

図解
100

個人でできる 情報セキュリティ入門 100

IEC

はじめに

他人事ではない情報セキュリティ対策

ニュースなどで、よく「IT (Infomation Technology = 情報技術)」という言葉を見聞きします。ITとは、あらゆる情報をデジタル化してコンピュータによって処理する技術を指します。この言葉が一般に広まったのは、20世紀の終わりが近づき、21世紀という新しい時代が幕を開けようとする時期でした。当時、コンピュータの性能が飛躍的に向上し、安価で扱いやすいパソコンが爆発的に普及し始めていました。同じころ、一部の機関に限定されていたインターネットが一般に開放され、自宅に居ながらも離れた場所からの情報収集やコミュニケーションが可能な通信環境が整いました。21世紀に入ると携帯電話とコンピュータが融合した「スマートフォン」が登場し、私たちはいつ、どこにいてもITの恩恵を受けられるようになりました。

こうした一連の変革は「IT革命」と呼ばれています。私たちの生活スタイルはIT革命により「それ以前のスタイル」が思い出せないほど激変しました。今ではショッピングや銀行の振り込みといった経済活動や、メールや会議などのビジネス活動、さらに家族や友人との気の置けない会話や写真・動画のやりとりまでもが、インターネットで行われます。そして2020年代では、オフィスへの通勤をなくし、会社の業務を自宅で行う「リモートワーク」というビジネススタイルも普及しつつあります。

しかしITは便利な生活をもたらす一方で、リスクもあります。仕事に関わる機密情報や自分の財産に関わる情報、プライベートな情報などを、すべてコンピュータで管理しなければなりません。これらの情報が盗まれたり破壊されたりするリスクは、インターネットに接続している限り消えることはありません。単なる不注意だけでなく、第三者による故意の攻撃や自然災害による偶然によっても発生します。1箇所から流出した情報が連鎖的な被害を生む可能性や、コンピュータが乗っ取られて自分が犯罪者に仕立て上げられる危険性など、IT社会ではあらゆるリスクと隣り合わせであり、アナログ情報が主体だった時代とは異なる注意が必要です。

情報セキュリティとは、パソコンやスマートフォンといったデジタル機器を安全・安心して使うための技術や取り組みです。IT社会におけるリスクを抑えるために、セキュリティ対策に意識を向ける必要があります。本書を読んでデジタル機器を扱う際に発生し得る危険性と、それに対する対策方法を具体的に理解し、実践しましょう。

目次とスケジュール

それではテキスト学習に入ります。途中で投げ出したりしないために、計画を立ててから取り組みましょう。自分自身のペースに合わせて無理のない計画を立てましょう。

1日2項目を学習するのが平均的なスケジュールです。

□は、診断で間違ったところやこれは特に重要だ、覚えておきたいという項目をチェックするために使いましょう。

章	内 容	P	予定日	終了日
1	セキュリティの重要性を認識する	10		
	☐ 1 なぜセキュリティ対策が必要なのか	10	/	/
	☐ 2 情報セキュリティにおける3つの脅威	11	/	/
	☐ 3 情報セキュリティの3要素「CIA」	12	/	/
	☐ 4 ノーガードでは済まされないセキュリティ	13	/	/
	☐ 5 安全性とコストのバランス	14	/	/
2	セキュリティ事件簿	15		
	☐ 6 ラブレターにも注意—セキュリティ事件簿①	15	/	/
	☐ 7 偽サイトに注意—セキュリティ事件簿②	16	/	/
	☐ 8 金融犯罪の恐怖—セキュリティ事件簿③	17	/	/
	☐ 9 過去には1億人の情報漏えいも—セキュリティ事件簿④	18	/	/
	☐ 10 特定の企業を狙い撃ち—セキュリティ事件簿⑤	19	/	/
3	代表的な攻撃、ウイルスと迷惑メール	20		
	☐ 11 ウィルスとは何か	20	/	/
	☐ 12 銀行から預金が盗まれるフィッシング詐欺	21	/	/
	☐ 13 大量に送られるメールボム/スパムメール	22	/	/
	☐ 14 パソコンへの侵入を容易にする「バックドア」	23	/	/
	☐ 15 スピード勝負で行われるゼロデイ攻撃	24	/	/
4	ウイルスへの対策	25		
	☐ 16 なぜウイルス対策が必要なのか	25	/	/
	☐ 17 パソコンのウイルス対策機能	26	/	/
	☐ 18 標準機能のウイルス対策は「最低限」	27	/	/
	☐ 19 ウィルス対策ソフトで常に有効にすべき機能	28	/	/
	☐ 20 ウィルスに感染したらどうすればいい?	29	/	/
5	不審なメールから身を守る	30		
	☐ 21 電子メールによる攻撃/迷惑行為の種類	30	/	/
	☐ 22 フィッシングメールは見分けられるか?	31	/	/
	☐ 23 メールアドレスの使い分けで対策する	32	/	/
	☐ 24 フィッシングサイトを間違えて開いてしまったら	33	/	/
	☐ 25 メールソフトの迷惑メール対策	34	/	/

