未来の Kids サイバーセキュリティ教室プロジェクト
サイバーセキュリティ授業の手引き

はじめに

学校教育の中ではスマートフォン・タブレット端末・SNSの利用については啓発が行われているが、具体的なサイバーセキュリティに触れている学校や教職員は少ない。2022年現在、独立行政法人情報処理推進機構(以下、IPAと呼称) が発行している「情報セキュリティ１０大脅威　２０２２」[*1]では、個人への１０大脅威が記載されているが、フィッシング詐欺などが挙げられており、そのいずれもが児童も巻き込まれる可能性を有した脅威である。

昨今のサイバー攻撃はより苛烈に、より身近なものになっており、児童自身が不正アクセスを行ってしまうケースや、サイバー犯罪に巻き込まれるケースに備える必要性が増している。もはや家庭内での教育や外部からの情報だけでは、すべての子供たちに自らを守るために適切なサイバーセキュリティ意識を芽生えさせることが難しくなってきた。そのため、学校教育の中ですべての児童へのサイバーセキュリティ教育が必要とであると考え、本手引きを作成した。全国の小学校教育に従事される方が本手引きを活用していただくことで、サイバーセキュリティに対する教育も交通安全教室と同様に、当たり前となる未来を実現するための一助になればと考える。

当ドキュメントで説明しているコンテンツ・カリキュラムは、ITリテラシー向上やサイバーセキュリティについての啓発・意識向上を学校教育の中で授業として教育しやすくするために準備したものである。

IPA産業サイバーセキュリティーセンター(以下、ICSCoEと呼称)中核人材育成プログラムの卒業プロジェクトにて作成された児童向けサイバーセキュリティ教育コンテンツおよび、カリキュラムを実施するための手順を記載する。

各カリキュラムは連続しているものではなく、状況に応じて選択していただくのが望ましい。細かな内容や伝えるポイントは、講師と生徒の関係性や状況により、効果的と判断する内容に柔軟に変更することを勧める。

尚、当カリキュラムの一部は複数の小学校で効果測定を実施しており、
90%の児童が「楽しく理解できた」と回答している。

当ドキュメントで説明しているコンテンツ・カリキュラムには以下の狙いがある。

１．児童のITリテラシー向上
２．児童が自らサイバー攻撃から身を守れるようにする
３．サイバーセキュリティ事態の認知度を向上させる
４．教育を受けた児童が成長するに従い、日本のサイバーセキュリティ能力の向上
５．日本のセキュリティエコシステムの発展

[*1]:https://www.ipa.go.jp/security/vuln/10threats2022.html

～免責事項～

・このドキュメントは単に情報として提供され、内容は予告なしに変更される場合がある。

・このドキュメントやコンテンツに誤りが無いことの保証や、
商品性又は特定目的への適合性の黙示的な保証や条件を含め
明示的又は黙示的な保証や条件は一切無いものとする。

・このドキュメントやコンテンツの内容は、独立行政法人情報処理推進機構および
産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいている。

・このドキュメントやコンテンツの利用によるトラブルに対し、
本書作成者ならびに監修者は一切の責任を負わないものとする。

スタディ１　動画で学ぶパスワードの大切さ

概要

現代の子供たちは、幼少期からスマートホンやタブレット端末などでオンラインゲームやSNSなどのインターネットを有効利用している。また、GIGAスクールの普及により、自分でIDやパスワードを持つ状況となっている。そのため、パスワード管理の重要性を認識させる必要がある。

スタディ１では、動画から、パスワード管理の重要性を学習し、不正アクセスは犯罪であり罪に問われることを認識してもらう。

狙い

情報社会におけるインターネット利用時のトラブルを未然に回避する方法を学ぶ。
グループワークでの授業を行い、自主性や協調性などの能力向上や、自ら考える力を養う。

授業の流れ

導入

普段、インターネットをどのように利用しているか講師と生徒にて対話する。
利用している中で、パスワードをどのように管理しているかをヒアリングする。
インターネットをあまり利用しない生徒に対しては、これから行う授業は
将来必要な内容でありしっかりと学習してほしい点を強調する。

準備

動画を視聴するための準備を行う。
グループワーク形式での授業が望ましいため、グループを作成する。
スタディ１用のワークシートを各班に配布する。

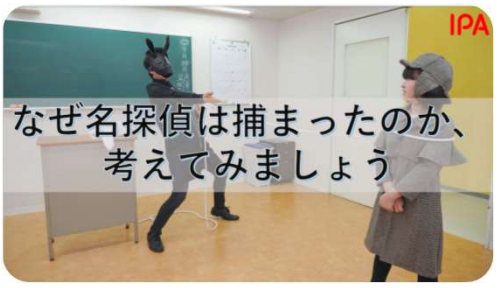
視聴

動画全体の視聴時間は、約13分。
9分のタイミングで動画を停止し、グループワークの時間に入る。
【動画URL】※
日本語のみ　：https://youtu.be/wJAsfxjMTuw
英語字幕版　：https://youtu.be/mjtW8_2u8a8
※ youtube IPA Channel より　https://www.youtube.com/user/ipajp/videos

