。

サイバー脅威から自分を守るためにこのガイドブックがどう役に立つのか？

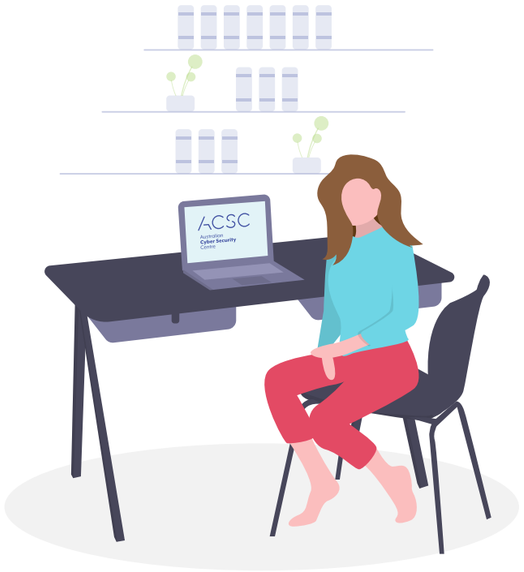
サイバーセキュリティについて初めて学ぼう、あるいは最新情報を知っておこうという方にはこのガイドブックはうってつけのスタートです。「個人のサイバーセキュリティガイド：最初のステップ」は、みなさんにサイバーセキュリティの基本を理解していただくための三冊あるガイドブックの第一巻です。

サイバー脅威とは何か？

ふつうのオーストラリア国民をおびやかす主要なサイバー脅威といえば**詐欺とマルウェア**です。

- **マルウェアというのは危害を及ぼすために作られた悪意のソフトウェアを指す**総称です。こうしたものにはウィルス、ワーム、スパイウェア、トロイの木馬、ランサムウェアなどが含まれます。サイバー犯罪者はマルウェアを使ってあなたのデータや金銭を盗み取ったり、デバイスやアカウントを不正に操作することを狙っています。
- **サイバー詐欺はサイバー犯罪者から送られてくるメッセージで**あなたを騙して機密情報を漏洩させたり、あなたのデバイス上でマルウェアを起動させたりすることを狙っています。

こうしたサイバー攻撃は被害者個人に多大な影響と金銭的被害をもたらすおそれがあります。またこうした攻撃は巧妙さも頻度も増加の一途にあります。



自動アップデートをオンにする

アップデートとは何か？

アップデートとはパソコンやモバイルデバイスなどにインストールしたソフトウェア（プログラム、アプリやオペレーティングシステム）の改良バージョンのことを指します。

- **ソフトウェアのアップデートは**ソフトウェアのバグ（コーディングの誤りや脆弱性）を直すことにより**デバイスを保護します**。サイバー犯罪者やマルウェアはこのようなバグを利用してデバイスにアクセスし個人データ、アカウント、財務情報や本人確認情報などを盗み取ろうとするのです。
- **新たなソフトウェアのバグは常に発見され、**サイバー犯罪者に悪用されています。デバイスにインストールされたソフトウェアをアップデートすることでサイバー攻撃から自分を守ることができます。

自動アップデートをどうやって設定するのか？

自動アップデートとは、新しいアップデートが発表され次第インストールするデフォルトあるいは「いったん設定したらそのまま」の設定を指します。

ヒント:あなたのデバイスのソフトウェアをアップデートするようにというプロンプトが来たらなるべく早く実行しましょう。

- **自動アップデートを**すべてのソフトウェアとデバイスで**オンにし、確認する。**
- **自動アップデートを**どうやってオンにするかは**ソフトウェアやデバイスごとに違います。**
- 可能であれば例えば寝ている時やふだんデバイスを使っていない時間のように**都合の良い時間に自動アップデートをセットしましょう。**

