鳥取湖陵高校 3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
～Webに関するセキュリティの脅威と対策～

2025年11月13日（木）

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？（復習）

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

① Webサイトに「罠」を仕掛ける（クロスサイトスクリプティング）

② データベースを不正に操り，情報を盗む（SQLインジェクション）

③ サーバに不正な指示を出す（OSコマンドインジェクション）

④ 不正な操作からサーバを守る（エスケープ処理・ハッシュ化）

３．おわりに

1．情報セキュリティの基本

○そもそも「情報セキュリティ」って何だろう？

▶ウイルス対策

▶迷惑メール・架空請求

▶SNSの使い方・闇バイト など

○「情報セキュリティ」＝ 情報の安全を守る対策

▶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！

→コンピュータのデータ，個人情報，機密情報など

▶個人だけでなく，企業や公的機関までもが被害を受ける時代に…

→間違いなく他人ごとではないが，どうすればいいのだろうか？

1．情報セキュリティの基本

○「情報セキュリティ」の定義

▶日本産業規格（JIS：Japanese Industrial Standards）

→情報の機密性・完全性・可用性を維持すること（JIS Q 27000）

	用語の意味	主な対策
機密性	アクセス許可された人だけが， 情報を扱うことができること	暗号化
完全性	情報が最新で正確であり， 欠損がないことが保証されること	電子署名 なりすましや改ざんを防ぐための 電子的な署名
可用性	アクセスを許可された人が， いつでも情報にアクセスできること	システムの冗長化 障害に備えて，予備の設備など バックアップを運用しておく

演習の準備

①Webブラウザを立ち上げてください

→種類は問いません（Google Chrome 推奨）

②アドレスバーにURLを入力してアクセスしてください

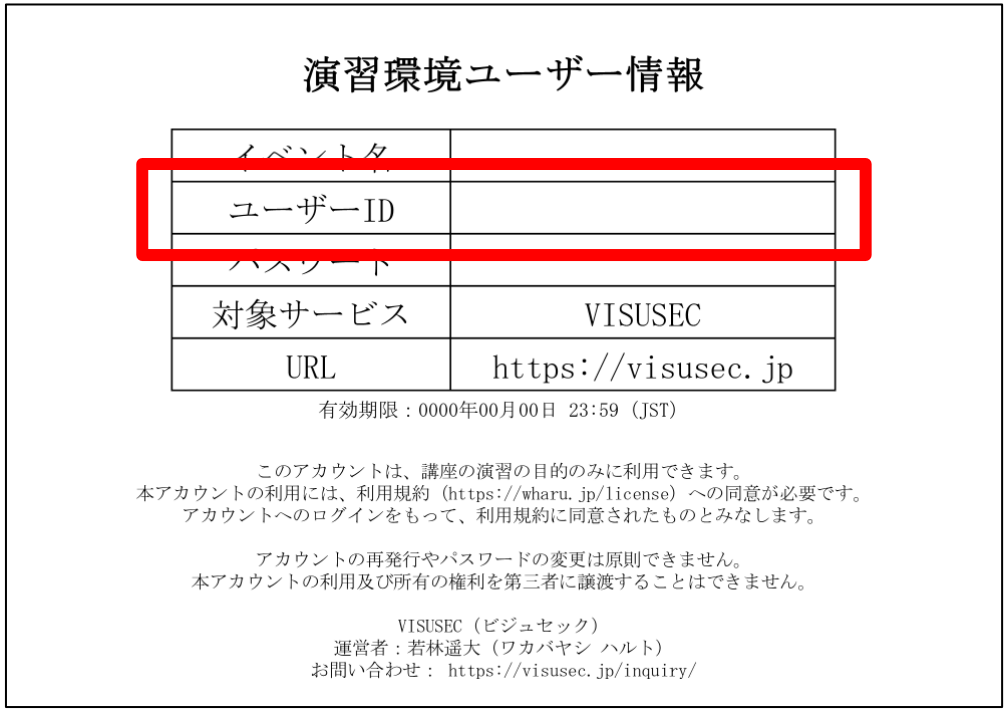
→ https://visusec.jp/

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）

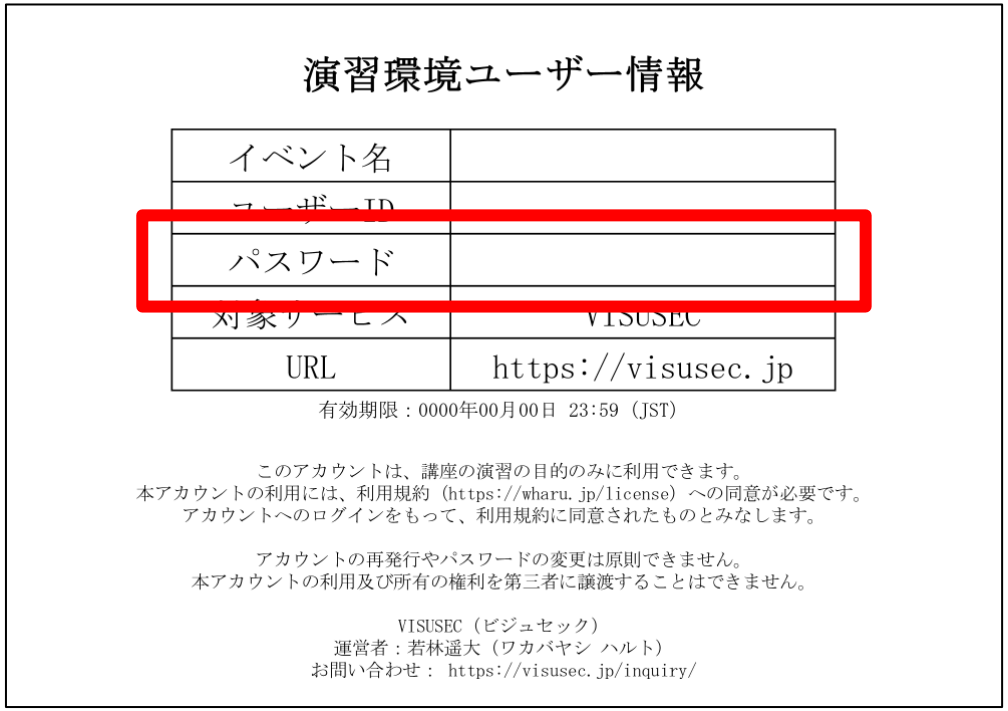
このアカウントは、講座の演習の目的のみに利用できます。
本アカウントの利用には、利用規約（https://wharu.jp/license）への同意が必要です。
アカウントへのログインをもって、利用規約に同意されたものとみなします。

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ログイン完了

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

○Webアプリケーションとは？

▶インターネット経由でWebブラウザ上で動作するアプリケーション

SNS（X・Instagram・YouTube など）

ECサイト（Amazon・楽天市場・Yahooショッピング など）

ネットバンキング

○WebアプリケーションとWebサイト

▶Webサイト

→ブログや企業の紹介サイトなど，情報を得ることが目的なページ

▶Webアプリケーション

→ユーザと提供者で双方向のやりとりができる高度な機能を有する

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

○Webアプリケーションの特徴

▶インストール不要

→ブラウザがあれば，どこからでもアクセス可能

▶幅広い環境から利用可能

→PCやスマートフォン，OSを選ぶことなく利用可能

▶インターネット接続が必要

→常に最新の情報に書き変わるのはメリット

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

〇Webアプリケーションの構成

▶プログラム

→大きく分けると2つの種類のプログラミング言語に分類される

〇クライアントサイド言語（マークアップを含む）

▶主に画面の表示をつかさどる

→HTML・CSS，JavaScript など

〇サーバサイド言語

▶サーバとのデータのやり取りなど高度な処理をつかさどる

→PHP・Java・Python・Ruby など

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

〇Webサーバ

▶ネットワークを通じて情報や機能を提供するコンピュータ

→サーバ内に必要なプログラムやデータベースが保存される

▶最近は，サーバは借りる時代に

→さくらのVPS（利用する演習環境もこちらに構築）

→AWS など

２．Webに関するセキュリティの脅威と対策

⓪ Webに関するセキュリティ上の脅威とは？

〇Webアプリケーションにはどんな脅威があるだろうか？

- ▶サーバ・サービスへの不正侵入
- ▶プログラム・ファイルの改ざん
- ▶データベースの破壊
- ▶データベースの情報の奪取
- ▶提供者の意図しない偽サイトへの誘導

〇具体的な脅威を演習で学び，その対策まで理解しよう！

２．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

○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

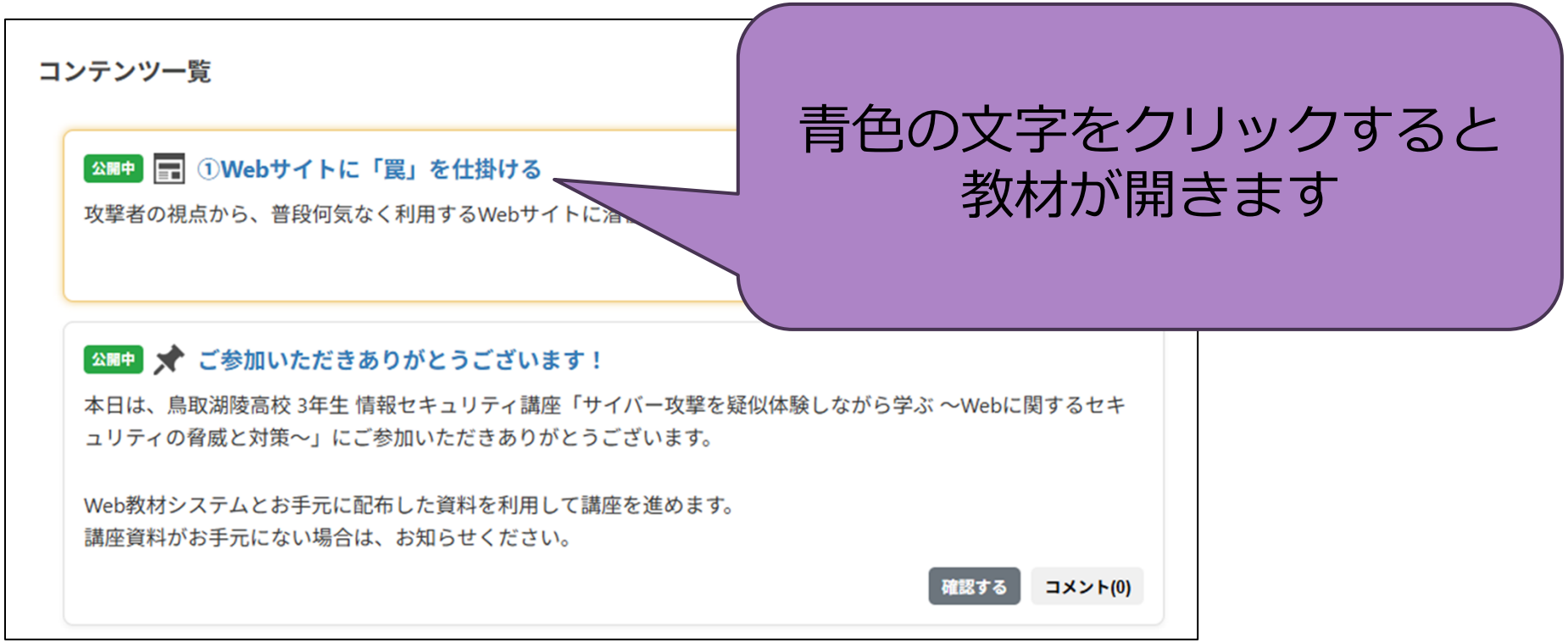
▶Webサイトを閲覧する利用者が影響を受ける

→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．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