スタディ1 授業の流れ （続き）

グループワーク

ワークシートの課題１、課題２を各グループで進める。
生徒個人個人が意見を出し合えるように、各グループへフォローを行うことが望ましい。

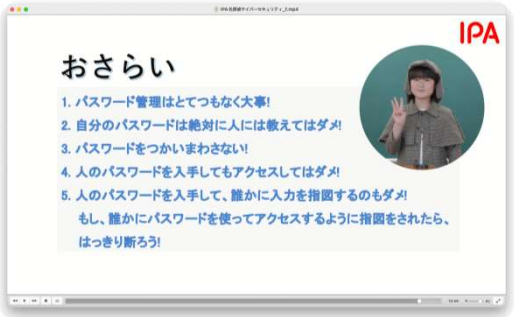


発表

各グループで検討した課題１、課題２のアウトプットを行う。
同じ内容が発表されても否定せず、グループ同士でも活発な意見交換を実施することが望ましい。生徒の意見を尊重する。

視聴続き

続きを最後まで視聴する。
動画内では、一般的な回答を示しているのみなので、生徒自身が気づいた点と相違がある場合でも問題はない点を伝える必要がある。



まとめ

続きを最後まで視聴する。
動画内では、一般的な回答を示しているのみなので、生徒自身が気づいた点と相違がある場合でも問題はない点を伝える必要がある。

スタディ1：動画で学ぶパスワードの大切さ

クラス：　　年　　組　　グループ：　　日付：　　年　　月　　日

学習テーマ：インターネットは便利だけど危険がいっぱい！
パスワード管理の重要性を学ぼう！

課題1：なぜ名探偵は捕まってしまったのか考えよう
※自由に書いてみましょう

課題2：自分たちは何に気をつけた方がいいか考えよう
※気づいた事を自由に書いてみましょう

スタディ2　フィッシングの学習

概要

児童でもメールを使うケースが増え、標的型メールなどによるサイバー犯罪に巻きまれる可能性が大いにある。IPAが発行している「情報セキュリティ１０大脅威　２０２２」では、「フィッシングによる個人情報等の詐取」が第１位に順位付けられており、危険性が非常に高まっている。
生徒には、フィッシングとはなにかを覚え、どのような危険があり何をするべきかを学んでもらう。

狙い

世の中には偽物のWebサイトがあり、個人情報やパスワード情報などの重要な情報を盗まれてしまうかもしれない危険性を認識してもらう。
偽物と本物は全く見分けがつかない場合があることを認識してもらう。
Webサイトにアクセスするときは、大丈夫かな？と一息置くことを意識付けする。
「おかしいなと思った時は大人に相談すること」の大切さを学んでもらう。

