サイバーセキュリティの基本的な知識を紹介

インターネットの安全・安心ハンドブック

ご家庭や職場の仲間、
ご友人・知人の皆さまとご一緒に、
サイバーセキュリティへの知識を深めましょう。

国家サイバー統括室（NCO）では、サイバーセキュリティに関する普及啓発活動の一環として、「インターネットの安全・安心ハンドブック」を公開しています。本ハンドブックは、皆さまにサイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、さらに安全・安心にインターネットを利活用してもらうことを目的に制作したものです。

CONTENTS

国家サイバー統括室
National Cybersecurity Office

「インターネットの安全・安心ハンドブック」の
ダウンロードはこちら ▶

https://security-portal.cyber.go.jp/guidance/handbook.html

【シニア層向け】啓発パンフレット

サイバーセキュリティ普及啓発

知っておきたい インターネットの安全対策

トラブルを防ぐための大切なポイント

1 外出先におけるリスク

外出中はスマートフォンを常に身につけるようにしましょう

スマートフォンには、連絡先や写真、各種サービスの情報など、大切な情報が多く保存されています。

外出先でスマートフォンをテーブルに置いたまま席を離れてしまうと、盗難や情報漏えいにつながるおそれがあります。

外出中は、スマートフォンを常に身につけるようにしましょう。

スマートフォンには必ず画面ロックを設定しましょう

ロック画面の通知には重要な情報を表示させないようにしてください。

また、人が多い場所では、画面をのぞき見されることで、情報を知られてしまうこともあります。

紛失や盗難に備えて、スマートフォンには必ず画面ロックを設定しましょう。

第4問 突然パソコンに「ウイルスに感染しました！今すぐこの番号へ連絡を」と警告が出ました。正しい対応はどれですか？

1. 警告に従って、すぐに表示された番号に電話する
2. 気にせずに、そのまま操作を続ける
3. 慌てず操作を止め、家族や公的な窓口に相談する
4. パソコンが壊れたので買い替える

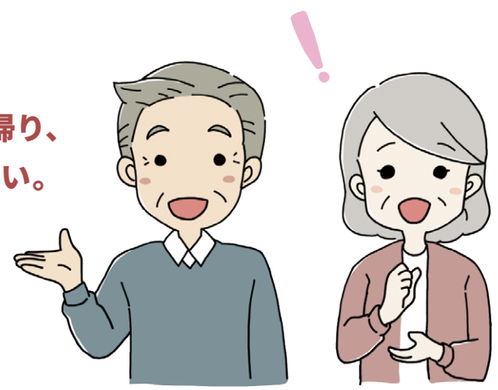
回答記入欄

第5問 防犯カメラやスマートテレビなどの「家庭用IoT機器」を安全に使うための正しい方法はどれですか？

1. 初期設定のまま使用できるのであれば、そのまま利用する
2. 初期設定のまま使用せず、適切なパスワードを設定して使う
3. ファームウェアの更新は、手動で気が向いたときに行う
4. いつもと挙動がちがっても、一旦そのままにしておく

回答記入欄

このパンフレットは、ご自宅等に持ち帰り、
ご家族の皆さんにもお見せしてください。



クイズの答え 第1問：③、第2問：③、第3問：③、第4問：③、第5問：②

サイバーセキュリティ クイズ

第1問 外出先のレストランなどで、スマートフォンをテーブルの上に置いたまま席を離れても大丈夫でしょうか？

1. 短時間であれば問題ない
2. 画面を伏せておけば問題ない
3. 常に身につけるようにする
4. 適切なパスワードを設定しているので、問題ない

回答記入欄

第2問 安全なパスワードを設定するポイントとして、次のうち不適切なものはどれですか？

1. 誕生日や名前など、推測されやすいパスワードを使用しない
2. サービス間で同じパスワードの使い回しをしない
3. 忘れないように「1111」など、簡単なパスワードを設定する
4. できるだけ長く複雑なパスワードを設定する

回答記入欄

第3問 知らない相手から「リンク（URL）」のついたメールが届きました。どうするのが一番安全ですか？

1. どのような内容か気になるので、まずはクリックしてみる
2. リンクをコピーして友人に送る
3. 絶対にクリックせず、メールを無視する
4. 返信して、誰からのメールか問い合わせる

