インターネットの
安全・安心ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

リーフレット（一般利用者向け）

知る・守る・続ける

サイバーセキュリティ普及啓発

Ver 5.10

はじめに

本リーフレットの目的

　みなさん、はじめまして。内閣サイバーセキュリティセンター(NISC)です。NISCは日本の政府機関で、国のサイバーセキュリティ政策を担当しています。
　みなさんが日頃使っている、スマートフォンやPCは、便利で日常生活になくてはならないものになった反面、対策をしなければ、常にサイバー攻撃のリスクにさらされています。
　本リーフレットは、サイバーセキュリティを、ひとりでも多くの方に正しく知って頂き、対策をしてもらうことを目的に作成しました。サイバー攻撃の手口にどんなものがあるのか、被害に遭うとどの様な事態になるのか、身近な例を取り上げながら解説し、被害を受けないようにするために、最低限必要なことについて、 紹介しています。
　本リーフレットを読んで、安全・安心なインターネット空間を一緒に作っていきましょう。

各ページに「インターネット安全・安心ハンドブックVer5.10」における記載箇所や、各省庁・各機関の参考となる取組を載せています。ぜひ確認し、より理解を深めてください。

本リーフレットの対象者

学校で

中高生の方と
その先生方に

ご家庭で

こどもから
シニアの方々にも

身の回りのリスクチェック

あなたの身の回りに潜(ひそ)むサイバー攻撃のリスクを知るために、現在の状況をチェックしてみましょう！

リスクチェック	
□	忘れないようにするため、パスワードは同じものを使っている。
□	家庭のネットワーク機器のパスワードは初期パスワードから変更していない。
□	スマホのアプリは気が向いたときにアップデートする。
□	公衆Wi-Fiの利用先は無料かどうかで決めている。
□	公衆Wi-Fiを利用するために個人情報を求められたら、気にせず入力している。
□	電子メールを受信したら、必ずメールを開封するようにしている。
□	料金未払いの督促(とくそく)のお知らせが来たら、メールに記載されているリンクにアクセスする。
□	サイバー攻撃なんて、めったに起こらないことだと思う。

1つでも該当したら…

あなたの情報は狙われているかも！？

あなたの情報を守りましょう

突然、知らないカード会社から、知らない請求が、あなたの名前宛に。しかも住所の情報はあっている…。

この場合、何らかの形であなたの個人情報が漏れて、誰かに勝手に使われた可能性があります。

個人情報の漏えいの原因はいろいろなものが考えられます。その中で、特にスマホやPC、普段使っているECサイトやネット銀行などに関するセキュリティ対応は重要です。

本書では、３つのテーマに分けて、あなたの情報を守るための方法をお伝えします。

1 パスワードの適切な設定・管理

2 スマホやPC、ネットワークを安全な状態にする

3 攻撃の手口を知り、被害を防ぐ

パスワードの適切な設定・管理

1 パスワードの適切な設定・管理

パスワードは、スマホやPC、様々なサービスを利用するための「鍵」です。鍵の管理がずさんだと、泥棒が入ってきてしまうのと同様、パスワードも適切に管理しないと、悪意のある攻撃者がサービスなどに侵入してしまいます。その結果、個人情報が盗まれたり、勝手に買い物されたりしてしまう可能性があります。