目次とスケジュール

章	内 容	P	予定日	終了日
6	不正アクセスから身を守る	35		
	☐ 26 不正アクセスとは何か	35	/	/
	☐ 27 不正アクセスでパソコンが操られる	36	/	/
	☐ 28 脆弱性にはどんなものがあるのか	37	/	/
	☐ 29 不正アクセスを許す出入り口「ポート」	38	/	/
	☐ 30 不正アクセスを防ぐ防火壁「ファイアウォール」	39	/	/
7	サイバー攻撃から身を守る	40		
	☐ 31 サイバー攻撃は誰もがターゲットになり得る	40	/	/
	☐ 32 サイバー攻撃には無差別型と標的型がある	41	/	/
	☐ 33 企業へのサイバー攻撃の二次被害	42	/	/
	☐ 34 大量のパソコンを操る「ボットネット」とは	43	/	/
	☐ 35 サポートが終了した OS やアプリの危険性	44	/	/
8	ユーザー情報（アカウント）の安全な管理	45		
	☐ 36 アカウントの乗っ取りと、その危険性	45	/	/
	☐ 37 アカウントはどのように乗っ取られるのか	46	/	/
	☐ 38 匿名のアカウントでも油断は禁物	47	/	/
	☐ 39 乗っ取られないためのパスワード作り	48	/	/
	☐ 40 アカウントを乗っ取られてしまったら	49	/	/
9	パスワードの安全な管理	50		
	☐ 41 簡単なパスワードはすぐに破られる	50	/	/
	☐ 42 パスワードは覚えるべきではない	51	/	/
	☐ 43 パソコンやスマートフォンでは PIN を活用する	52	/	/
	☐ 44 指紋や顔などがパスワード代わりになる「生体認証」	53	/	/
	☐ 45 次世代のオンライン認証方式「FIDO」	54	/	/
10	狙われる機密情報	55		
	☐ 46 自分のデバイスを業務でも使う「BYOD」の対策	55	/	/
	☐ 47 インターネットの深層「ダーク Web」	56	/	/
	☐ 48 行動が狙われるソーシャルエンジニアリング	57	/	/
	☐ 49 まるで本人が語る動画でだます「ディープフェイク」	58	/	/
	☐ 50 ウイルスにも漏えいにも強い「シンククライアント」	59	/	/
	☐ 添削課題		/	/