デバイスは電源が入った状態かつ コンセントに差し込んだ状態でなければならず、ストレージの空き容量が必要です。

自動アップデートをオンにするやり方に関するさらに詳細な情報については、ホームページ cyber.gov.auから「Updates」を検索してください。

自動アップデートが設定できない場合は？

自動アップデートが設定できない場合は、ソフトウェアやデバイスの環境設定メニューを使って定期的にアップデートの有無をチェックしインストールしましょう。

ソフトウェアやデバイスが古くてアップデートを受け取れない場合は？

あなたのデバイス、オペレーティングシステムやソフトウェアが古すぎると、製造元や開発元に既にサポートされていないこともあります。

製品がこの「サポート終了」段階を迎えるとアップデートが提供されることはありません。これによりあなたがサイバー攻撃に弱い状態になってしまう可能性があります。サポート終了になってしまった製品の例としてはウィンドウズ7オペレーティングシステムやiPhone7のようなデバイスがあります。

あなたのデバイス、オペレーティングシステムやソフトウェアのサポートが終了してしまった場合は、ACSCでは安全のためできるだけ早い時期のアップグレードをお勧めします。

さらに詳細な情報については、ホームページ cyber.gov.auから「End of support」を検索してください。

多要素認証(MFA)をオンにする

MFAとは何か？

多要素認証(MFA)を使うことにより、あなたの最も大切なアカウントのセキュリティを向上させることができます。MFAではアカウントにアクセスする際に次のような複数の方法で本人確認を行います。

- **覚えているもの**（例：暗証番号、パスワード、パスフレーズなど）
- **持っているもの**（例：スマートカード、物理トークン、認証アプリ、テキストメッセージやメールなど）
- **自分の一部であるもの**（例：指紋、顔認識、虹彩スキャンなど）

MFAによりあなたのアカウントへのサイバー犯罪者による最初のアクセスがずっと困難になります。認証手続きの段階が増え、アカウントに不法侵入するために余計な時間・努力・資源が必要になります。

最も大切なアカウントを守るためにMFAをオンにするには？

MFAをオンにする方法はアカウント、デバイスやソフトウェアごとに違います。次のような大切なアカウントではMFAを今すぐに設定しましょう：

- すべてのオンラインバンキング・財務関係のアカウント（例：銀行口座、ペイパルなど）
- すべての電子メールアカウント（例：ジーメール、アウトルック、ホットメール、ヤフーなど）

メールのアカウントをいくつも持っている場合は、オンラインバンキングなどの大切なサービスにリンクしているアカウントを優先しましょう。

多要素認証の設定方法に関する詳細については cyber.gov.auから「Multi-factor authentication」または「MFA」を検索してください。

定期的にデバイスをバックアップする

バックアップとは何か？

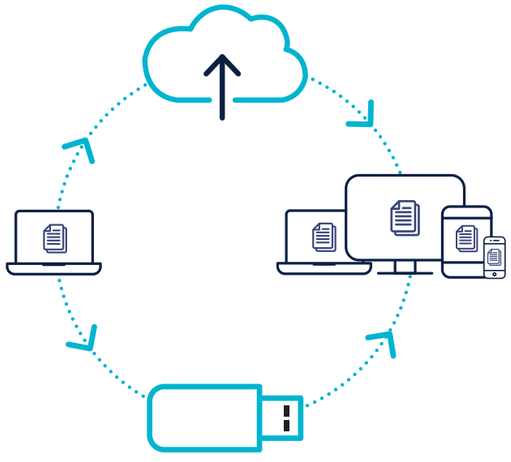
バックアップとはあなたの情報やデータのデジタルコピーです。これには外部記憶装置やクラウドストレージなどに保存した写真、財務情報その他の記録などが含まれます。

バックアップをしておくことは万が一あなたのデータが失われたり、盗まれたり、損傷したりした時のデータ復旧のための予防措置です。

デバイスやファイルのバックアップ方法は？

定期的にファイルやデバイスをバックアップしましょう。どんな形で行うのか、それが毎日・毎週・毎月に一回なのかは最終的にあなたが判断することです。バックアップの頻度を左右するのは次のような数字です：

