鳥取湖陵高校 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
～不正アクセスとその対策～

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？

２．不正アクセスとその対策

⓪不正アクセスって何？どのように発生するのだろう…

①不正アクセスの侵入経路を特定して，封鎖しよう！

②特定されやすいパスワードって何だろう？

③情報にアクセスできる人を決める？できない人を制限する？

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

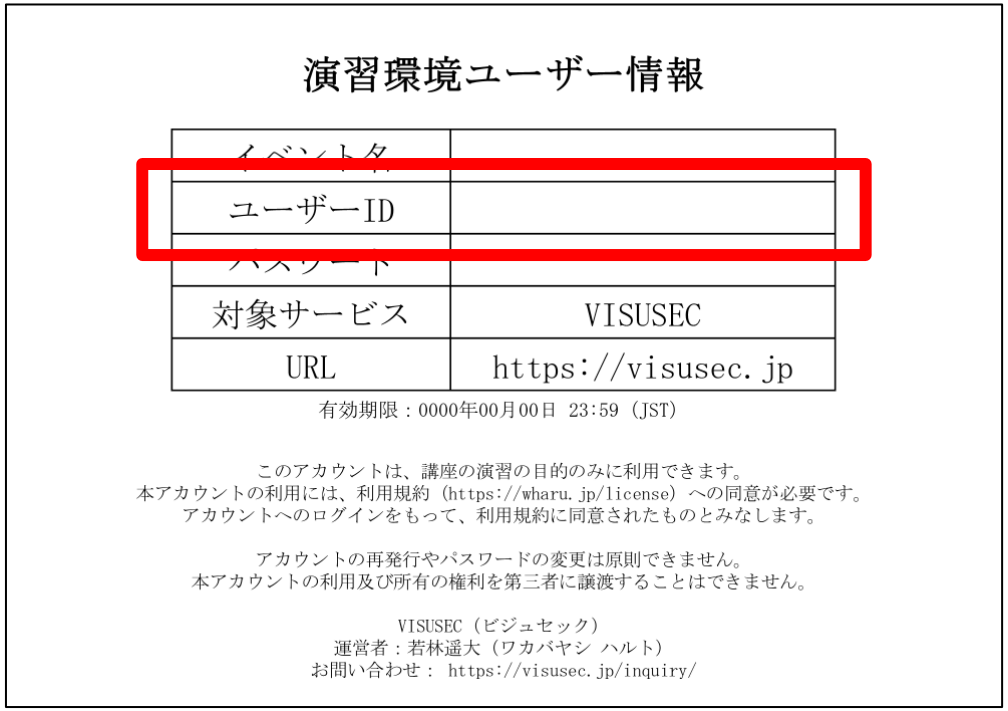
→ https://visusec.jp/

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）

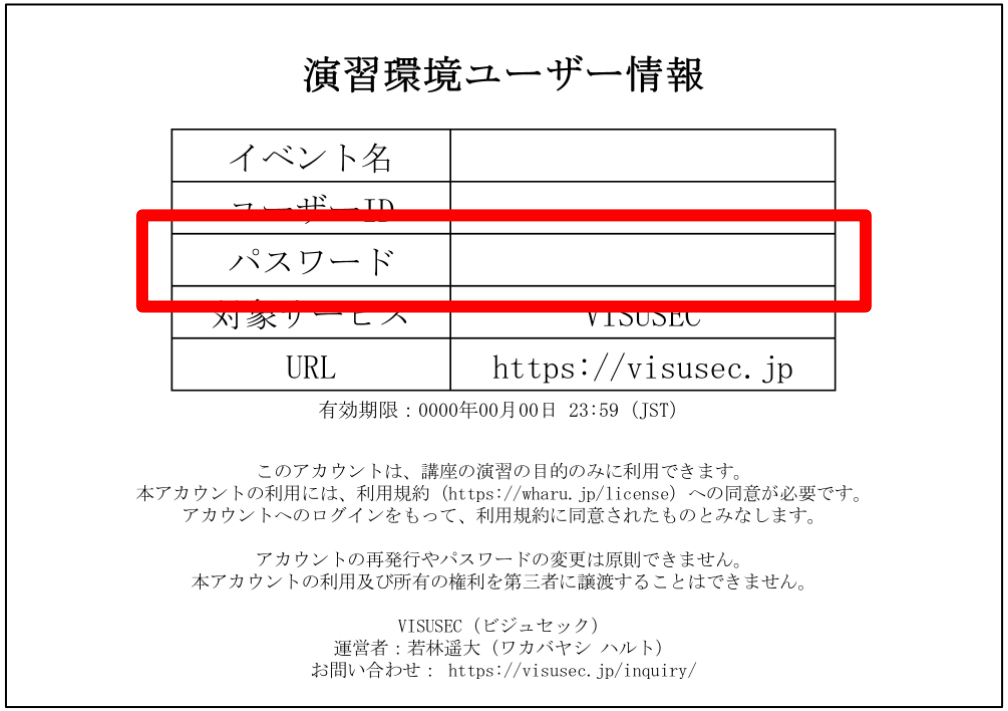
このアカウントは、講座の演習の目的のみに利用できます。
本アカウントの利用には、利用規約（https://wharu.jp/license）への同意が必要です。
アカウントへのログインをもって、利用規約に同意されたものとみなします。