目次とスケジュール

章	内 容	P	予定日	終了日
11	キャッシュレス時代のセキュリティ	62		
	☐ 51 通販サイトの安全性	62	/	/
	☐ 52 クレジットカードには 3D セキュアを設定する	63	/	/
	☐ 53 通販サイトやオンラインバンキングは専用のアプリの利用を	64	/	/
	☐ 54 おサイフケータイや Apple Pay を安全に使うために	65	/	/
	☐ 55 カードが不正利用されたときの損害は？	66	/	/
12	本人認証の仕組み	67		
	☐ 56 3 種類の認証の方式を知る	67	/	/
	☐ 57 2 段階認証と多要素認証の違いを理解する	68	/	/
	☐ 58 ワンタイムパスワードとは	69	/	/
	☐ 59 SMS 認証とは	70	/	/
	☐ 60 本人確認は KYC から eKYC へ	71	/	/
13	Wi-Fi の安全な利用	72		
	☐ 61 なぜ Wi-Fi にセキュリティ対策が必要なのか	72	/	/
	☐ 62 Wi-Fi の暗号化方式の違い	73	/	/
	☐ 63 暗号化されていないフリー Wi-Fi の危険性	74	/	/
	☐ 64 SSID の取り扱いにおける注意点	75	/	/
	☐ 65 設定画面の管理パスワードに注意	76	/	/
14	モバイル機器の安全な利用	77		
	☐ 66 外に持ち出すパソコンのストレージは暗号化を	77	/	/
	☐ 67 パソコンの共有設定に注意する	78	/	/
	☐ 68 データを持ち出さずに外出先で作業する方法	79	/	/
	☐ 69 ショルダーハッキングの手口とその対策	80	/	/
	☐ 70 パソコン処分時はデータを完全消去する	81	/	/
15	SNS の安全な利用	82		
	☐ 71 ネットの匿名性はどの程度？	82	/	/
	☐ 72 考えておきたい著作権侵害	83	/	/
	☐ 73 ネットの悪口は犯罪行為になり得る	84	/	/
	☐ 74 フェイクニュースを見分ける	85	/	/
	☐ 75 SNS から漏れる個人情報	86	/	/

目次とスケジュール

章	内 容	P	予定日	終了日
16	情報漏えいに備える	87		
	☐ 76 なぜ情報漏えいが発生するのか	87	/	/
	☐ 77 情報を扱うルールを整備し遵守する	88	/	/
	☐ 78 メール誤送信による情報漏えいを防ぐ	89	/	/
	☐ 79 情報漏えいを防ぐシステム「DLP」とは	90	/	/
	☐ 80 情報漏えいに備える方法	91	/	/
17	実は危険な Web 閲覧	92		
	☐ 81 Web にアクセスすると伝わる情報	92	/	/
	☐ 82 Cookie（クッキー）とは	93	/	/
	☐ 83 ドライブバイダウンロード	94	/	/
	☐ 84 個人情報を保護する暗号化技術、SSL/TLS	95	/	/
	☐ 85 クロスサイトスクリプティング	96	/	/
18	IoT 機器の危険性にも気を配る	97		
	☐ 86 IoT に潜むリスク	97	/	/
	☐ 87 IoT 機器を安全に利用するための基本	98	/	/
	☐ 88 ネットワークカメラや Web カメラへの侵入	99	/	/
	☐ 89 サポートが終了した IoT 機器は利用しない	100	/	/
	☐ 90 ルータのウイルス感染	101	/	/
19	無視できない自然災害への備え	102		
	☐ 91 災害への備えも情報セキュリティの一つ	102	/	/
	☐ 92 自然災害に備えるには	103	/	/
	☐ 93 複数のバックアップ手段や NAS を活用する	104	/	/
	☐ 94 クラウドストレージを活用する	105	/	/
	☐ 95 災害に便乗した攻撃に要注意	106	/	/
20	押さえておきたい情報セキュリティの法と制度	107		
	☐ 96 個人のデータを守る個人情報保護法	107	/	/
	☐ 97 ネットワーク越しの攻撃を禁止する不正アクセス禁止法	108	/	/
	☐ 98 著作権法とクリエイティブ・コモンズ	109	/	/
	☐ 99 マイナンバーの取り扱いに注意	110	/	/
	☐ 100 サイバーセキュリティ基本法	111	/	/
	☐ 添削課題		/	/

