米子南高校 2年生
情報セキュリティ講座

Web公開用

サイバー攻撃を疑似体験しながら学ぶ
～企業と顧客を守る「信用」と情報セキュリティ～

2026年1月20日（火）

講師紹介

〇若林 遥大（わかばやし はると）

▶専攻科生産システム工学専攻 2年（大学4年相当）

→プログラミング・情報セキュリティ・工学教育などについて研究

▶鳥取県警察サイバー防犯ボランティア

→主に，Webセキュリティ演習ツールの開発 など

▶米子高専サイバーセキュリティ同好会 副会長

→高専生がセキュリティについて啓発する活動の後進育成

本日の内容

１．情報セキュリティの基本

▶情報セキュリティとは？

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

③ネット上に公開された情報から個人情報を収集してみよう

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

３．おわりに

１．情報セキュリティの基本

〇企業と顧客を守る情報セキュリティ

▶企業の規模・個人にかかわらず被害を受ける時代

→誰もが対策や意識を高く持つことが重要

▶世の中の大多数は顧客がいるから成立する

→企業にとって社会的な信用は非常に重要

▶情報セキュリティにかかわるトラブルは企業の責任

→十分な対策をしていないと損害賠償などの可能性がある…

→事業が停止することで、資金的な問題が発生する懸念も

1．情報セキュリティの基本

○「情報セキュリティ対策」とは？

▶情報の盗難・破壊・サービス提供の妨害からどれだけ守れるか！

→自身の利益や継続的な事業のために

▶サービスを提供する側の社会的責任

→利用者の情報を預かる立場として信用・信頼のために

○「不正アクセス」とは？

▶正当な権限を持たないものが，ネットワークを通じて情報システムに不正にアクセスすること

1．情報セキュリティの基本

○「不正アクセス」がどのように発生するのか…

①調査（事前調査）

→「脆弱性のある入り口ないかな～，あれここなら突破できるかも」

②発見（権限取得）

→「パスワード解析して，正規のユーザーのふりをするぞ～」

③攻撃（不正実行）

→「アクセスできたから，ファイル盗んだり，削除して邪魔するぞ」

→「このユーザーの友達や仕事仲間にも攻撃を仕掛けるぞ～」

④制御（後処理）

→「また来るときのための通路の準備しとこうかな～」

→「不正アクセスした証拠を隠滅しとこう」

演習の準備

①Webブラウザを立ち上げてください

②アドレスバーにURLを入力してアクセスしてください

→ https://visusec.jp/

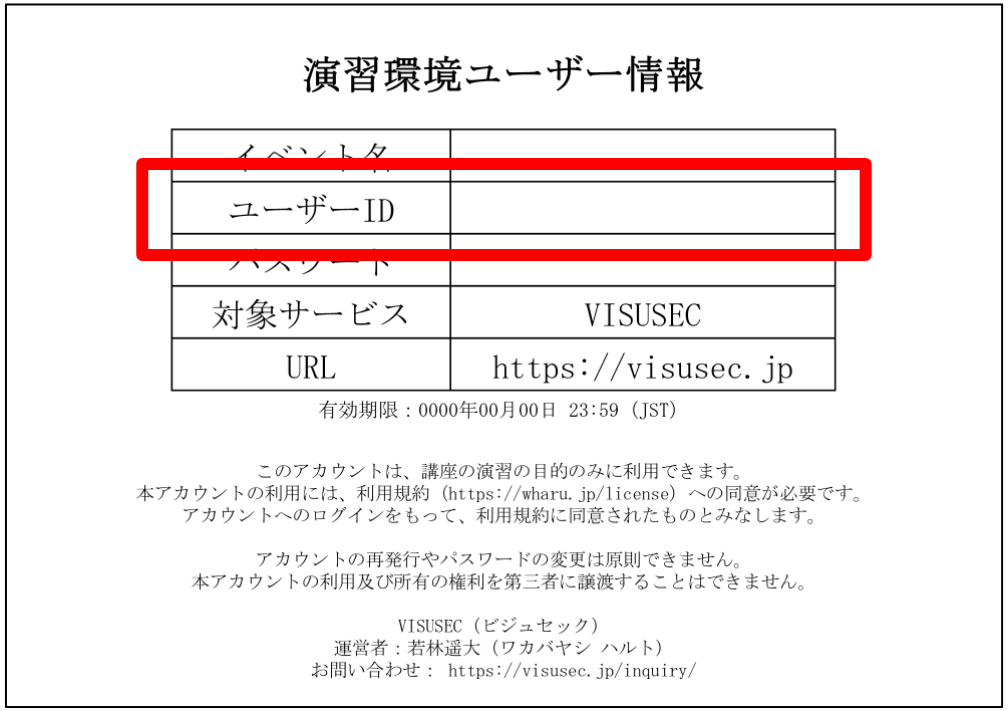
※VISUSEC（ビジュセック）は、若林が開発をしている
情報セキュリティに関する教材を提供するプラットフォームです

演習の準備

③表示されたページ画面中央，緑の「ログイン」ボタンを押してください

演習の準備

④ユーザーIDを入力し，「次へ」を押してください



演習環境ユーザー情報

イベント名	
ユーザーID	
パスワード	
対象サービス	VISUSEC
URL	https://visusec.jp

有効期限：0000年00月00日 23:59（JST）

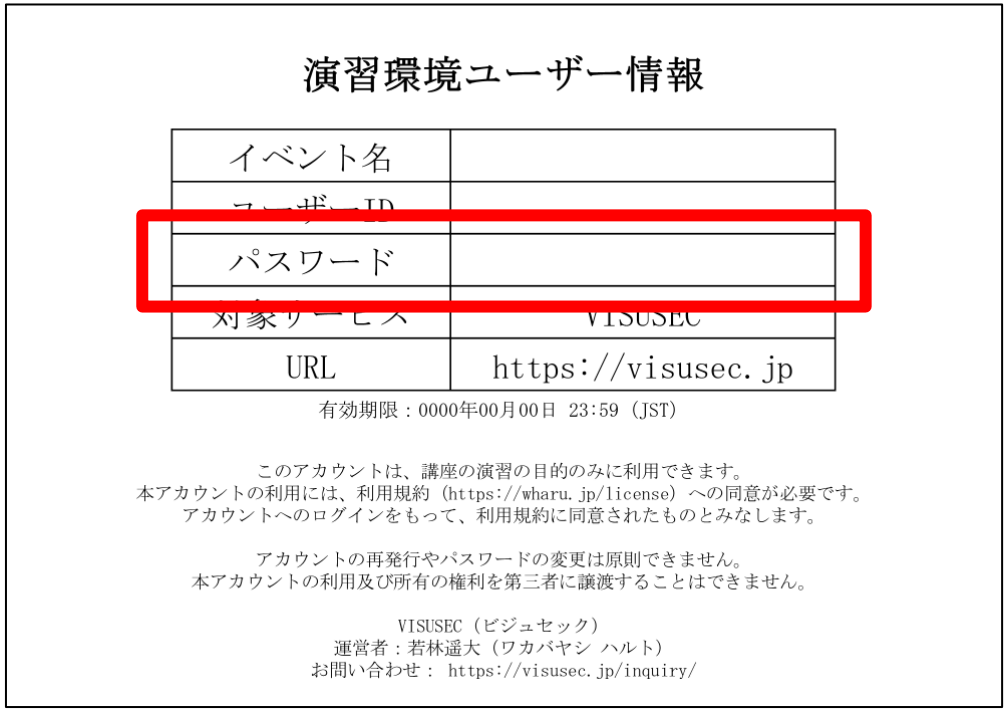
このアカウントは、講座の演習の目的のみに利用できます。
本アカウントの利用には、利用規約（https://wharu.jp/license）への同意が必要です。
アカウントへのログインをもって、利用規約に同意されたものとみなします。

アカウントの再発行やパスワードの変更は原則できません。
本アカウントの利用及び所有の権利を第三者に譲渡することはできません。

VISUSEC（ビジュセック）
運営者：若林遥大（ワカバヤシ ハルト）
お問い合わせ： https://visusec.jp/inquiry/

演習の準備

⑤パスワードを入力し，「ログイン」ボタンを押してください



演習環境ユーザー情報

イベント名	
ユーザーID	
パスワード	
対象サービス	VISUSEC
URL	https://visusec.jp

有効期限：0000年00月00日 23:59（JST）

このアカウントは、講座の演習の目的のみに利用できます。
本アカウントの利用には、利用規約（https://wharu.jp/license）への同意が必要です。
アカウントへのログインをもって、利用規約に同意されたものとみなします。