- デバイスに読み込む新しいファイルの数
- ファイルの内容を変更する回数



ヒント：バックアップを定期的にチェックしファイルの復旧プロセスに慣れておきましょう。バックアップがきちんと作動していることを常に確かめましょう。

バックアップに関するさらに詳細な情報については、ホームページcyber.gov.auから「Backups」を検索してください。

大切なアカウントの安全のためパスフレーズを使う

多要素認証(MFA)はサイバー犯罪者からあなたのアカウントを守る最も効果的な方法の一つです。**MFAが使えない場合、**簡単なパスワードよりも強固で固有性の強いパスフレーズの方がアカウントの保護には有効です。

パスフレーズとは何か？

パスフレーズとは、ふつう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。

例えば、「crystal onion clay pretzel」などです。

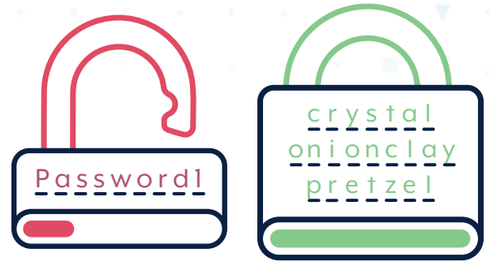
- 簡単なパスワードよりも**パスフレーズの方が安全です。**
- パスフレーズは**サイバー犯罪者による推測が困難**な一方**ユーザーには 覚えやすい**のです。

パスフレーズの作り方は？

次のようなパスフレーズを作りましょう：

- **長いもの：**最低14文字以上、無作為に組み合わせた単語を最低4つ。パスフレーズは長いほど安全です。
- **推測しにくいもの：**最低4つ以上の無作為に組み合わせた互いに関連のない単語を選びましょう。有名なフレーズや引用句、歌詞などは避けましょう。
- **固有性の高いもの：**複数アカウントで同じパスフレーズを使わないこと。

ホームページやサービス利用の際のパスワードに文字以外のシンボルや大文字、数字などが必要な場合、こうしたパスワードをパスフレーズに組み込むこともできます。最も安全なパスフレーズはそうしたものも含めて長く、推測しにくく、固有性の高いものを選びましょう。



パスフレーズはどのアカウントに使うべき？

次のような一番大切なアカウントでMFAが使えない場合、パスワードをパスフレーズに切り替えましょう：

- オンラインバンキング・財務関係のアカウント
- 電子メールアカウント

メールのアカウントをいくつも持っている場合は、オンラインバンキングなどの大切なサービスにリンクしているアカウントを優先しましょう。

パスワードを固有性の高い強固なパスフレーズに切り替えるにはふつうアカウントの設定メニューから行います。

ヒント：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。詳細はホームページcyber.gov.auから「password manager」を検索ください。

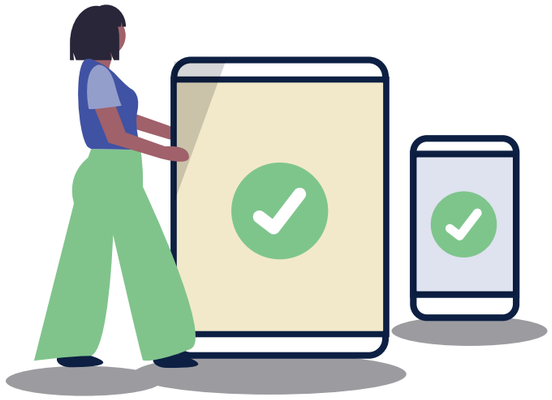
セキュアなパスフレーズの作り方に関するより詳しい情報は、ホームページcyber.gov.auから「Passphrases」を検索してください。