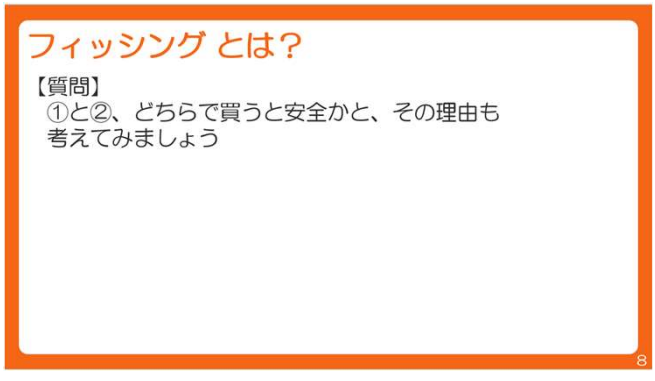
授業の流れ

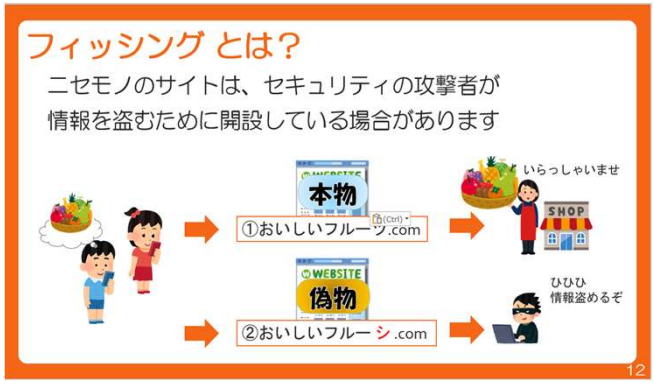
導入

[スタディ2_テキスト]を生徒へ配布する。

テキストを用いて授業を行う点を伝える

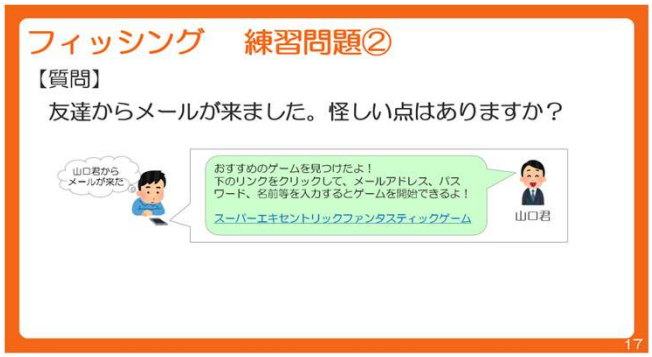
以下、テキストのポイントを記載する

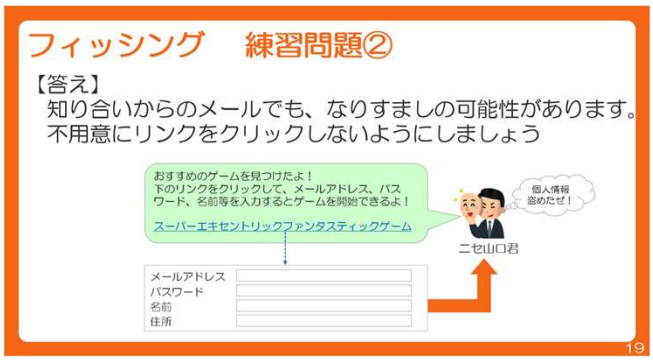




- 講師-生徒間で自由に意見交換を行う。意見を否定してはいけない。
- ”偽物” のサイトは、悪い人が情報を盗む為にWebサイトを利用している点を伝える。
- 後述される当テキストで定義している不正解の意見が発言された場合でも、現実では ”本物” である可能性も十分にある点を生徒に伝える。
- 逆に、当テキストで “本物” と定義しているWebサイトも、現実では “偽物” である可能性も十分にある点も生徒に伝える。

スタディ２　授業の流れ（続き1/2）





・講師-生徒間で自由に意見交換を行う。
意見を否定してはいけない。

・フィッシング被害に合った場合、
自分にはどのような実害があるかを
ポイントに意見を述べてもらう。

・主に、[なりすまし被害]、[個人情報]
[金銭的被害]がイメージしやすいが、
その場の状況によりわかりやすい例え
を用いるのが望ましい。
(例) オンラインゲームでのなりすまし。
SNSなどに不正ログインされる。
友達の電話番号が悪い人に盗まれ、
知らない人から電話やメールがくる。

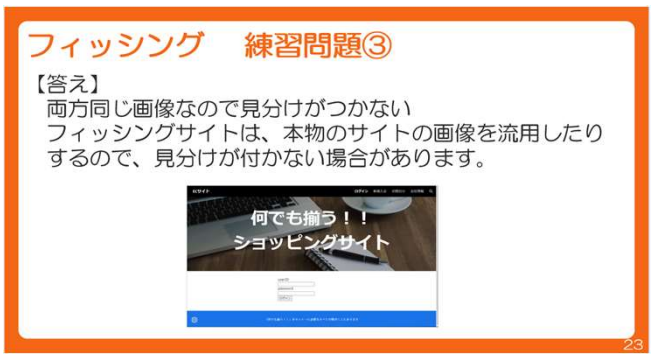
・講師自身にフィッシング被害の経験
があれば、実体験を伝えるのも効果的。

・自分が気を付けていても、
家族や友達がフィッシング被害に合い、
情報を盗まれているかもしれない点も
考慮してもらう。

・本人は気づかなくても、
実は個人情報を盗まれているケースも
存在している点を述べる。

・怪しいと思ったら親御さんや先生など
近くの大人に相談する点を伝える。

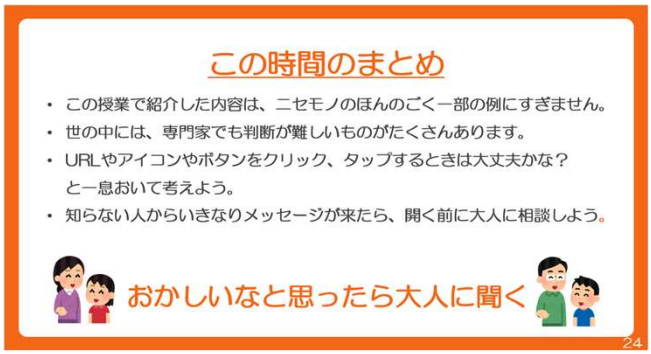
スタディ２　授業の流れ（続き2/2）



・講師-生徒間で自由に意見交換を行う。
意見を否定してはいけない。

・フィッシングサイトとは、
本物のサイトをそのまま流用される
ケースが多く、本物と偽物は全く
見分けがつかない点を伝える。

・普段の利用時と挙動が変わっていたり
違和感を感じた場合は、親御さんや
先生など身近な大人に相談する。



・あくまで、
当ドキュメントでのまとめであり、
授業の形態、講師と生徒の関係性や
状況により適当な内容を柔軟に伝える
ことが望ましい。

スタディ3 不正アクセス体験から学ぶパスワード管理の重要性 Security Learning SNS for Kids (ハンズオン)

概要

GIGAスクールの普及により、児童でも早い段階で自分用のID/パスワードを持つことが多くなった。
しかし、パスワード管理がずさんになり、他人の情報で勝手にログインしなりすましなどを行うことで、いじめに発展するケースも発生した。パスワード管理は大事だと知ってるだけではなく、しっかりと理解する事が必要と考える。
スタディ３では、模擬SNSサイトを利用して不正アクセス自体を体験する。
不正アクセスを行う事の実体験を通じて、サイバー攻撃者の動きからセキュリティのリスク・脅威を深く理解してもらう。

狙い

実体験から、パスワードを知られてしまう事の危険性を理解する。
不正アクセスのみならず、サイバー攻撃は非常に身近で危険であると理解する。
不正アクセスは絶対に行ってはいけない事であると理解する。
パスワード管理のポイントを学習し、生徒が帰宅した後も御家族と話してもらえる事が望ましい。

事前準備

スタディ３用模擬SNSサイトが、現在のOA環境で利用できるかを確認する。
パソコンやタブレット上のブラウザで下記URLにアクセス。
URL：**https://kids-cyber-security.jp/**