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ログイン完了

２．不正アクセスとその対策

⓪不正アクセスって何？どのように発生するのだろう…

○「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

○主な不正アクセスの事例

▶なりすまし
→アカウントの乗っ取り・不正なプログラムの実行 など

▶改ざん
→情報の書き換え・暗号化して利用不可にする など

▶盗聴
→個人情報や機密情報を不当に収集・第三者に公開 など

２．不正アクセスとその対策

⓪不正アクセスって何？どのように発生するのだろう…

○「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」

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○不正アクセスの一番最初の要因って？

▶不正アクセスの原因は，ずばり無駄な入り口や脆弱性のある入り口
→家の扉が開けっ放しとか，壊しやすい扉のイメージ

○コンピュータの通信の出入り口「ポート」

▶ポートは，通信の目的ごとに割り当てられた通信の出入り口
▶例えば，HTTP（Webページ）は80番，SMTP（メール送信）は25番

○「ポートスキャン」とは？

▶ポートの開閉を総当たりで確認，サービスの稼働状況を特定する
→この方法により，脆弱性のあるポートを探す

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○不正アクセス原因となるポートを閉鎖する

▶そもそも使わないポートをきちんと閉鎖する

▶脆弱性のあるポートがないようにソフトウェアの更新をする

○サービスの運用上大切なこと

▶セキュリティリスクをいかに減らすか（完全性）

→情報流失やシステムが停止されるなどは避けたい

▶サービスの提供を止めないこと（可用性）

→正規の利用者の利用が止めることも避けなければならない

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

〇実際に体験してみよう

▶あなたはサーバ管理者

→サービスの安全・安定運用はあなたに託されました

〇ミッション

▶Webサイトの閲覧とメールの送受信機能を提供する

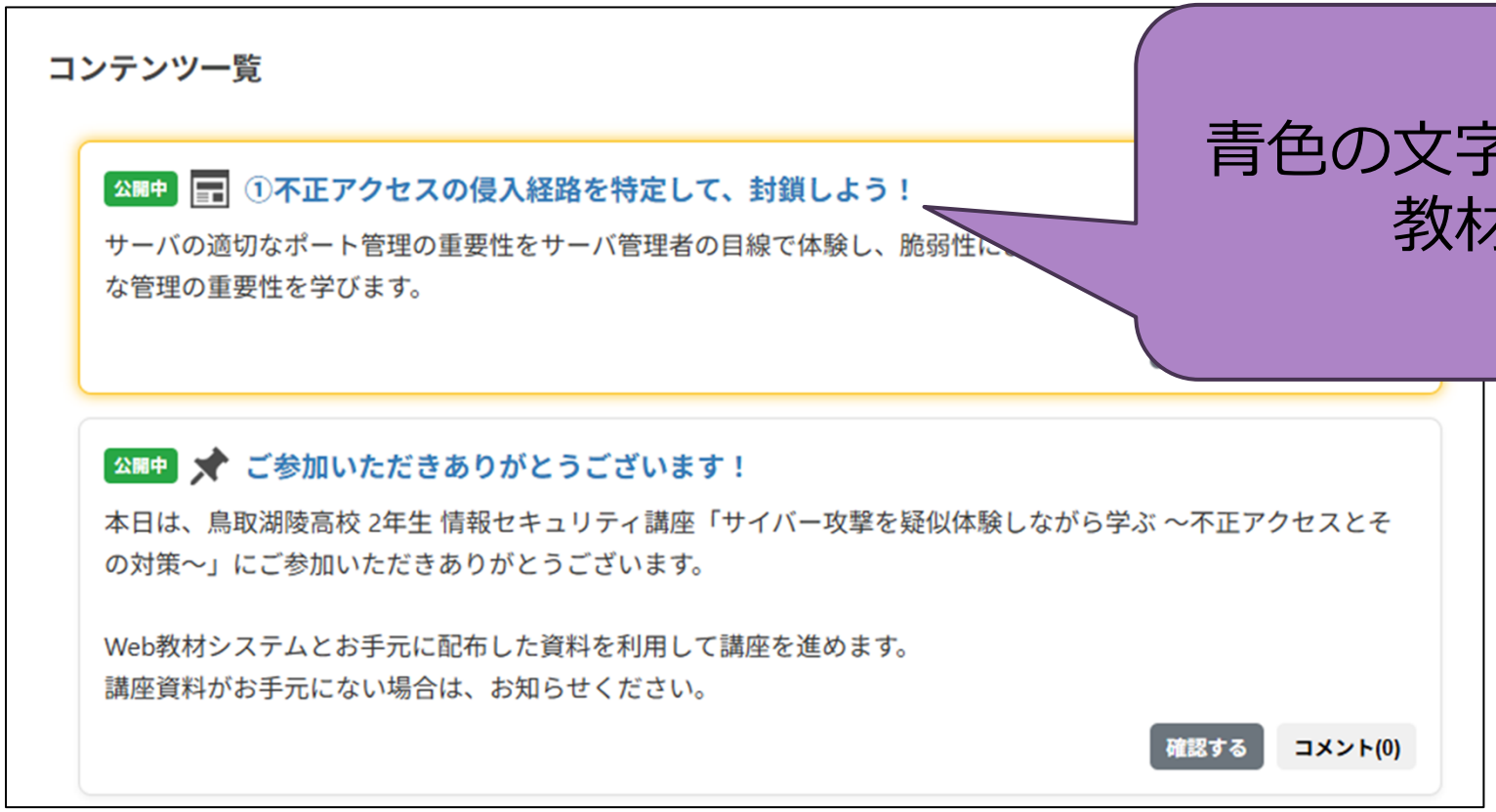
→無駄なポートを閉鎖してサーバリスクを0%にしよう！

→利用者に絶対に迷惑はかけないこと！

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○教材を配信します



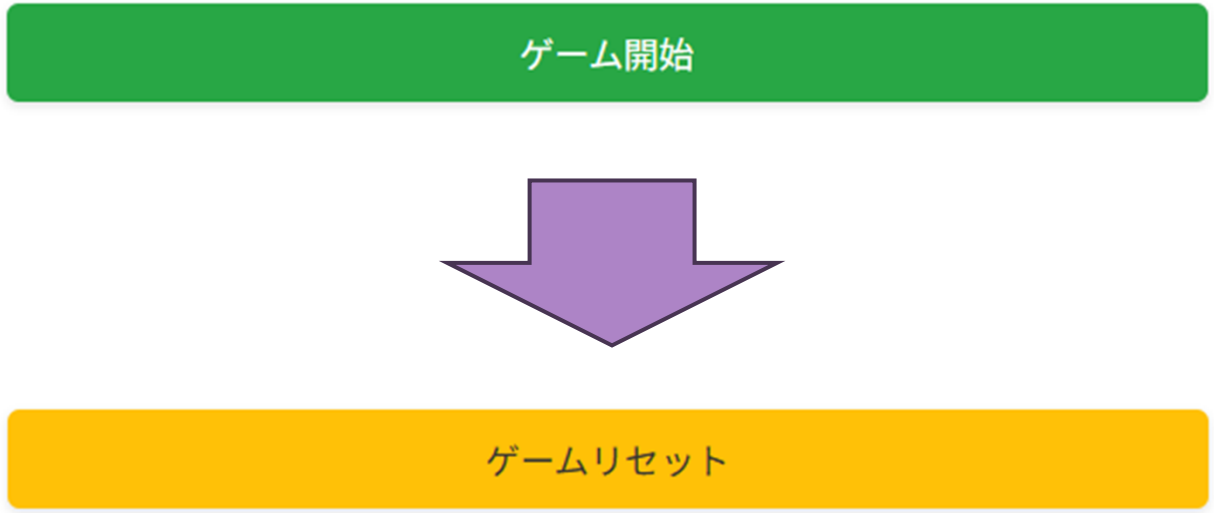
青色の文字をクリックすると
教材が開きます