○教材を配信します



２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

〇お題１：Webページの背景色を，黄色から赤色に変更する

２．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

○お題１：Webページの背景色を，黄色から赤色に変更する

２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

○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

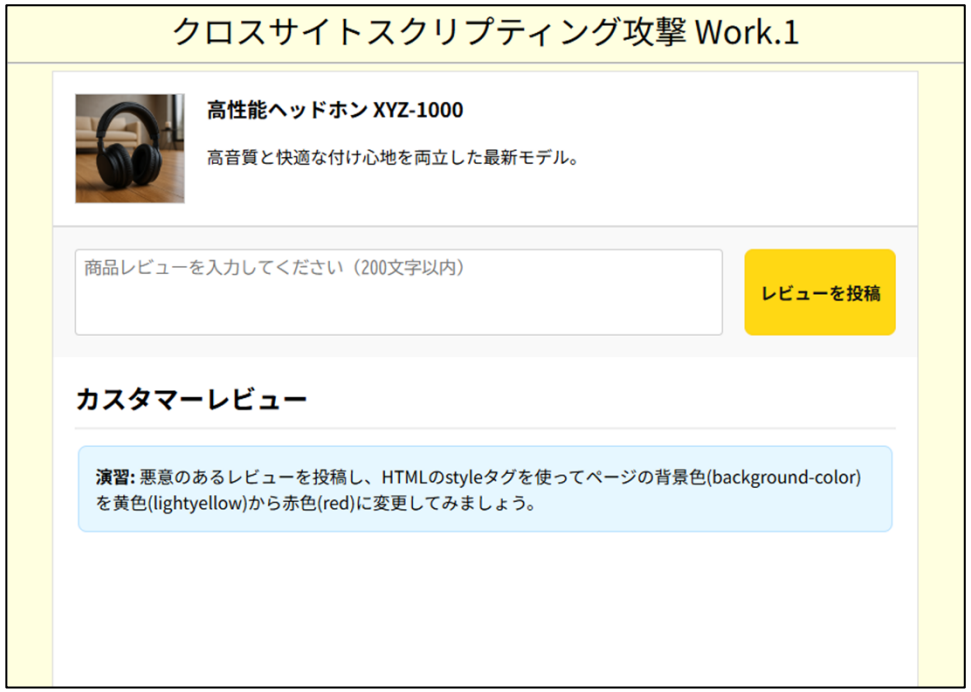
○HTMLのstyleタグを悪用して間接的にCSSを上書きする

2．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

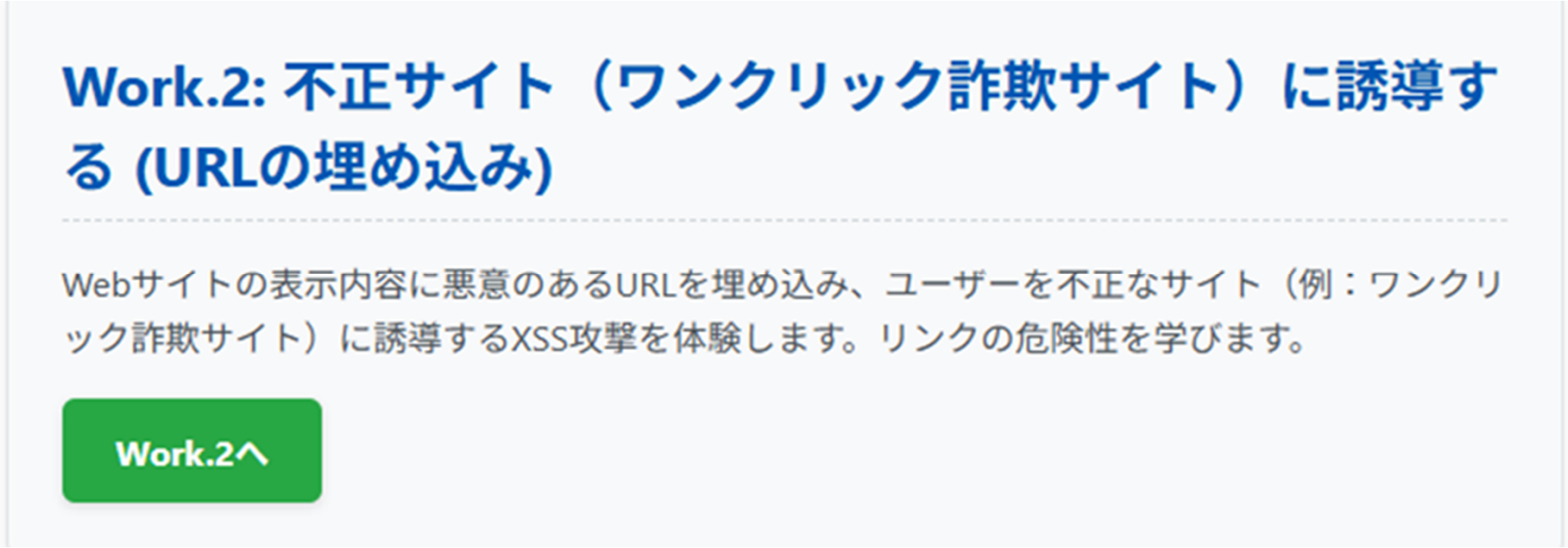
〇商品レビューの投稿欄に以下のHTML文を入力し送信

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



２．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

〇お題２：利用者を偽サイトに誘導する

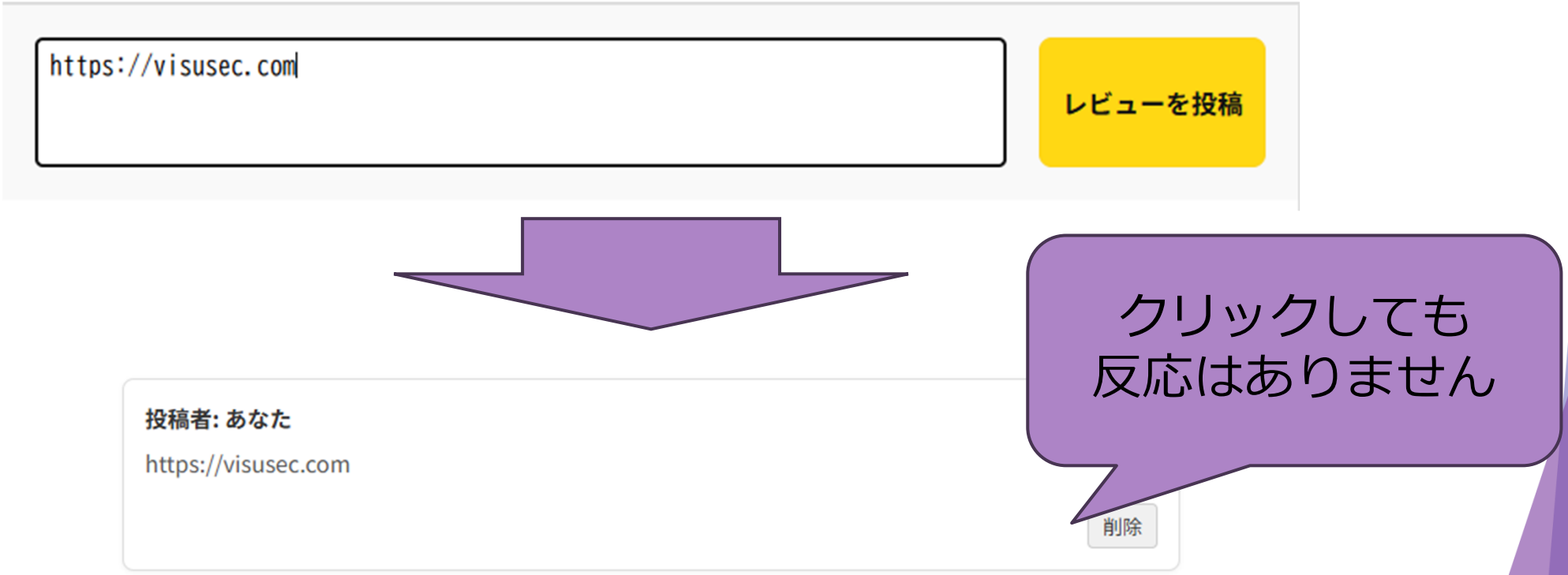


２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

○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．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

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

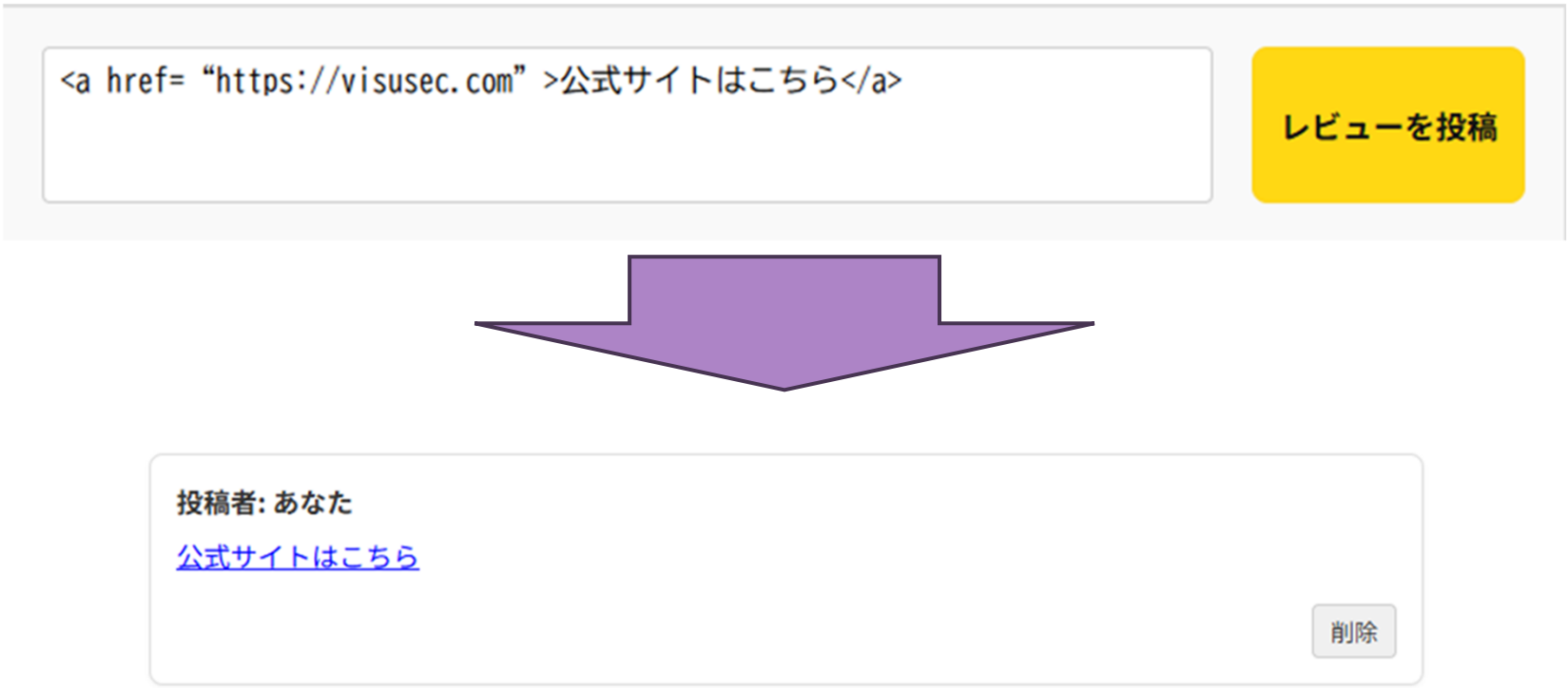
→aタグ

２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

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



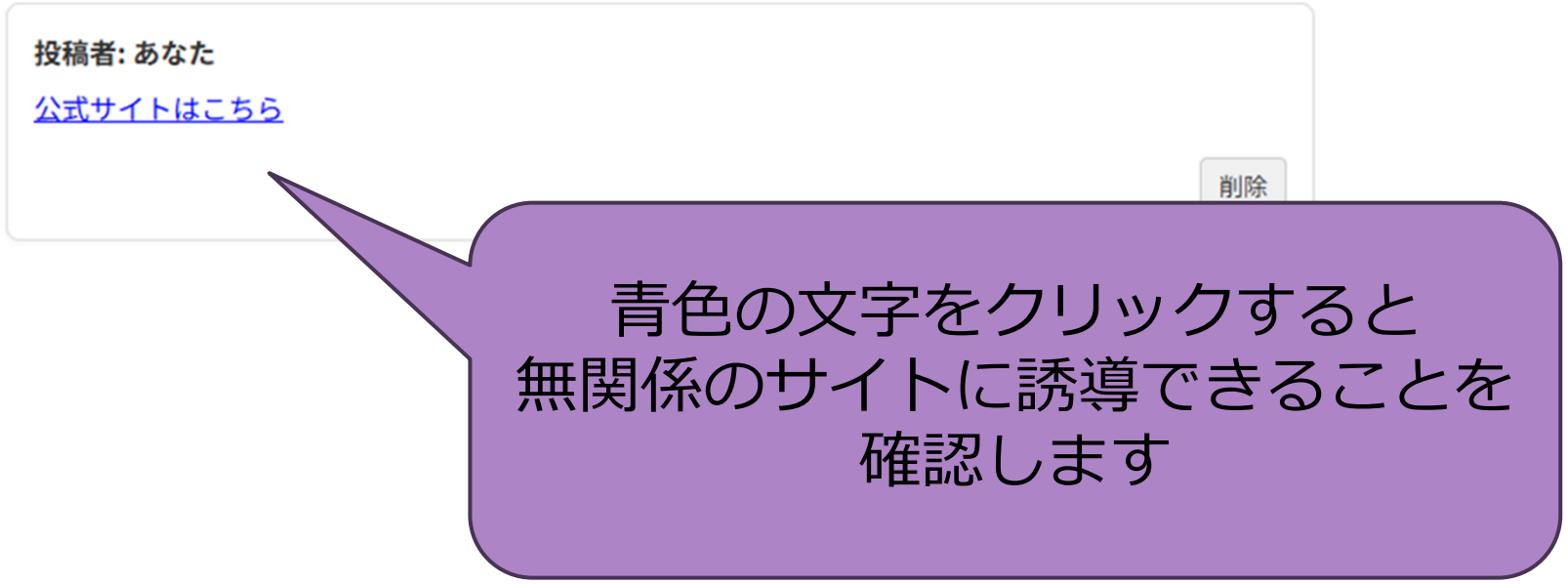
２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