アカウントの再発行やパスワードの変更は原則できません。
本アカウントの利用及び所有の権利を第三者に譲渡することはできません。

VISUSEC（ビジュセック）
運営者：若林遥大（ワカバヤシ ハルト）
お問い合わせ： https://visusec.jp/inquiry/

演習の準備

⑥ニックネームを決めてください

山田 太郎さんの場合は，
ステップ①は，苗字の「Y」
ステップ②は，名前の「T」
を選択します．

ステップ③は，自由に
好きな数字を選んでください．

演習の準備

⑦ログイン完了

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇そもそもパスワードって

▶正規の利用者であるか認証するためのあらかじめ決められた文字列

〇パスワードに求められること

▶本人がきちんと管理できる

→他人に知られないように管理する

→もちろん自分自身も忘れないこと

▶簡単に推測・解読されないこと

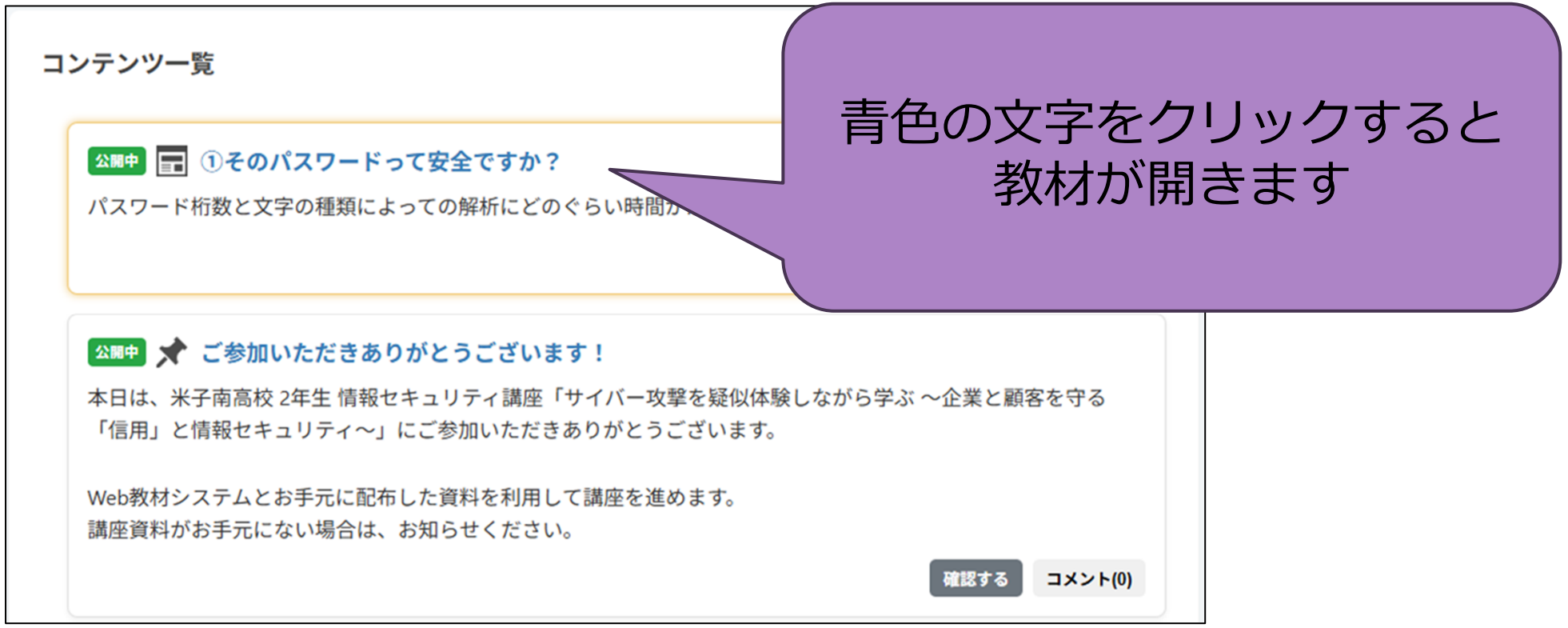
→大文字・小文字・数字・記号などを組み合わせる

→なるべく桁数を多くする

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○教材を配信します



２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○実際に体験してみよう

▶攻撃者の視点でパスワードを解析して，強度を確認しよう

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇総当たり攻撃（ブルートフォースアタック）

▶想定されるパスワードをすべて試す

〇総当たり攻撃の仕組み

▶文字を徐々に変えながら，すべてのパターンを試す

→桁数による違いと文字の種類の組み合わせによる変化を体験します

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードの桁数による違い

▶まずは，4桁「yona」で試してみましょう

補足

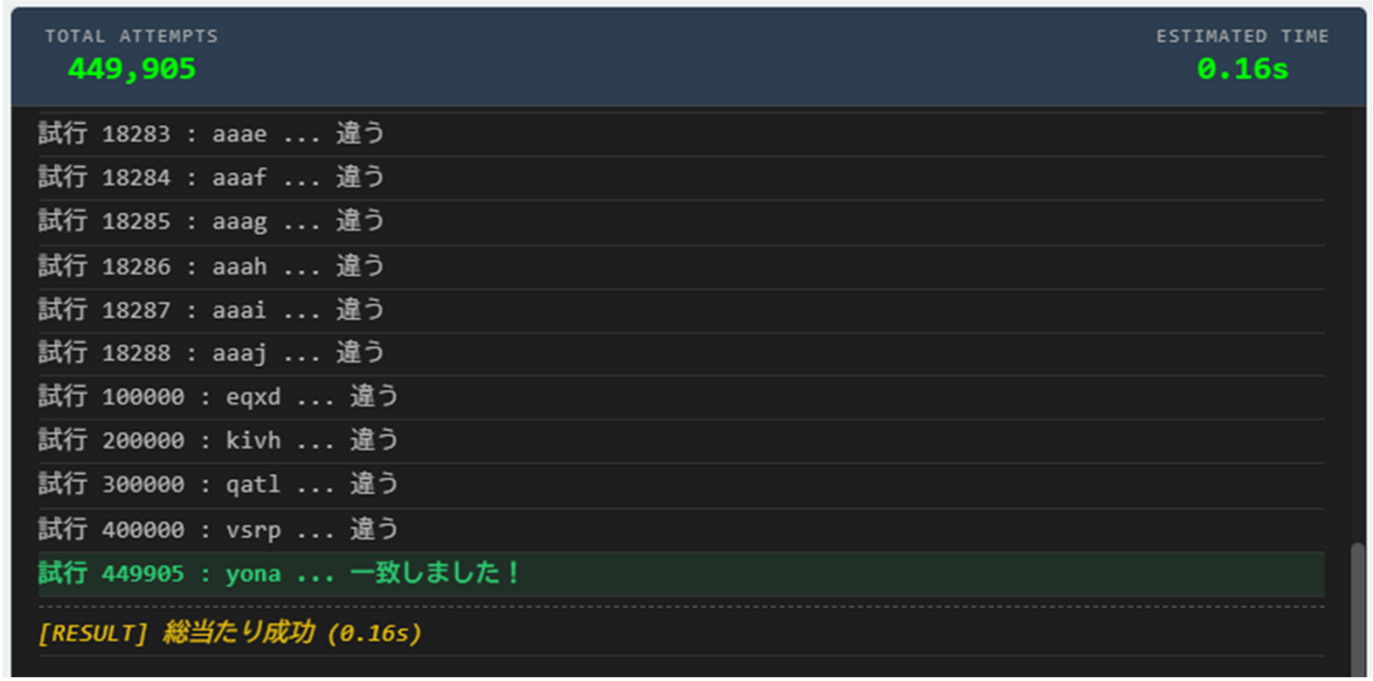
実行時間の短縮を目的に
文字の種類を小文字の
アルファベットに
絞って解析します