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう

▶「ゲーム開始」ボタンを押してください



2．不正アクセスとその対策

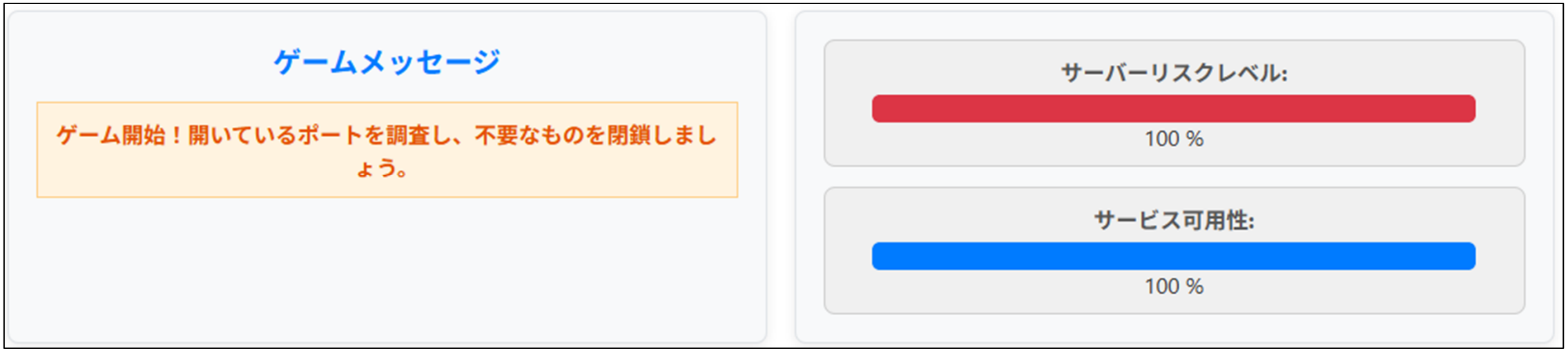
①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう



2．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう

ポートを閉じる前に，
各ポートの役割や
セキュリティ上の懸念の
有無を確認しましょう！

「調べる」ボタンを
押してください.

2．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう

21 / FTP (vsftpd 2.3.4)

一般的な用途

ファイル転送プロトコル。このバージョンには既知のバックドア脆弱性があります。

セキュリティ上のリスク

高リスク。攻撃者にシステムを完全に掌握される可能性があります。

既知の脆弱性 (バージョン固有)

vsftpd 2.3.4にはバックドアが組み込まれている既知の脆弱性があります (CVE-2011-2523)。

対策のヒント

即座に閉鎖するか、より安全なSFTP/FTPSへの移行とアップデートが必要です。

例としてFTPについて
確認してみましょう....

特定のバージョンに
脆弱性が報告されてる.