〇うまくいきましたか？

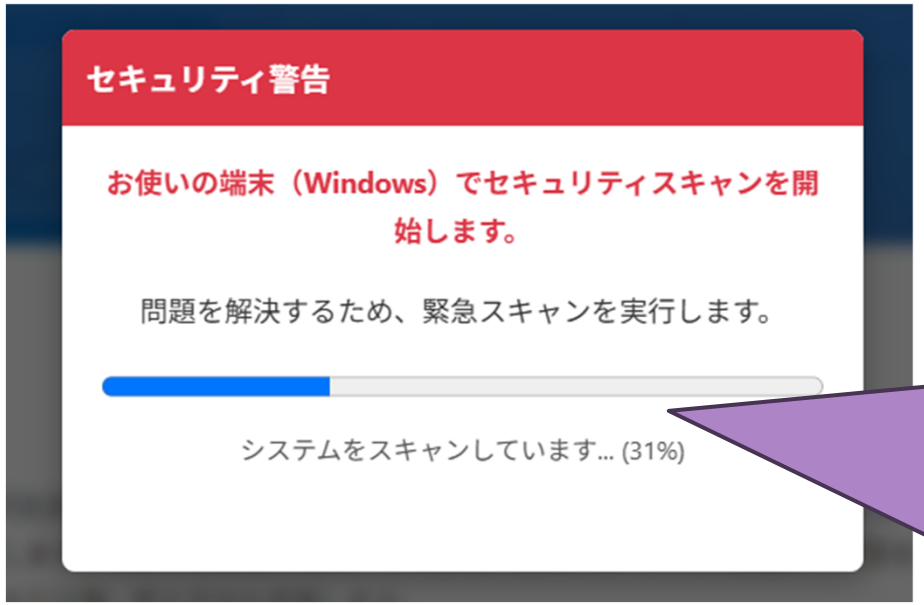
この演習をすると，システムから
ログアウトしてしまうので，
緑の「ログイン」ボタンから
再度ログインしてください

２．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

○トップレベルドメイン（Top Level Domain：TLD）名とは？

▶ウェブサイトの種類や目的を分類する文字列

▶ドメインには多くく分けて2種類ある

→国別（ccTLD：Country Code Top-Level Domain）

→分野別（gTLD：Generic Top-Level Domain）

TLD	役割	種類
.com	商業用組織	gTLD
.net	ネットワーク関連用	gTLD
.jp	日本国内の個人や法人	ccTLD

２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

○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．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

〇企業や団体がすべてのドメインを保護するのは無理…

▶利用者が注意するしかない

→ドメインを手入力しない今だからこそ要注意

	ドメイン名
正規のドメイン名・TLD	visusec.jp
偽のドメイン名・TLD	visusec.com
サブドメインを悪用するパターン	visusec.whr.jp
短縮リンクを悪用するパターン	whr.jp/k9TFiNAS
ハイパーリンクを悪用するパターン	詳細はこちら

２．Webに関するセキュリティの脅威と対策

① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策
① Webサイトに「罠」を仕掛ける

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．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

○データベースを不正に操り，情報を盗む

▶正しいパスワードを入力せずにログインできるシステムってあるの？

→個人情報が流失したらどうしよう…

○Webアプリケーションにおいて利用者を識別する仕組み

▶ID（メールアドレス など）とパスワードを入力するのが一般的

○IDとパスワードをどのように管理して認証しているんだろう

▶データベース

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

○データベースとは…

▶検索や管理を容易にできるように整理された情報の集まり

→ユーザリスト

→商品リスト

→電子カルテ

▶SQLで操作

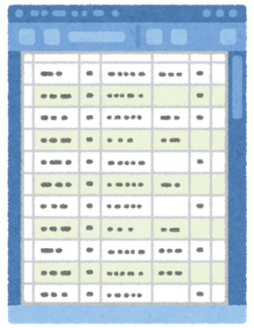
→データベースを管理するための命令を含むプログラミング言語

2．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

OSQLはどのように実行されるのか？

システムに
ログインしたいです．
IDとパスワードを
お渡しします

このIDとパスワードは
存在する・正しいのか？
DBに確認する命令を出そう
（SQL文）



Webサーバソフトウェア

データベース管理システム

アカウント存在したし
正しいパスワードだから
アクセスしていいよ！
ページ表示するための
データ渡すね！

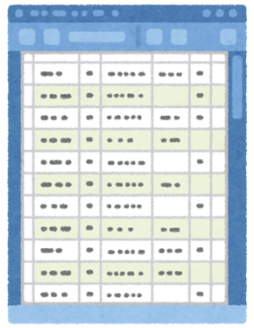
Webサーバの指示通りに
ユーザ名簿作成したよ！

2．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

○SQLはどのように実行されるのか？

パスワード入力する欄に
直接SQL文が書けるな…
ユーザ認証を
ごまかす指示を出そう

DBにユーザが存在するか確認
する命令を出そう
「AがAであるときは正しい」
とみなしてね



Webサーバソフトウェア

データベース管理システム

ユーザ名簿取得できたから
アクセスしていいよ！
ページ表示するための
データ渡すね！

Webサーバの指示通りに
ユーザ名簿作成したよ！
「AがAであるとき」って常に
正しいけどいいのかな？

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

OSQLインジェクション攻撃

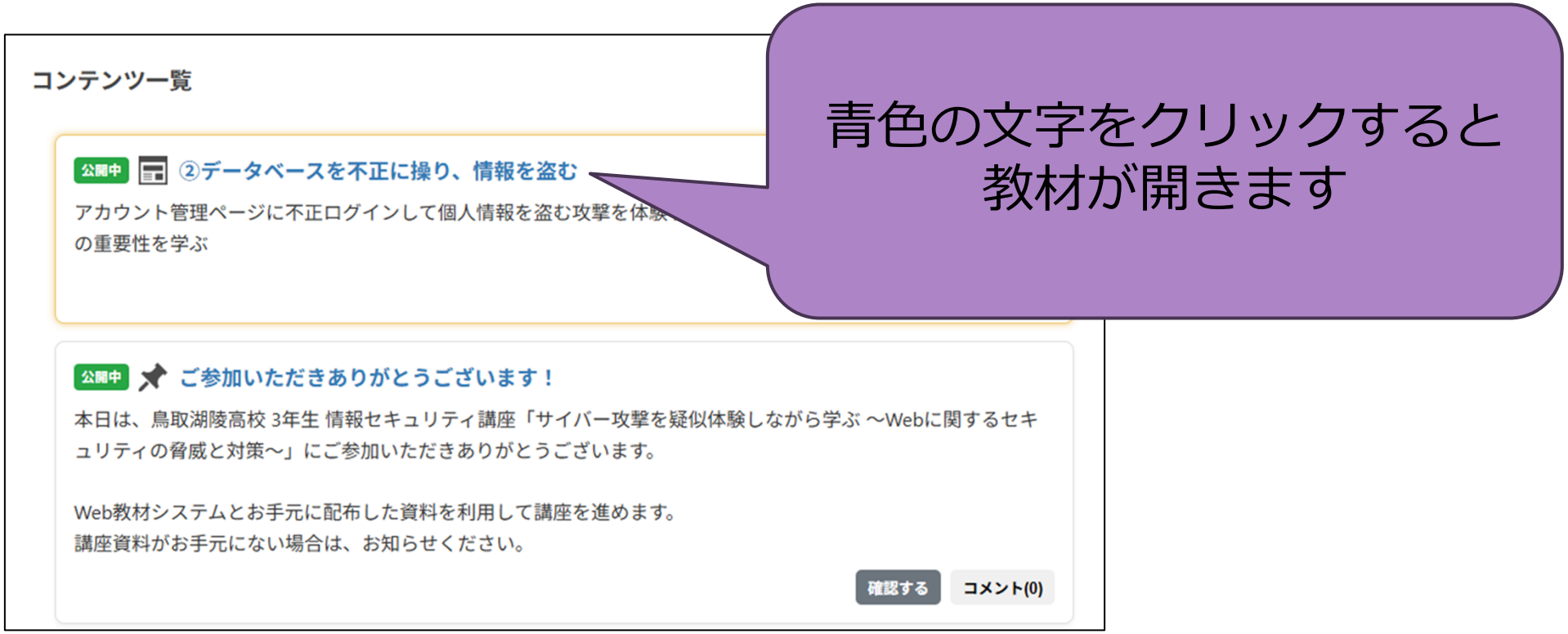
▶データベースに送信するデータの中にSQL文を混入する
→サービス提供者の意図しない不正な操作をすること

▶不正なログインが可能に
→ユーザ認証をごまかす

▶データベースのデータをすべて削除される
→編集や削除の指示をすることによって可能

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇教材を配信します



２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇演習の想定

▶社内システムのログイン画面に脆弱性があります

〇どのような脆弱性があるのか…

▶パスワードの入力欄にSQL文を記述することが可能です
→認証するときにそのままSQL文を送信してしまいます

▶不正にログインすることで個人情報をすべて閲覧できます

▶すべてのユーザのパスワードが閲覧できます
→詳しい説明は，後ほどします

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

○お題１：正しいパスワードを入力することなくシステムにログインする

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題１：正しいパスワードを入力することなくシステムにログインする

▶まずは普通にログインしてみましょう

IDに「admin」パスワードに
「password」と入力してください

初期アカウントとパスワード
あるあるですね…絶対だめですよ！

2．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題１：正しいパスワードを入力することなくシステムにログインする

▶まずは普通にログインしてみましょう

普通にログインできました.
なんも不思議な点は
ありません….

まあ，実はこれが
怖いところなんですが….

確認出来たら「ログアウト」
しておいてください.

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題１：正しいパスワードを入力することなくシステムにログインする

▶では，不正にログインをしてみましょう

〇その前に，以下の言葉を聞いてどう思いますか？

▶AがAであるとき正しい

→かなり違和感があるけど，まあそうだよね

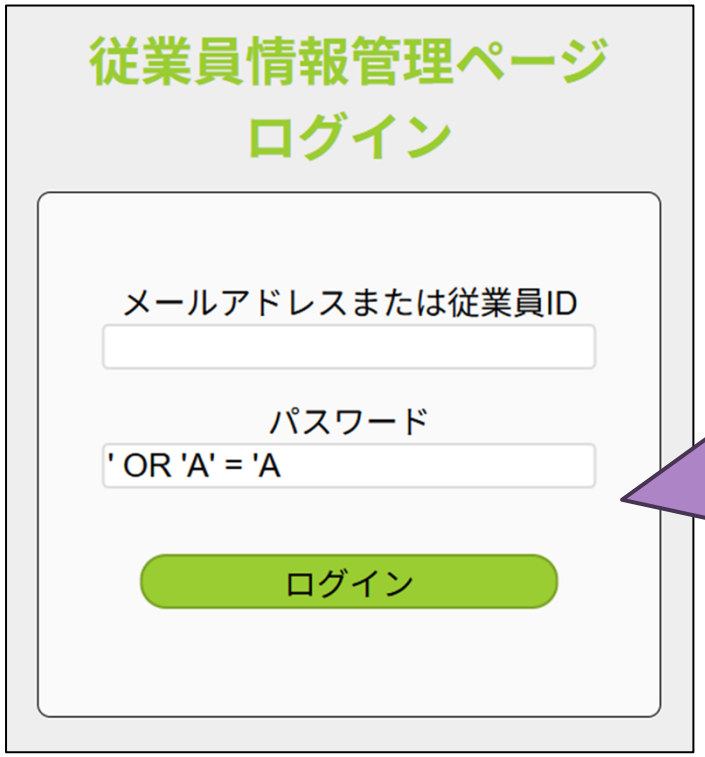
▶1が1であるとき正しい

→これも当たり前だよね

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

○お題１：正しいパスワードを入力することなくシステムにログインする

▶では，不正にログインをしてみましょう



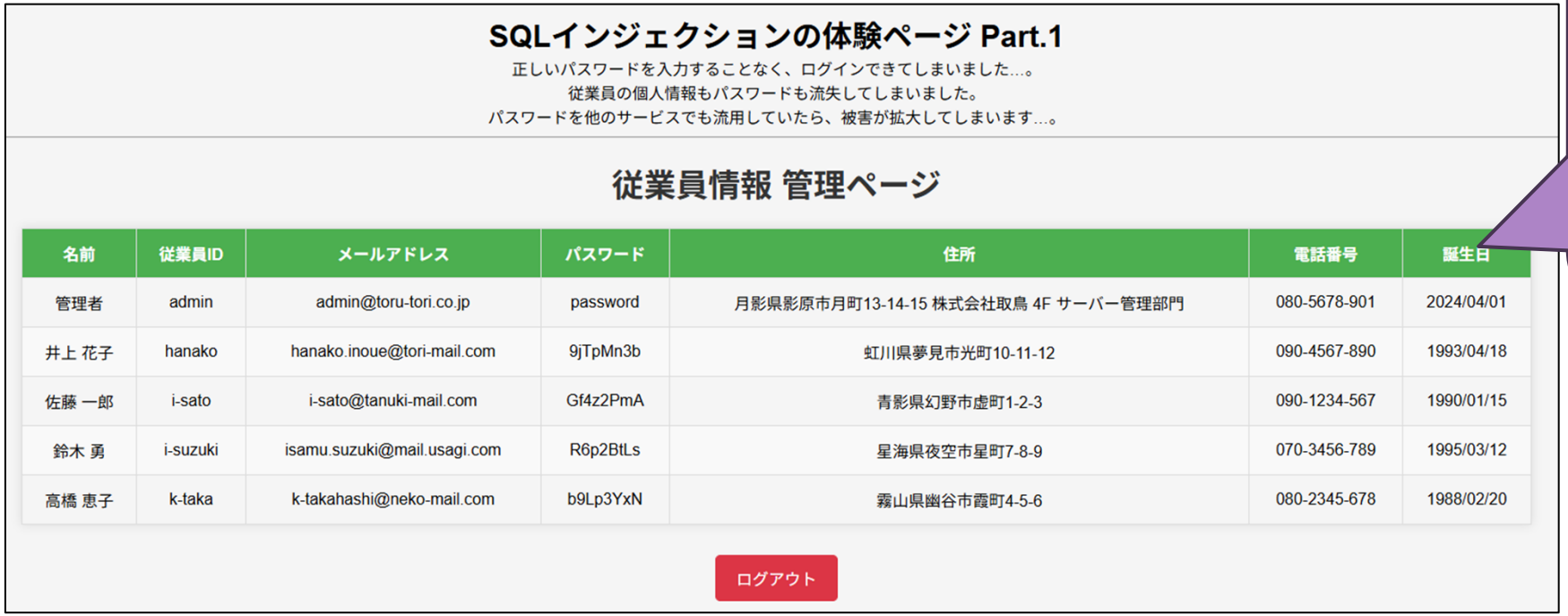
IDは入力しなくていいです
パスワードを以下のように
入力してください

' OR 'A' = 'A

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題１：正しいパスワードを入力することなくシステムにログインする