アクセス確認手順

①アクセスするためには、
認証が必要となります。

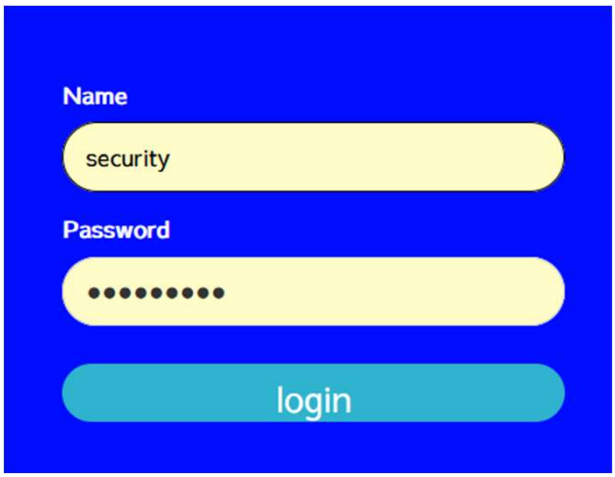
模擬SNSサイトへのアクセスが成功した場合、ユーザー名/パスワードを求められるので、以下を入力しログインします。

ユーザー名：Mirai
パスワード：Securitykids

スタディ３　アクセス確認手順の続き(1/2)

②左図の画面が表示されれば認証は成功しています。

※ 注意 ※
インターネットに制限がかかっている環境や、パソコン・タブレット端末内で制限がかかっている場合など、環境によってはアクセスができない場合があります。その場合は、各環境での対応が必要です。



③授業で利用する画面が最後まで閲覧できるかどうかを確認します。

以下を入力し、模擬SNSサイトへログイン。

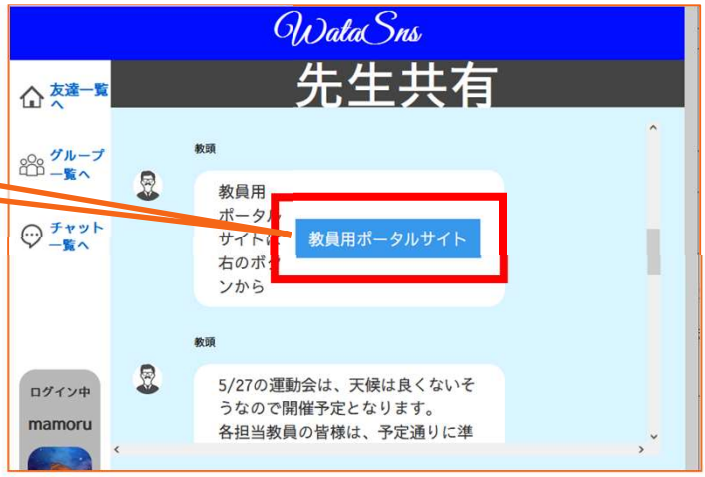
Name：security
Password：Password！

④「グループ一覧」をクリック

⑤「先生共有」をクリック

スタディ３　アクセス確認手順の続き(2/2)

⑥上部へスライドし、
「教員用ポータルサイト」をクリック



⑦以下を入力し、ログインする。

name：mamoru
Password：mamoru19850604

⑧左図の画面が表示されれば、アクセス確認は完了です。

スタディ３　授業の流れ

準備

別途[スタディ３_テキスト]を生徒へ配布する。

パソコンまたはタブレットと、テキスト、ワークシートを用いて授業を行う点を伝える。
グループワーク形式での授業が望ましいため、グループを作成する。
スタディ３用のワークシートを各班に配布する。
※ワークシートは**<u>17ページを裏面とし両面印刷する</u>**

アクセス確認が完了し、SNSのログイン画面が表示されている、
パソコンまたはタブレットを各班で１台用意する。環境により、柔軟に変更することが望ましい。

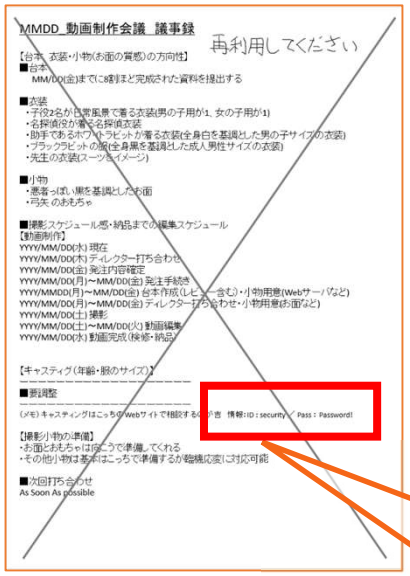
導入

模擬SNSサイトを利用した不正アクセスという攻撃を行う点を伝える。
攻撃者の目線から、サイバー攻撃の怖さや危険性を理解してもらうために行う。

※ 重要 ※
「不正アクセスは、現実では絶対に行ってはいけない」と繰り返し伝えること。

生徒に対して、
サイバー攻撃者は様々な所から、パスワードの情報を盗もうとし、
皆さんは「マモル先生」(模擬サイトで設定されている架空上の先生)
の大事な情報を集めてみましょう、というミッションを与える。