これを放置していたら
危険！！！

2．不正アクセスとその対策

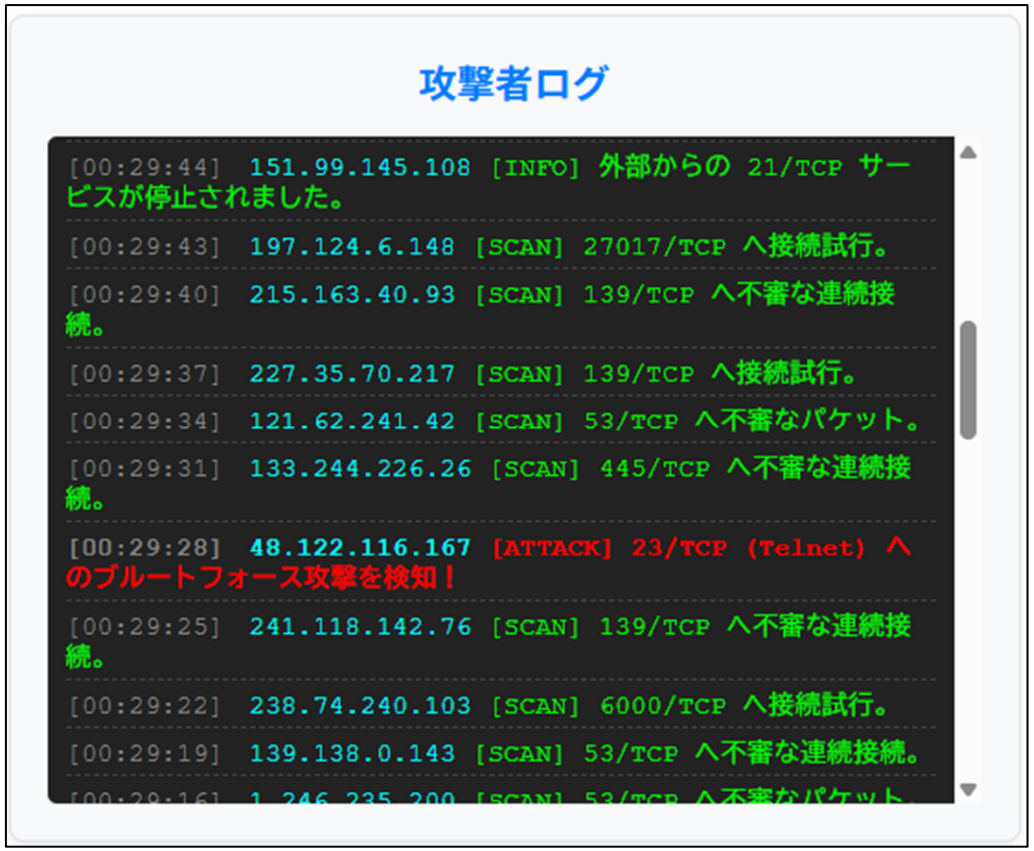
①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう

2．不正アクセスとその対策

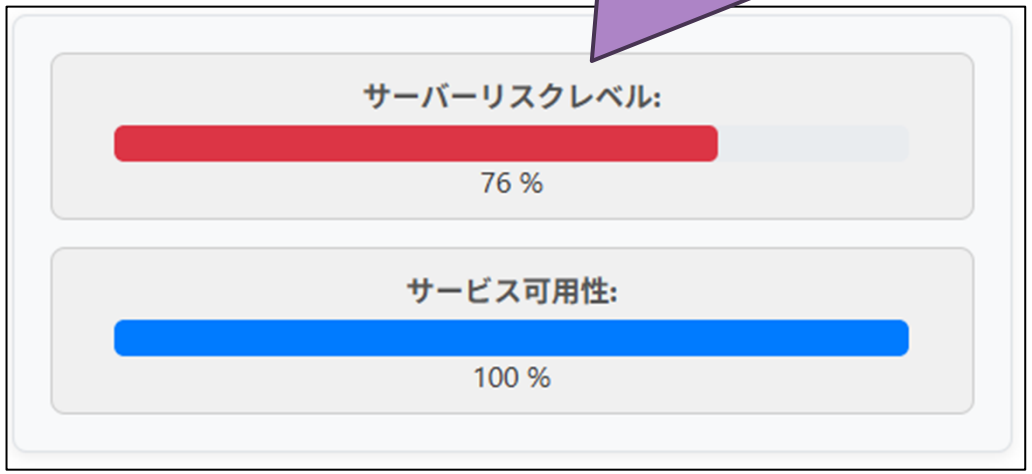
①不正アクセスの侵入経路を特定して，封鎖しよう！

○実際に体験してみよう



閉鎖したらセキュリティリスクが低減されました！

サービスの可用性は維持されたままです



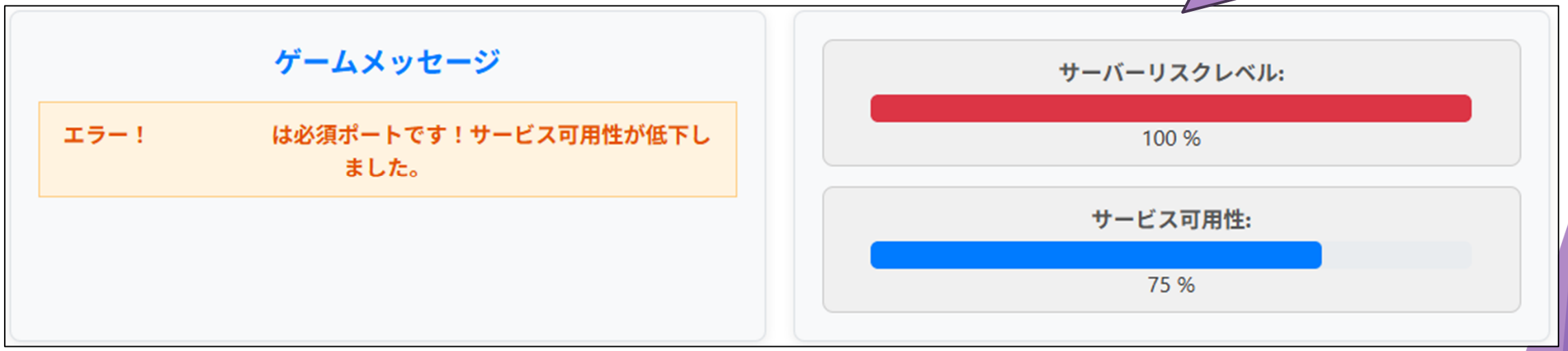
2．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

〇実際に体験してみよう

必要なポートを閉鎖すると
可用性が失われてしまいます.

必ず可用性は100%を維持してください



２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

〇実際に体験してみよう

▶今から５分程度時間をとります

→サーバリスク 0%・サービス可用性100%を目指しましょう！

〇ミッション

▶Webサイトの閲覧とメールの送受信機能を提供する

→無駄なポートを閉鎖してサーバリスクを0%にしよう！

→利用者に絶対に迷惑はかけないこと！

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

〇皆さんできましたか？

▶この体験アプリは無駄なポートがたくさん開いていました
→閉鎖したことで大幅にリスクが低減できました！
→それなりに面倒な作業ではなかったですか？

▶無駄なポートを開けない・脆弱性を放置しない
→サイバーセキュリティの基本中の基本だけど重要

▶世の中にはこの基本が徹底できていない会社も…
→実際に情報流失した事例もありました

２．不正アクセスとその対策

①不正アクセスの侵入経路を特定して，封鎖しよう！

〇考えてみよう

Ｑ１．必要なポートを間違って閉じてしまった人はいない？

→誤ったポートを閉じてしまうことを防ぐには？

Ｑ２．リスク0%と可用性100%，どちらがより重要だと思う？

→過剰なセキュリティ対策するのって，どうなんだろう…

２．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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