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードが4桁「yona」の場合

▶4桁の場合は，**449,905**通りの試行をしたようです

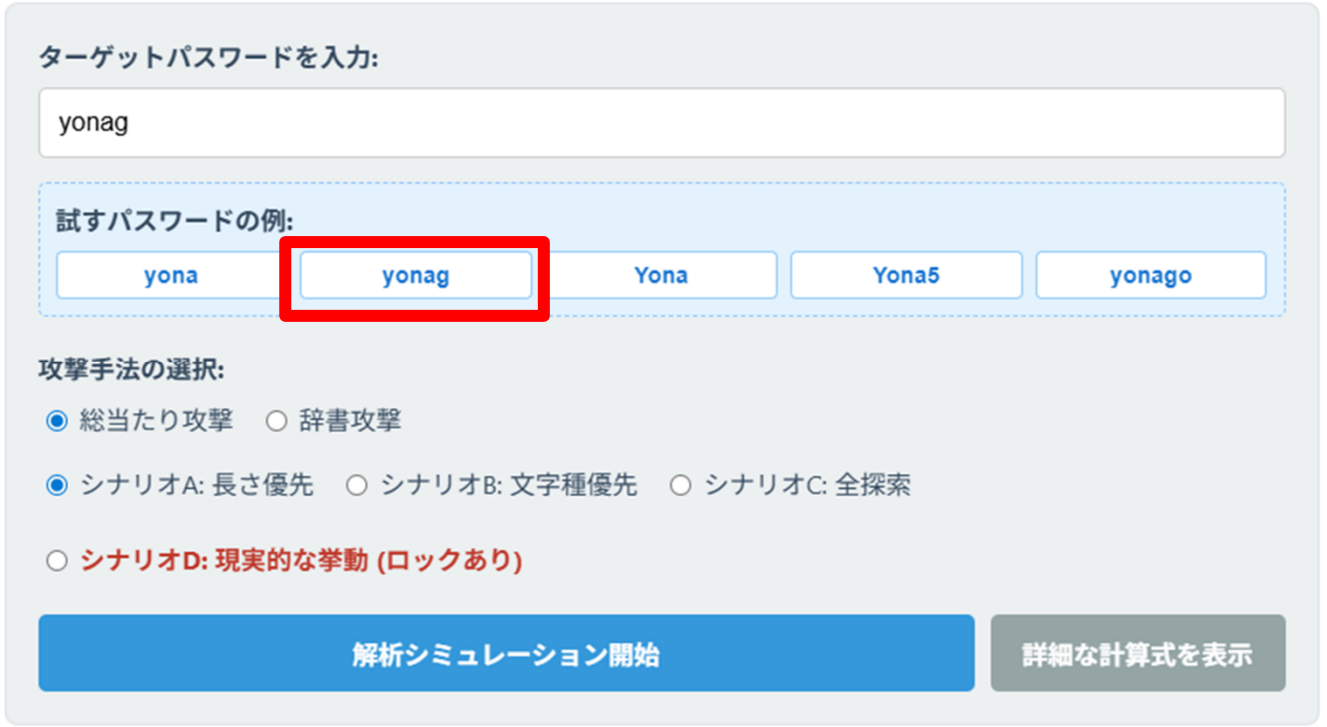


２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードの桁数による違い

▶次は，5桁「yonag」で試してみましょう

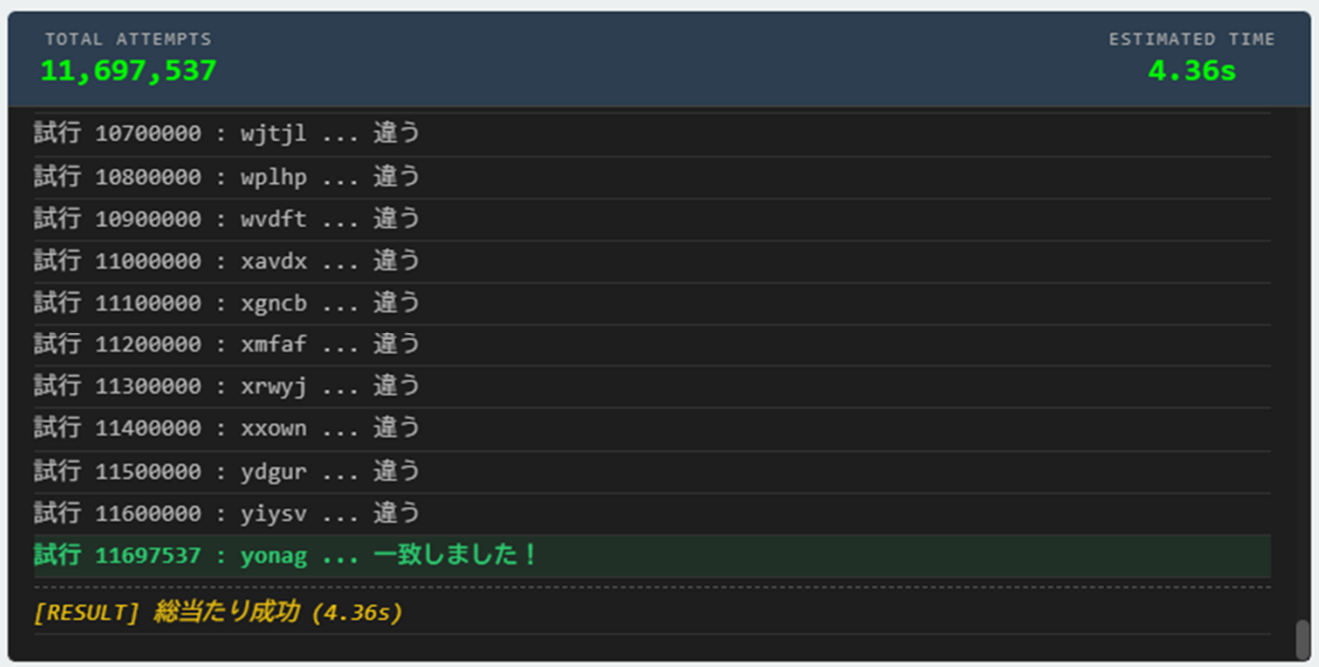


２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードが5桁「yonag」の場合

▶5桁の場合は，**11,697,537**通りの試行をしたようです



２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇桁数の違いによる試行回数を比べてみましょう

パスワード	試行回数
yona	449,905
yonag	11,697,537
yonago	304,135,977

〇1桁増えるごとに試行回数は非常に多くなる！

▶短いパスワードほど解析がすぐ終わってしまう！

→パスワードの桁数はなるべく多いほうがいい

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇複数種類の記号を含むと何がいいのだろうか？

▶今回は4文字「yona」を徐々に変化させながら体験します

補足

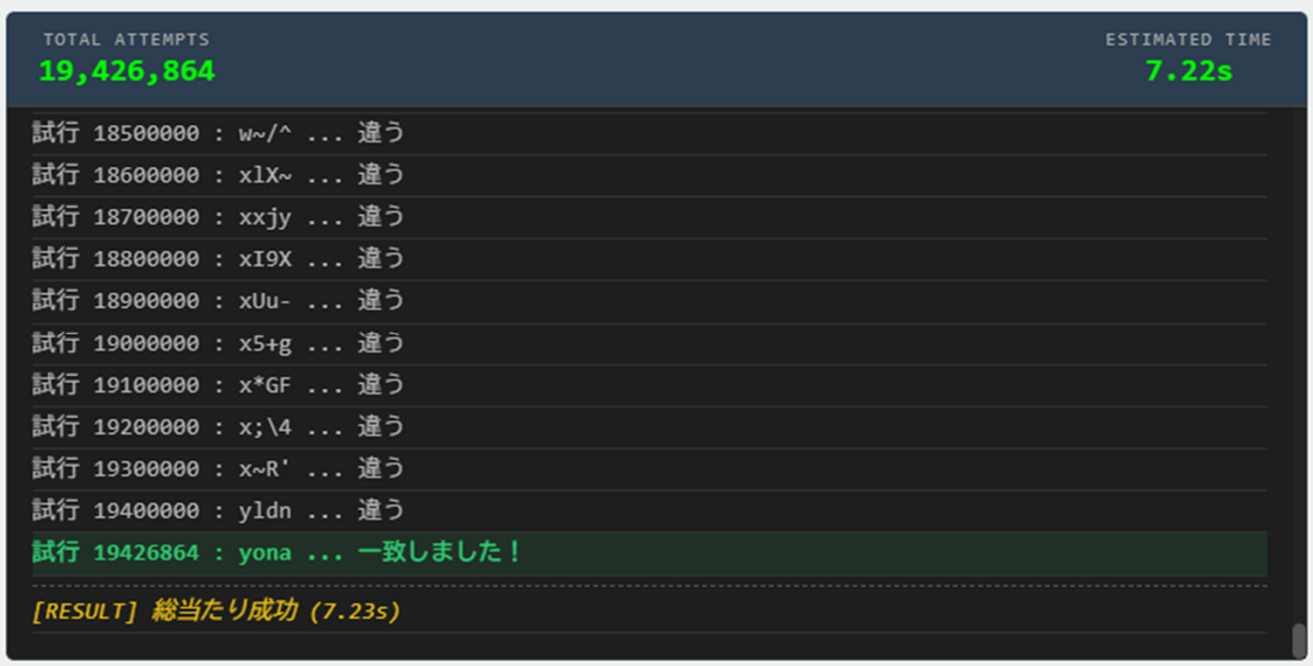
実行時間の短縮を目的に
文字数が分かっている
状態で解析をします

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードが4桁「yona」の場合

▶4桁の場合は，**19,426,864**通りの試行をしたようです

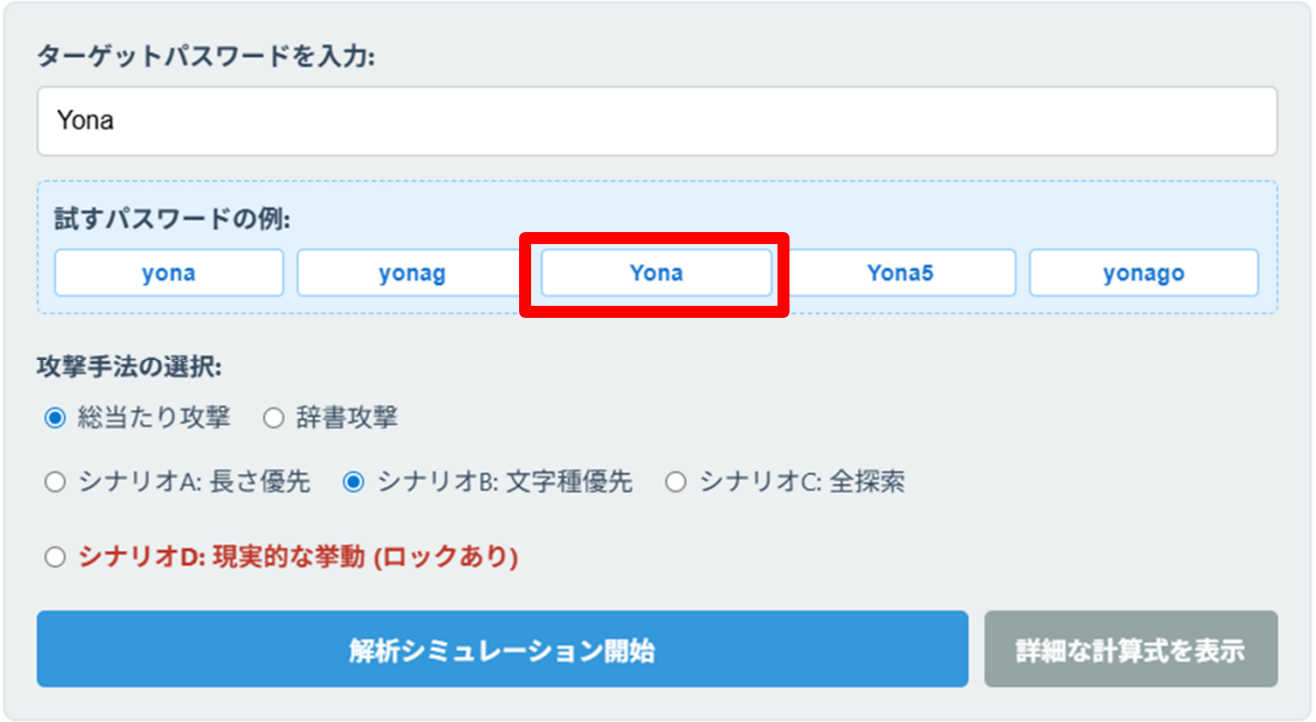


２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○「y」を大文字「Y」にしてみましょう

▶「Yona」で実行してみましょう

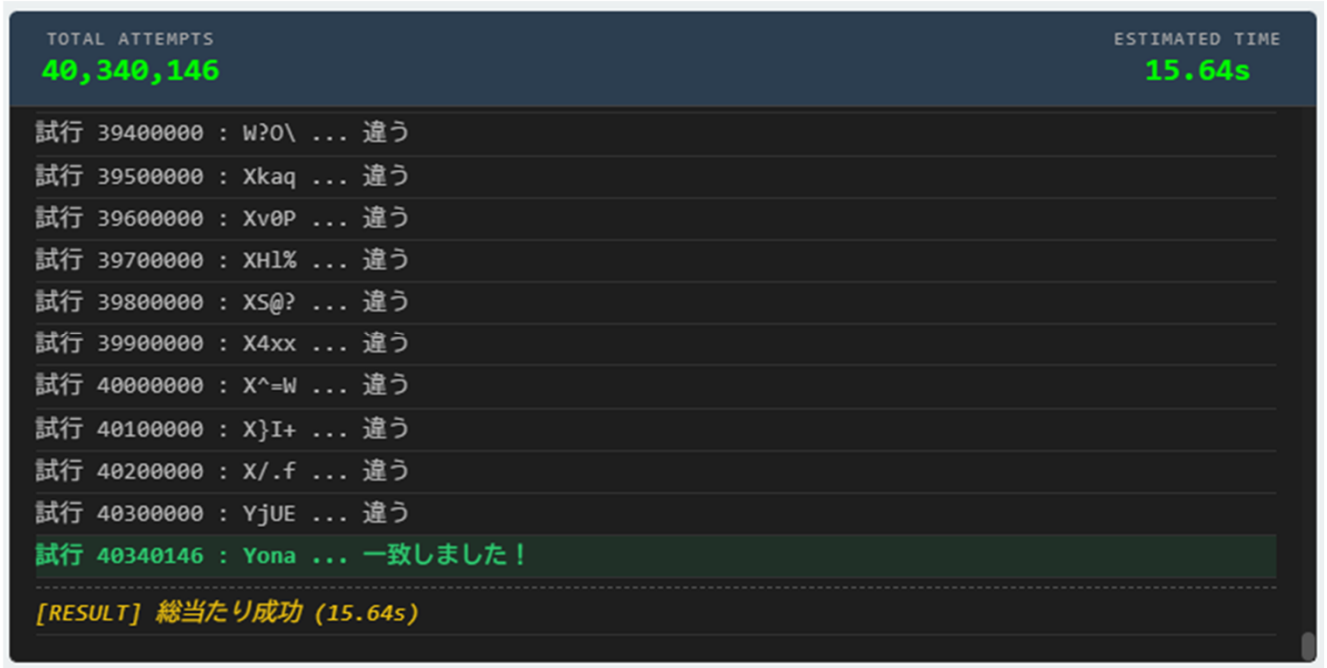


２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○パスワードが4桁「Yona」の場合

▶4桁の場合は，**40,340,146**通りの試行をしたようです



２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇文字の種類の違いによる試行回数を比べてみましょう

パスワード	試行回数
yona	**19,426,864**
Yona	**40,340,146**

〇文字の種類が1種類増えるだけでも試行回数に大きな違いが！

▶複数の種類の文字を組み合わせることは大きな効果がある

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇辞書攻撃

▶パスワードによく利用される単語や，被害者ゆかりの情報を使う

〇辞書攻撃の仕組み

▶パスワードの解析にあたり，辞書（攻撃対象）

→今回は，パスワードによく利用される文字列を用意しました

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○よく使われるパスワードって何でしょう？

▶パスワードを覚えるために
簡単にしている

▶初期パスワードから
変えていない…

ランキング	世界	日本
1	123456	123456789
2	123456789	password
3	12345678	12345678
4	password	1qaz2wsx
5	qwerty123	asdfghjk
6	qwerty1	asdf12345
7	111111	aa123456
8	12345	asdf1234
9	secret	123456
10	123123	1234567890

Top 200 Most Common Passwords - Nord Security
https://nordpass.com/most-common-passwords-list/

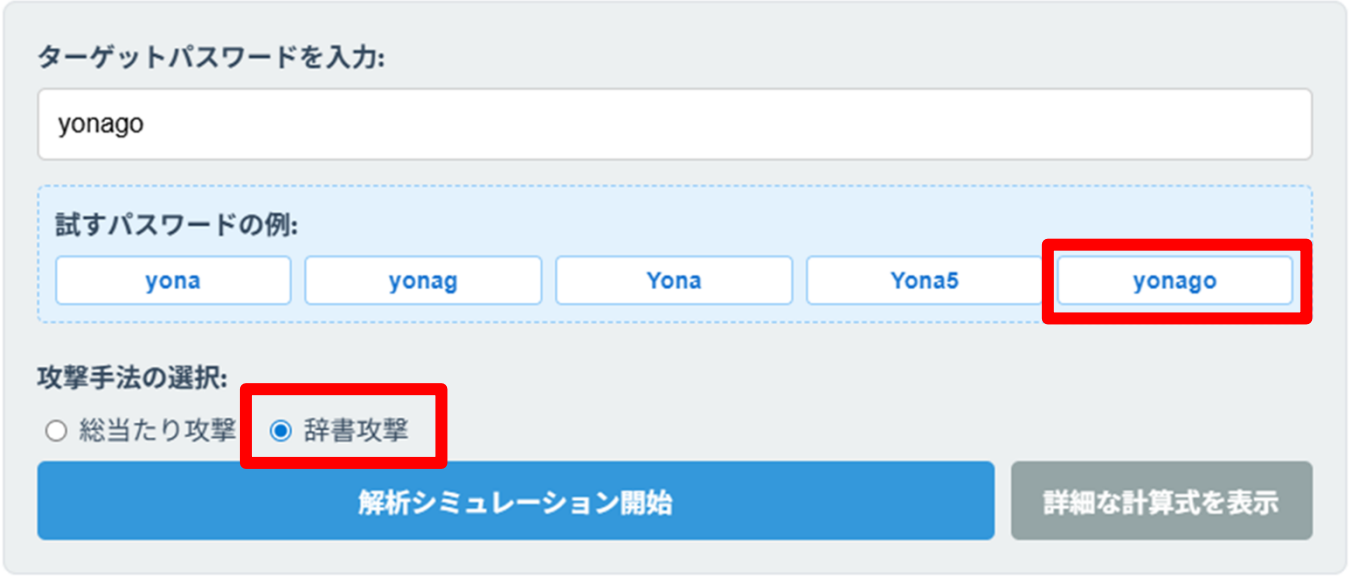
２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○辞書攻撃を試してみよう