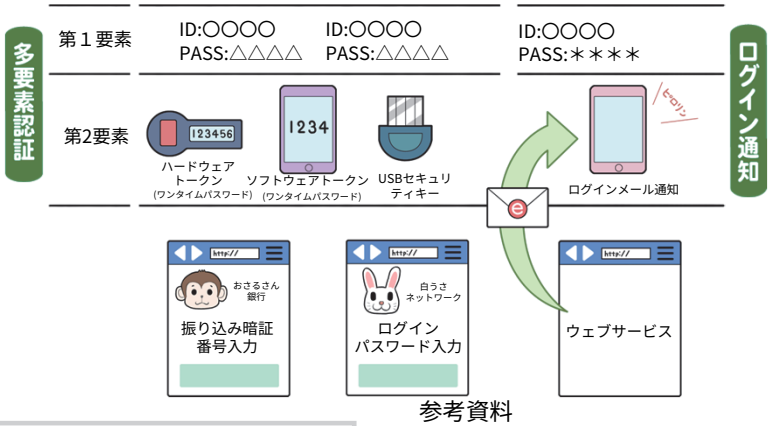
パスワードを適切に設定・管理しましょう

□	同じパスワードを使うことはやめましょう。一か所から漏れればすべてのサイトでログインが可能になってしまいます。
□	似たパスワードや、単純な法則性のあるパスワードも、推測されやすいため、避けましょう。
□	パスワードは、英大文字・小文字・数字を組み合わせてできるだけ長いものを使うようにしましょう。より安全性を高めるには、記号を追加しましょう。
□	パスワードは適切なものを用いるほか、可能であれば、パスワードが万が一漏えいしても第三者からのログインをブロックできる多要素認証を用いたサービスやシステムを利用しましょう。

同じパスワードを使い回さない。似たパスワード、単純な法則性のあるパスワードも×

	白うさ ネットワーク	おさるさん 銀行	三毛猫電気	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽（いちもうだじん）
×単純な法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	法則性がばれたらおしまい

多要素認証やログイン通知でセキュリティを向上



参考資料

総務省「国民のためのサイバーセキュリティサイト」

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/06/

ハンドブック記載箇所
第５章 パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう

スマホやPC、ネットワークを安全な状態にする

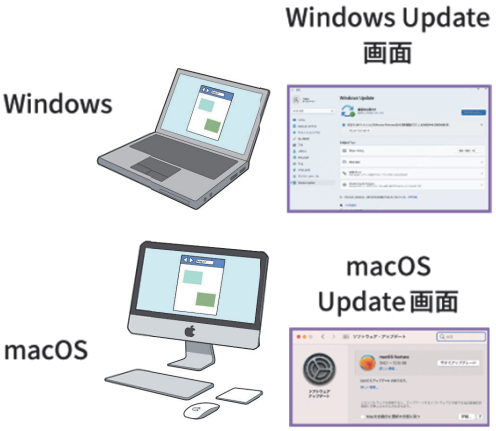
2 スマホやPCを最新の状態に

サイバー攻撃は、PCやソフトウェアの脆弱性を攻撃することが多くあります。OS、ソフトウェア、ファームウェアを、常に最新の状態に保つように、アップデートをしましょう。

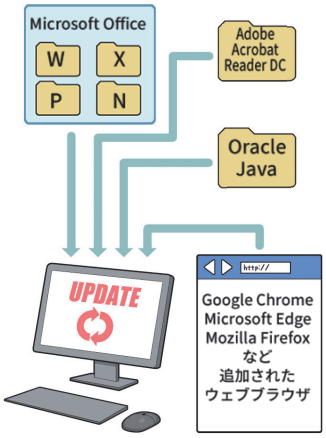
利用する機器は常に最新の状態にしましょう

□	セキュリティを最新に保ち、各種のアップデート（バージョンアップ）は自動更新にしつつ、まめにチェックしましょう。
□	アップデートが提供されなくなったOS、ソフトウェア、スマートフォンなどは、使用しないようにしましょう。