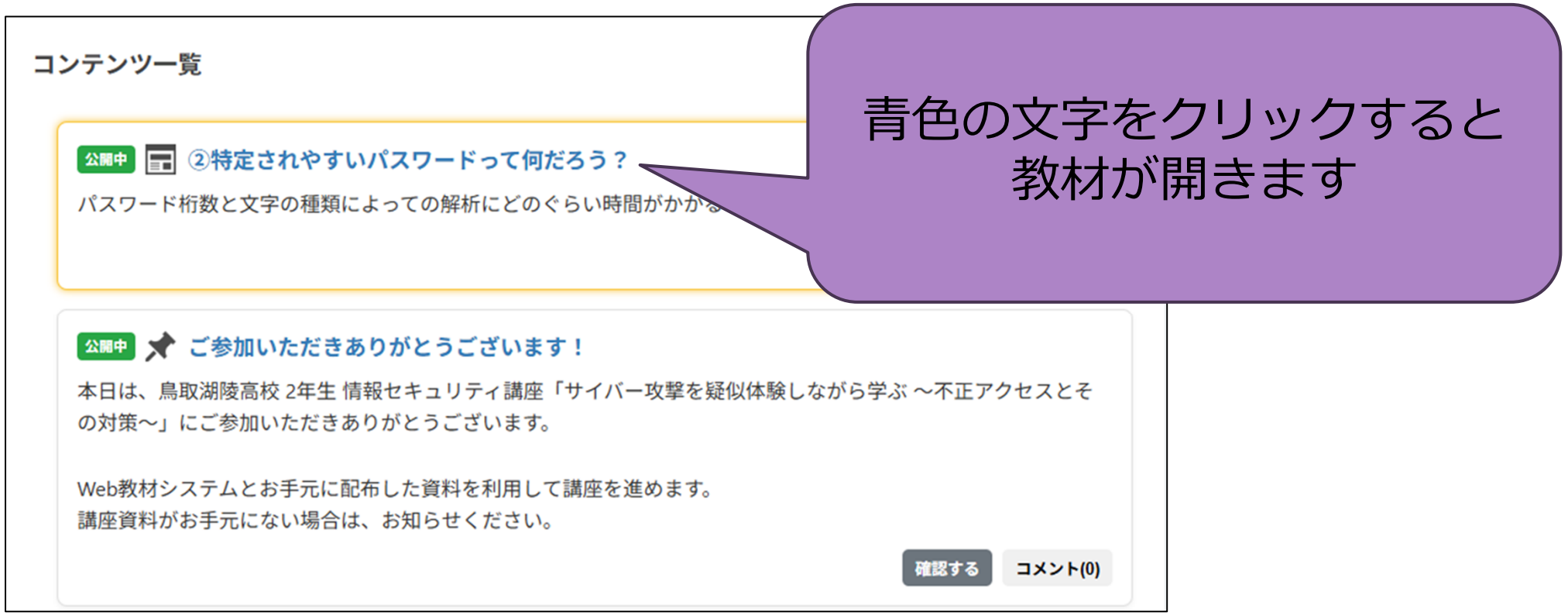
▶簡単に推測・解読されないこと

→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．不正アクセスとその対策
②特定されやすいパスワードって何だろう？

○教材を配信します



2．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

〇総当たり攻撃

▶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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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
絞っています

2．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○パスワードの桁数による違い

▶次は，6桁「yonago」で試してみましょう

2．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○パスワードが6桁「yonago」の場合

▶6桁の場合は，**304,135,977**通りの試行をしたようです

２．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○パスワードが4桁「yona」の場合

▶4桁の場合は，**20,239,963**通りの試行をしたようです

2．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○「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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

○辞書攻撃「yonago」の場合

▶たったの**203**通りで解析が終わりました…

２．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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	**203**

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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

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

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．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

〇パスワードを解析するのに総当たりや辞書攻撃が必要なのか

▶多くのシステムは，平文のまま保存せず，ハッシュ化して保存する

→流出するデータの多くは，直接読み解けない

→解析するためには，総当たりや辞書攻撃などきっかけが必要

〇ハッシュ化とは？

▶元のデータを「ハッシュ関数」と呼ばれる特殊な計算方法を用いて，復元不可能な一意の文字列（ハッシュ値）に変換する処理

詳細は，教材の末尾にあります

興味のある人は読んでみてください！

２．不正アクセスとその対策

②特定されやすいパスワードって何だろう？

〇考えてみよう

Ｑ３．理想的なパスワードってどんなの？

→そのパスワードって本当に覚えられるかな？

Ｑ４．理想的なパスワードが難しいなら，どうするのが良い？

→パスワードには限界が…

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇情報にアクセスできる人を決める？できない人を制限する？

▶ネットワークの出入り口をそもそも通過できる人を制限します

→不正にアクセスされるそもそもの原因を排除する

〇ファイアウォール（防火壁）とは？

▶不正侵入を防止する装置

▶ネットワークの出入り口に設置する

▶ハードウェア または ソフトウェアとして提供される

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇ファイアウォールの種類（考え方）

▶ホワイトリスト方式

→利用できる人を指定して，通過できる人を管理する

▶ブラックリスト方式

→利用できない人を指定して，通過できる人を管理する

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇身近な例（SNSの公開アカウント・鍵アカウントに似ている）