回答記入欄

2 パスワードと多要素認証

長く複雑なパスワードを設定し使い回しはしないこと

インターネットサービスを安全に利用するためには、パスワードの管理がとても重要です。誕生日や名前などは避け、できるだけ長く、推測されにくいパスワードを設定しましょう。

また、同じパスワードを複数のサービスで使い回さないようにしましょう。

パスワードが流出した可能性がある場合は、速やかにパスワードを変更しましょう。

また、スマートフォンアプリなどの多要素認証を設定してさらに安全性を高めましょう。

安心して使うために推測されにくいパスワードを設定する

パスワードの設定ポイント

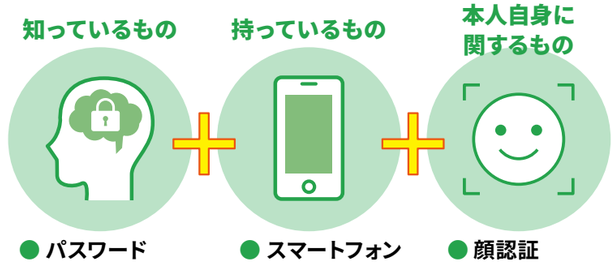
- ★ 長く複雑にするほど安全
- ★ 使い回しは絶対にしない
- ★ 多要素認証で安全性UP

- ● パスワードの定期変更は基本は必要なし。
- ● ただし、流出の可能性がある場合などは、速やかに変更してください。

多要素認証とは？

多要素認証とは、パスワードだけでなく、他の要素による認証を追加して安全性を高くする方法です。

2つ以上の要素を組み合わせる



3 家庭用IoT機器のセキュリティ対策

初期設定を見直し、不要な機能はオフにする

防犯カメラやスマート家電など、インターネットにつながる機器も攻撃の対象になります。
初期設定のまま使うのではなく、適切なパスワードを設定し、使わなくなった機器や不要な機能はオフにするなど、利用状況に応じた設定を行いましょう。
また、機器の設定内容を定期的に確認し、不審な動作がないか注意することも大切です。

4 偽メール・偽サイトに注意

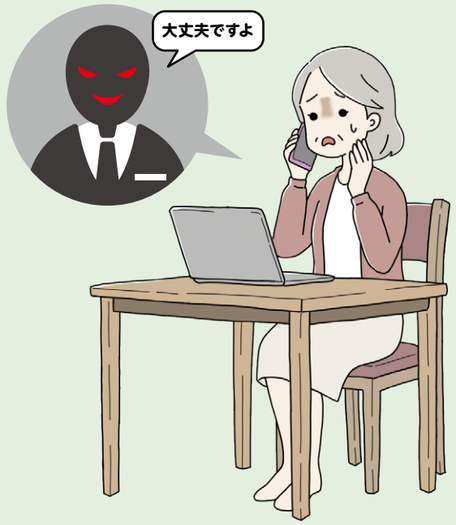
怪しいメール・SMSにご用心
添付ファイル・リンクは開かない

偽のメールや偽サイトを使った攻撃は多様化し、日々、巧妙になっています。
添付ファイルやリンクは、攻撃でよく使われる手段です。
心当たりのないメールには用心し、添付ファイルやリンクは開かないようにしましょう。
また、検索結果の上位に表示されているウェブサイトでも、安全とは限りません。

5 サポート詐欺の手口

警告や、不安を煽る表示が出ても、慌てて操作しない

インターネットを利用していると、突然、画面に「ウイルスに感染しました」「このままでは危険です」といった警告が表示されることがあります。
これは、不安をあおって電話をかけさせ、金銭や個人情報をだまし取る「サポート詐欺」と呼ばれる手口です。
実在する企業やサポート窓口を装って表示される場合もありますが、慌てて操作しないことが大切です。



6 困ったときは相談しよう

一人で悩まず、まず相談を！

インターネットで不安なことが起きたときや、「これって大丈夫かな？」と感じたときは、一人で悩まず、相談することが大切です。
家族や公的機関に相談しましょう。