模擬SNSサイトへのログイン


MMDD_動画制作会議_議事録

再利用してください

【台本、衣装・小物(お面の質感)の方向性】
■台本
MM/DD(金)までに雛形まで完成された資料を提出する

■衣装
・子役2名が自宅風景で着る衣装(男の子用が1、女の子用が1)
・名探偵役が着る名探偵衣装
・助手であるホワイトラビットが着る衣装(全身白を基調とした男の子サイズの衣装)
・ブラックラビットの衣装(全身黒を基調とした成人男性サイズの衣装)
・先生の衣装(スーツをイメージ)

■小物
・悪者っぽい、黒を基調としたお面
・弓矢 のおもちゃ

■撮影スケジュール感・納品までの編集スケジュール
【動画制作】
YYYY/MM/DD(火)現在
YYYY/MM/DD(木)ディレクター打ち合わせ
YYYY/MM/DD(金)発注内容確定
YYYY/MM/DD(月)～MM/DD(金)発注手続き
YYYY/MMDD(月)～MM/DD(金)台本作成(レビュー含む)・小物用意(Webサーバなど)
YYYY/MM/DD(月)～MM/DD(金)ディレクター打ち合わせ・小物用意お面など)
YYYY/MM/DD(土)撮影
YYYY/MM/DD(土)～MM/DD(火)動画編集
YYYY/MM/DD(水)動画完成(検修・納品)

【キャスティング(年齢・服のサイズ)】
■要調整
(メモ)キャスティングはこっちのWebサイトで相談する

吉　情報:ID：security／Pass：Password!

【撮影小物の準備】
・お面とおもちゃはこっちで準備してくれる
・その他小物は基本はこっちで準備するが臨機応変に対応可能

■次回打ち合わせ
As Soon As possible

このカリキュラムでは、「マモル先生」が用意した紙の裏紙内に情報が書かれてしまっているという設定となっている。

(例)マモル先生は環境には配慮するが、
　　大事な情報には配慮しなかった

これは、パスワード流出ケースのごくごく１例に過ぎず、様々な場所・要因でパスワードは流出してしまう点を伝える。

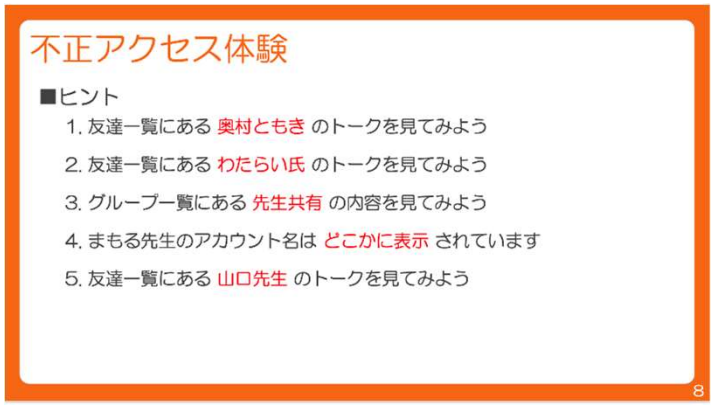
スタディ３　授業の流れ（続き）

ハンズオン開始

全ての児童が模擬SNSサイトにログインできたらハンズオンを開始する。模擬SNSサイトを自由に触ってもらい不正アクセス（秘密の部屋へのログイン）を体験してもらう。この時間に合わせて、ワークシートの課題１．～３．を各自に記載してもらう。

ヒントの提示

擬似SNSは色々な人のトークがあり、情報量が多く、児童が不正アクセスを成功させるために必要な情報に気づけない危険性が高い。効率良く授業を進めるため、３分～５分ごとにヒントを提示することをお勧めする。本スライドはアニメーションになっており、１行ずつ画面に表示させることが可能である。



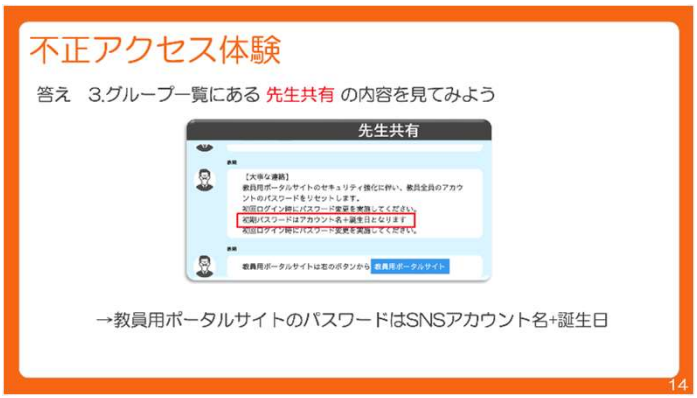
ハンズオン終了

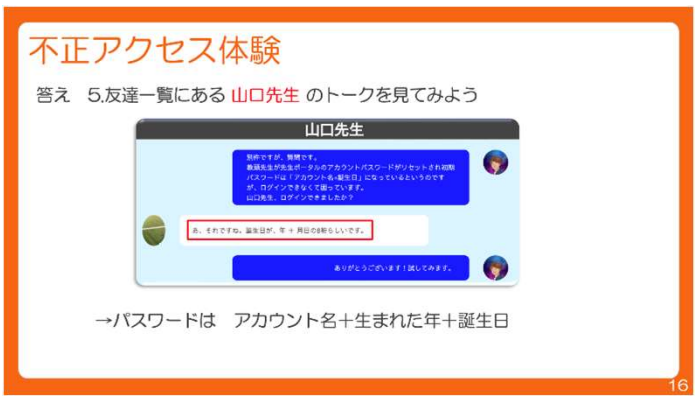
ハンズオンは授業時間を考慮して、２０分程度で区切ることをお勧めする。ハンズオン時間を終了したら、ワークシートの記入状況を確認し、課題３が未記入であれば、少し時間を設けて、課題３を記入してもらう。