▶まずは普通にログインしてみましょう



SQLインジェクションの体験ページ Part.1

正しいパスワードを入力することなく、ログインできてしまいました…。
従業員の個人情報もパスワードも流失してしまいました。
パスワードを他のサービスでも流用していたら、被害が拡大してしまいます…。

従業員情報 管理ページ

名前	従業員ID	メールアドレス	パスワード	住所	電話番号	誕生日
管理者	admin	admin@toru-tori.co.jp	password	月影県影原市月町13-14-15 株式会社取鳥 4F サーバー管理部門	080-5678-901	2024/04/01
井上 花子	hanako	hanako.inoue@tori-mail.com	9jTpMn3b	虹川県夢見市光町10-11-12	090-4567-890	1993/04/18
佐藤 一郎	i-sato	i-sato@tanuki-mail.com	Gf4z2PmA	青影県幻野市虚町1-2-3	090-1234-567	1990/01/15
鈴木 勇	i-suzuki	isamu.suzuki@mail.usagi.com	R6p2BtLs	星海県夜空市星町7-8-9	070-3456-789	1995/03/12
高橋 恵子	k-taka	k-takahashi@neko-mail.com	b9Lp3YxN	霧山県幽谷市霞町4-5-6	080-2345-678	1988/02/20

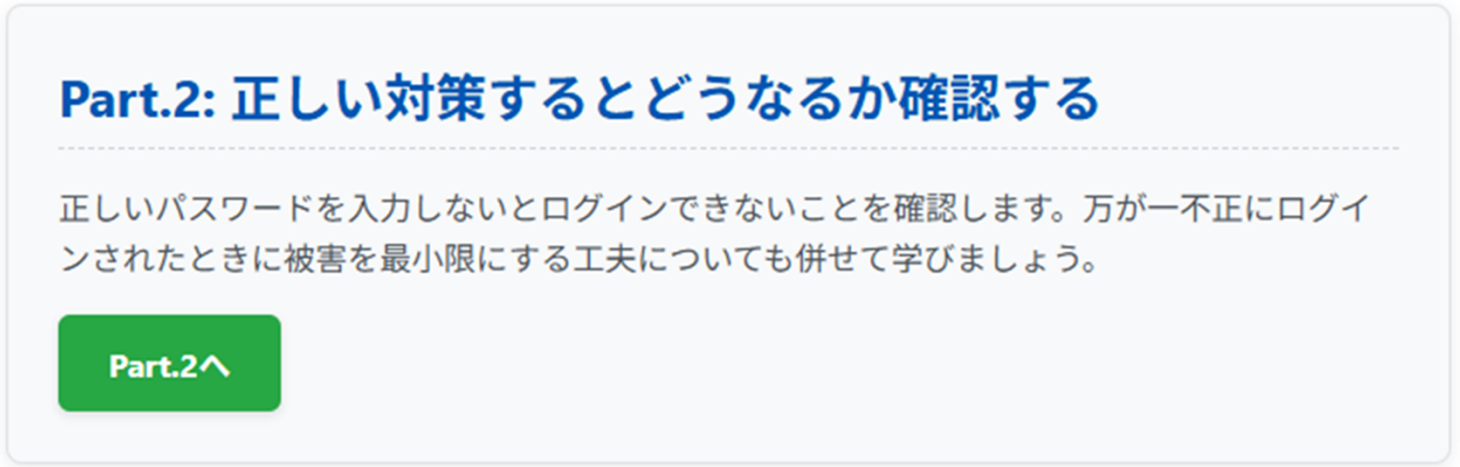
ログアウト

あれ…
ログインできた…

個人情報丸見え…

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

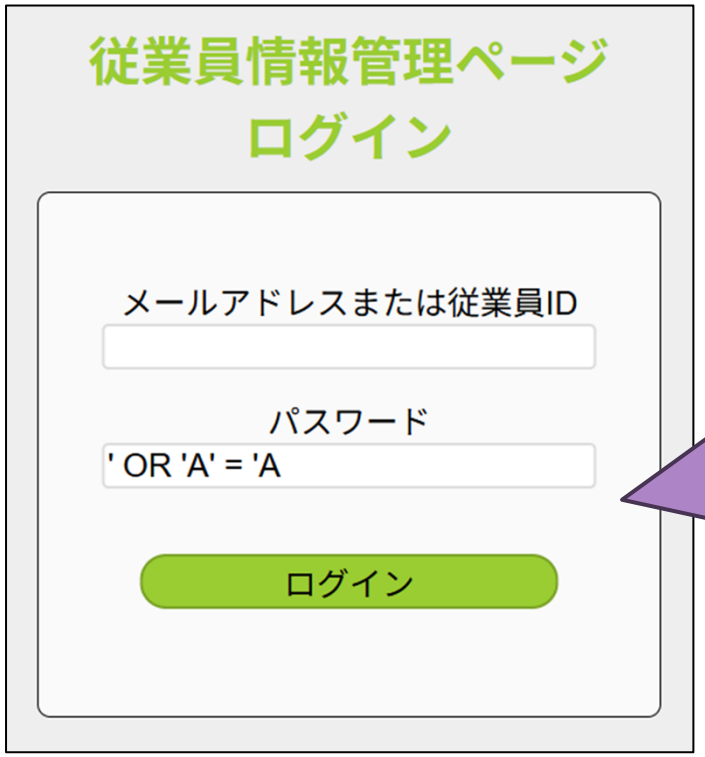
〇お題２：対策済みのログインページでも確認しておこう



２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題２：対策済みのログインページでも確認しておこう

▶不正ログインを試しておきましょう



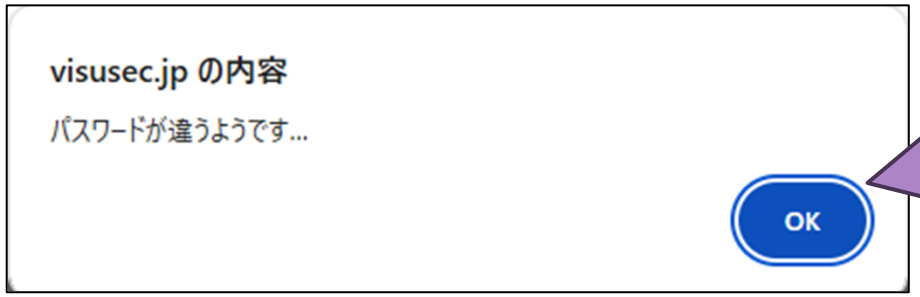
IDは入力しなくていいです
パスワードを以下のように
入力してください

' OR 'A' = 'A

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題２：対策済みのログインページでも確認しておこう

▶不正ログインを試しておきましょう



当然ログインできないですよね

もしできるなら，世の中の
システム不正し放題ですよ(笑)

違いは後ほど説明します

2．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇お題：正しいパスワードを入力することなくシステムにログインする

▶なぜログインできたのか

〇DBに確認する命令に問題が…

▶SELECT * FROM USERS WHERE id = '$id' AND pass = '$pass'

→変数として入力した内容をそのまま検索の命令に利用…

SQL文	役割
SELECT * FROM USERS	USERSテーブルの一覧を取得したいです
WHERE	検索条件を次に示します
id = '$id' AND pass = '$pass'	idに関する情報が入力した変数idと一致するとき さらにpassに関する情報が入力した変数passと一致するとき