モバイルデバイスをセキュアに使用する

スマートフォンやタブレット型コンピュータは毎日の暮らしに使われています。このようなデバイスのおかげでいつでもどこでもインターネットに接続し、買い物をしたり、仕事を片付けたり、銀行の支払いを済ませたり、健康状態のチェックをしたりといったさまざまなことができます。

もしも自分のモバイルデバイスに誰かが不正侵入をしたり、紛失、盗難に遭ったらどうなるのでしょう？

- サイバー犯罪者に悪用されて財産や個人情報を盗まれる可能性があります。このような犯罪は、ソーシャルメディアやメールのアカウントなども含めた、デバイス上に保存されているデータを使って行われます。
- 写真、ノートやメッセージなど（バックアップしていなければ）取り替えの効かないデータを失う可能性があります。



- サイバー犯罪者があなたの電話番号を使って他の人に対してサギを行う可能性もあります。

モバイルデバイスをセキュアに使う方法は？

デバイスのセキュリティ：

- パスフレーズ、パスワード、暗証番号やパスコードを使って**デバイスをロックしましょう。**推測しにくくしましょう。誕生日やパターンロックでは簡単に推測されてしまいます。最適なセキュリティのためにはパスフレーズを使いましょう。（6ページ参照）。顔認識や指紋などを使ってデバイスをロック解除することも考えましょう。
- デバイスは短時間使用しないだけでも**必ず自動ロック**するように設定しましょう。
- デバイスを**公共充電ステーションでは充電せず**、第三者メーカー製の充電器の使用は避けましょう。
- **スマートフォンは財布と同じ**ように扱いましょう。常に安全な場所に置き、手元から離さないようにしましょう。

ソフトウェアやアプリのセキュリティ：

- デバイスの**自動アップデート機能を使って**アプリケーションやオペレーティングシステムのアップデートがリリースされ次第インストールしましょう。
- アプリケーションがインストールされる前にパスフレーズやパスワードの**入力が必要になるように設定**しましょう。保護者による制限機能も同様に活用できます。
- 新しいアプリや特に無料アプリをデバイスにインストールする際には**プライバシー許可をチェック**しましょう。きちんとした評判のある販売元からのアプリ以外はインストールしないようにしましょう。

データセキュリティ：

- デバイスに機能があればリモートロックとリモートデータ**消去機能をオン**にしましょう。
- デバイスを売却や処分する際には必ず**個人データを完全に取り除いて**からにしましょう。

接続上のセキュリティ：

- **使っていない時は**ブルートゥースやWi-Fiは**切りましょう。**
- デバイスが新たなWi-Fiネットワークに**自動的に接続しないように**気をつけましょう。

携帯電話をセキュアに使うためのさらに詳細な情報については、ホームページ cyber.gov.auから「Secure your mobile phone」を検索してください。

サイバーセキュリティを念頭においた考え方を身につける

個人のサイバーセキュリティは単にデバイスの設定を変えることだけではありません。考え方や行動を変えることも含まれます。

サイバー詐欺に注意しましょう

サイバー犯罪者はメールやテキスト、ソーシャルメディアや電話などを使って国民に詐欺を仕掛けようとすることが知られています。このようなメッセージは、一見ユーザーが知っている、あるいは信用できるはずだと思えるような個人や団体組織から送られてきたように見せかけてあります。

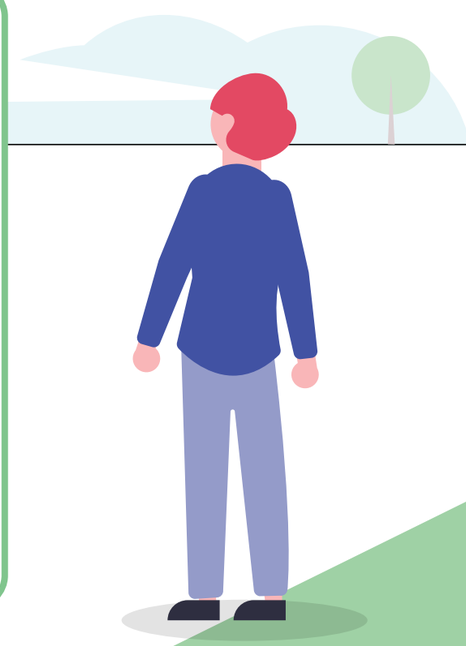
こうしたメッセージや電話の狙いはあなたを騙して次のような特定の行動を取らせることにあります：