なぜセキュリティ対策が必要なのか

学習のポイント

POINT ① 仕事や生活に便利なコンピュータは、犯罪者にとっても便利

POINT ② 家に鍵をかけるように、コンピュータにもセキュリティ対策を

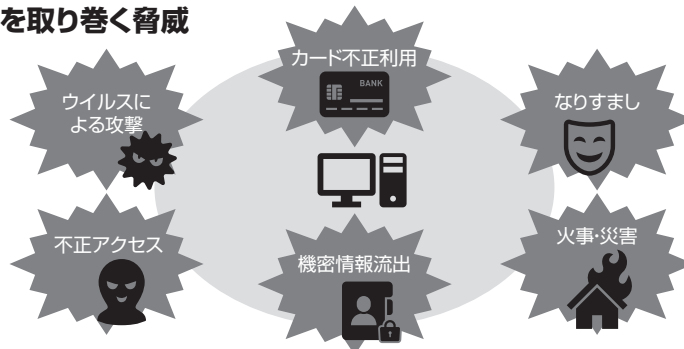
コンピュータやインターネットは、社会の至るところで利用されるインフラであるとともに、個人が日々の生活を送る上でも必要不可欠なものになっています。パソコンやスマートフォンといったコンピュータが仕事、プライベートの双方で当たり前のように使われるようになった現在、扱われるデータの重要性はますます増えています。

そしてこれらの全てのデータは、犯罪者のターゲットとなり得ます。犯罪者によってデータが破壊され、金銭が盗まれ、ときには犯罪の片棒を担がされることもあります。インターネットの普及で国境が取り払われ、誰もが世界中の犯罪者に狙われているのが現代です。そうした環境では「自分だけは大丈夫」といった安易な考えは禁物です。例えば、2019年における国内のサイバー犯罪の検挙件数は9,519件（警視庁「令和元年の犯罪情勢」）でしたが、これはあくまで検挙数にすぎず、背後にはその何十倍もの被害があるとされています。

攻撃だけが問題ではありません。パソコンを盗まれたり、自分のミスで大切なデータを消してしまったり、情報を流出させてしまったりすることも考えられます。さらには、災害や事故によってデータが失われることもあります。

こうした問題から身を守り、コンピュータや情報を安全に利用するために重要なのがセキュリティ対策です。セキュリティ対策は、何らかのツールを導入するだけで完了するわけではありません。発生するアクシデントは多岐にわたるので、特性に応じた検討が必要です。とはいえ、個人で意識すべきことはそれほど複雑ではありません。ソフトのインストールや機器の設定変更の他、少し意識を変えるだけで安全が守れるものもあります。家で戸締まりをして、もしものために保険に入るのと同様、誰もが取り組むべき安全対策が情報セキュリティです。どんな危険があり、どんな対策方法があるのかを知れば、より便利で安心した生活を実現できるのです。

■ パソコンを取り巻く脅威



情報セキュリティにおける3つの脅威

学習のポイント

POINT ① 技術的脅威・人的脅威・物理的脅威の3つがある

POINT ② 3つの脅威に合わせたセキュリティ対策が必要

デジタル機器を使うことで発生する脅威は、一般的に「技術的脅威」「人的脅威」「物理的脅威」の3つに分類されます。

1つ目の技術的脅威は、コンピュータウイルスに代表される、ソフトウェアなどのIT技術を使った脅威を指します。ウイルスへの感染が原因でパソコンの情報が盗まれる、データが破壊されるなどの被害が発生します。この他にWebサイトやパソコンへ第三者が不正に侵入して犯罪行為を行う「不正アクセス」、データやWebサイトの内容を書き換えてしまう「改ざん」など、多くの攻撃が存在します。

2つ目の人的脅威は、人間が原因となる脅威を指します。会社のパソコンを電車に置き忘れたり、紛失したり、メールの宛先を間違えたりといった誤操作、パソコンを盗み出される盗難や、不用意な発言で問題を起す、いわゆる「炎上」も人的脅威に含まれます。

そして3つ目は物理的脅威です。これは火災や自然災害による破損、ハードウェアの故障、

物理的な破壊といった脅威を指します。

セキュリティ対策は、これらの脅威から情報を守るための対策です。技術的脅威に対しては、それぞれの攻撃に合わせた防御技術が存在しており、そうした技術を導入します。人的脅威に対しては、従業員に対するルールの徹底や教育を通じたりテラシーの向上、また、管理者による従業員の監視などを行います。物理的脅威に対してはデータのバックアップ、盗難・破壊を防ぐための戸締まりや警備の強化といった対策を講じます。