２．Webに関するセキュリティの脅威と対策
② データベースを不正に操り，情報を盗む

〇理解してほしいこと

▶SQL文を利用するときに入力された情報をそのまま利用するのは危険

→危険だけど認証するには入力された情報を利用する必要はある…

→何らかの形で処理をする？

▶情報の流失や破壊につながること

→DBをつかさどる命令を外部からされることは非常に危険

→大事なデータなどの資産喪失

→顧客からの信頼の喪失・売り上げにおける損失

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇サーバに不正な指示を出す

▶今回の標的は，サーバ全体（OS）にダメージを与えること
→XSSとSQLインジェクションはあくまで一機能に被害を与えた

▶OSは，コンピュータを動作させるための基本ソフトウェア
→プロセスの管理やファイルの管理など様々な指示が飛び交う

〇 OSの指示（コマンド）の中に不正な指示を紛れ込ませれば…

→サーバに壊滅的なダメージを与えられる…
→不正にファイルを奪取される…

２．Webに関するセキュリティの脅威と対策

③ サーバに不正な指示を出す

○ OSコマンドインジェクション

▶サーバに対して意図しないコマンドを強制的に実行させる攻撃
→ウェブアプリケーションの脆弱性を利用する

▶サーバ内の情報が漏洩，改ざん，削除

▶マルウェアなど不正なソフトウェアの実行

２．Webに関するセキュリティの脅威と対策

③ サーバに不正な指示を出す

○ OSコマンドインジェクションはどのように実行されるのか？

▶基本的にはSQLインジェクションと同じ

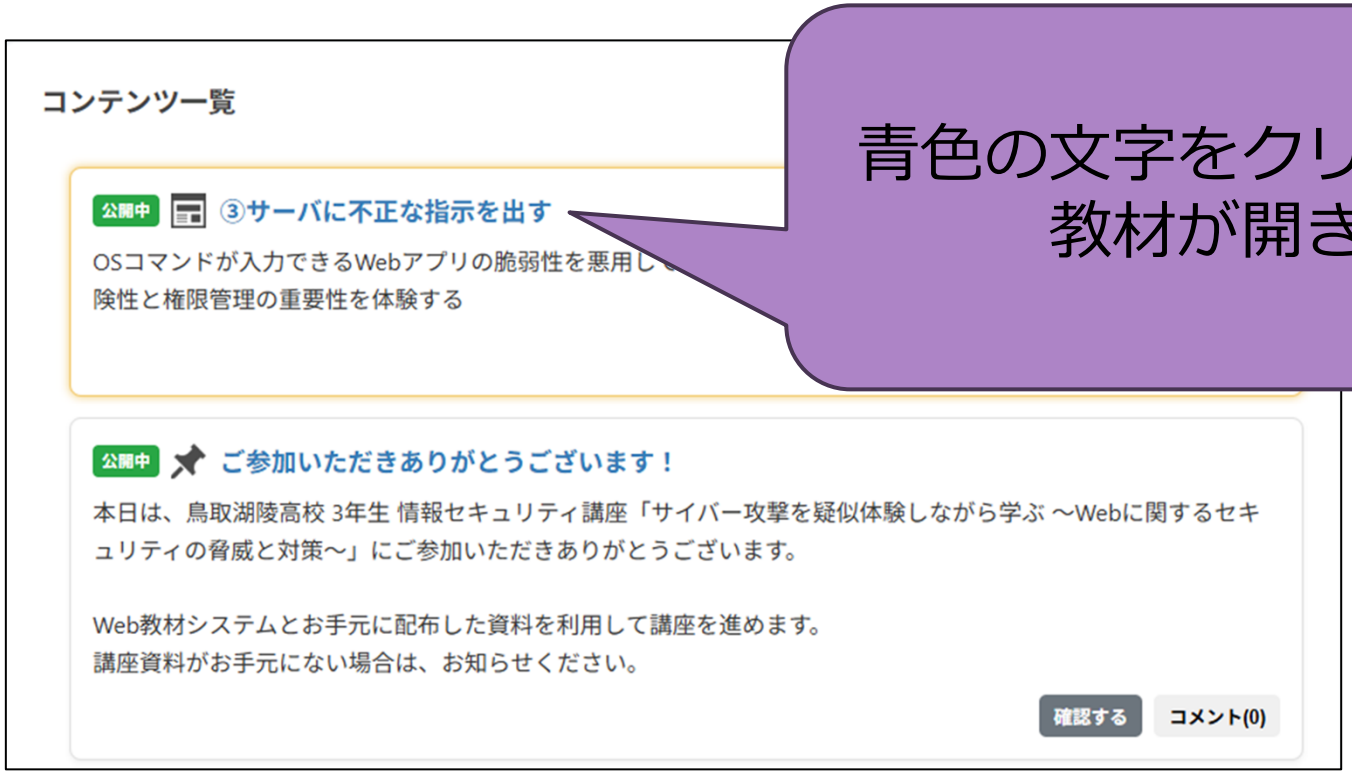
→結局は，Webアプリケーション側に脆弱性がある

▶攻撃手段が「SQL文」なのか「OSコマンド」なのかの違い

→ファイルの検索などにOSコマンドを直接利用すると危険…

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇教材を配信します



２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇演習の想定

▶クラウドストレージサービスを想定します

→Google Drive・OneDrive・Dropbox　など

〇どのような脆弱性があるのか…

▶ファイルの検索機能に脆弱性がある

→OSコマンドを実行することでファイルの一覧を取得する

〇 OSコマンドを実行してファイル一覧を取得する？

▶スマホで写真のアプリを開いたときに一覧表示されるのと一緒

→内部的にはOSコマンドを利用している

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題１：ファイルが検索できるかの確認

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇お題１：ファイルが検索できるかの確認

▶ファイル検索の仕組みを理解しよう

〇ファイル検索にあたり実行するOSコマンドは？

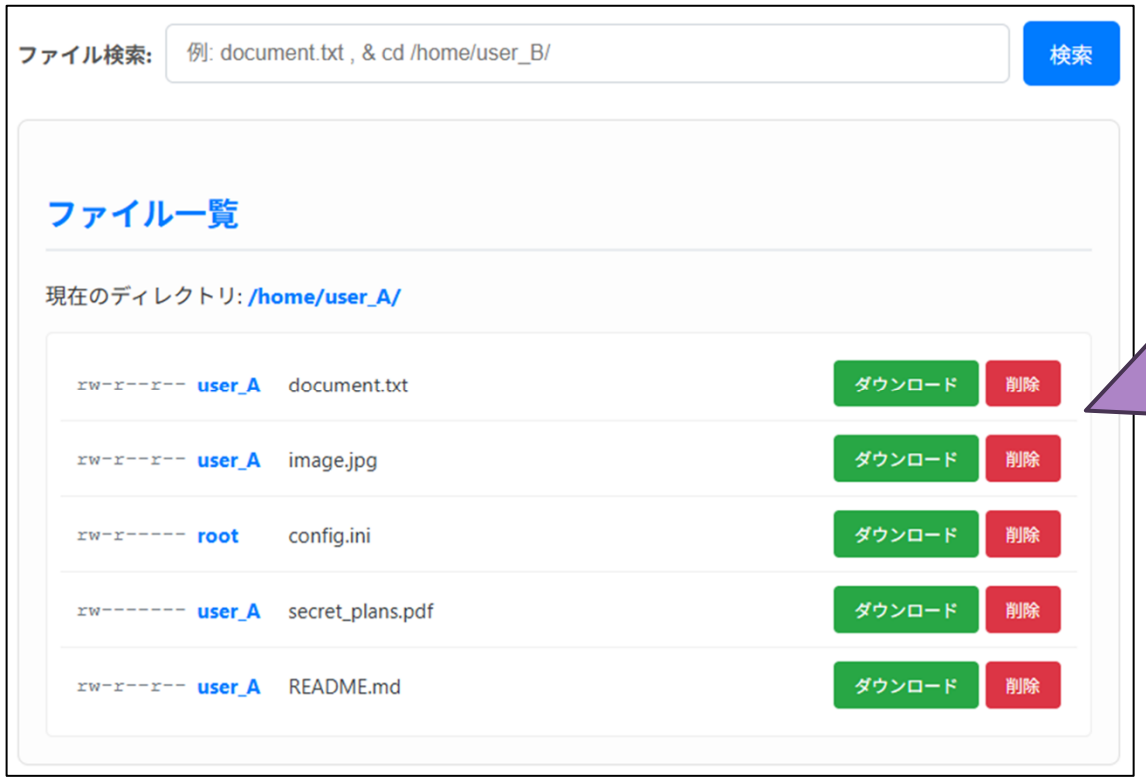
▶find $dir -name $keyword

→変数として入力した内容をそのまま検索の命令に利用…

SQL文	役割
find	ファイルやディレクトリを検索するためのコマンド
$dir	現在のディレクトリの情報が入った変数dir
-name $keyword	変数keywordに入っている情報を用いて， 完全一致または部分一致のファイルがあるか検索