- 銀行口座の詳細、パスワードやクレジットカードの番号を漏らす
- あなたのパソコンへのリモートアクセスを許可する
- マルウェアの入った添付ファイルを 開ける
- 金銭やギフトカードを送る

詐欺メッセージを見分けるには？

詐欺メッセージは見分けるのが難しいこともあります。あなたを騙そうとサイバー犯罪者がよく使うテクニックは大体決まっています。次のような特徴のあるメッセージには要注意：

- **正規組織を名乗る**：そのメッセージは、例えばあなたの銀行のように正規の組織からのものということになっていますか。
- **緊急性**：何かの問題があって、限られた時間内に返事をするように言われていますか。
- **感情に訴える**：パニックや恐怖感を煽ったり、期待感や好奇心に訴えるようなメッセージですか。
- **希少性**：不足している品物やサービスを提供する、あるいはお買い得だと謳っていますか。
- **時事問題**：現在の時事問題や大事件に関係のあるメッセージですか？



フィッシング詐欺や詐欺メッセージの見分け方については、ホームページ cyber.gov.auから「Learn the basics」を検索してください。

詐欺メッセージが送られてきた時の対処法は？

詐欺メッセージや電話が送られてきた場合は、無視または削除するかACCCの詐欺監視サービスに ホームページscamwatch.gov.auから通報してください。

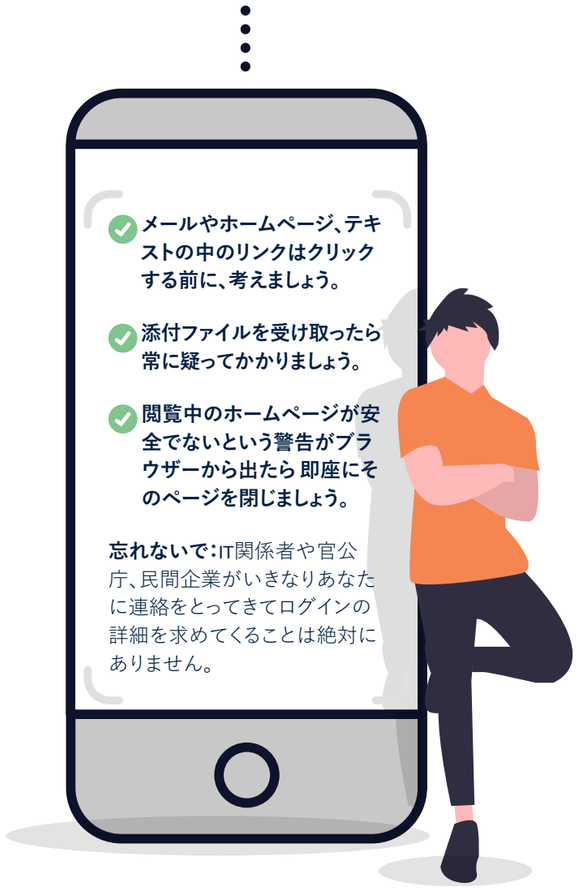
サイバーセキュリティについて心配な方はACSCのサイバーセキュリティホットライン **1300 CYBER1** (1300 292 371)に問い合わせることもできます。

もしも詐欺にかかって銀行口座やクレジットカード、キャッシュカードなどが悪用されるかもしれないと思った場合は即座に自分の金融機関に連絡しましょう。金融機関側で口座を閉鎖したり、取引を止めることができるかもしれません。