学びを発表

今回の不正アクセス体験を通じて、児童が感じたことを自由に発表してもらう。最終的に不正アクセスに成功した児童と成功しなかった児童では感じた内容が異なることも想定されるが、ここではみんなの意見を自由に発表してもらう。
解説や一般論としてパスワード管理ついて学んで欲しいことは、以降の解説にて説明して、学びを与えるようにする。

スタディ３　解説





解説では、まず最初にヒントに対する答えを１個ずつ紹介する。これら５つのヒントを組み合わせることで、ハンズオンサイトにログインするために必要な、アカウント名とパスワードを推測することが可能となる。

・ヒント１．からは、奥村ともきのトークを見ることで、まもる先生の誕生日が6月4日であることが確認できる。

・ヒント２．からは、わたらい氏のトークを見ることで、まもる先生は、1985年の生まれであることが確認できる。

・ヒント３．からは、先生共有の内容を見ることで、今回のハンズオンのゴールである教員用ポータルサイト（秘密の部屋）にログインするためのパスワードはSNSアカウント名+誕生日であることが確認できる。

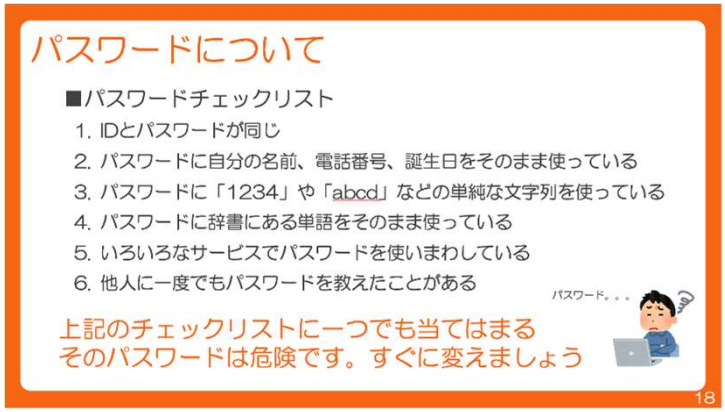
・ヒント４．からは、ログインするためのアカウント名は、SNSの左下に表示されるているmamoruであることが確認できる。

・ヒント５．からは、ヒント３．で提示されたパスワードのヒントを捕捉しており、生年月日が８桁（19850604）であることが確認できる。

スタディ３　解説

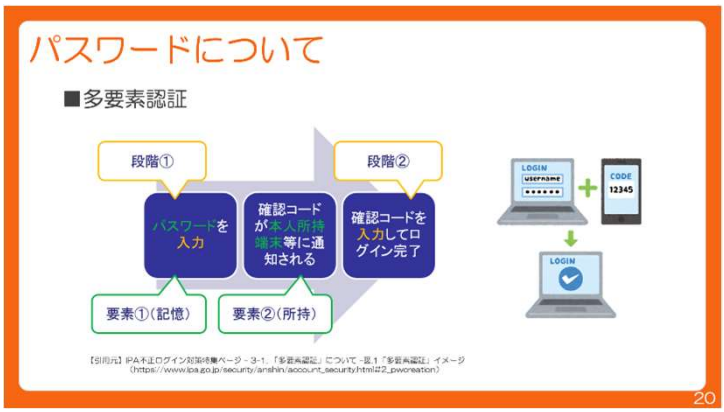
ヒント１．～５．の情報を全て加味すると、秘密の部屋にログインするためのアカウント名、パスワードはどこにも公開されていないにも関わらず、以下であることが推測され、不正アクセスが出来てしまう。

アカウント　mamoru
パスワード　mamoru19850604



・パスワードについて児童に学んで欲しいことを解説。
１～４はいずれも問題のあるパスワードであり、利用は避けるように注意すること。
また色々なサービスで利用しているパスワードは別のものを利用する注意し、同じパスワードは使いまわさないように伝える。同じパスワードを使いまわしていると１つのサービスから情報が漏洩すると他のサービスにも不正ログインされる危険性がある。

・安全なパスワードにするには、１～３で記載しているように、色々な種類の文字を利用した複雑なパスワードにすることと、サービスごとに異なるパスワードを利用することを伝える。



最近はユーザアカウントがメールアドレスのサービスが多く、パスワードを機械的に推測して、何度もログインを試行することで不正にログインされる危険性もある。このような問題に対策するために、多要素認証という技術がある。
ログイン時に、ユーザアカウントとパスワードだけでなく、追加の認証手段を求めるため、多要素と言われている。一般的には、ランダムな文字列を入力したり、交通系のIDカードや、マイナンバーカードといったカードや、指紋や顔、指静脈や虹彩などの生体情報を用いる。
以下のサイトに詳細が紹介されている。