▶先ほど総当たり攻撃で利用した「yonago」で試してみましょう

→総当たり攻撃では，**304,135,977**通り試行しましたが…

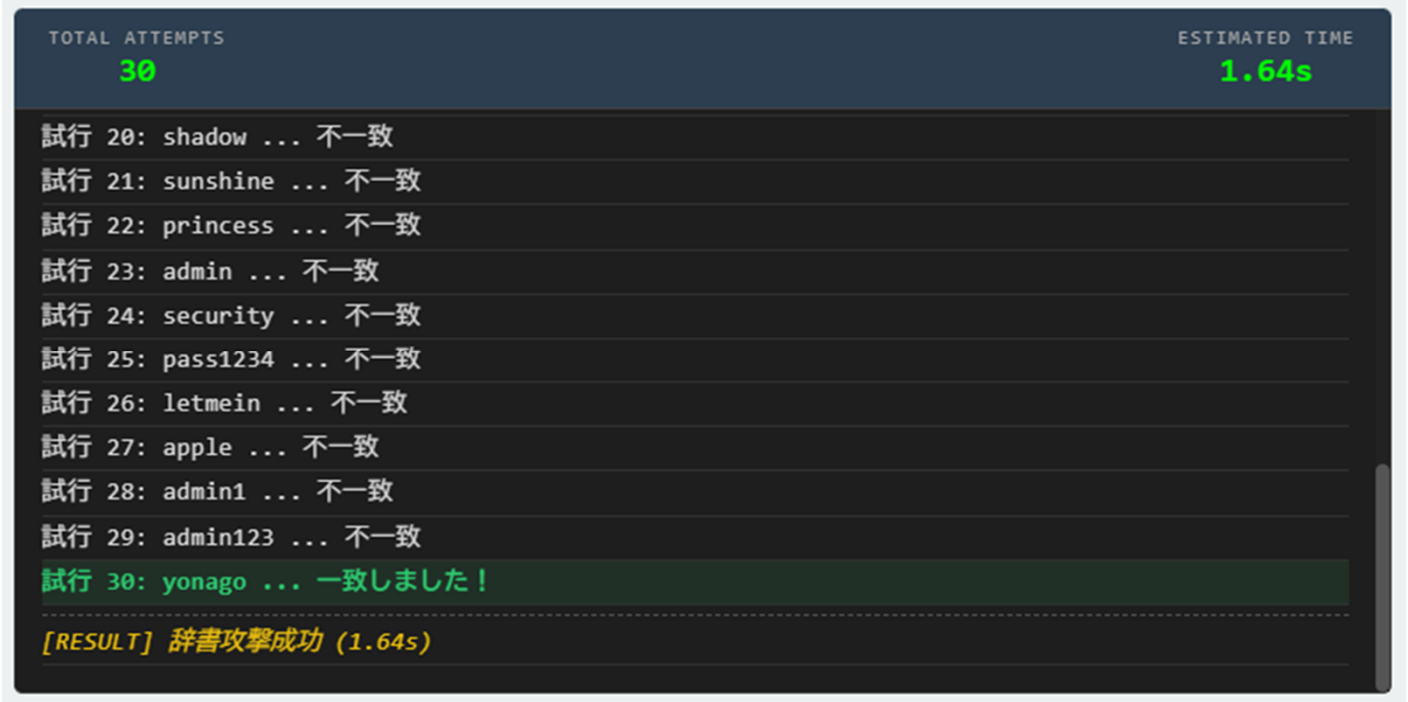


２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

○辞書攻撃「yonago」の場合

▶たったの**30**通りで解析が終わりました…



２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇辞書攻撃と総当たり攻撃を比較してみる

パスワード	試行回数
総当たり攻撃	**304,135,977**
辞書攻撃	**30**

〇あらかじめ辞書（攻撃リスト）に「yonago」を登録していました

▶攻撃者は身近な人の可能性もあります

→身近な情報やSNSに公開しているような情報は避けましょう！

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

〇実行結果でわかること

▶桁数は多いほうが良い（長すぎても覚えられないと意味がない…）

▶大文字・小文字・数字・記号などを組み合わせることが大切

▶身近な情報やSNSに公開しているような情報は避ける

→使いまわしを避けることも重要

→InstagramやTikTokのIDとパスワード共通にしてない？

〇パスワードが解析されると…

▶不正侵入，乗っ取りの危険性がある！

→踏み台にされて，家族や友人が2次被害を受けることも…

２．企業と顧客を守る「信用」と情報セキュリティ～

①そのパスワードって安全ですか？

Oディスカッションしよう

▶理想的なパスワードのために文字種・長さの両方を意識すると複雑になりすぎて覚えられません。どうするべきでしょうか…。

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇情報流出・盗聴の被害を防ぐには…

▶情報を第三者にわかりにくい形に変換をする

→暗号化

〇身近な暗号化って何がある？

▶インターネット通信

→Webサイトのアクセス時やデータのやり取りを秘匿する

▶ファイルやストレージの暗号化

→パソコン内のファイルやクラウドストレージなど

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇公衆Wi-Fiとは

▶公共施設や商業施設などで利用できる無料のWi-Fi通信

→パスワードなどが設定されず，だれでも通信の傍受が可能に

〇通信が傍受されると…

▶専門知識と装置を用いることで，他人の通信を解析可能

→情報のやり取りが丸見えで，それを悪用されることも…

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇通信内容が丸見え！？

▶公衆Wi-Fiで特に危険なのが，通信内容が暗号化されていない時

→URLが「http」から始まるもの

〇通信内容が暗号化されないと…

▶アクセスしたWebサイトの情報

→他人に自身の趣味嗜好が見られる…ストーカなどの要因にも

▶メールアドレスやパスワード・住所などの個人情報が流出

→クレジットカード番号などを入力してしまうと不正決済の原因に

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇公衆Wi-Fiで通信の内容を守るためには

▶通信内容が暗号化されていないWebサイトにアクセスしない

→特に個人情報を入力するのは基本的に**NG**

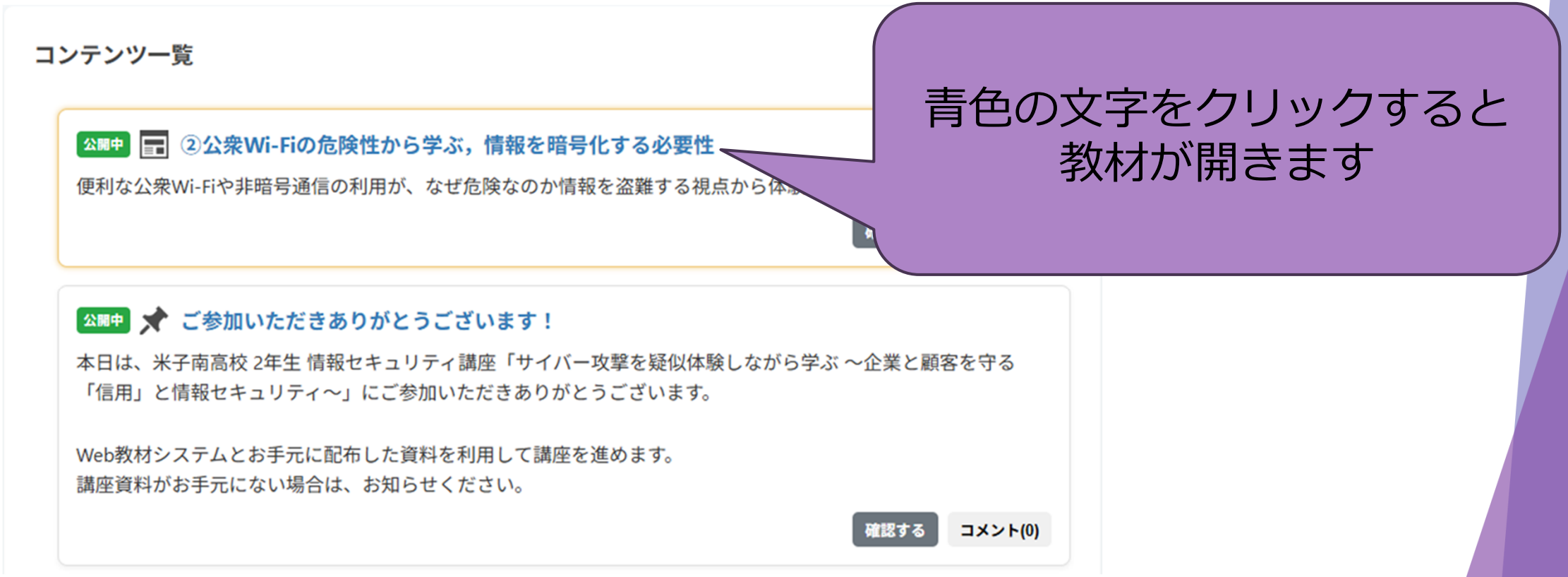
▶VPN（Virtual Private Network：仮想専用線）を利用する

→インターネット上に専用の通り道を作成して，データを暗号化して
専用サーバーに一度送ってから，目的の通信先に送受信する仕組み

→接続先すらもわからない状態にできる！

２．企業と顧客を守る「信用」と情報セキュリティ～
②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇教材を配信します