OSと基本ソフトの更新



重要ソフトも更新

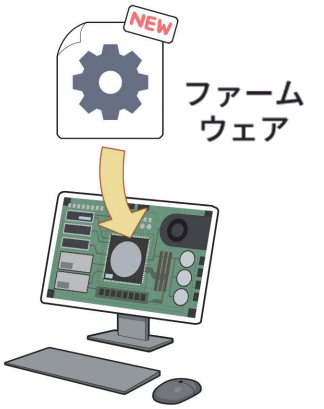


アプリはまめに更新

アップデートが提供されなくなったアプリは
使用しない、または、アンインストールを！

セキュリティソフトも更新

本体のファームウェアも更新



ハンドブック記載箇所
第1章 2
①OSやソフトウェアは常に最新の状態にしておこう

参考資料

総務省「国民のためのサイバーセキュリティサイト」

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/01/

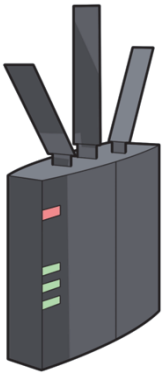
スマホやPC、ネットワークを安全な状態にする

2 ネットにつながるIT機器も更新

ネットにつながるIT機器（ルータやプリンタ等）も最新の状態に置くことが重要です。ファームウェアと呼ばれる、機器の作動に必要なソフトウェアも含め、最新の安全なものにしましょう。
加えて、必ず初期パスワードから変更しましょう。

ネットにつながるIT機器も更新して常に最新の状態にしましょう	
□	必ず、初期パスワードは購入時の初期のものから変更しておきましょう。なぜなら同じ機種の初期パスワードが全て同じだった場合などに、不正アクセスされ乗っ取られ、サイバー攻撃に使われてしまう可能性があるためです。 また、不正アクセスされ、乗っ取られてしまった場合、設定が変更されてしまうこともあります。
□	利用している機器のサポート期限も把握し、サポート期限が切れている場合は機器の買い替えも検討しましょう。

無線LANアクセスルータ



ネットワーク対応プリンタ

ネットワークカメラ

ネットにつながるIT機器(ルータやIoT機器)も初期パスワードの変更やファームウェア更新をしておくこと

ハンドブック記載箇所
第1章 2
①OSやソフトウェアは常に最新の状態にしておこう

参考動画

IPA「あなたの家も狙われている！？　家庭教師が教えるネット家電セキュリティ対策！」
https://www.youtube.com/watch?v=xbn8SZIib90

スマホやPC、ネットワークを安全な状態にする

2 安全なネットワークか確認を

無線LANは、適切な設定をしないと、外部から通信内容が盗聴されたり、ネットワークを勝手に使われることがあります。

利用するネットワークを確認しましょう

□	無線LAN通信（Wi-Fi）はケーブルがなくても利用できるため、大変便利ですが、接続する先（だれが提供しているのか）をよく確認しましょう。 暗号キー（パスワード）が貼り出してあるような公衆無線LAN は、通信内容が盗聴される等のリスクがあります。
□	ブラウザに「！」アイコンや「保護していない通信」「安全ではありません」などと表示されたときは、個人情報などを入力しないようにしましょう。
□	ブラウザに接続する場合は、暗号化ありのアイコンが表示されていることを確認しましょう。但し、ブラウザに暗号化ありのアイコンが示されている場合でも、必ずしも安全性が担保されているわけではないことに注意しましょう。

スマホやパソコンの画面から見た無線LAN暗号化

各OSに表示されるアイコンはWi-Fiの接続先を選択する際に確認することができます。

接続	Android	iOS、mac OS	Windows
×（暗号化無し）			
△（暗号化有り）			 ＊1

＊1：Windows ではバージョンによってアイコンに「セキュリティ保護あり」と表示される場合もあります。

ハンドブック記載箇所
第５章２
安全な無線 LANの利用を支える暗号化について学ぼう

参考資料

総務省「無線LAN（Wi-Fi）のセキュリティに関するガイドライン」
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