メッセージが本当に詐欺なのかどうかよくわからない場合は？

メッセージや電話が本当に信用できる団体組織(あなたの銀行など)からかもしれないと思った場合は、自分が信頼できる連絡方法を見つけましょう。公式ホームページを見つける、広告されている電話番号にかける、店舗や支店があれば実際に行ってみる、などです。送られてきたメッセージや電話口で聞いただけのリンクや連絡先は本物でない可能性がありますから使ってはいけません。

ヒント：
クリックする前に、考える



もしもサイバー犯罪の犠牲になったと思ったら、ACSCのReportCyberサービスにホームページ cyber.gov.au/report を通じて通報するかサイバーセキュリティホットライン 1300 CYBER1 (1300 292 371)にご連絡ください。

サイバー脅威の最新情報についてはACSCの無料警報サービスにお申し込みください。ホームページ cyber.gov.au から「Subscribe to the ACSC alert service」を検索の上お申込みください。新しいサイバー脅威が発見され次第警報をお送りします。

ソーシャルメディアに投稿する前に立ち止まって考える

サイバー犯罪者はあなたがソーシャルメディアに投稿した情報を詐欺やサイバー攻撃に悪用できます。

インターネット上の情報はいったん投稿したら完全に取り除くことはできず、永久に残るということを忘れずに。

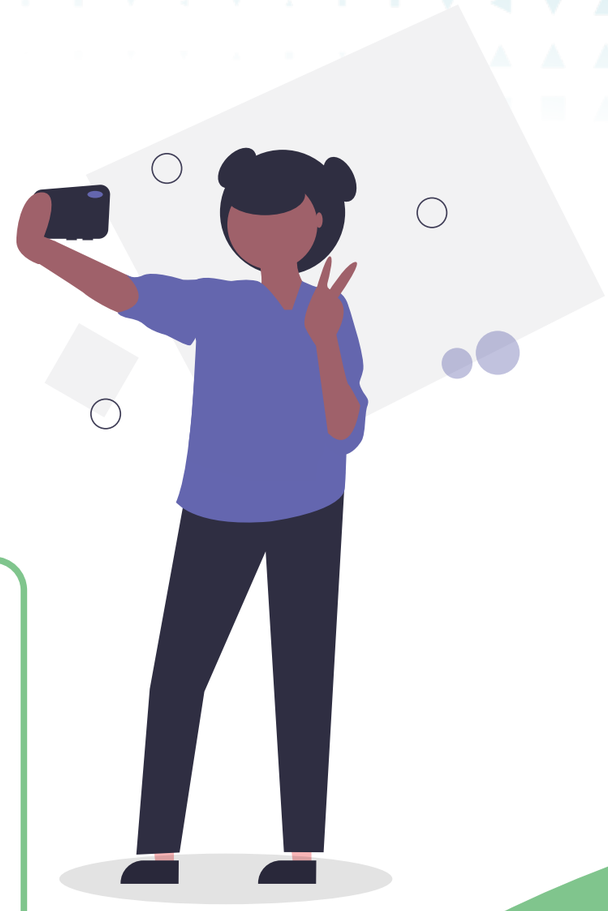
投稿前に立ち止まって考える方法は？

- **考える：** サイバー犯罪者がこの情報を使ってどのように自分や自分のアカウントを狙うことができるか
- **考える：** この情報や画像をオフラインで全くの赤の他人に見せても自分は平気だろうか

投稿を避けるべき情報は？

サイバー犯罪者があなたを特定できたり、詐欺行為であなたを利用したり、アカウント回復用の質問の推測に使ったりすることができる情報(写真も含む)の共有は避けましょう。こうした情報とは：