２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう

▶攻撃者の視点で通信内容を傍受する仕組みと守る方法を確認します

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう

これは仮想の
Webサイトです．

Wi-Fiを利用する人の
画面を想定しています．

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

① Free Wi-Fi + HTTP

まずは，公衆Wi-Fiで通信内容が暗号化されない通信を想定します．

この時，IDとパスワードを入力してログインするとどうなるでしょうか？

2．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

① Free Wi-Fi + HTTP

ユーザー名とパスワードを
入力してログインをする
簡単なシステムです．

ユーザー名：user
パスワード：password

入力したら「ログイン」を
押してください

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

① Free Wi-Fi + HTTP

この画面になったら
ログイン成功です

この時の攻撃者
コンソールを見てください

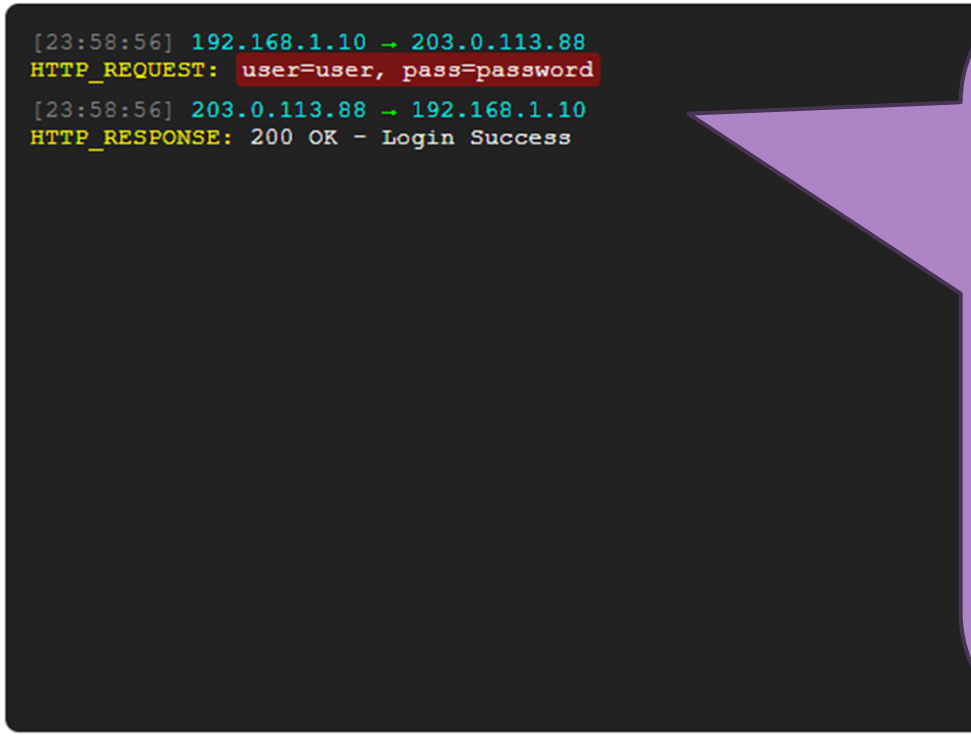
２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう

① Free Wi-Fi + HTTP

攻撃者コンソール



この画面は，攻撃者が
通信内容を盗聴するための
システムを想定した画面です．

ユーザー名とパスワードを閲覧する
ことが可能になっています…
しかもログインに成功したという
メッセージが出てます…

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

② Free Wi-Fi + HTTPS

次は，公衆Wi-Fiで
通信内容が暗号化されて
いる通信を想定します．

この時，IDとパスワード
を入力してログインする
とどうなるでしょうか？

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

② Free Wi-Fi + HTTPS

ユーザー名：user
パスワード：password

入力したら「ログイン」を
押してください

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

② Free Wi-Fi + HTTPS

この画面になったら
ログイン成功です

この時の攻撃者
コンソールを見てください

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう

② Free Wi-Fi + HTTPS

攻撃者コンソール

```
[0:15:18] 192.168.1.10 → 203.0.113.88
HTTPS_REQUEST: [Encrypted Application Data]
[0:15:18] 203.0.113.88 → 192.168.1.10
HTTPS_RESPONSE: [Encrypted Server Response]
```

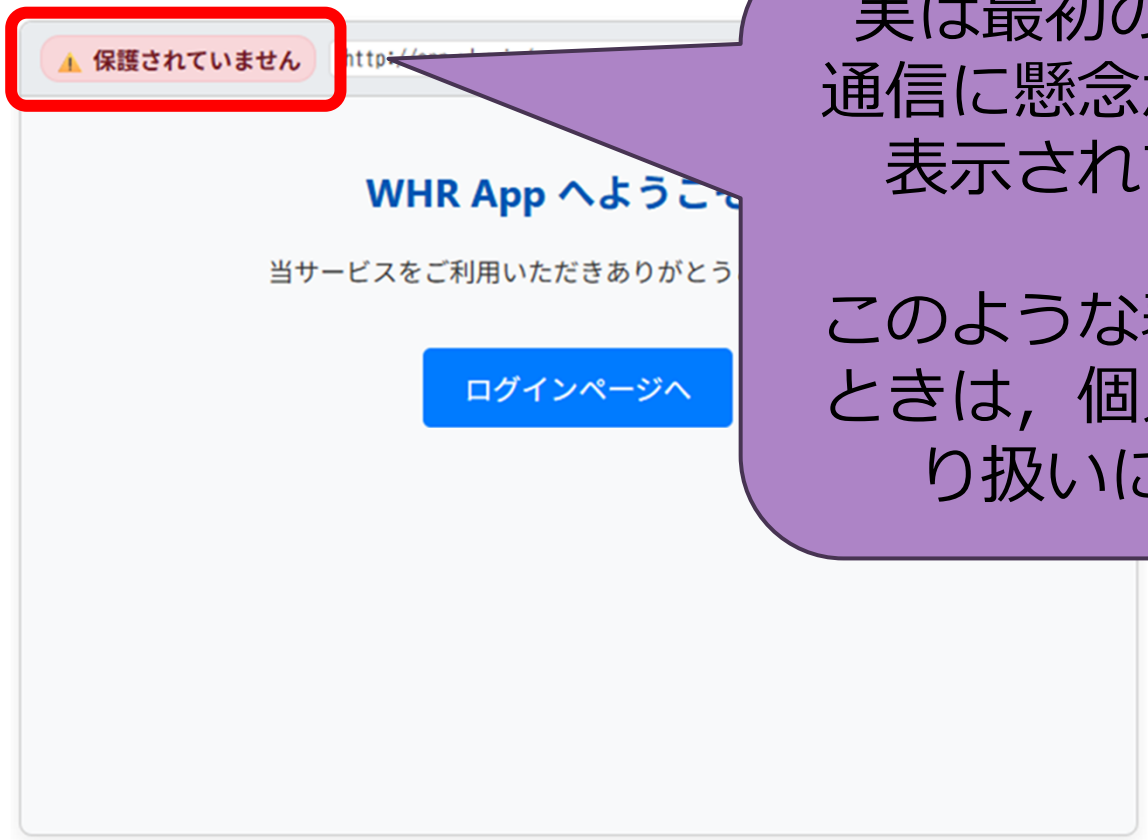
攻撃者の画面を見てみましょう

ユーザー名とパスワードが
閲覧できなくなりましたね！
ログインに成功したのか，失敗した
のかもわからなくなりました！

２．企業と顧客を守る「信用」と情報セキュリティ～

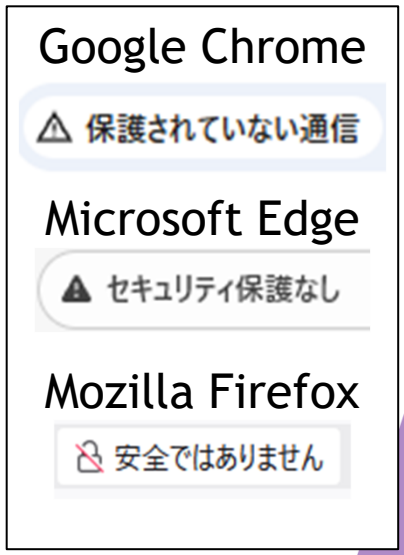
②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう



実は最初の画面の時点で
通信に懸念があることは，
表示されていました．

このような表示が出ているときは，個人情報などの取り扱いには要注意！



２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○実際に体験してみよう

② Free Wi-Fi + HTTPS

攻撃者コンソール

```
[0:15:18] 192.168.1.10 → 203.0.113.88
HTTPS_REQUEST: [Encrypted Application Dat
[0:15:18] 203.0.113.88 → 192.168.1.10
HTTPS_RESPONSE: [Encrypted Server Response]
```

先ほどの画面をもう
一度見てみましょう

実はIPアドレスによって
アクセスした先がどのような
Webサイトかばれてしまいます…

実害が出ることは少ないですが
プライバシーにかかわる問題です！

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

③ Free Wi-Fi + VPN/HTTP

最後に，公衆Wi-Fiで
通信内容が暗号化
されない通信をVPNを
経由すること想定します

この時，IDとパスワード
を入力してログインする
とどうなるでしょうか？

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

③ Free Wi-Fi + VPN/HTTP

ユーザー名：user
パスワード：password

入力したら「ログイン」を
押してください

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

③ Free Wi-Fi + VPN/HTTP

この画面になったら
ログイン成功です

この時の攻撃者
コンソールを見てください

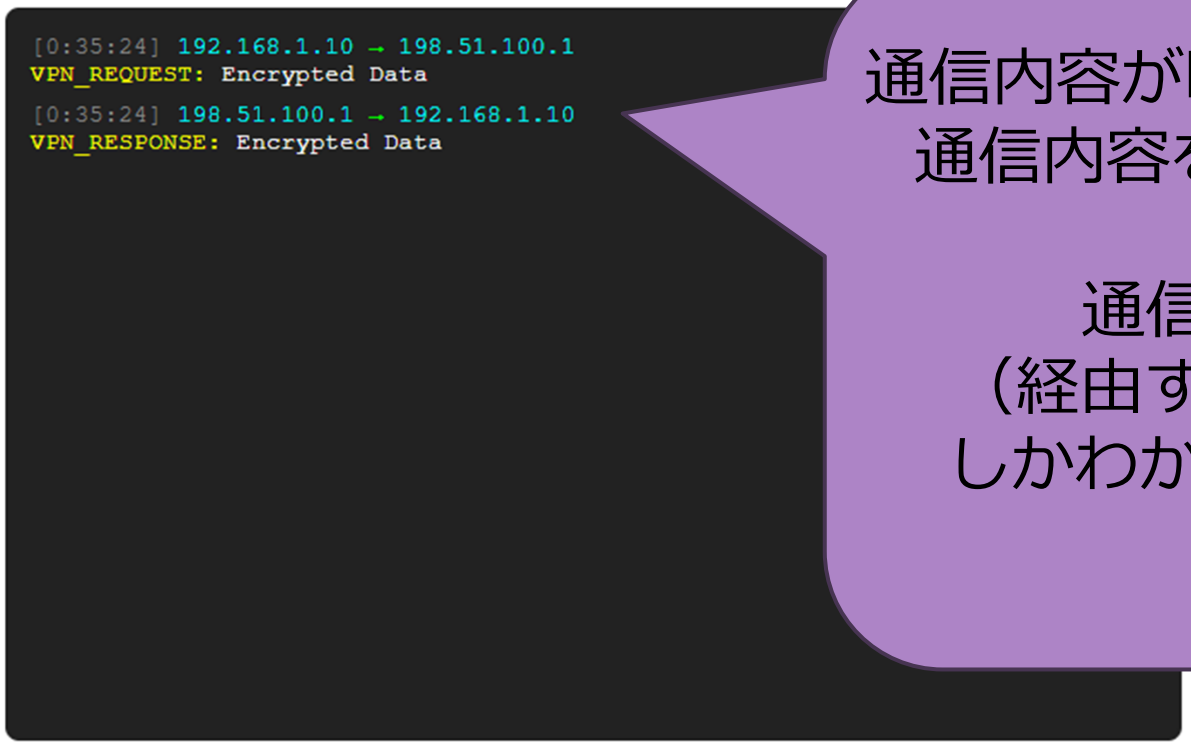
２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇実際に体験してみよう