攻撃の手口を知り、被害を防ぐ

3 攻撃の手口を知ろう

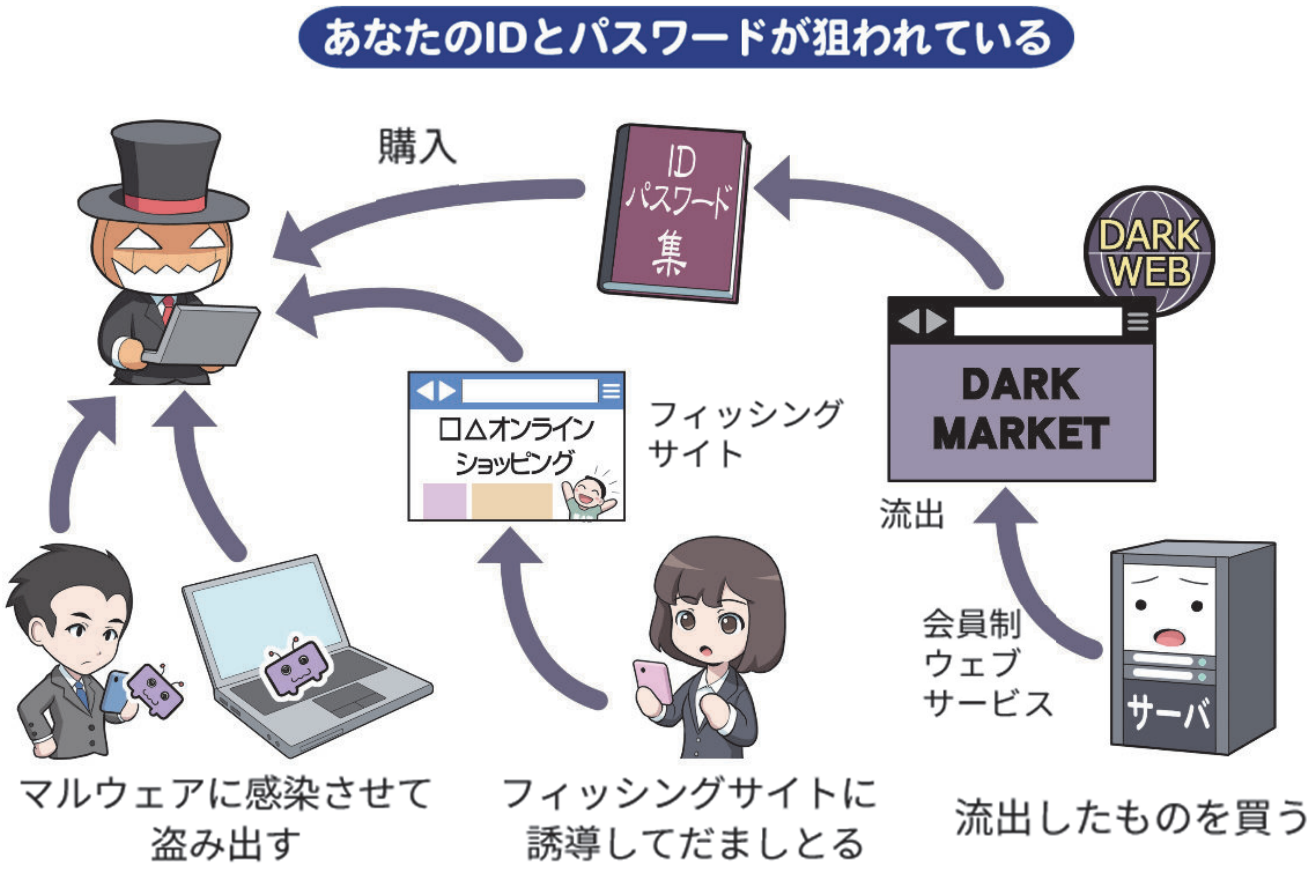
セキュリティ対策をきちんと行っていても、最近では、パスワードやクレジットカードなどの情報を盗み取るために巧妙な攻撃が行われています。例えば、

〇不正なプログラム（マルウェア）に感染させてIDやパスワードを盗み取る

〇銀行やクレジットカード会社などを装ったメールを送信し、偽のサイト（フィッシングサイト）に誘導して個人情報やID、パスワード、クレジットカードなどの情報を入力させる