https://www.ipa.go.jp/security/anshin/account_security.html#2_pwcreation

スタディ3：Security Learning SNS for Kids

クラス：　　年　　組　　グループ：　　日付：　　年　　月　　日

学習テーマ：インターネットは危険がいっぱい！
WataSNSでパスワードの重要性を学ぼう！

課題1：mamoruさんの情報を集めましょう。
※どんな情報を集められるか自由に書いてみましょう。

課題2：教職員用ポータルサイトのURL、ID、パスワード を探しましょう。

教職員用ポータルサイトURLの情報のありか：

ID：　　パスワード ：

課題3：パスワードを他人に知られてしまうと、どんな事が起きるか考えてみましょう？
※気づいた事を自由に書いてみましょう

MMDD_動画制作会議　議事録

再利用してください

【台本　衣装・小物（お面の質感）の方向性】

■台本

MM/DD(金)までに8割ほど完成された資料を提出する

■衣装

・子役2名が日常風景で着る衣装(男の子用が1、女の子用が1)
・名探偵役が着る名探偵衣装
・助手であるホワイトラビットが着る衣装(全身白を基調とした男の子サイズの衣装)
・ブラックラビットの服(全身黒を基調とした成人男性サイズの衣装)
・先生の衣装(スーツをイメージ)

■小物

・悪者っぽい黒を基調としたお面
・弓矢 のおもちゃ

■撮影スケジュール感・納品までの編集スケジュール

【動画制作】

YYYY/MM/DD(水) 現在
YYYY/MM/DD(木) ディレクター打ち合わせ
YYYY/MM/DD(金) 発注内容確定
YYYY/MM/DD(月)～MM/DD(金) 発注手続き
YYYY/MMDD(月)～MM/DD(金) 台本作成（レビュー含む）・小物用意(Webサーバなど)
YYYY/MM/DD(月)～MM/DD(金) ディレクター打ち合わせ・小物用意(お面など)
YYYY/MM/DD(土) 撮影
YYYY/MM/DD(土)～MM/DD(火) 動画編集
YYYY/MM/DD(水) 動画完成（検修・納品）

【キャスティグ（年齢・服のサイズ）】

――――――――――――――――――――

■要調整

――――――――――――――――――――

（メモ）キャスティングはこっちで相談する予定。　　備忘メモ：ID : security ／ Pass : Password!

【撮影小物の準備】

・お面とおもちゃは向こうで準備してくれる
・その他小物は基本はこっちで準備するが臨機応変に対応可能

■次回打ち合わせ

As Soon As possible

スタディ４　ゲームで学ぶCyberSecurity

概要

児童の興味を引くことや意欲を高める学習方法であるゲーミフィケーションの教育コンテンツとして、セキュリティ擬似体験型アドベンチャーゲーム「CYBER SECURITY =The Seeds of Salvation=」を作成した。

サイバーセキュリティの世界を疑似体験させるために、ゲーム内には現実のセキュリティ対策でも実際に利用するツールやインシデント事例など、リアルなコンテンツを散りばめている点が特徴である。

ゲームプレイヤーのサイバーセキュリティに対する興味関心を喚起し、更なる学習を促進するため、2種類のゲームモード（ストーリーモード、学習モード）を用意した。

◆ストーリーモード：ストーリーを通じて、サイバーセキュリティの世界の疑似体験が可能。
◆学習モード： サイバーセキュリティの更なる学習に役立つコンテンツを紹介。

◆ストーリーモード
Stage1 Prologue = やさしい
Stage2 Incident = やさしい
Stage3 Network = やさしい
Stage4 Cyber Attack = やや難しい
Stage5 Operation = 難しい
Stage6 Epilogue = やさしい

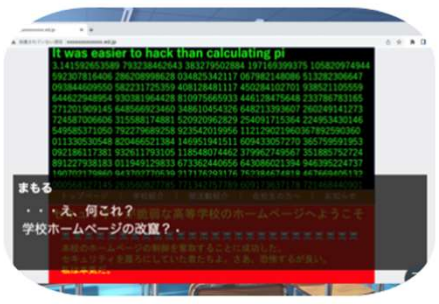
◆学習モード
Study1 CyberSecurity = やさしい
Study2 P4ssw0rd = やさしい
Study3 Crypto = やさしい
Study4 FinalExamination = やや難しい
Study5 CTF = やや難しい
Study6 Hardening = やや難しい

※児童だけでなく大人も学習出来る難易度を設定した。小学生には意味が伝わりづらい言い回しや単語もある。児童自身で調べるのが望ましいが、必要に応じて、教師・保護者がフォローを行う。

狙い

アドベンチャーゲームを通じて、サイバーセキュリティに関連するインシデント、事件、事故を擬似体験することで、ゲームプレイヤーにサイバーセキュリティのリスク・脅威を認識させ、興味関心を喚起することができる。