③ Free Wi-Fi + VPN/HTTP

攻撃者コンソール



通信内容が暗号化されない通信ですが，
通信内容を見ることができません！

通信相手もVPNサーバー
（経由するサーバ）のIPアドレス
しかわからないのでアクセス先が
わかりません！

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇皆さんできましたか？

▶通信の内容を暗号化しないことの危険性を理解できたでしょうか？
→実際にこのようにIDとパスワードが盗まれる危険性があります

〇情報の暗号化は重要です

▶暗号化は盗まれないためではなく，盗まれたときの被害を減らすため
→Wi-Fiに限らず，あらゆる情報資源に言えることです！

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

〇公衆Wi-Fiの向き合い方

▶便利なものだから積極的に活用したい
→誤った使い方をすると非常に危険！！！

▶個人情報を取り扱わない
→どうしても取り扱いたいときは，VPNを活用！

▶公衆Wi-Fiを装った偽物のWi-Fiにも要注意
→割と身近にあるので要注意！

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

○VPNの利用上の注意

▶無名な企業や組織のVPNは危険性も…

→VPNサーバー側で通信内容を盗聴される可能性も

▶無料のVPNには要注意！

→信頼できる企業・組織であるか確認

→有料だから必ずしも安全というわけではない

２．企業と顧客を守る「信用」と情報セキュリティ～

②公衆Wi-Fiの危険性から学ぶ，情報を暗号化する必要性

Oディスカッションしよう

▶旅先のカフェで急ぎで仕事をしないといけなくなりました。
Free Wi-Fiはあるのですがパスワードで保護されていません…。
どうするべきでしょうか？

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇専門的な話が続くと疲れるので…

▶少しレクリエーション的な活動でリラックスしましょう！

〇インターネット上で公開されている情報から，撮影地が特定される！？

▶嘘のような話だけど，本当…

▶Googleのストリートビューを利用したゲームも話題だよね…

→「GeoGuessr」

▶生成AI（ChatGPT）の精度も高くなっている

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

○「OSINT」とは？

▶Open-Source Intelligence

→誰でも入手可能な膨大な情報の中から，必要な情報を収集・分析

→セキュリティ対策や犯罪捜査などで活用される

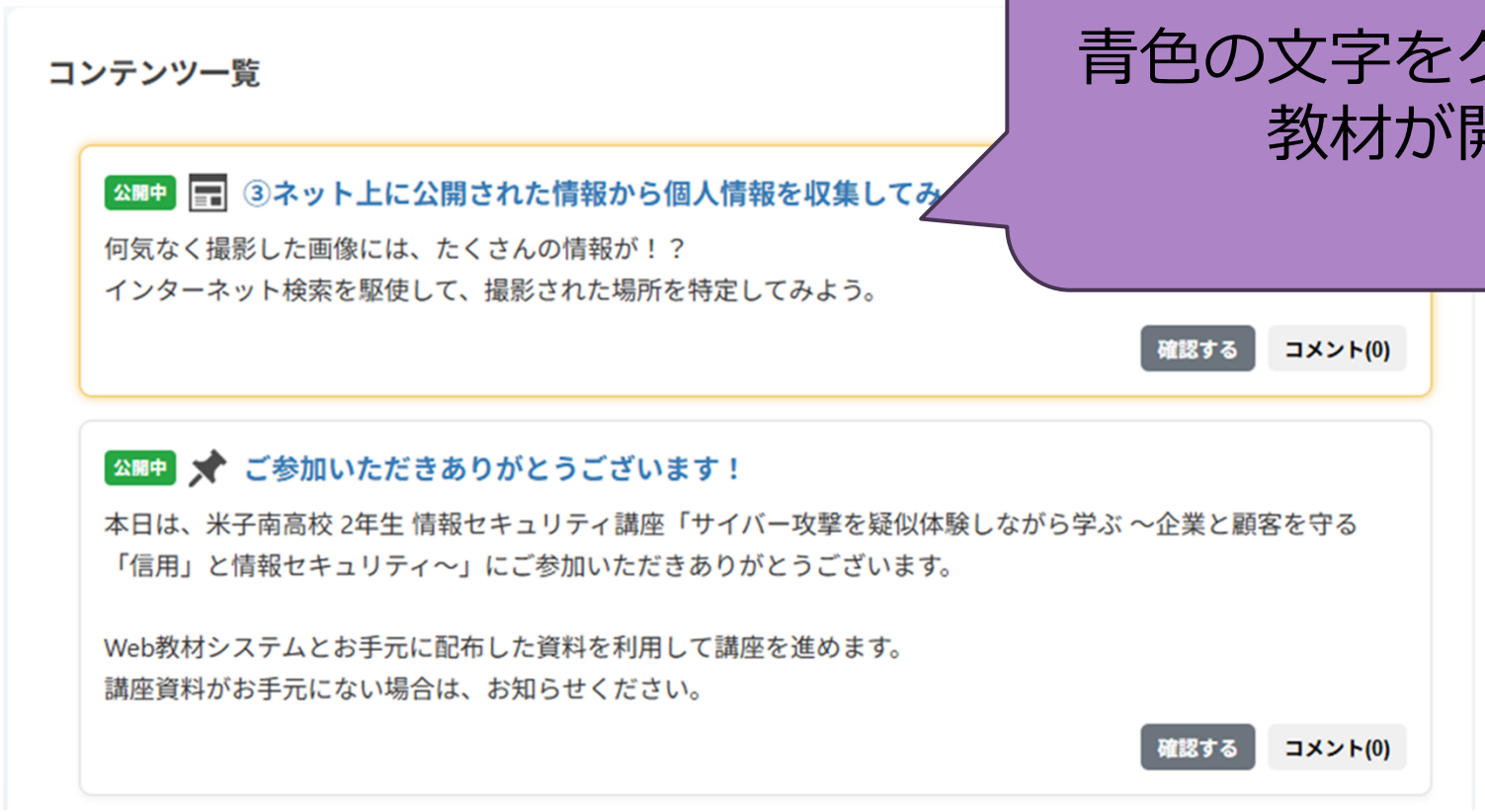
○実際に体験してみよう

▶写真から撮影地を特定してみよう！

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

○教材を開きましょう



青色の文字をクリックすると
教材が開きます

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

画面は表示されましたか？

画像をクリックすると拡大して表示することが可能です．

答えが分かったら，回答欄に入力して「送信」を押してください！

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

間違った答えを入力すると
送信ボタンの下に不正解である
ことを伝えるメッセージが
表示されます．

難度でも回答できますので，再度
チャレンジしてください！

２．企業と顧客を守る「信用」と情報セキュリティ～
③ネット上に公開された情報から個人情報を収集してみよう

正しい回答を入力すると
送信ボタンの下に正解である
ことを伝えるメッセージが
表示されます．

順位も表示されますが，演習が終わる
までは静かに待っていてください．

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇例題の答え合わせ

▶1枚目は，京都貨物駅

▶2枚目は，東寺

▶3枚目は，銀閣寺

▶4枚目は，金閣寺

➡「京都府京都市」が答え

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇問題1に挑戦します

▶準備はよろしいでしょうか？

→画面が正しく表示されない場合はお知らせください

▶下記のどちらかが表示されていれば問題ありません

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇解説

▶答えは，「島根県出雲市」

▶各画像の詳しい情報

- 1枚目：稲佐の浜
- 2枚目：島根ワイナリー
- 3枚目：出雲ドーム
- 4枚目：出雲大社

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇問題2に挑戦します

▶準備はよろしいでしょうか？

→画面が正しく表示されない場合はお知らせください

▶下記のどちらかが表示されていれば問題ありません

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇解説

▶答えは，「神奈川県藤沢市」

▶各画像の詳しい情報

・1枚目：江島神社の辺津宮

・2枚目：江の島から見る由比ヶ浜海岸

・3枚目：江の島

・4枚目：江ノ電江ノ島駅と江ノ電車両

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇画像の特徴をとらえてWeb検索する

▶1枚目：神社，緑の屋根，狛犬（こまいぬ）

▶2枚目：海岸，ヨット，海

▶3枚目：島，タワー，日本，陸続き

▶4枚目：江の島駅

〇Googleの画像検索などもある

▶画像をアップロードして検索

→高い精度で特定可能（誤った情報を表示する可能性あり）

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

〇「OSINT」で自宅や職場が特定されることも…

▶犯罪につながる可能性（ストーカーや詐欺など）

▶アカウントを忘れた時の，秘密の質問の特定に繋がるかも

〇写真を公開するときは，個人が特定される情報には注意する

▶今の時代投稿するべきでないとは，言えない

→リスクがあることは必ず理解すること

▶SNSのプロフィール欄に，学校名・クラス・部活など書いてない？

→フォロワーから芋づる式にほかの人に迷惑が及ぶ可能性も

２．企業と顧客を守る「信用」と情報セキュリティ～

③ネット上に公開された情報から個人情報を収集してみよう

Oディスカッションしよう

▶あなたは、小売店の店長です。従業員が事務所の中で
自撮りをしています。
どのように理由を説明して注意すべきでしょうか？

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇Webサイトに「罠」を仕掛ける

▶Webサイトに偽サイトへのリンクがあると知ったら，どう思う？

→ 怖い，間違って触れたらどうしよう…

→ 私なら騙されるわけない…

〇もしもそれが，信頼していたWebサイトだったら？

▶運営会社や組織が信用できる

→信用している以上，注意するなんてことはないよね

→常に気を張ってWebサイトを閲覧するわけにはいかないし…

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○クロスサイトスクリプティング

▶悪意のあるスクリプトをWebサイトに埋め込む攻撃

→落とし穴みたいなイメージ

→当然簡単には見抜けないように偽装される

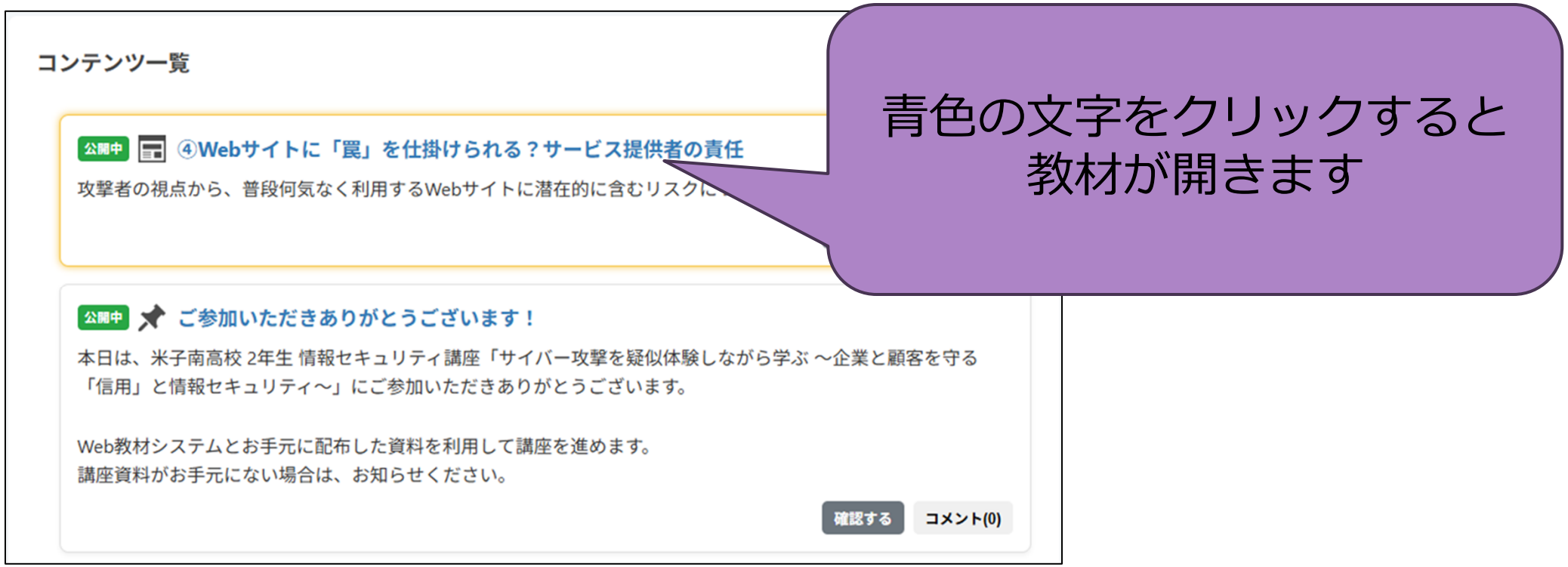
▶Webサイトを閲覧する利用者が影響を受ける

→偽サイトに誘導されるなどの直接的な被害

→Webサイトを閲覧できなくするなどの嫌がらせ行為

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇教材を配信します



２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇演習の想定

▶ECサイトのレビュー投稿欄に脆弱性があります

〇どのような脆弱性があるのか…

▶Webサイトのデザインをつかさどるタグを投稿できる
→背景色を変えて，見ずらいサイトに変える

▶ハイパーリンクを投稿できる
→誤ってクリックしてしまった人を偽サイトに誘導する

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○お題１：Webページの背景色を，黄色から赤色に変更する