といった手口があります。

このような攻撃への対策の一つとして、どのような手口があるのかを知り、攻撃を受けてもしっかり対応することが重要です。



ハンドブック記載箇所
第２章
よくあるサイバー攻撃の手口やリスクを知ろう

参考資料

IPA　情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

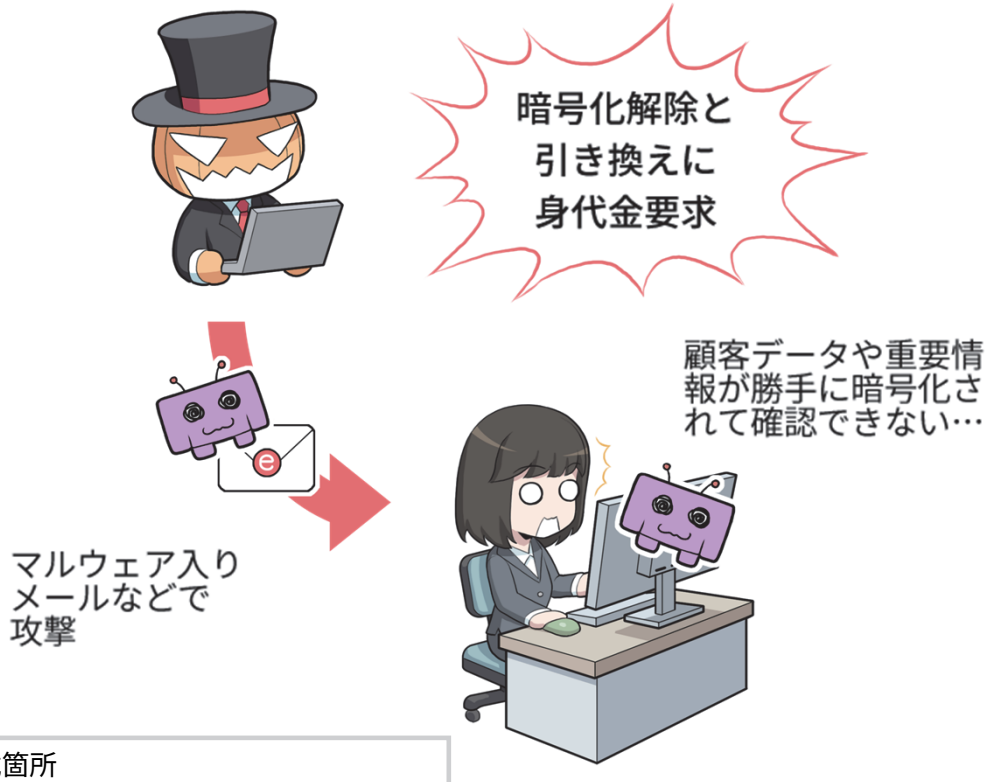
攻撃の手口を知り、被害を防ぐ

3 攻撃の手口を知ろう

偽メールなどによる誘導

水飲み場攻撃による感染

ランサムウェアで暗号化して身代金要求



ハンドブック記載箇所
第２章
よくあるサイバー攻撃の手口やリスクを知ろう

家族をサイバー攻撃から守るには

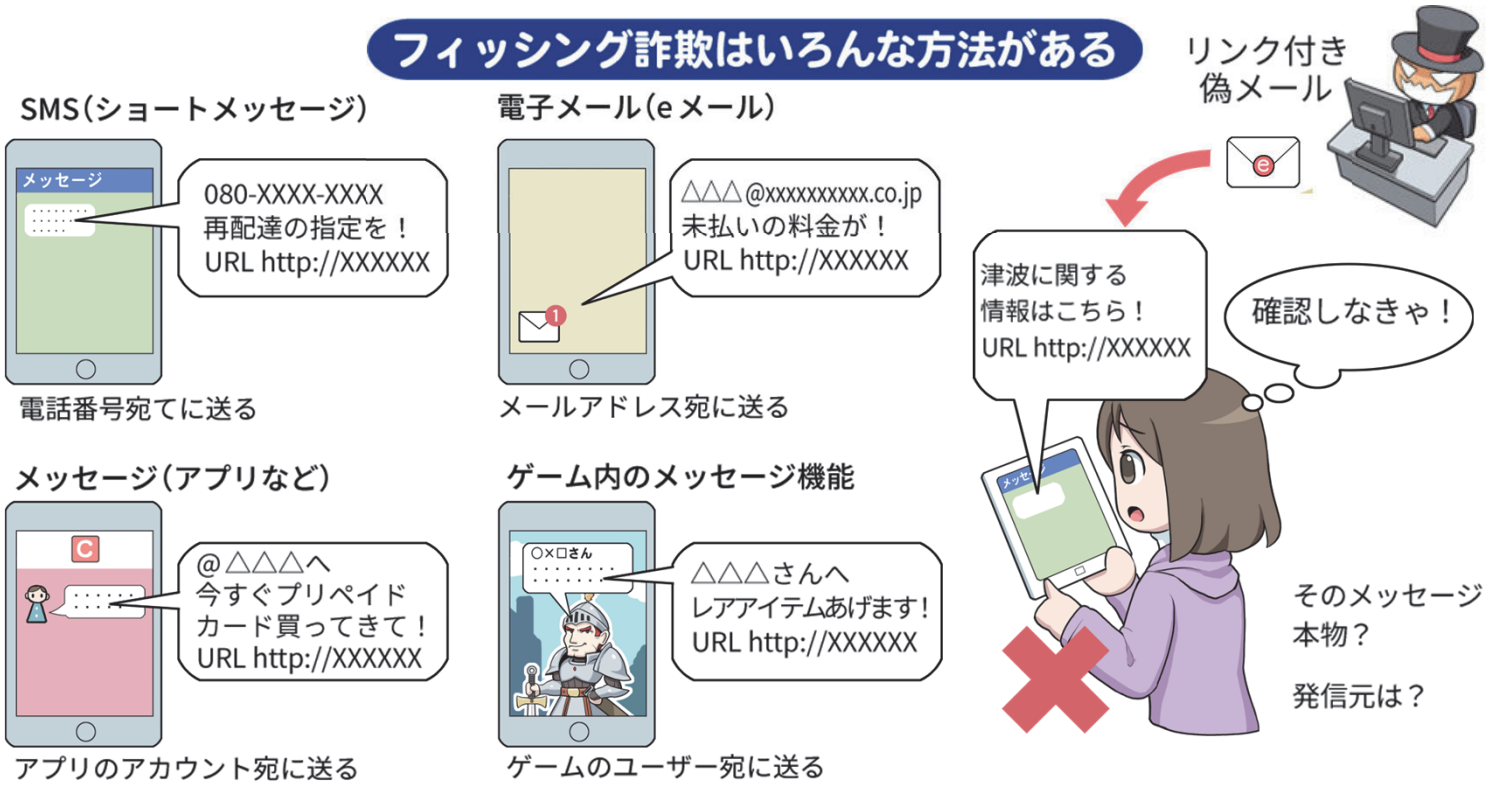
実在する企業や公式のサイトを装ったサイバー攻撃が増えています。家族を守るための対策の方法はこれまで述べてきたものと共通ですが、家族とのコミュニケーションが重要になってきます。

どういったサイバー攻撃がどのように行われるのか、ハンドブックなどを使ってお互いに認識を共有しましょう。

アプリや正規のWebサイトで情報を得るようにし、メールに書かれている内容やリンクは信用しないようにしましょう

□	ハンドブックを用いて、サイバー攻撃の内容や手口を知りましょう。
□	不審（ふしん）なメッセージや通知は内容や発信元を落ち着いて確認するように伝えましょう。
□	不審なリンクや添付ファイルは開かないように伝えましょう。
□	求められるまま個人情報を入力したり、表示された番号に焦（あせ）って電話をしないように伝えましょう。