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題２：他人のディレクトリにアクセスしよう

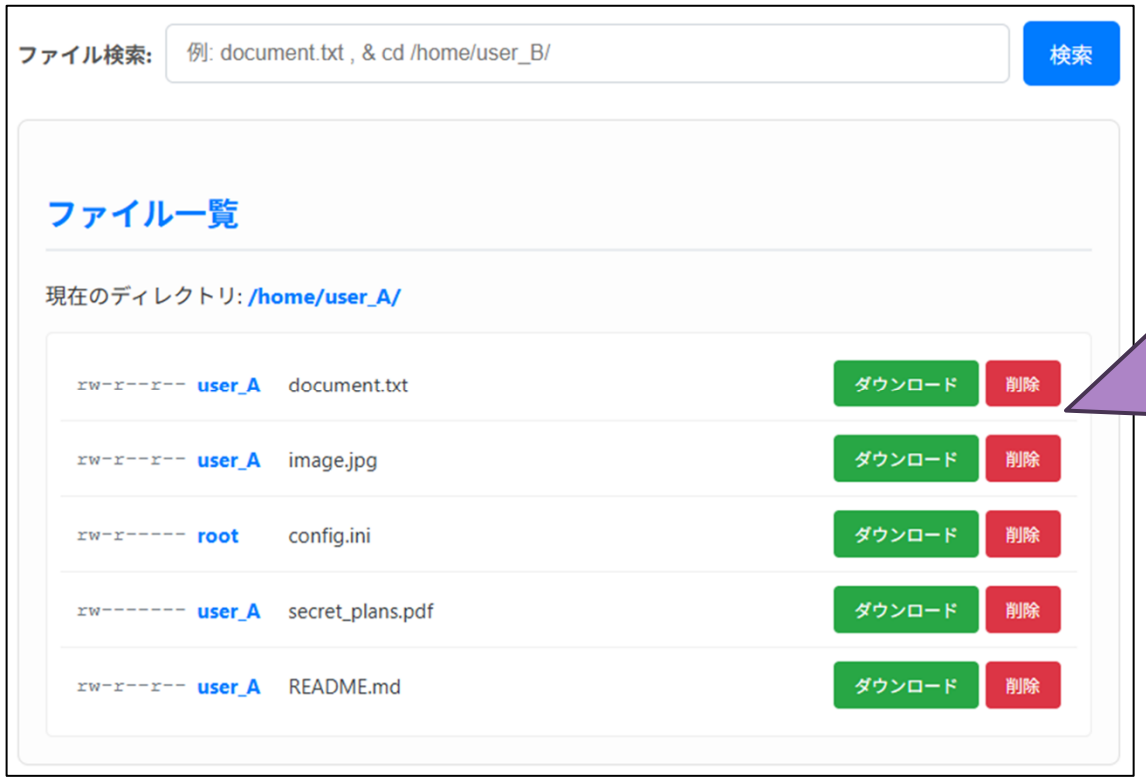


今は，/home/user_A/を
閲覧している状態です

user_Aはあなたのユーザ
ですから見ることが
できるのは当然ですね

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題２：他人のディレクトリにアクセスしよう

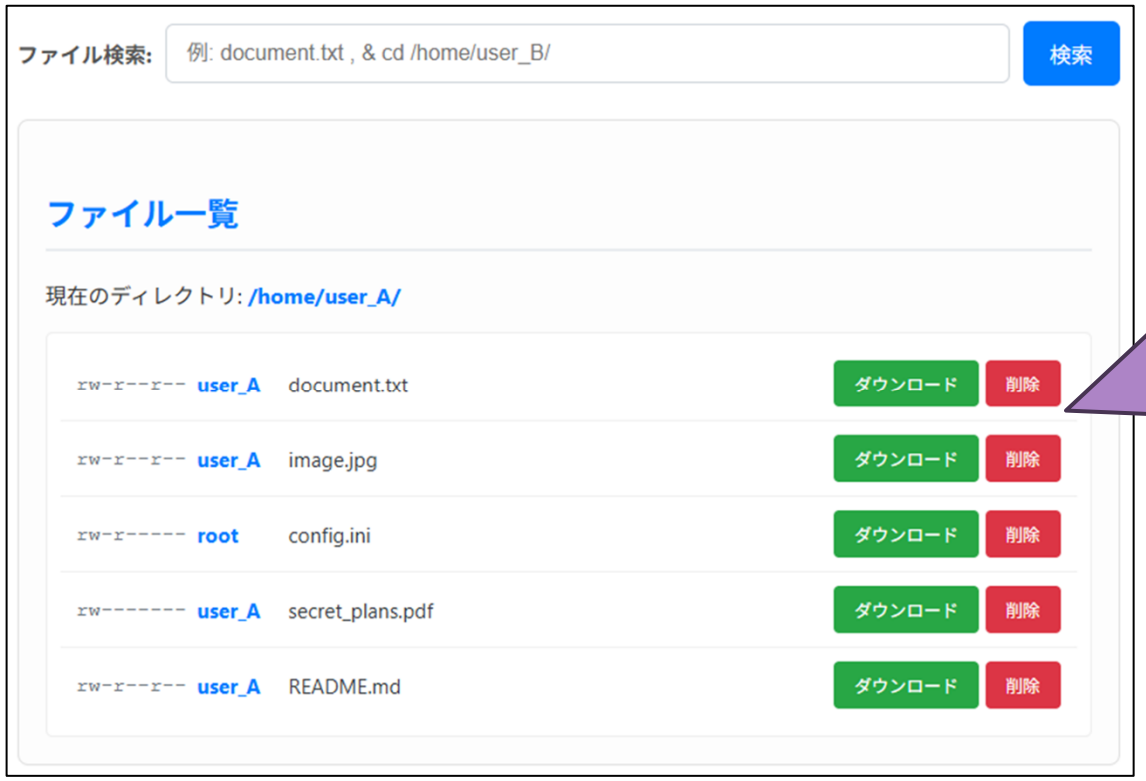


もしも，他人のディレクトリを
見ることができたら…

この画面を探しても，どこにも
ユーザを変更する
ボタンなどはないよね…

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題２：他人のディレクトリにアクセスしよう

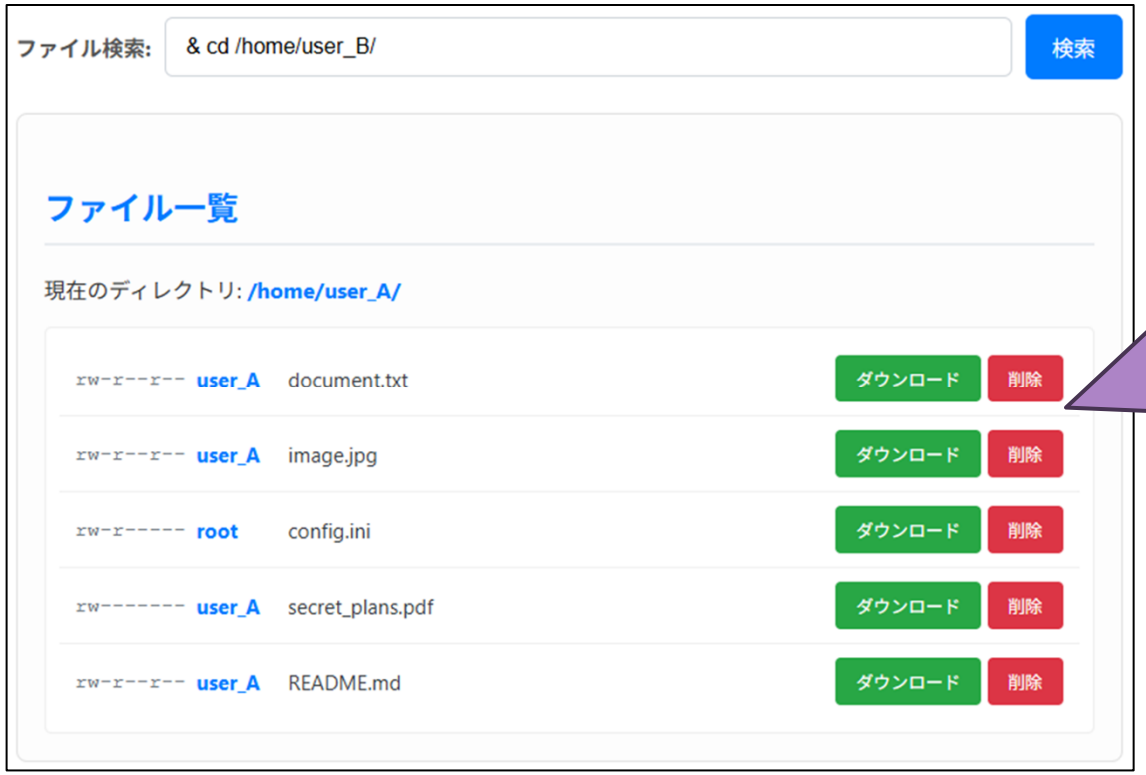


もしも，他人のディレクトリを
見ることができたら…

この画面を探しても，どこにも
ユーザを変更する
ボタンなどはないよね…

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題２：他人のディレクトリにアクセスしよう

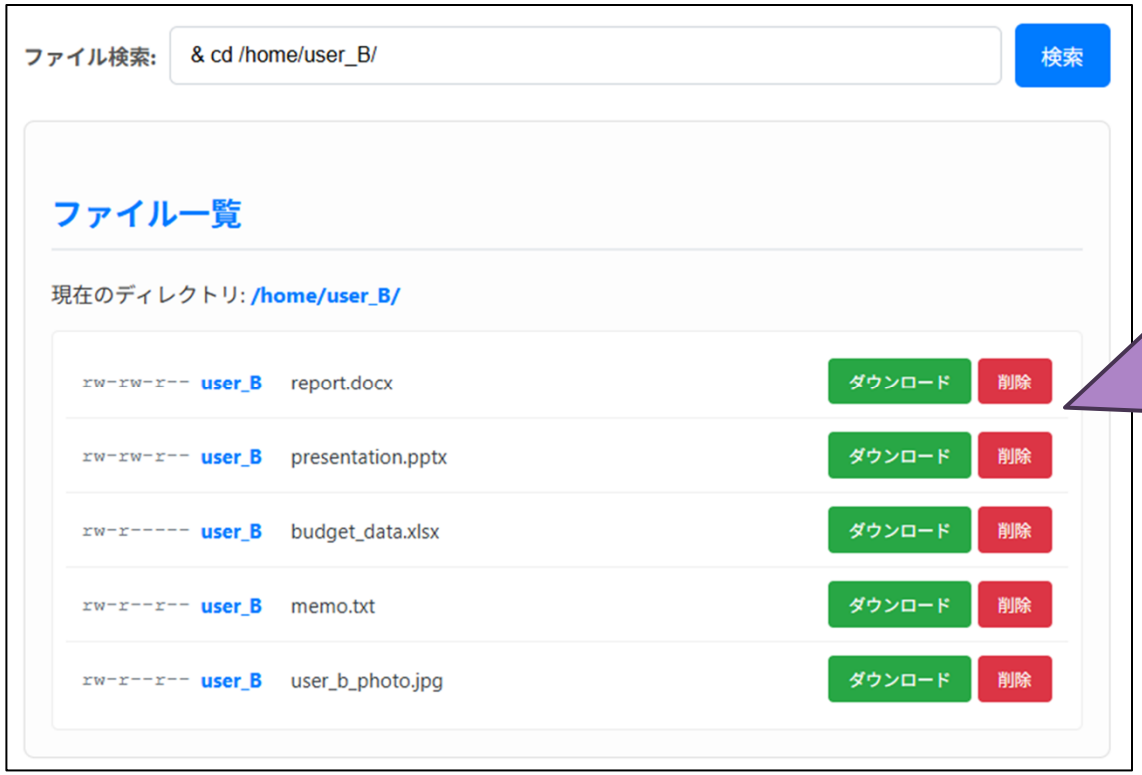


ファイル検索の欄に以下の内容を入力して「検索」を押してください

& cd /home/user_B/

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題２：他人のディレクトリにアクセスしよう



今は，他人のディレクトリ
/home/user_B/を
閲覧している状態です…

先ほど入力したcdコマンドは，
change directory（ディレクトリを変更する）指示でした

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇お題２：他人のディレクトリにアクセスしよう

▶なぜ，ディレクトリを切り替えることができたのか？

〇ディレクトリ切り替えにあたり実行するOSコマンドは？

▶find $dir -name $keyword

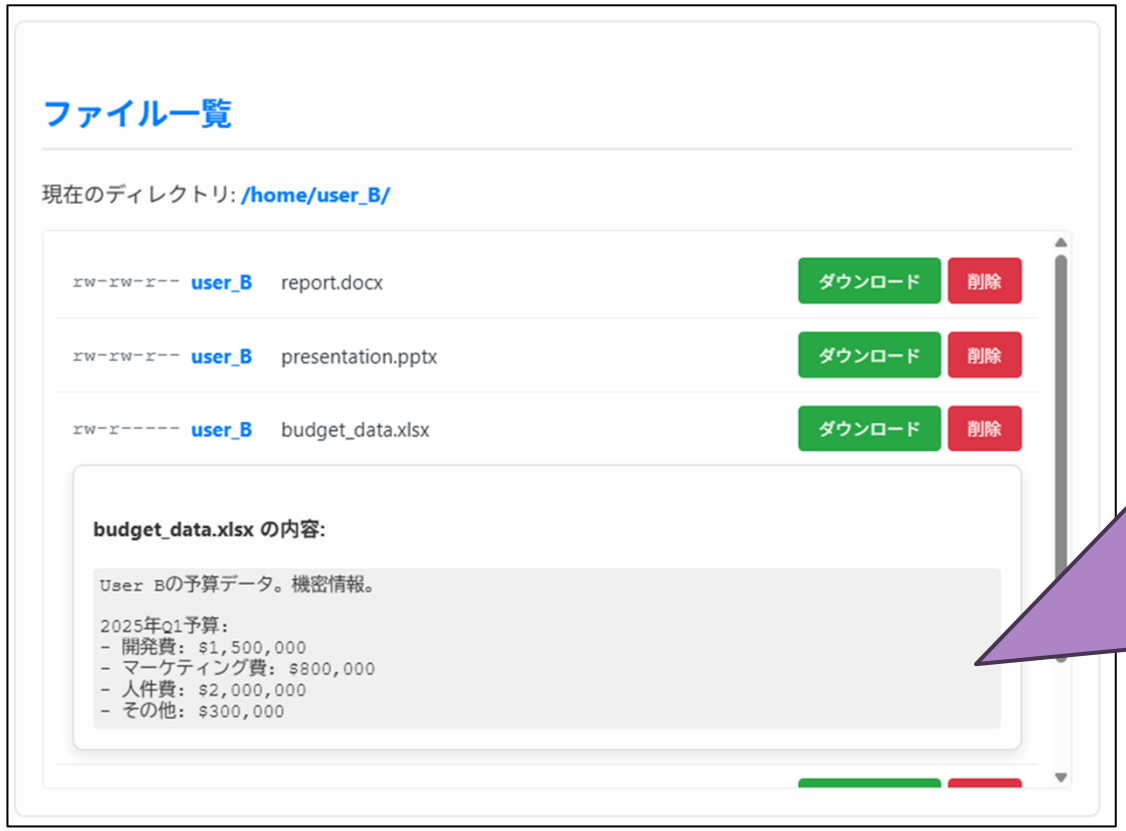
→ $keyword = 「& cd /home/user_B/」

▶実行すると「find $dir -name & cd /home/user_B/」

→「&」をつけると，別々の命令を結合して実行できる

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題３：他人のディレクトリを物色しよう



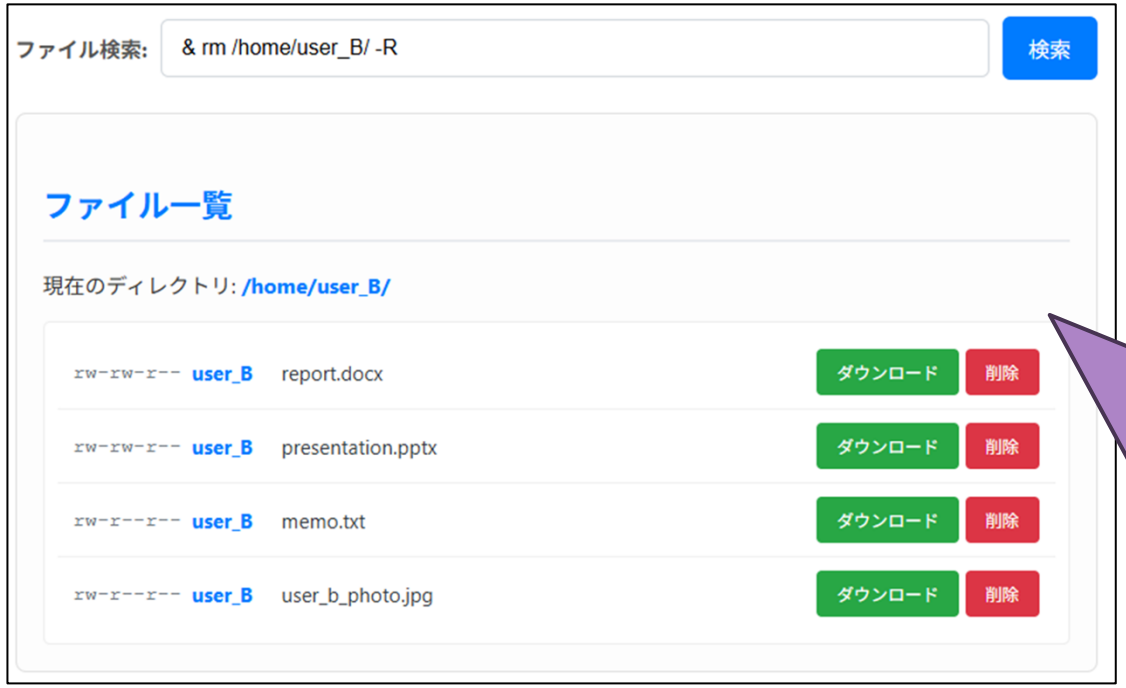
各ファイルをクリックすると
その詳細が閲覧できます．

機密情報が閲覧できましたね….
削除ボタンを押せば，削除も
できてしまいました．

１つずつ消すの面倒だな….

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題３：他人のディレクトリを破壊しよう



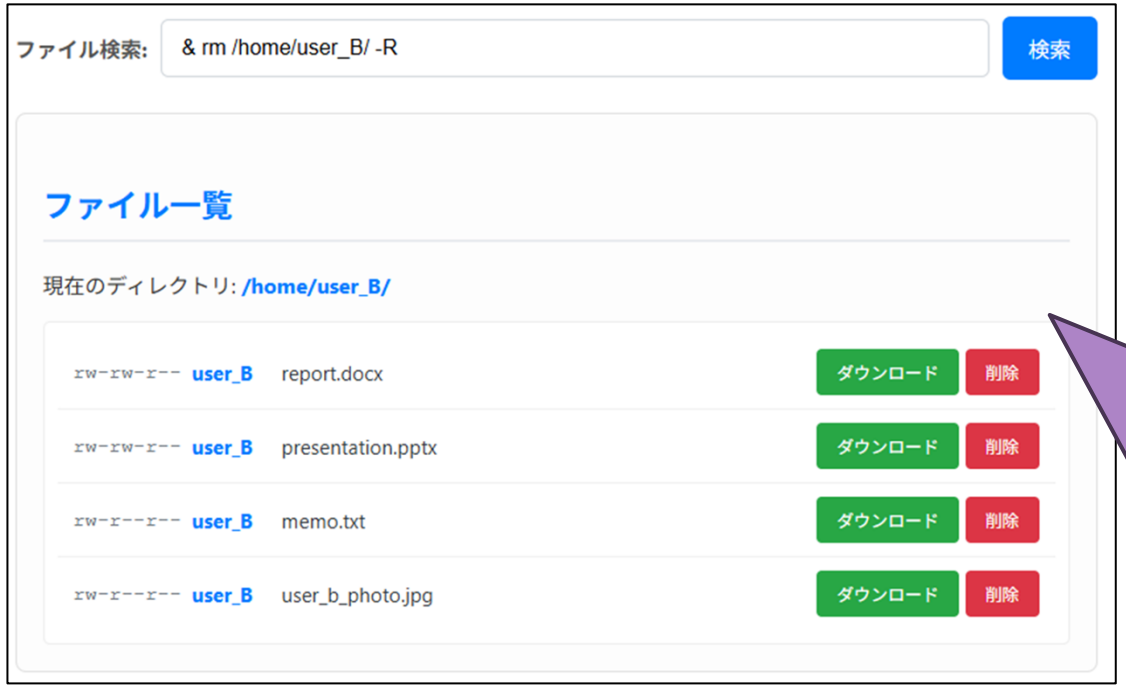
嫌がらせの最終形です.

全てのデータを
消してやりましょう....

& rm /home/user_B/ -R

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題３：他人のディレクトリを破壊しよう



嫌がらせの最終形です.

全てのデータを
消してやりましょう....

& rm /home/user_B/ -R

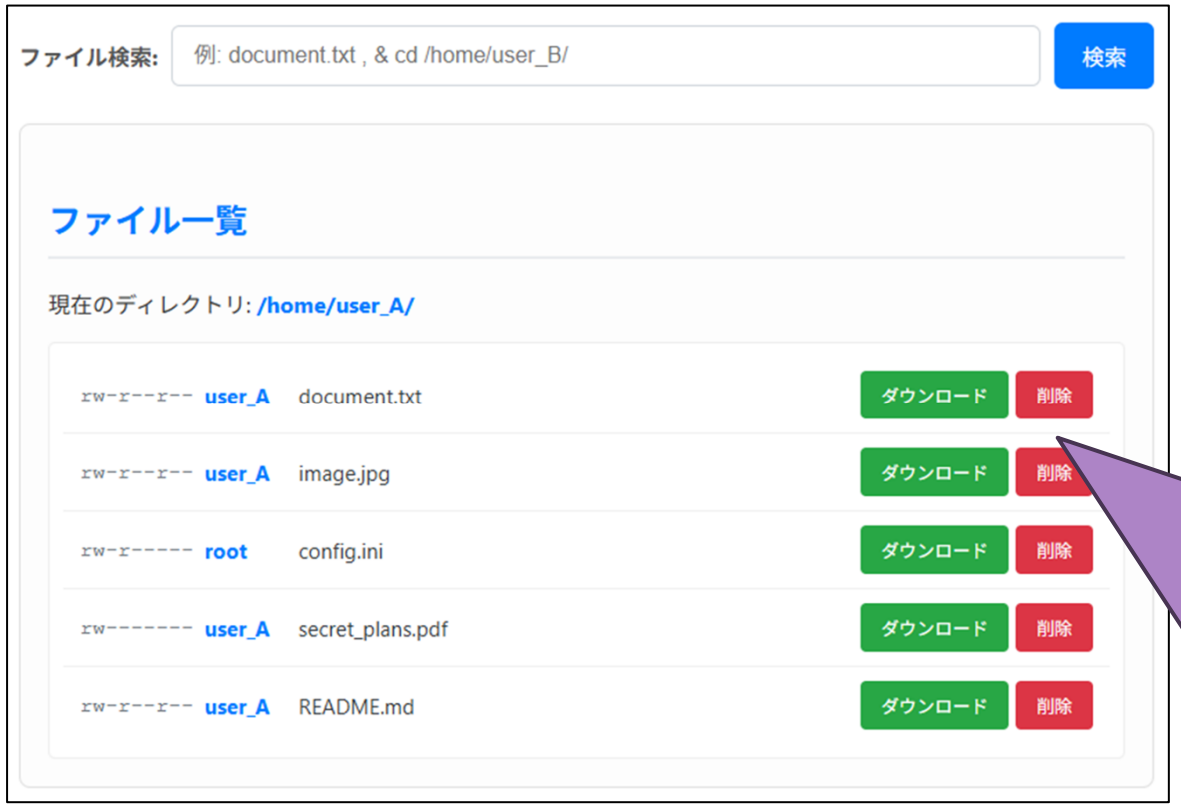
２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題３：他人のディレクトリを破壊しよう

あらら，すべてのファイルが消えましたね…

2．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題４：パスワードを閲覧してサーバの乗っ取りを目指す



サーバにはたくさんの情報が
格納されています.