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○お題１：Webページの背景色を，黄色から赤色に変更する

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○Webページの背景色を，黄色から赤色に変更する

▶どうやって実現する？

○Webサイトのデザインをつかさどるのは？

▶CSS（Cascading Style Sheets）

→サーバの保存されているCSSファイルを直接編集できない

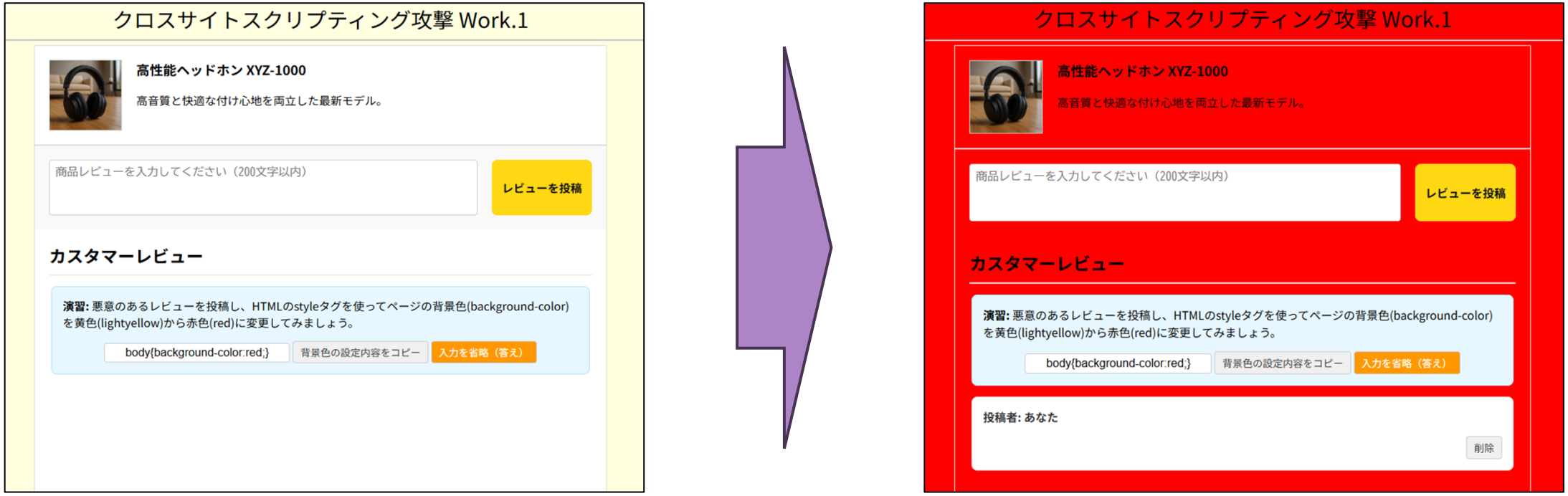
○HTMLのstyleタグを悪用して間接的にCSSを上書きする

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇商品レビューの投稿欄に以下のHTML文を入力し送信

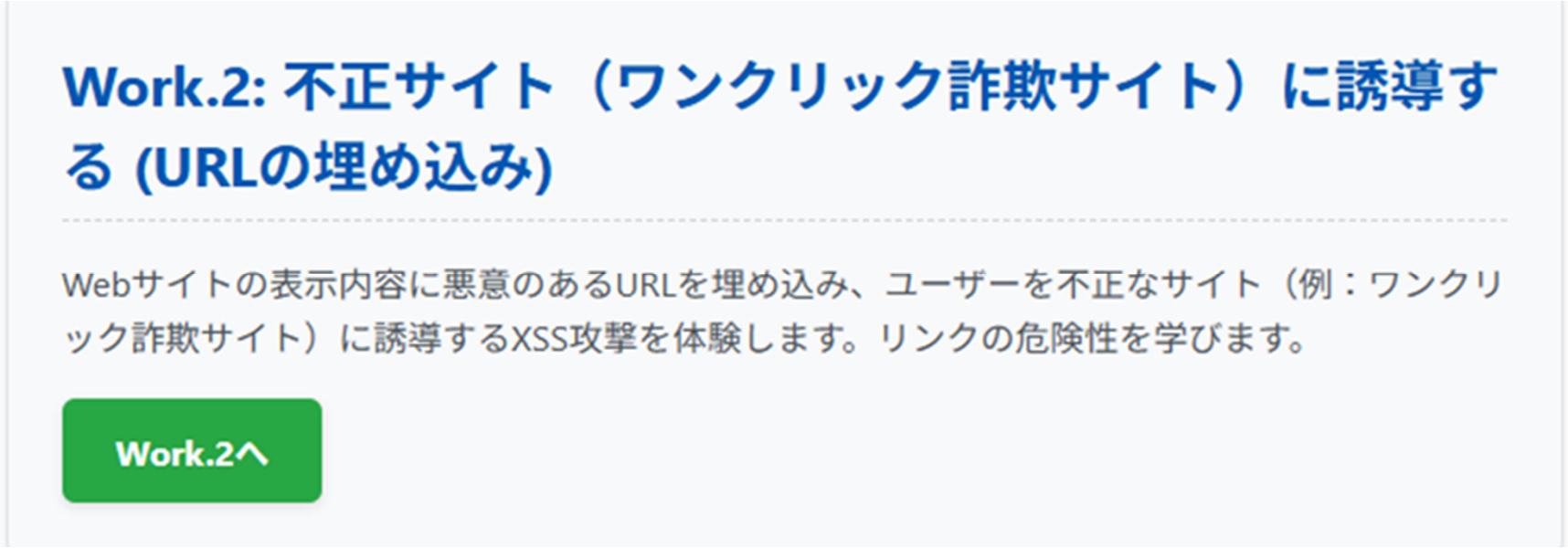
▶<style>body{background:**red**;}</style>