- 出生地や生年月日
- 住所や電話番号
- 勤務先や職歴
- 学歴
- このほかにもあなたを狙うのに悪用される可能性のある個人情報すべて。



要点チェックリスト

このガイドブックの内容すべてを実践しましたか？

次のチェックリストで進捗状況を確かめましょう：

- **全ての手持ちのデバイスの自動アップデートをオンにした：**
  - コンピュータ(パソコン・ノートパソコン含む)
  - 携帯電話
  - タブレット型コンピュータ
- **大切なアカウントでは全て多要素認証をオンにした：**
  - すべてのオンラインバンキング・財務関係のアカウント(例：銀行口座、ペイパルなど)
  - すべての電子メールアカウント(例：ジーメール、アウトルック、ホットメール、ヤフーなど)
- **デバイスを定期的にバックアップしている：**
  - コンピュータ(パソコン・ノートパソコン含む)
  - 携帯電話
  - タブレット型コンピュータ
- **MFAが使えない大切なアカウントでは固有性の高い強固なパスフレーズを使っている：**
  - オンラインバンキング・財務関係のアカウント
  - 電子メールアカウント
- **モバイルデバイスをセキュアに使用している：**
  - ノートパソコン
  - 携帯電話
  - タブレット型コンピュータ
- **サイバーセキュリティを念頭においた考え方を毎日実践している：**
  - 詐欺メッセージが見分けられる
  - 詐欺メッセージを受け取ったらどうしたら良いかわかっている
  - メッセージが本当に詐欺なのかどうかよくわからない場合でもどうやって調べればいいか わかっている
  - リンクや添付ファイルをクリックする前に必ず一回考える
  - ソーシャルメディアに何かを共有する前に必ず一回考える
- **もしもサイバー犯罪や詐欺の犠牲になった場合にはどこに助けを求めるかわかっている**

用語集

アカウントの回復
一連の質問や他の確認方法を用いてアカウントを復旧したりアカウントへのアクセスを回復したり、あるいはアカウントのパスフレーズやパスワードを変更するプロセス。

アプリ
携帯アプリケーションと呼ばれることもある。スマートフォンやタブレット型コンピュータに使われる一般的なソフトウェアのこと。

添付ファイル
電子メールに添付されて送られてくるファイル。

認証アプリ
多要素認証(MFA)を通じてパソコンユーザーの本人確認を行うのに使われるアプリ。

クラウドストレージ
大容量の分散ストレージと処理能力を提供するリモートサーバーのネットワーク。

サイバー犯罪者
違法にコンピュータシステムやアカウントにアクセスし被害を与えたり情報を盗んだりする人。

デバイス
コンピュータ処理や通信用の機器例えば、パソコン、ノートパソコン、携帯電話、タブレット型コンピュータなど。

サポート終了
製品やサービスの開発を行なった会社がその製品・サービスに対するサポートを中止する状態を指す。ハードウェアやソフトウェア製品の新しいバージョンがリリースされ旧バージョンに対するサポートが終わってしまうなどの場合が一般的。

マルウェア
ユーザーのパソコンに不正にアクセスしてこれを操作し、情報を盗んだりネットワークを混乱させたり停止させたりするのに使われる悪意ソフトウェア。

オペレーティングシステム
コンピュータのハードウェアとプログラムが交信しプログラムを起動することを可能にする、ハードドライブにインストールされたソフトウェア。例：マイクロソフトウィンドウズ、アップルマックOS、iOS、アンドロイドなど。

物理トークン
ふつうキーホルダーなどに付けられるような大きさの物理的デバイスで、MFAを使っているユーザーの本人確認を行うのに使われるセキュリティコードを生成する。

リモートアクセス
離れた場所からデバイスやネットワークにアクセスしこれを遠隔操作すること。

ソフトウェア
ふつうプログラムと呼ばれる。ユーザーがパソコンやそのハードウェアと交信しさまざまなタスクを実行させるためのコンピュータへの命令の集まり。

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