参考情報：ゲーム画面紹介



スタディ４　準備

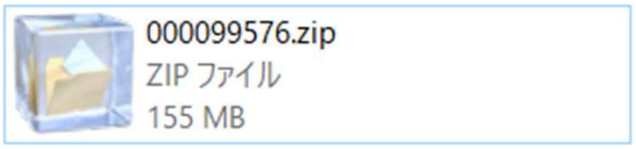
準備

・IPAの以下公開サイトへアクセスする。

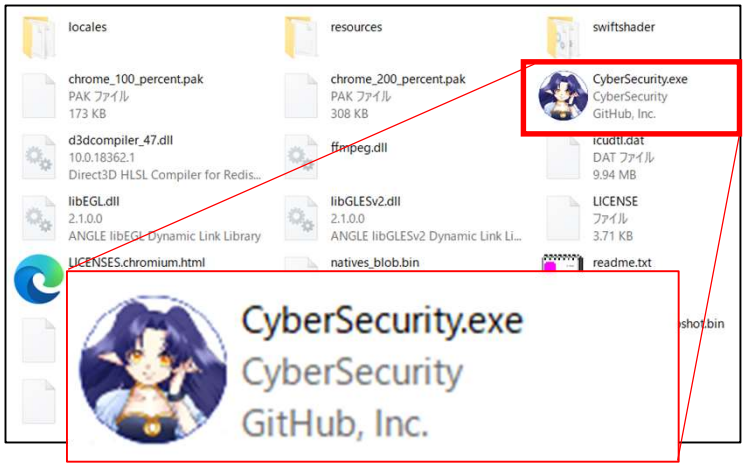
【IPA公開サイトURL】
IPA>産業サイバーセキュリティセンター>事業内容のご案内>中核人材育成プログラム>未来のKidsサイバーセキュリティ教室 ～No SEC No Life～
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/sec-kids.html

・ゲーム用ファイルをパソコンへダウンロードする。

セキュリティ擬似体験型アドベンチャーゲーム「CYBER SECURITY =The Seeds of Salvation=」

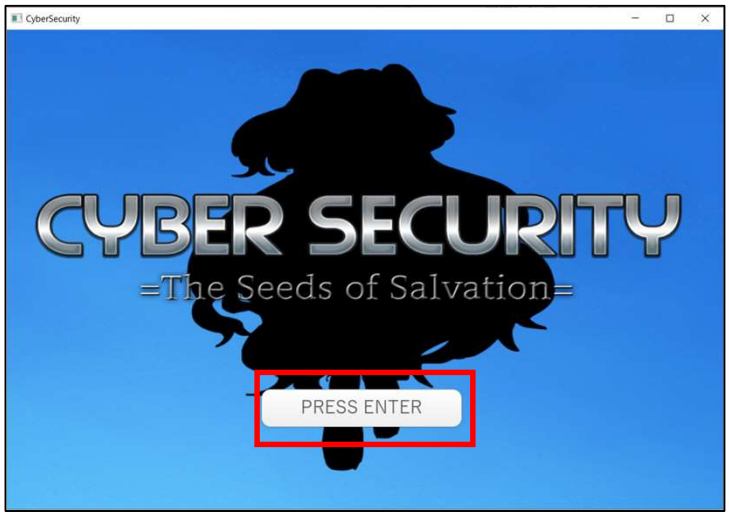


・ダウンロードされたファイルを解凍する。



・解凍されたフォルダを開き、“CyberSecurity.exe” を実行する。

※ご利用の環境やセキュリティ製品によっては、セキュリティ設定の警告画面などが表示される場合がある。



・左図画面が表示されれば、プレイ可能。“PRESS ENTER” をクリックし、プレイ。

※操作方法や詳細な説明内容は、ダウンロードしたフォルダ内の、“readme.txt” を参照すること。

活用方法①：授業で実施する

導入

最近のサイバー攻撃事例(※)などを題材として、サイバーセキュリティの脅威が身近に溢れていることを講師と生徒にて対話する。
※児童にとっても身近なサイバー攻撃事例が望ましい。
　(例)2022年5月 某アニメ会社に対するサイバー攻撃など

デジタル社会において、サイバーセキュリティは将来必要な内容であり自分事として興味関心持って欲しいことを強調する。

教師は授業で実施するゲームモード・ステージを指定する。

ゲームプレイ

事前に準備しておいた端末で個人またはグループ毎にゲームプレイをする。
※ゲームプレイ中も児童は自由に意見交換を実施することが望ましい。

発表

個人またはグループ毎にゲームプレイした感想を発表する。
※一人一人児童の意見を尊重する。

まとめ

教師のゲームプレイした感想を児童に共有して授業を終了する。
児童がサイバーセキュリティに興味を持ち、授業で指定したゲームモード・ステージ以外もゲームプレイしたいという要望があった場合には、学校でゲームプレイな端末を貸与するか、ゲームの準備手順を示すことが望ましい。

活用方法②：児童・保護者に対して本ゲームを紹介・推奨する

ゲームプレイ

児童・保護者に本ゲームの内容・準備手順を紹介し、宿題による自宅でのゲームプレイを推奨する。

※その他にも、自習の時間など、様々な利用形態を検討することが出来る。
　学校、児童・保護者の環境や状況に合わせて本ゲームを活用する。
　その際、強制はせずに児童の自主性を尊重することが望ましい。

参考情報

インターネットの安全・安心ハンドブック
https://security-portal.nisc.go.jp/handbook/

IPA
＃ 今こそ考えよう　情報モラル　セキュリティ
https://www.ipa.go.jp/security/keihatsu/imakoso/

IPA
映像で知る情報セキュリティ
https://www.ipa.go.jp/security/keihatsu/videos/index.html

IPA
情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

IPA
インターネット安全教室
https://www.ipa.go.jp/security/keihatsu/net-anzen.html

文部科学省
情報モラル学習サイト
https://www.mext.go.jp/moral/#/

警察庁
サイバーポリスエージェンシー
https://www.npa.go.jp/cybersecurity/index.html

IPA
ここからセキュリティ！
https://www.ipa.go.jp/security/kokokara/index.html