２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

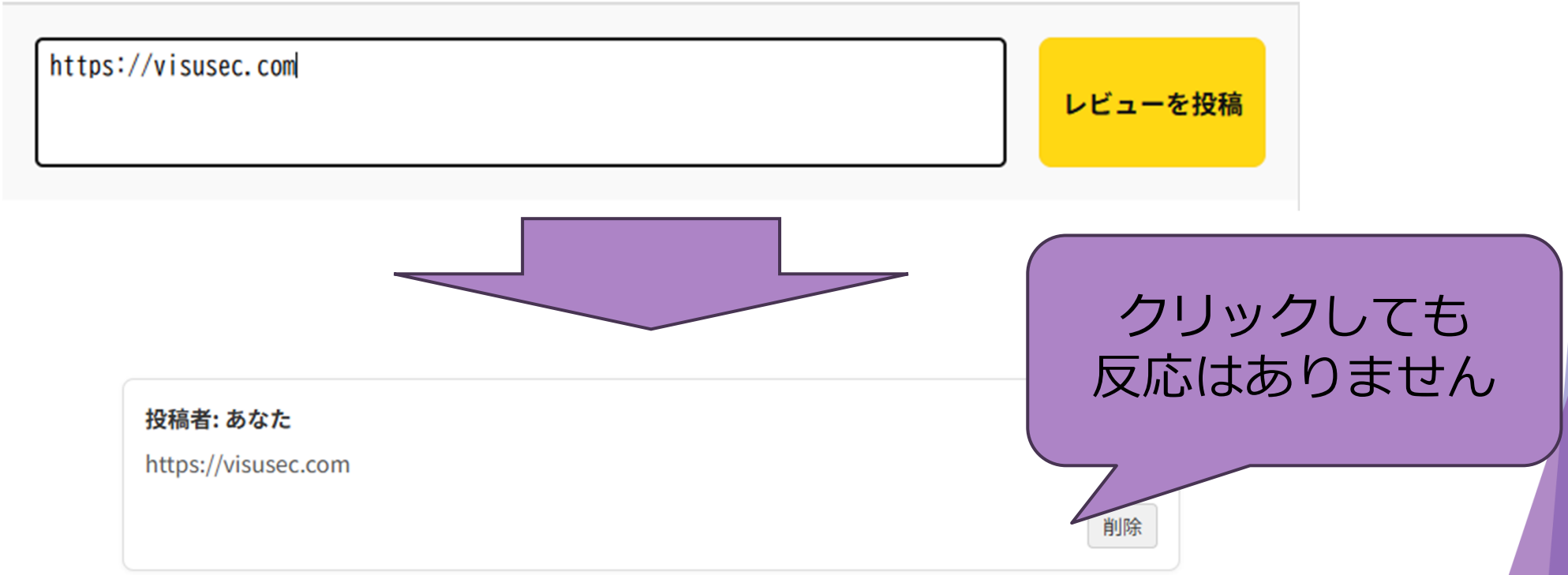
○お題２：利用者を偽サイトに誘導する



２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇お題２：利用者を偽サイトに誘導する

▶URLを直接貼り付けてもハイパーリンクにはなりません



２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇お題２：利用者を偽サイトに誘導する

▶URLを直接貼り付けてもハイパーリンクにはなりません

→誤ったアクセスは期待できないですね…

▶URLがそのまま張られてたら，警戒しますよね…

→見た目をごまかすことができればいいのに…

〇どうやって実現する？

▶HTML標準のハイパーリンク化するタグが利用できそう

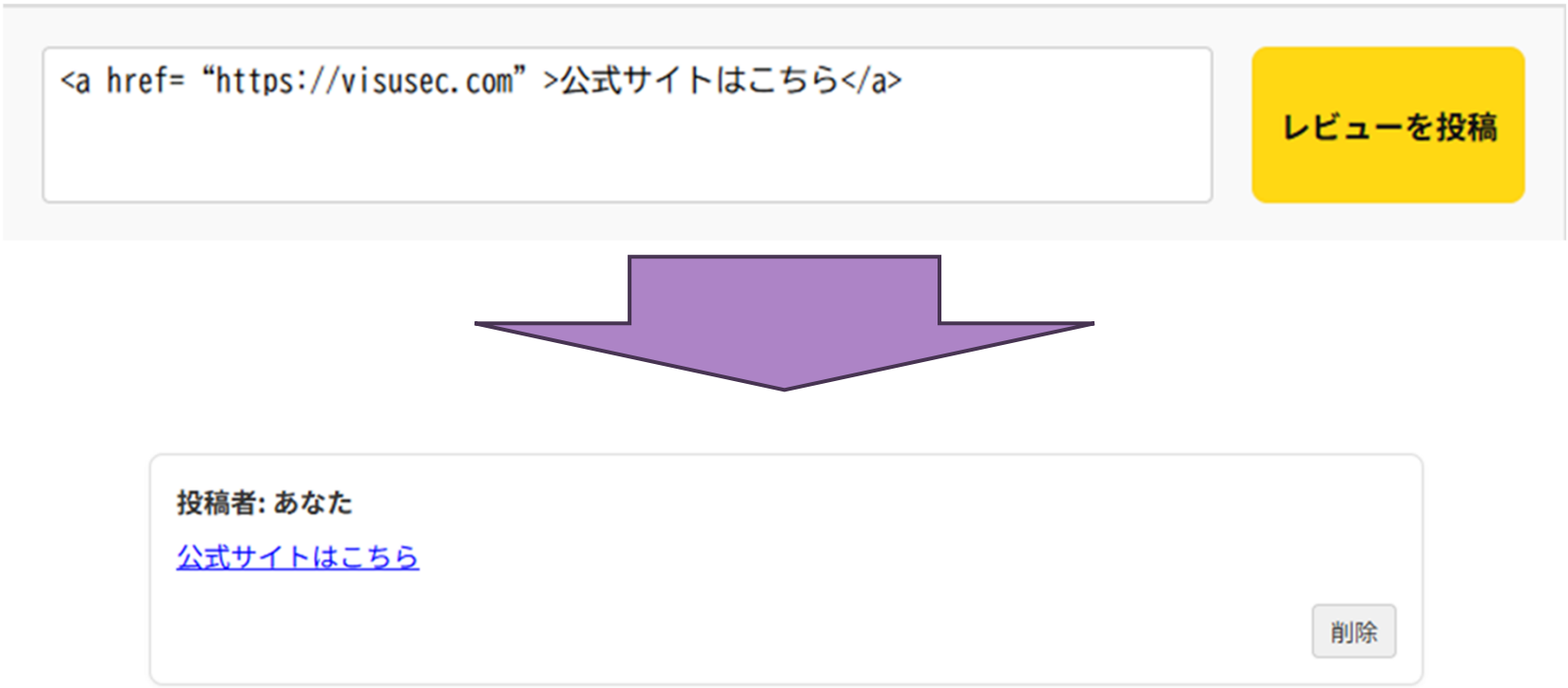
→aタグ

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇商品レビューの投稿欄に以下のHTML文を入力し送信

▶公式サイトはこちら



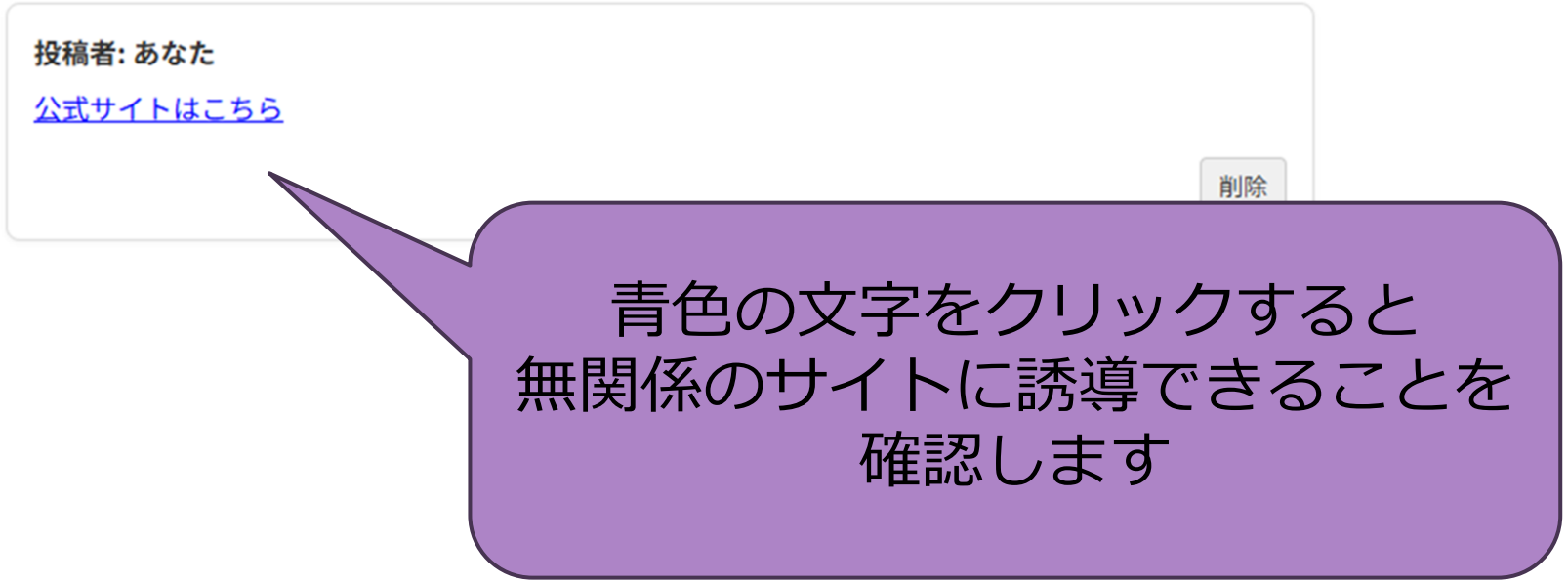
２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇表示されたハイパーリンクをクリックすると

▶現在使っているWebサイトに移動したと思います

→ECサイトとは無関係のページに誘導することができました



２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○うまくいきましたか？

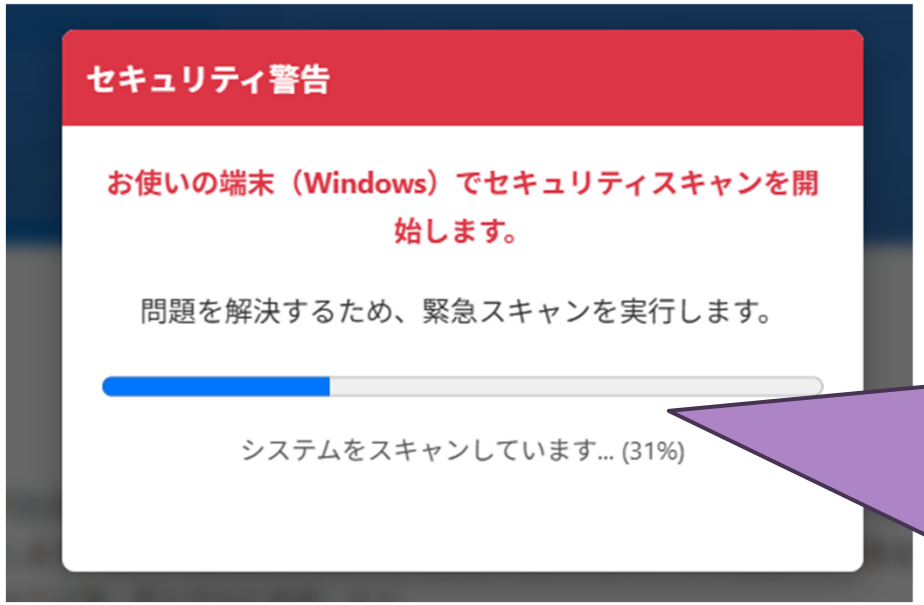
この演習をすると，システムから
ログアウトしてしまうので，
緑の「ログイン」ボタンから
再度ログインしてください

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇騙されましたか？

▶元のWebサイトのURLは，「visusec.jp」

→偽サイトとして皆さんにお渡ししたURLは，「visusec.com」です



最近はドメインを気にする人は
減っている…
だからこそ狙われる可能性がある

有名企業だと様々なTLDを取得して
対策するぐらい深刻…

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

○ドメインを偽装される

▶企業や団体にとって偽サイトなどに誘導されるのは死活問題
→お客さんを取られるだけでなく，社会的信用を失う可能性…

○ネットにアクセスするときは，「TLD」に注目してみよう

▶多くのサービスは複数のTLDを抑えている
→「visusec.jp」と「visusec.com」を取得している

▶すべてのドメインを取得することには限界がある…
→金銭的なコストが大きすぎる
→Googleなどの大手は幅広く取得している

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇理解してほしいこと

▶Webサイトに偽サイトへのリンクを張り付けることは可能
→URLを何も考えずに開くとリスクが非常に高いということ
→Webサイトだけじゃなく，SMS・メールなどにも言える

→この攻撃ができるようにしていると，管理責任を問われる可能性も

▶背景色の変更ぐらいなら別にいい？
→社会的な信用を失う
→ECサイトなら売り上げに影響する可能性も

２．企業と顧客を守る「信用」と情報セキュリティ～
④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

〇理解してほしいこと

▶サービス提供者としてリスクを最小化するにはどうすればいいか
→主要なTLDに関しては抑えることが推奨されます
→日本人向けサービスは、.com と .jp をセットで取得が良いかも

▶信用できるリンクか、しっかりと確認すること
→分からない・不安ならアクセスしないこと！
→短縮リンクやサブドメインで偽装するケースは多い！
→システム開発の目線では、外部リンクは確認してから移動させる

２．企業と顧客を守る「信用」と情報セキュリティ～

④Webサイトに「罠」を仕掛けられる？サービス提供者の責任

Oディスカッションしよう

▶自社のサイトが改ざんされて、顧客が偽サイトに誘導されて被害に遭いました。『私たちは悪くない、ハッカーが悪い』という言い訳は通用すると思いますか？ただし、対策が適切でなかったとします。

3．おわりに

〇ここまでお疲れさまでした！

▶情報セキュリティーについて少し詳しくなったでしょうか？

〇今回は攻撃者の目線を中心に講座を進めてきました

▶どこが狙われるのか（脆弱性）を客観的に知ることは重要です

→もちろん，実際のサービスに攻撃したら**犯罪です！！！**

３．おわりに

〇今日のまとめ

▶パスワードはなるべく長く，文字種類を増やす

→長くすることは安全になるけど，利便性は悪くなるよね…

▶SNSに公開した画像から住所などが特定される可能性が…

→公開する前に一度立ち止まって，確認すること

→マンホールや電柱など何気ないものに要注意！

３．おわりに

〇今日のまとめ

▶情報を守るためには，暗号化が大切

→Webサイトにアクセスするときは，「https」であることを確認

→暗号化されていないときは，VPNを活用！（信頼できる？）

▶今回のセキュリティ事例の多くは人為的なミス

→防げるリスクもたくさんある

3．おわりに

〇もっと詳しく学びたいと思ったら

▶今回利用したWebアプリは視覚的な理解を重視しています

→実際の挙動と多少異なる点があります（極端な誤りはないです）

▶他にも様々な事例があります

→身近なものから，少しディープな世界まで

▶インターネットや文献などをぜひ調べてみてほしいです

→公的機関や企業などのサイトが信用性が高いです

3．おわりに

〇講座の内容・教材に関するお問い合わせ先

▶若林 遥大（ワカバヤシ ハルト）

Mail : wakabayashi.haruto@whr.jp