フィッシング詐欺はいろんな方法がある



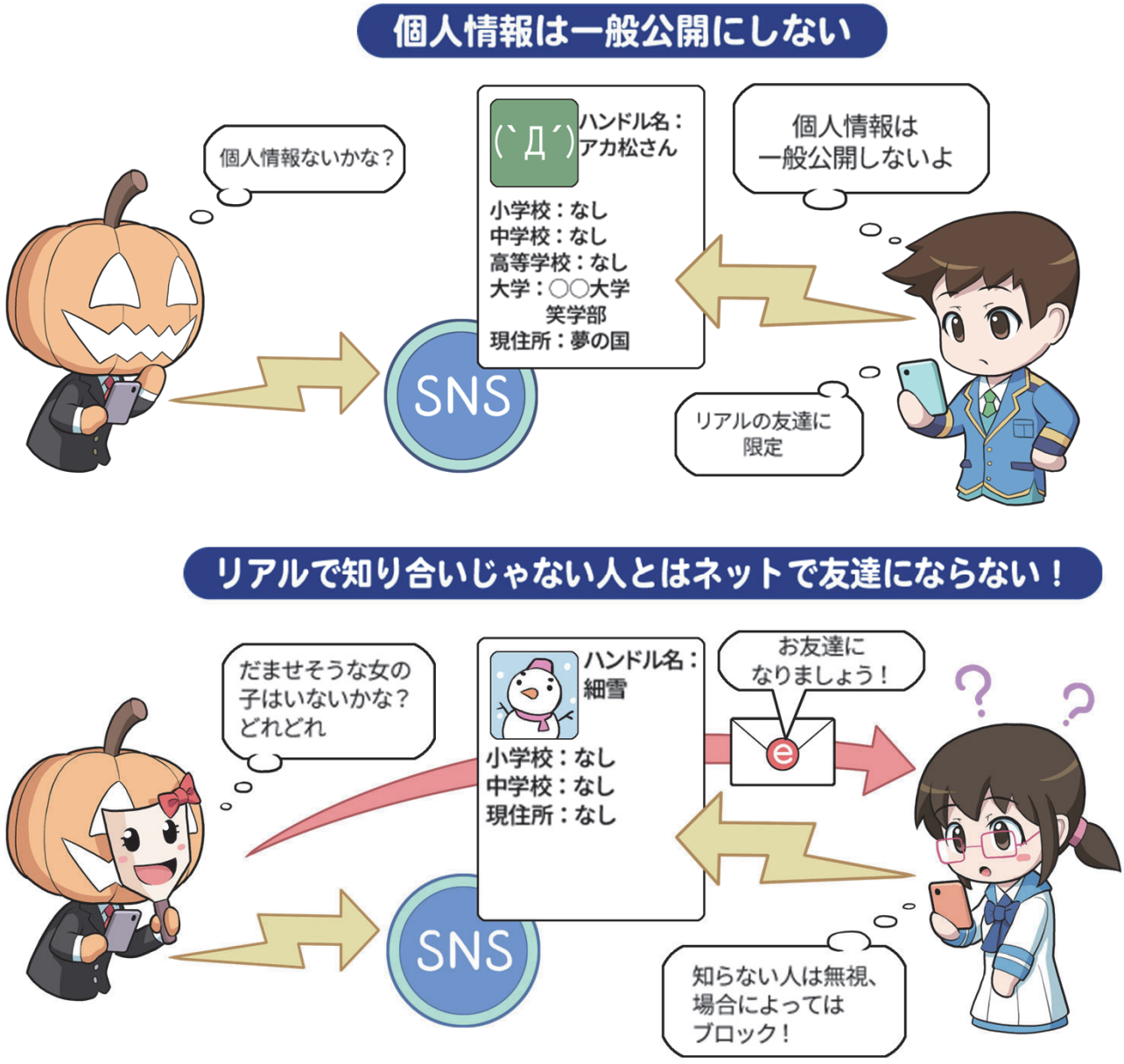
ハンドブック記載箇所
第1章５
④偽メールや偽サイトに騙されないように
用心しよう

参考動画集

IPA　手口検証動画シリーズ
https://www.ipa.go.jp/security/anshin/measures/verificationmov.html