企業と個人では対策の規模は異なりますが、基本的な考え方は変わりません。人間の心理的な隙を突いて企業の情報を盗む「ソーシャルエンジニアリング」などは、個人が脅威を知っておかなければ対策できません。単にセキュリティソフトを導入するだけでなく、どのような脅威が存在するかを知ることで、セキュリティへの意識をより高めていくことが大切です。

■ コンピュータの3つの脅威

技術的脅威

- ・ ウイルス
- ・ 不正アクセス
- ・ フィッシング詐欺
- ・ なりすまし
- ・ DoS攻撃
(大量のデータでコンピュータを
パンクさせる攻撃)

人的脅威

- ・ 紛失・盗難
- ・ 誤操作
- ・ 炎上
- ・ ソーシャルエンジニア
リング
(人の行動や心理状態に
つけこんで情報を盗む行為)

物理的脅威

- ・ 火事
- ・ 地震
- ・ 台風
- ・ 故障
- ・ 破壊
- ・ ソフトウェアのバグ

不正アクセスとは何か

学習のポイント

POINT 1 データの出入り口の不具合が不正アクセスを引き起こす

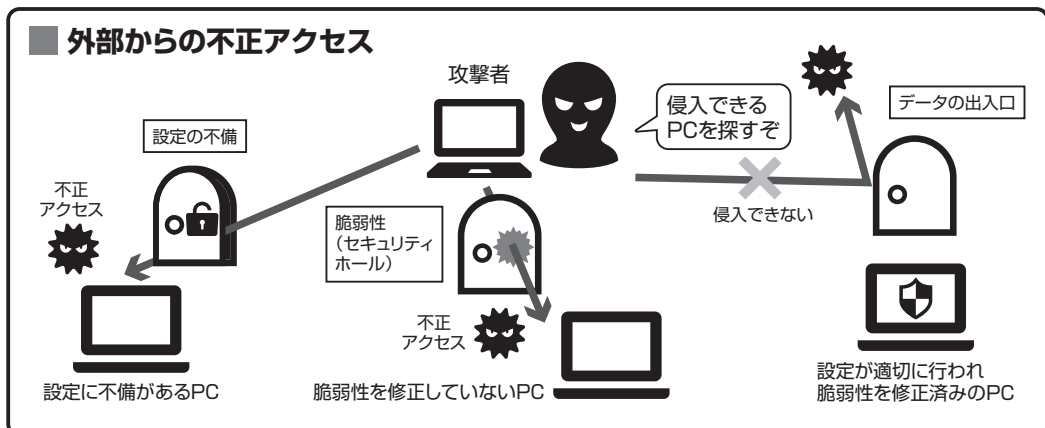
POINT 2 脆弱性の修正プログラムは必ず更新する

権限のない第三者が、直接またはネットワークを通じて間接的にコンピュータにアクセスし、勝手にデータの閲覧や改ざん、持ち出しなどを行うことを不正侵入（不正アクセス）といいます。特に近年はインターネットの普及により、直接コンピュータを操作するのではなく、インターネットを通じて間接的にアクセスする不正アクセスが後を絶ちません。自分がインターネットを通じて情報を受け取ることができるということは、他人（他のコンピュータ）がインターネットを通じて、そのコンピュータにアクセスしているという意味なのです。

パソコンがインターネットに接続する際は、利用するサービスごとに「情報の出入り口」を内部に設けて通信を開始します。こうした出入り口を悪用するのが、一般的な不正アクセスの攻撃方法です。とはいえ簡単に攻撃されないように、通常はパソコンが送った接続要求に対応するデータ以外は受け入れないよう、出入り口

が制限されています。ところが設定に問題があって制限が不十分な場合や、ソフトウェアに不具合があって制限が機能しない場合があります。後者の不具合を脆弱性（またはセキュリティホール）と呼び、攻撃者はこれを突いてパソコンに不正アクセスします。ソフトウェアの開発者は、脆弱性が見つければ修正プログラムを提供します。ところが修正プログラムを適用せずに放置されているパソコンはたくさんあります。攻撃者は、そうした設定の不備や脆弱性があるパソコンを探索し、侵入する準備をします。

最新のOSを使っている環境なら、デフォルトである程度のセキュリティが保たれています。セキュリティの設定を個別に変更しなければ問題ないでしょう。問題は、脆弱性が見つかったときです。修正プログラムを適用し、脆弱性を修正しないと不正アクセスのリスクが残り続けるため、OSは常に最新の状態にアップデートするよう心がけましょう。



まるで本人が語る動画でだます「ディープフェイク」

学 習 の ポ イ ン ト

POINT ① 本人そのものの動画や音声ができる

POINT ② 単一の情報だけで判断しない

近年飛躍的な進歩を遂げたAI（人工知能）を悪用し、人をだますコンテンツを「ディープフェイク」といいます。AI技術を支える代表的な手法の「ディープラーニング」と、偽物を意味する「フェイク」の2つの言葉を合成した言葉で、実在しないコンテンツを精巧に作り上げてしまう恐るべき技術です。

インターネット上では、以前からフェイクニュース（嘘のニュース）が蔓延しており、政治的なデマで世論を誘導したり、株価を不正に操作したりすることが問題視されています。これをさらに高度化したディープフェイクでは、文章や写真だけではなく、音声や動画も容易に作り出せてしまいます。

ディープラーニングは、コンピュータに大量のデータを読み込ませてパターンを学習させることで、コンピュータ自身が新たなコンテンツを作り出せる技術です。実在する人物の表情や声のパターンを学習すれば、その人が映った架空の動画も生成できます。特に有名人は、動画

などのデータが多く公開されているため、より正確な学習が可能です。これ自体は問題ではなく、日本では年末の恒例番組で、故人の国民的歌手が新曲を披露する試みが行われたことがありました。しかしこうした技術を悪用すると、ディープフェイクと呼ばれます。アメリカではオバマ元大統領のフェイク動画が作成され、問題になりました。

著名人が実際には語っていないことを話す動画は、大きな問題をはらんでいます。「あの〇〇さんが推薦」と嘘をついて高額な商品を購入させたり、有名人と一緒に写った写真を使って人を信用させてお金をだまし取ったり、振り込め詐欺にも悪用されたりするかもしれません。ディープフェイクにより真実味が増した動画にだまされる事件は、これから増えていくことでしょう。著名人の動画だから、知り合いの声だからなど、単一の情報だけで判断するのではなく、多角的に事情を調査する習慣をつける必要があります。

■ ディープフェイクの仕組み

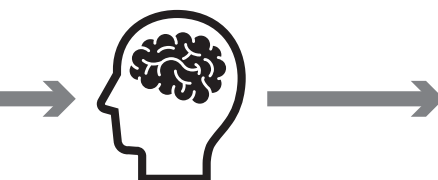
実在する人物のデータ

ディープラーニングで合成

偽のデータ



実在する人物のデータを用意し、ディープラーニングに読み込ませる



ディープラーニングによって単純な切り貼り、繋ぎ合わせではない自然な合成を行う



本物と見分けのつかない精巧な偽のデータが生成される

設定画面の管理パスワードに注意

学習のポイント

POINT 1 管理IDやパスワードはデフォルトだと危険

POINT 2 Wi-Fiルータ導入後にただちに変更する

自宅に設置するWi-Fiルータの各種設定は、設定画面から確認・変更できます。パソコンやスマートフォンなどのWebブラウザからアクセスでき、プロバイダへの接続設定やWi-Fiの各種設定など、ルータを利用するためのさまざまな設定項目がまとめられています。そして、通信の暗号化設定やパスワードの設定、ファイアウォールの設定、インターネットからネットワーク（LAN）内の機器へのアクセス設定など、セキュリティを保つ上で重要な設定もここから管理が行えます。このように設定画面は、Wi-Fiを安全に利用するための要と言っても過言ではありません。設定画面へのアクセス方法はマニュアルに記載されているので必ず確認しましょう。