重要度は様々ですが,
ユーザ情報とパスワードが
取得出来たらどうでしょう…

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

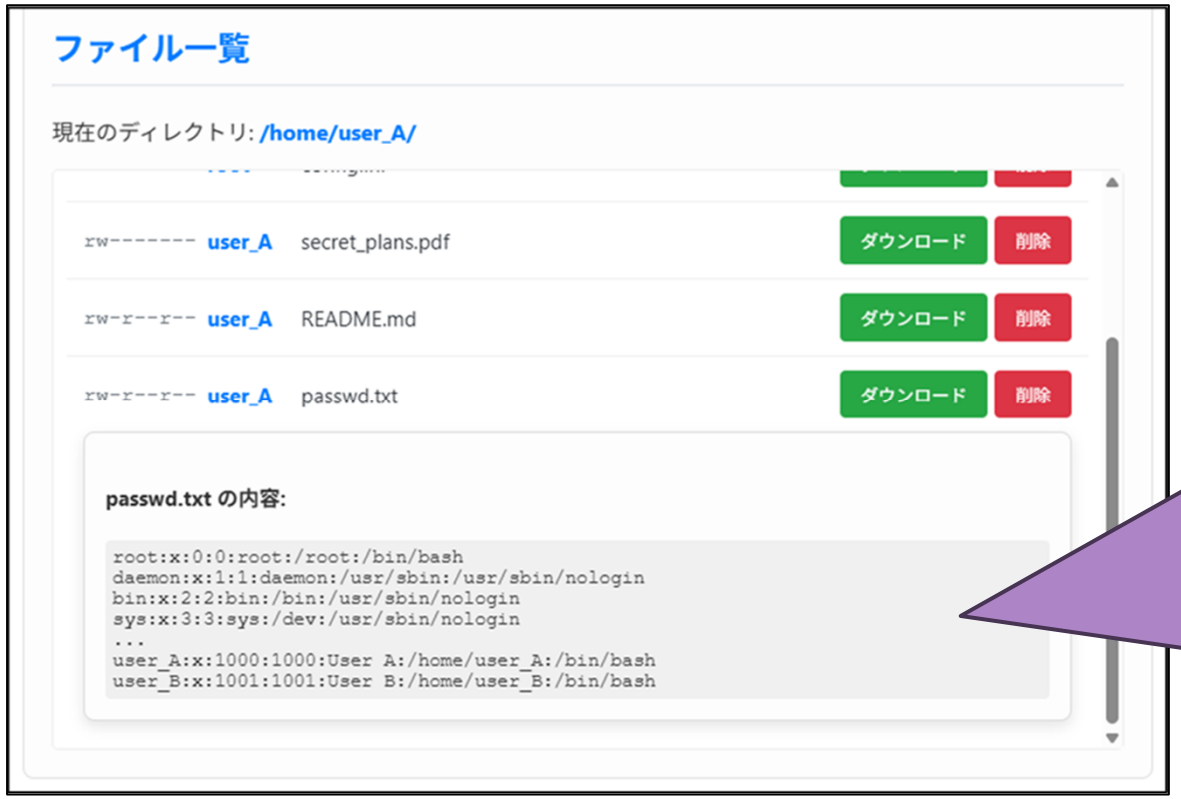
○お題４：パスワードを閲覧してサーバの乗っ取りを目指す

サーバの情報を直接見ることはできないので，一度ファイルに保存してから閲覧したいと思います．

& cp /etc/passwd passwd.txt

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

○お題４：パスワードを閲覧してサーバの乗っ取りを目指す



今のOSはパスワードを
直接閲覧できることは
ほとんどないのですが…
ユーザの一覧がばれましたね.

この情報もかなり収穫ですよ.
これを手掛かりにパスワードを
解析するなんてことも….

２．Webに関するセキュリティの脅威と対策
③ サーバに不正な指示を出す

〇理解してほしいこと

▶サーバ本体（OS）を外部から操作できるのは危険
→直接操作できないように対策する必要がある

▶情報の流失や破壊につながること
→大事なデータなどの資産喪失
→顧客からの信頼の喪失・売り上げにおける損失

▶アクセス権限の管理を徹底する必要がある
→ユーザごとに操作できる機能・領域を制約する
→仮にOSコマンドを使う場合でも，被害は軽減できる

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇不正な操作からサーバを守る

▶どのような対策を取ることが有効か考えてみよう

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇そもそもDBやOSに対する命令を入力させない

▶これが一番安全・安心な方法

→とはいえ，それができないことはある…

〇できることをしっかりと制限する

▶XSS：HTMLタグなどWebサイトの表示に影響を与える機能を制限

▶OSコマンドインジェクション：アクセスできるディレクトリの制限

→権限管理を明確にすることで，被害の拡大を抑止

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○エスケープ処理

▶特別な意味を持つ記号を別の文字列に置換する処理
→SQL・OSコマンドとして機能しない形に変更する

▶空港の保安検査と同じで，手荷物としてナイフを持ち込むと危険
→荷物を預ければ（管理方法の変更）取り出せないので，安全

元の文字	HTML	SQL・OSコマンド
&	&amp;	\&
<	<	\<
>	>	\>
'	&apso;	\'

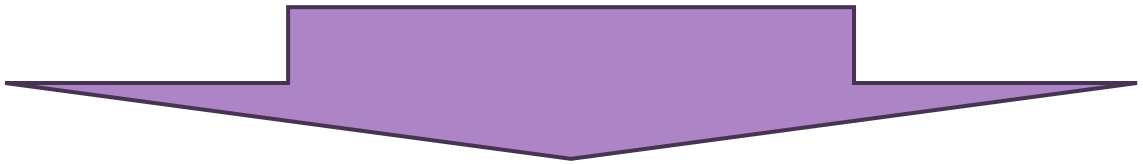
２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○エスケープ処理（SQL・OSコマンド）

▶引用符「'」という命令からただの文字列へ

→無害化に成功

SELECT * FROM USERS WHERE id = AND pass = OR 'A' = 'A'

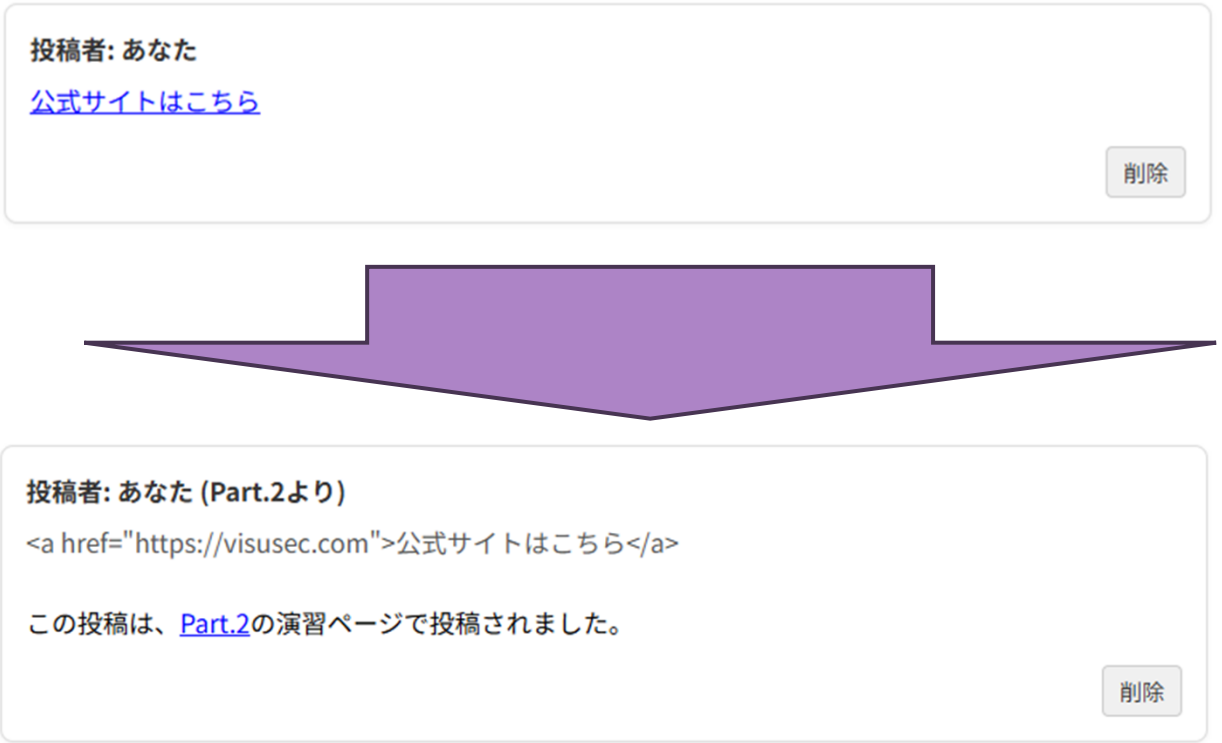


SELECT * FROM USERS WHERE id = AND pass = OR \'A\' = \'A\'

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○エスケープ処理（HTML）

▶括弧「<」「>」「"」「/」という命令からただの文字列へ
→無害化に成功



２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇万が一情報流出したときのための保険

▶流失しても簡単に読み解けない形のデータとして保管する
→流出はあってはいけないが，万が一に備えることが重要
→対策がずさんだと他のシステムにも不正侵入されるなど二次災害も