家族をサイバー攻撃から守るには

　金銭などの利益目的ではない攻撃として、個人情報や写真の入手などを目的とするものもあります。
　少しでも変だなと思ったら、厳重に注意するように家族に伝えましょう。



ハンドブック記載箇所
第1章コラム４
利益が目的ではない攻撃に備えるには

参考動画

IPA　「キミはどっち？
－パソコン・ケータイ・スマートフォン 正しい使い方－」
https://www.youtube.com/watch?v=k2VT6x4wBSk

困ったときは…

サイバー攻撃に気付いたり、あるいは第三者からの連絡で気付いた場合は、必要な各種窓口に相談しましょう。
※ハンドブック第４章４　それでも攻撃を受けてしまったときの兆候と対策を知ろう　も参照しましょう。

各種連絡窓口のウェブサイト等	QRコード
一般利用者が情報セキュリティやネット詐欺に関する相談をしたい場合には・・・ IPA「情報セキュリティ安心相談窓口（個人向け）」 電話　**03-5978-7509**（受付時間：10時～12時　13時30分～17時 ※土日祝祭日、年末年始除く）	https://www.ipa.go.jp/security/anshin/about.html
ランサムウェア被害や不正アクセス等による情報漏えい被害等に遭った場合には・・・ 都道府県警察「サイバー事案に関する相談窓口」 よくある相談事例と対応方法のほか、オンラインの相談窓口も設置されています。被害届は最寄りの警察署等に連絡をお願いします。 なお、緊急性を要する場合は、110番通報しましょう。	https://www.npa.go.jp/bureau/cyber/soudan.html
消費生活のトラブルや困った場合には・・・ 消費者庁「消費者ホットライン」188 **188** をダイヤルしてください。	https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/

最低限実施すべきサイバーセキュリティ対策を理解しよう

サイバーセキュリティ対策9か条

対策1

OSやソフトウェアは常に最新の状態にしておこう

対策2

パスワードは長く複雑にして、他と使い回さないようにしよう

対策3

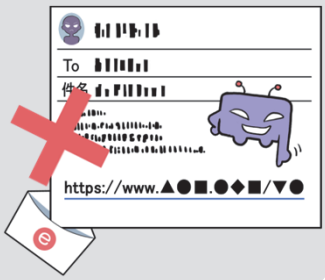
多要素認証を利用しよう

対策4

偽メールや偽サイトに騙されないように用心しよう

対策5

メールの添付ファイルや本文中のリンクに注意しよう



対策6

スマホやPCの画面ロックを利用しよう

対策7

大切な情報は失う前にバックアップ(複製)しよう

対策8

外出先では紛失・盗難・覗き見に注意しよう

対策9

困った時はひとりで悩まず、まず相談しよう

NISC　IPA「サイバーセキュリティ対策9か条」
https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

ハンドブック記載箇所
第１章
まずはサイバーセキュリティの基礎を固めよう

ハンドブック本体の使い方

インターネットの安全・安心ハンドブック

セキュリティという言葉の意味を知っている。
- No → まず、**プロローグ**と**第１章**を読みましょう。
- Yes ↓

セキュリティ対策と聞いて何をするか知っている。
- No → まず、**プロローグ**と**第１章**を読みましょう。
- Yes ↓

サイバー攻撃とは何か知っている。
- No → **第２章**の内容を読んでサイバー攻撃への理解を深めましょう。
- Yes ↓

メールやSMS、SNSを安心して使う方法を知っている。
- No → **第３章**の内容を読んでSNSの使い方の理解を深めましょう。
- Yes ↓

スマホやPCでどんなセキュリティ設定をしているか知っている。
- No → **第４章**の内容を読んで端末の設定の理解を深めましょう。
- Yes ↓

ネット上のサービスを安心して使う方法を知っている。
- No → **第２章・第４章**の内容を読んでなりすましや漏えいの避け方の理解を深めましょう。
- Yes ↓

セキュリティについて全般的に理解されています。
改めてハンドブック全体の内容を確認しましょう。

インターネットの安心・安全ハンドブック　Ver5.10
リーフレット（一般利用者向け）

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　　内閣官房　内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity