

説明書

利用する先生方や親御さんへ

このサイトはお子様一人で使用することもできますが、教えながらの使用を前提として作成されています。説明するポイントやこのサイトの使い方を記載しています。良かったら参考にしてくださいと嬉しいです。

“”アルゴリズム×セキュリティ””

・アルゴリズムとは、問題を解く手順や計算方法のこと。変数、条件分岐、ソート、二分探索などプログラミングで役に立つ。

・今回のゲームはウイルスを退治するアルゴリズムを考える問題です。真ん中の緑の旗を押すことでスタートです。説明する動作は3点。

- ① 青色/前に進む：前進する
- ② 赤色/右に進む：右に向き前に進む
- ③ 緑色/左に進む：左に向き前に進有進む。

これらの3つを1つの□の中につき1つ置き、ウイルスに見立てたモンスターへとペンギンがたどり着くアルゴリズムを構築してください。それぞれのボタンはマウスを左クリックを押した状態でつかむことができ、移動させたい場所でマウスの左クリックを押している指を話すことで置くことができます。これをドラッグアンドドロップといいます。できたら、↑キーを押すことで配置完了とされ、進みます。進まない場合は、青色/前に進むボタンをマウス左でクリック、押し、つかみ、ペンギんに触れさせてください。きっと進むはずです！

“”パスワード管理””

・ユーザーID、パスワードなど、現在よく利用するSNSをはじめ、コロナ渦により加速したオンライン決済などでも使用していると思います。では、この中にパスワードが123456の人はいますか？なんとこのパスワードは世界で一番使用されているパスワードです。このパスワードで過去に約2,400万件のパスワード流出がありました。（<https://haveibeenpwned> のサイト結果から）。なぜ、123456という数字が一番使用されているのかというと数字の順番であり、キーボードの半角/全角の横にある1キーから指を押したままスライドすることで押してしまう番号だからです。他にもq, a, zなどキーボードの端からのそれぞれ、qwerty, asdfgh, zxcvbnなども押しやすい番号で記憶する必要がないという意味で選ばれる。日本語で表記できる英語なども簡単に使用されやすい（例：hello, apple, lemon等）。

このゲームはパスワード検討という点から作成しました。自分がパスワードを作るときに安全面に最も重きを置き作成すると仮定して自分がより安全性が高いと思うパスワードの

道へキーボードの矢印キーを押して進んでね。ゲームは真ん中に表示されている緑の旗をクリックすると開始します。第1問目：どちらのほうが安全性の高いパスワードですか？123456 または 1b2a3c。123456 はさきほど話したように世界で一番使用されているパスワードなので安全性は最も低い。よって、123456 の世界で最も安全性の低いパスワードよりは安全性の高いパスワードは 1b2a3c。左←に進む。間違いの 123456 の道に進んでも道の途中にある色がついている棒を踏むと解説がついていて行き止まりとなるので、解説を読んでから引き返して正解の道に進んでください。黒い枠からでないように作成されているのであまりに黒い枠に近づきすぎると動かなくなる時があるので、その際は少し下がってから操作してください。以下使用されている回数が多いパスワードランキング 2020 を 15 位まで載せておきます。問題には 1 位、4 位が使用されています。

○多いパスワードランキング

1	123456	9	1234567890
2	123456789	10	senha
3	picture1	11	1234567
4	password	12	qwerty
5	12345678	13	abc123
6	111111	14	Million2
7	123123	15	000000
8	12345		

(引用先：“後藤大地”, “使ってはいけないダメなパスワード Top200 発表-2020 年版”, 2020, url=” <https://news.mynavi.jp/article/20201124-1520971/>”)

+同じパスワードを他のサイトでも使用することはやめましょう

・記憶するパスワードが増えると忘れてしまうことが増えてしまいますが、一つのパスワードが破られると、同じパスワードを使用していた場合同じパスワードで使用していたサイトの情報まで盗まれてしまい被害が倍になります。

+生年月日など自分に関連するデータをパスワードに使用することはやめましょう

・生年月日などの情報は個人情報としての認識が薄く、出回ってしまっている可能性が極めて高いです。例えば、高校生になって塾の案内がやたらと届くなどが例にあげられます。出回ってしまっている情報をパスワードに使用することはパスワードを公開してしまっていることと同じです。使用しないようにしましょう。生年月日だけでなく、名前もね。

“”SNS 物語“”

・このゲームはダウンロードしていただければ、話の中に説明が入っていますので説明なしでも遊ぶことができます。

<ダウンロード方法>

“フィッシングサイト”

フィッシングサイトとは偽サイトに誘導し、アカウントの ID やパスワード、クレジットカードなどのいわゆる個人情報とよばれる重要な情報を入力させてその個人情報とよばれる重要な情報を入力させてその個人情報を盗みとるためのサイトのこと

この問題では実際のサイトやメールに似た画像が表示されています。実際のサイトと見比べて穴埋め形式で問題が提示されます。ですので、例としていくつかのサイトを以下の変化されやすいポイントを重点的に紹介してあげてください。

- ・ http と https
- ・ サイト上に掲載されている企業名
- ・ 企業マーク
- ・ URL 末尾
- ・ リンク先




+ 困ったときの連絡先

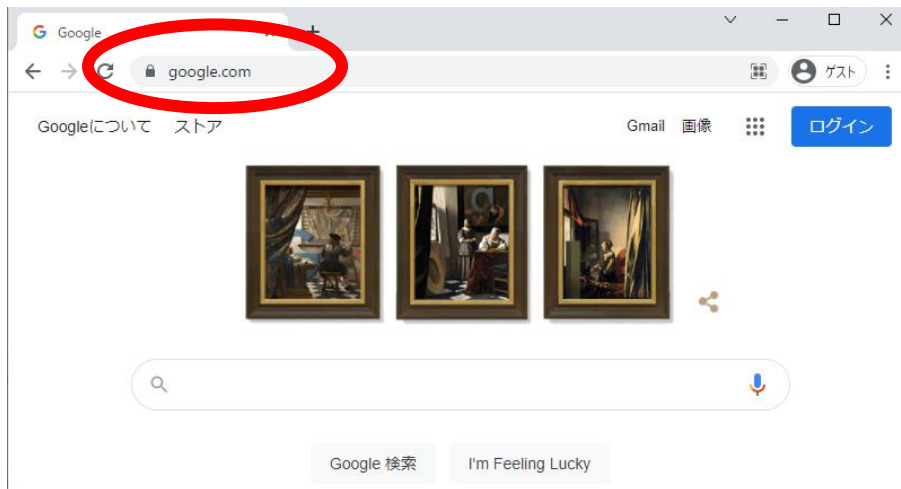
+ 悪質な海外ウェブサイト

- ・ フィッシング詐欺メール

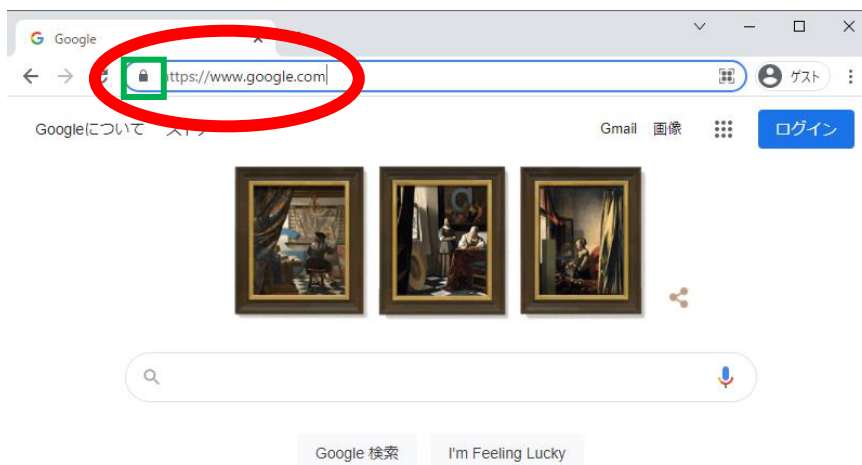
<重点ポイントの詳細確認>

① http と https

・ まず、http と https の違いですが、http とは Hyper Text Transfer Protocol の略でホームページのデータをサーバとブラウザ兼クライアントの間をやりとりするためのプロトコルのことです。https はそれに s=「Secure」、「安全で」「心配のない」「保証された」が加わったものです。https では通信が暗号化され情報を盗み取ろうとしている人にも解読されなくなっています。みなさんも http と https の二つのサイトがあったら、保証された https のサイトを利用したいですね。では、どのようにこの二つを見分けていくのか紹介していきます。画像 1 で示した赤い丸で囲まれている普段サイトの上記にあるバーを二回クリックしていただくと、画像 2 のように変化します。この際に http ではなく、https と記載されているかを確認しましょう。それに加え、このバーの一番左（画像 2 の緑色の□で囲まれているもの）が  マークになっているかも一緒に確認しておきましょう。この鍵マークもセキュリティがかけられているのかの証明になっており、 が  などもあるかもしれませんのでしっかりとみましょう。



←画像 1



←画像 2

② サイト上に掲載されている企業名

・例えば、調べている企業名。今回問題にもさせていただいている Amazonさんを例にあげてみましょう。先ほどの上のバーに張られている URL () にも amazon という文字がはいります。ここに記載されている小さな字を amozon にしたり、amaqon にしたりなどさまざまな似たようなアドレス () が作成されています。

③ 企業マーク

・amazonさんの企業マークはバット思い浮かびますでしょうか？そう！aの文字を含めたロゴマークを使用されています。かなり有名なロゴマークですが、そのaの部分がeになっていたら気がつくですか？はたまた似たような字のoであったら気がつくですか？ましてや下についている矢印の向きが→から←になっていたら気がつくかな？矢印の向きが違ったことに気付ける人が一番すくなそうだね。間違い探しみたいに注意深くみてみよう。(②③どんな間違いやすそうなものがあるのかグループで話し合いを行っても良いと思います。その際に使用しやすいように1つグラフを以下にのせておきます)

フィッシングサイトとして利用されることが多い企業ランキング

(8月3位で9月1位の Amazon さんのサイトは問題で使用しています。ランキングに記載のない PayPal を取り入れましたので、現在テレビ離れにより YouTube を見るお子さんが増えたことと思いますが、その YouTube にお金を入れたり、インターネット関連で最近使われることの多いサイトなので取り入れました。)

No	2021 年 8 月	2021 年 9 月
1	三井住友カード	Amazon
2	エムアイカード	Vpass
3	Amazon	三井住友カード
4	国際競技大会	ヨドバシカメラ
5	PayPay 銀行	ETC 利用照会サービス
6	ビューカード	PayPay
7	PayPay	Au
8	JCB	PayPay 銀行
9	ヤマト運輸	楽天
10	エポスカード	NTT docomo

(引用先：“Online Security”, “EC サイト事業者をかたるフィッシング詐欺が前月比 2.7 倍に増加”, 2021, url=” <https://www.onlinesecurity.jp/reports/2021/202110.html>”)

④ URL の末尾

・②でみた上記のバーの末尾にも注目してみましょう

<https://www.google.com/>

赤：通信プロトコル

通信プロトコル。こちらは①で紹介しましたね

青：ホスト名

ホスト名は www「World Wide Web」の略で世界中の張り巡らされたクモの巣を意味しています。こちらは自由に設定できますが、あまり変更されることはありません。

緑：ドメイン

インターネット上の住所を表すドメイン。ですので、同じドメイン＝住所は1つしか存在しません。ドメインの中でも緑の○で囲んだ部分をトップレベルドメインといい、よく見かける.jp は国別のコードに割り当てられたトップドメインです。おもに.com、.net があります。.xyz など無料で取得できるトップレベルドメインもあるので、そちらを使用している場合は少し危険性を疑いましょう

(引用先：“ferret”, “URL とは？意味やドメインとの違い、構成する要素を徹底解説！”, “記事”, 2020, url = “<https://ferret-plus.com/8736?page=2>”)

⑤ リンク先

・わかりにくいものとしてリンク先に引っ掛けがあることがあります。個人情報を入力させて、その下にあるログインボタンや新規登録ボタンなどのリンク先を書き換え自分宛てに送り個人情報を盗み取るなどの手口です。引っ掛けからしないためにも、リンク先の確認をできるかぎりしましょう。

+ 困ったときの連絡先

・インターネット（フィッシングサイト等をはじめとする）をめぐるトラブルにあったときに連絡しよう↓

国民生活センター (<http://www.kokusen.go.jp/>)

+ 外部提供情報の例

・消費者庁から提供されている海外のネット通販サイトで消費者トラブル相談が多く寄せられている悪質な海外のウェブサイトが掲載されています。

https://www.consumer_policy/caution/internet/

“”フィッシングメール””

実はフィッシングサイトは有名ですが、フィッシングメールも増えています。実際に私の親にも届いたのですが、SMS といわれる電話番号宛に届くメールに宅急便を名乗るメールが届きました。そこには、配達日時の指定をするよう個人情報の入力を求めてくる内容でした。よくある手口として以下に3つ挙げておきます。

- ・ ID/パスワード変更
- ・ 宅配便の不在通知
- ・ 不正サイトへの誘導

<手口の詳細>

① ID/パスワード変更

・よくある ID/パスワードの変更を求めるメールの内容としては、不正ログインが検知されましたので、安全性を保つにはすぐにログインし、パスワードの変更を行ってくださいと最速するようなメールです。しかし、そのメールに添付されているログイン用 URL は本物とは違い、個人情報を盗み出すように作られた URL サイトとなっているというのが実際です。このようなメールはメールの送信元やドメインを確認しましょう。ドメインの見方は送られてきたメールアドレスを確認しましょう。

@amazon.co.jp

緑の線の部分(@以下)がドメインです。日本国内の場合は、「.co.jp」や「.ne.jp」「.jp」がよく用いられます。無料で入手しやすい。「.xyz」「.pw」「.c0」などがフィッシングメールでは

用いられることが多いのでメールアドレスをその企業のホームページのお問い合わせ先まで調べ照らし合わせて確認することを推奨します・

② 宅配便の不在通知

・実際に私の親も体験した、有名宅配業者を名乗った宅急便の不在通知。宅配時間を指定するためにこちらに個人情報と時間を指定してくださいと URL のリンクが貼られてメールが届きます。こちら①同様に URL サイトが実際とは異なり、入力した個人情報を盗みに来ています。実際、宅配便業者が S M S でメッセージを送ってくることはありませんので届いた時点で無視をしましょう。有名業者を使用しているとその企業からホームページに警告のお知らせがでていることもありますのでそちらをよく確認しておくのも現在の状況をしれて良いでしょう。

企業のホームページからのお知らせの例：・ <https://www.sagawa/>
・ <https://www.yamato/>

③ 不正サイトへの誘導

・現在蔓延している新型コロナに関する給付金や、抽選などによる当選これらの話題から①②同様サイトへと移行を促します。対処法として①のメールアドレスを確認することにしてこのようなメールが外国から届くことをあります。外国語から日本語へ翻訳機にかけたかのような不自然な日本語や文字化けがメールの件名や、本文に含まれているとフィッシングメールを疑いましょう。

文字化け例：◆◆おめでとうございます！

100 万円プレゼント◆企画に当選しました◆

以下の URL を確認ください。

(引用先：“AMIYA”，“フィッシングメール詐欺とは | 見分け方と入力してしまった場合の対策”，“S E C U L A B O”，2020,
url=“https://www.amiya.co.jp/column/phishing_email_20210203.html”