▶特にパスワードなど高い機密性が必要な情報の保護
→ハッシュ化を活用

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇ハッシュ化とは？

▶特定の計算式を用いて，元データを不規則な文字列に変換すること

▶SHA-256 などのハッシュ関数を用いる

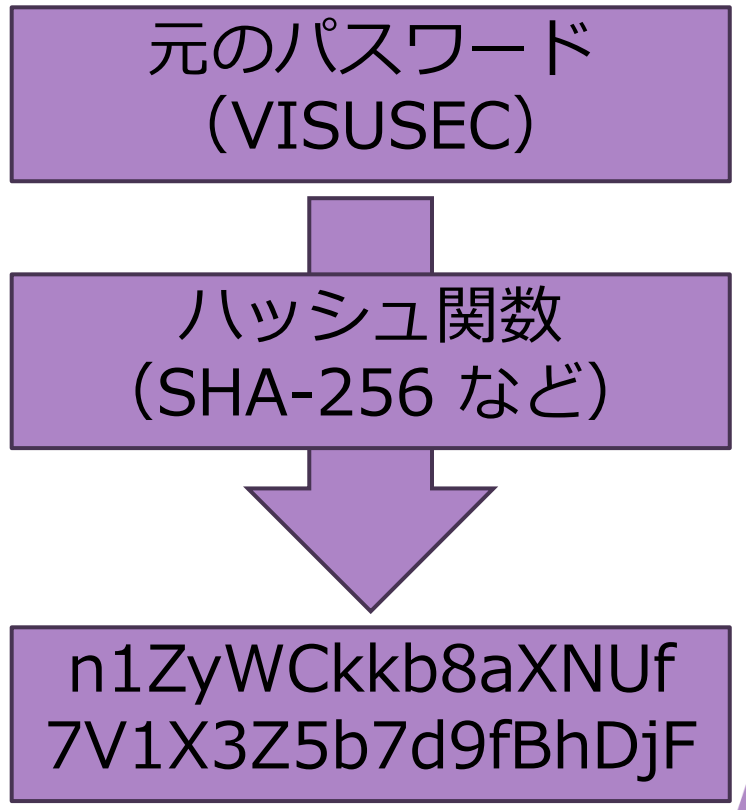
〇暗号化との違い

▶暗号化は可逆

→元の文字列に戻せる

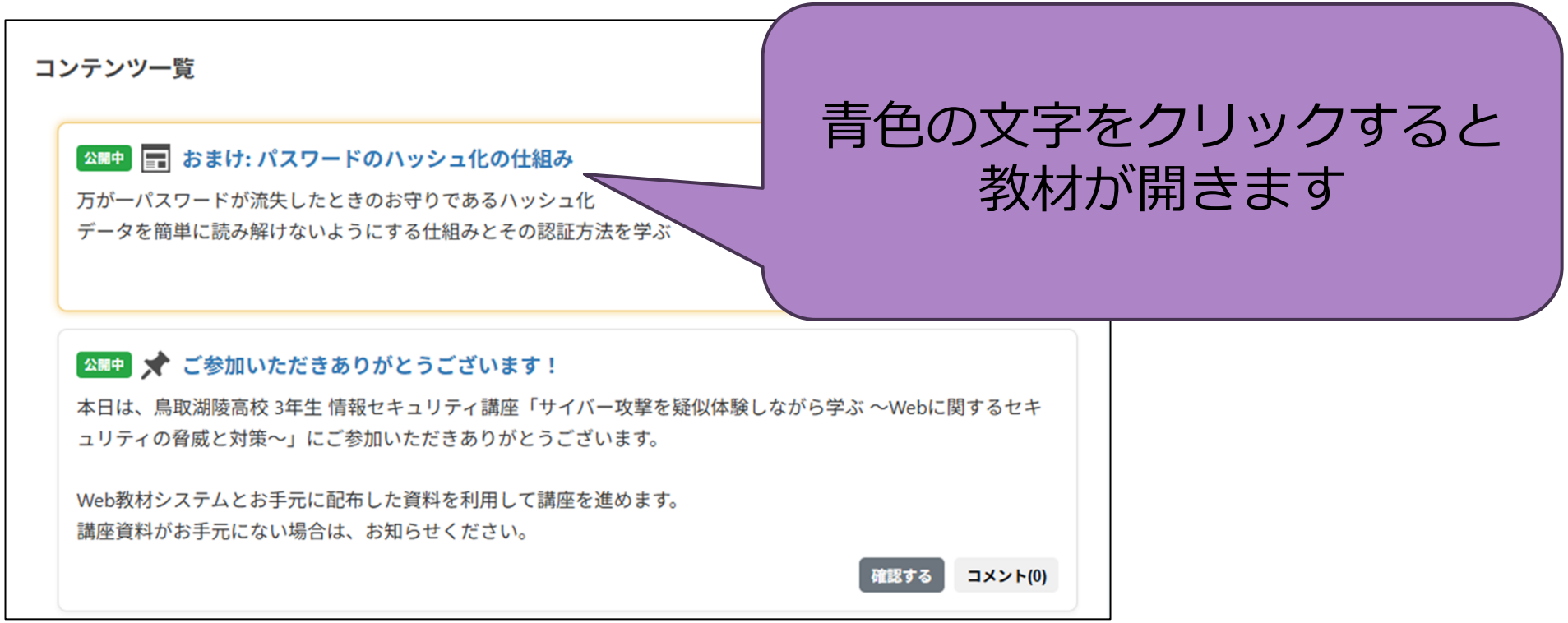
▶ハッシュ化は不可逆

→元の文字列に戻せないのでより安全



２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇教材を配信します（時間に余裕があれば…）

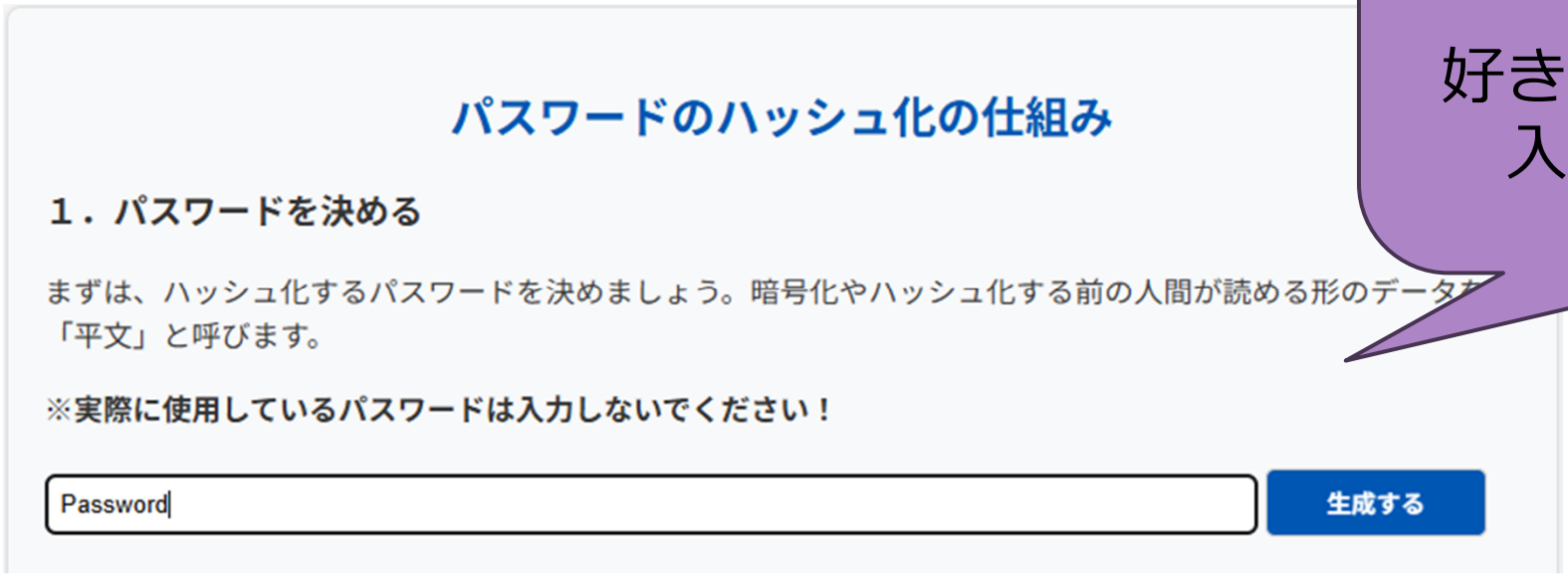


２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

パスワードをハッシュ化してみましょう.

好きな文字列でいいので入力してください.



２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

ハッシュ化の特徴は
ランダムな文字列を
利用して異なるハッシュ値
を作ることが特徴です．

ここでは，ランダムな
文字列（ソルト）を
作成します

２．ランダムな文字列（ソルト）を生成する

パスワードに追加するランダムな文字列を生成します。この文字列を「ソルト」と呼びます。ソル
で、同じパスワードでも異なるハッシュ値を生成し、安全性を高めることができます。

ハッシュ①	zuSVmBqfGW6Z1LqA
ハッシュ②	gMck2tYi6mPiF1J0
ハッシュ③	kC5ZoE00l4UN1Fu8

ソルト ＝ 塩ですが，料理などで塩の量を変えれば当然味は変わりますよね
食べ物に例えるなら，この塩加減による味の違いがハッシュ値の特徴です

2．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

元のパスワードにソルトを
加えてハッシュ値を
作成します

元のパスワードは同じなの
にハッシュ値は
全部違いますね

3．ソルトを利用してパスワードをハッシュ化する

生成されたソルトを使って平文のパスワードをハッシュ化します。これにより、パスワードはそのまま保存
ず、ハッシュ値として保存されるため安全です。

	元のパスワード	×	ソルト	=	ハッシュ値
ハッシュ①	Password	×	zuSVmBqfGW6Z1LqA	=	W2Y4a6c8eAgCiEkG
ハッシュ②	Password	×	gMck2tYi6mPiF1J0	=	QwSyU0W2Y4a6c8eA
ハッシュ③	Password	×	kC5ZoE00l4UN1Fu8	=	NtPvRxTzV1X3Z5b7

ソルト ＝ 塩ですが，料理などで塩の量を変えれば当然味は変わりますよね
食べ物に例えるなら，この塩加減による味の違いがハッシュ値の特徴です
一度混ぜてしまえば二度と戻せませんが，塩を混ぜた後の味がハッシュ値です

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

データベースに記録するときは，ソルトとハッシュ値を結合して保存します．

ソルトを保持しておくことが重要なんです

４．データベースにはソルトとハッシュ値を結合して保存する

データベースには、生成したソルトとハッシュ値を結合して保存します。この方法により、同じパスワード
っても異なるソルトが使われている限り、ハッシュ値も異なります。

	データベースに保存する形式
ハッシュ①	zuSVmBqfGW6Z1LqAW2Y4a6c8eAgCiEkG
ハッシュ②	gMck2tYi6mPiF1J0QwSyU0W2Y4a6c8eA
ハッシュ③	kC5ZoE00l4UN1Fu8NtPvRxTzV1X3Z5b7

つまりは，塩分をどれだか入れたかの情報と
その結果どんな味になったかを記録しておくわけですね
ちなみに，塩分の量が分かったところで，元の材料を正確には把握できません
そんなこと，たとえ有名シェフでもできないでしょ

2．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

5．認証時にハッシュ値が一致するか確認する

データベースに保存されたデータからソルトを取り出し、入力されたパスワードで新たなハッシュ値を生成します。

Password　　認証する

	再生成ハッシュ	保存ハッシュ	一致結果
ハッシュ①	W2Y4a6c8eAgCiEkG	W2Y4a6c8eAgCiEkG	一致
ハッシュ②	QwSyU0W2Y4a6c8eA	QwSyU0W2Y4a6c8eA	一致
ハッシュ③	NtPvRxTzV1X3Z5b7	NtPvRxTzV1X3Z5b7	一致

パスワードが一致するかの確認は，最初にソルトとハッシュ値の連結した文字列からソルトだけ取り出します．

入力したパスワードと取り出したソルトでハッシュ値を作成して，それらが一致するかを確認します

塩分をどれだけ入れたかの情報をもとに
新たに準備した食材（入力したパスワード）をもとに再度味付けをしてみます．
この時の味付けが全く同じになれば，晴れて認証成功という判断をするわけです

2．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

○ハッシュ値の作り方・認証の仕方

5．認証時にハッシュ値が一致するか確認する

データベースに保存されたデータからソルトを取り出し、入力されたパスワードで新たなハッシュ値を生成します。

password　[認証する]

	再生成ハッシュ	保存ハッシュ	一致結果
ハッシュ①	2Y4a6c8eAgCiEkGm	W2Y4a6c8eAgCiEkG	不一致
ハッシュ②	wSyU0W2Y4a6c8eAg	QwSyU0W2Y4a6c8eA	不一致
ハッシュ③	tPvRxTzV1X3Z5b7d	NtPvRxTzV1X3Z5b7	不一致

もちろん正しくない
パスワードを入れれば
同じハッシュ値ができない
ので認証失敗となります

塩分をどれだけ入れたかの情報をもとに
新たに準備した食材（入力したパスワード）をもとに再度味付けをしてみます．
この時の味付けが全く同じになれば，晴れて認証成功という判断をするわけです

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇どっちでパスワードを保存すればいいか…

▶一目瞭然だよね

名前	従業員ID	パスワード
管理者	admin	password
井上 花子	hanako	9jTpMn3b
佐藤 一郎	i-sato	Gf4z2PmA
鈴木 勇	i-suzuki	R6p2BtLs
高橋 恵子	k-taka	b9Lp3YxN

パスワード（ハッシュ化）
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e0f1a2b
e6f4a8e63a1f3c7e4b5f6d7c8a9b0c1d2e3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b
2e7a1b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e0f1a
5d83c3e8a9d0b1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇外部サービス（APIなど）の利活用の注意

▶昨今のWebサービスは自前で構築せず，外部に依存することがある
→開発コスト削減や開発期間の短縮が可能

▶非常に便利で特に小規模開発などに便利
→様々なAPIを組み合わせることはよくある

▶当然リスクもある…
→更新が頻繁に行われず，脆弱性がある…
→そもそも開発元に悪意がある…

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇連携コード（APIキー）などの流出（機密性）

▶外部システムと連携するうえでのIDとパスワードのような存在
→流出すると他人に悪用される懸念がある

▶クライアントサイド言語には絶対記載してはいけない
→端的に言えば，誰でも閲覧できるプログラム（JavaScriptなど）
→開発段階で試験的に記述したものの消し忘れが主な原因

▶通常は利用者からは閲覧できない場所に管理・記載する
→サーバサイド言語に記載するのが定石
→APIキーのみをファイルで管理する場合は，権限管理に要注意

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇APIへの不正なリクエストへの懸念（機密性・可用性）

▶APIとの情報のやり取りの方法が流出する
→通常想定されない利用のされ方をする懸念がある

▶外部から不正なリクエストが可能だと…
→無関係なデータを書き込まれるなど妨害を受ける可能性も
→アクセストークンなどを浪費して利用できなくなるかも

▶アクセス元を限定するなどの対策が必要
→特定のドメインやIPアドレスからに限定する

２．Webに関するセキュリティの脅威と対策
④ 不正な操作からサーバを守る

〇APIへの書き込みの際の懸念（完全性・機密性）

▶外部からだけでなく，内部からの不正なリクエストにも警戒
→XSSやSQLインジェクションと同じ

▶大手企業が提供する者は基本的には対策済み
→だからと言って過信しないこと

▶提供元に悪意はないですか？
→そもそも提供元に悪意があればいくら対策しても漏洩します

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

▶今回のセキュリティ事例の多くは人為的なミス

→SQLやOSコマンドといったシステムの核を露出させない

→楽に実装できる裏には，脆弱性が潜むことも少なくない

▶システムの脆弱性や更新情報にアンテナを立てること

→人為的なミスに次いで原因は，ハードウェア・ソフトウェアの不良

→OSやソフトウェアのアップデート，コミュニティからの情報収集

3．おわりに

〇今日のまとめ

▶適切な権限管理の必要性

→今回の演習環境は権限管理が滅茶苦茶だったことでやりたい放題…

→細かく管理をすればするほど強固にはなるけど，複雑に…

▶万が一に備えた対策をする

→いかなるミスも0にすることは難しい，万が一の備えが重要

→対策を怠ると，被害が拡大し社会的な責任・制裁を負うことに

→データの読み取りを難しくする・バックアップなど冗長化

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