設定画面にアクセスしてWi-Fiルータの管理を行う際は、管理ユーザ名や管理パスワードでログインします。ところが、この文字列がデフォルトでは単純なものになっている製品も多く存在します。管理ユーザ名や管理パスワードが同一メーカーの全ての製品で同じになっていた

り、管理パスワードが設定されていなかったりするケースも珍しくありません。悪意のある第三者がその点を悪用し、勝手に設定画面にアクセスしてセキュリティ設定を無効にした上で、Wi-Fiルータを乗っ取ったり、LAN内のパソコンやスマートフォンから各種情報を抜き出したりする可能性もあるため、セキュリティ上問題があります。こうした問題を防ぐため、管理ユーザ名と管理パスワードは、Wi-Fiルータ導入時に必ず変更しておくようにしましょう。特にパスワードは、連番や同じ文字を並べただけの簡単なものではなく、なるべく複雑で、他人が推測しにくい文字列にしましょう。

ちなみに多くの製品で、Wi-Fiネットワークの外部（インターネット側）から設定画面にアクセスできないようにする設定項目が用意されています（「Internetリモートアクセス設定」など）。外部からWi-Fiルータを乗っ取ろうとする試みを防げるので、この機能が利用できる機種なら有効にしておくことをおすすめします。

Wi-Fiルータの設定画面のパスワードは必ず変更する

LAN 無線設定 セキュリティ アプリケーション 管理 システム設定 ログ	システム情報 エアステーション名 管理ユーザー名 admin (変更することできません) 管理パスワード ☐ パスワードを表示する
--	---

Wi-Fiルータの設定画面にアクセスするパスワード(画面では管理パスワード)は、購入したら必ず変更しておく。メーカーによってはログインID(画面では管理ユーザー名)を変更できる製品もあるので、その場合はIDも変更しておくことより安心

Cookie(クッキー)とは

学習のポイント

POINT 1 基本的にはユーザーの利便性を向上させるために利用される

POINT 2 気になる場合は定期的にCookieを削除する

Webサイトにアクセスした場合に、「Cookie(クッキー)の使用に同意してください」という表示を見たことがある方も多いでしょう。

Cookieとは、アクセスしているサイトのWebサーバーが、自分のパソコンやスマートフォンへ残すデータのことです。そのサイトを訪れた日時、アクセス回数、ログイン情報、閲覧内容などが記録され、次回同じサイトを訪れたときに利用されます。ログインの必要なWebサイトにアクセスすると、1度IDとパスワードを入力すれば、一定の時間内はログイン状態でサイトを閲覧できます。また通販サイトでは、カートに入れた商品を決済せずにサイトから離れても、再度アクセスするとカートに商品が残っている場合があります。これは、自分のパソコン内のCookieに情報が保存されているからです。

Cookieに保存されている情報は広告表示のためにも使われます。多くのWebサイトでは、アクセスする人によって表示される広告が異な

ります。それは、Cookieに記録されたアクセス履歴や購入履歴をもとに、その人に合わせた広告を表示する「ターゲティング広告」という仕組みが採用されているためです。

Cookieによって利便性が高まりますが、懸念される点もあります。Cookie自体に個人情報は記録されませんが、通販サイトなどではログイン情報とあわせて解析すれば個人を特定することもできるため、大きな問題となる可能性もあります。ただ近年は、個人情報保護の観点から、必要以上のCookie利用を規制するようになっていきます。例えば、「サードパーティCookie」と呼ばれる異なるサイトをまたいで利用できるCookieは基本的に禁止されています。そのためブラウザのセキュリティ設定をデフォルトから変更しない限り、Cookieを不安視する必要はないでしょう。また、ブラウザにはCookieを削除する機能があるので、気になる場合には定期的にCookieを削除するようにしましょう。

Cookieを管理する

Cookieは、パソコンやスマートフォンのブラウザの設定画面から管理や削除ができる