▶公開アカウント（ブラックリスト方式）

→誰でもアクセスできるが，見られたくない人はブロックできる

▶鍵アカウント（ホワイトリスト方式）

→アクセスできる人を自分で決めることができる

〇どちらのほうが，優れている？

→実際に体験しながら，考えよう！

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう

▶あなたはネットワーク管理者です

→アクセスできる人とできない人を決めて，安全を守ってください

〇ミッション

▶情報にアクセスできる人・できない人を選別する

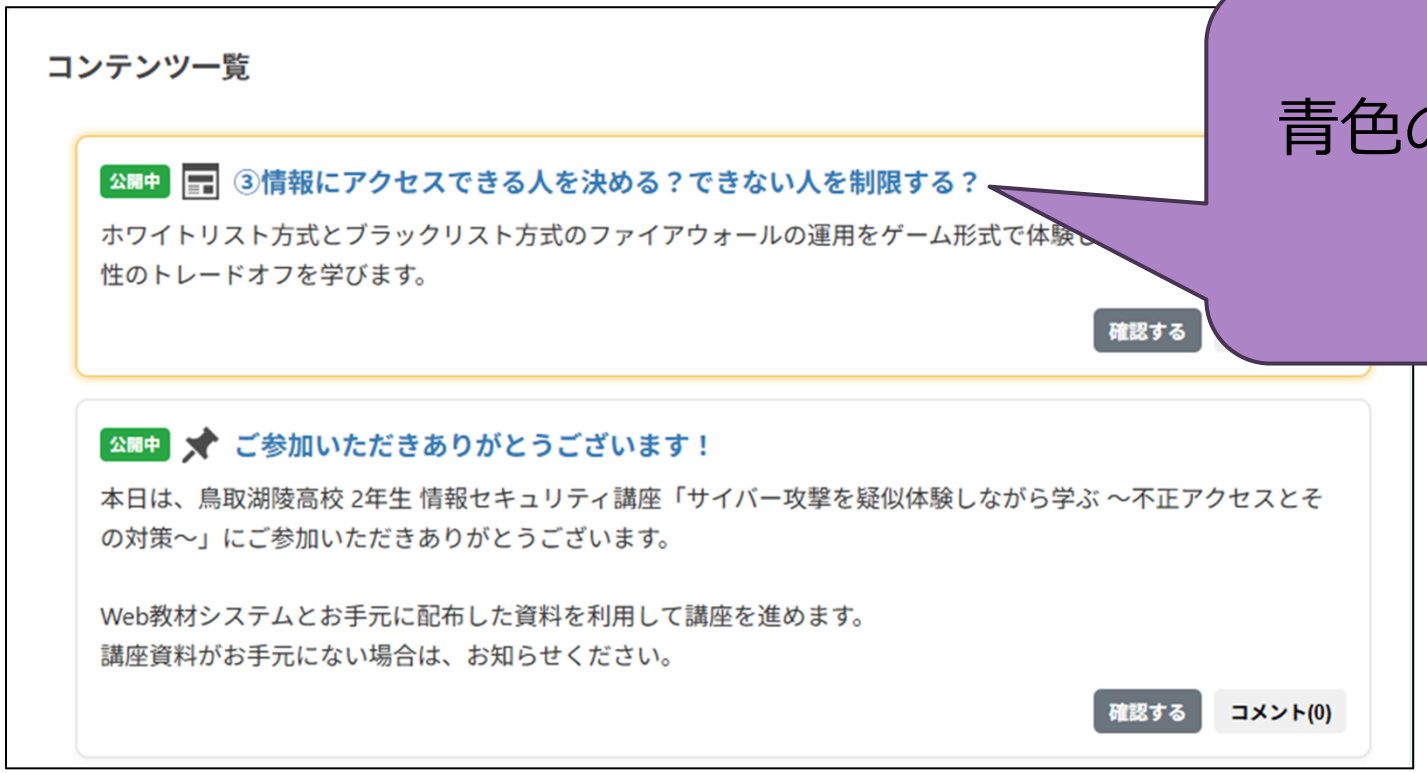
→不正な通信をしようとしている人の侵入を防いでください

→善良な通信をしようとしている人には絶対に迷惑はかけないこと！

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○教材を配信します



青色の文字をクリックすると
教材が開きます

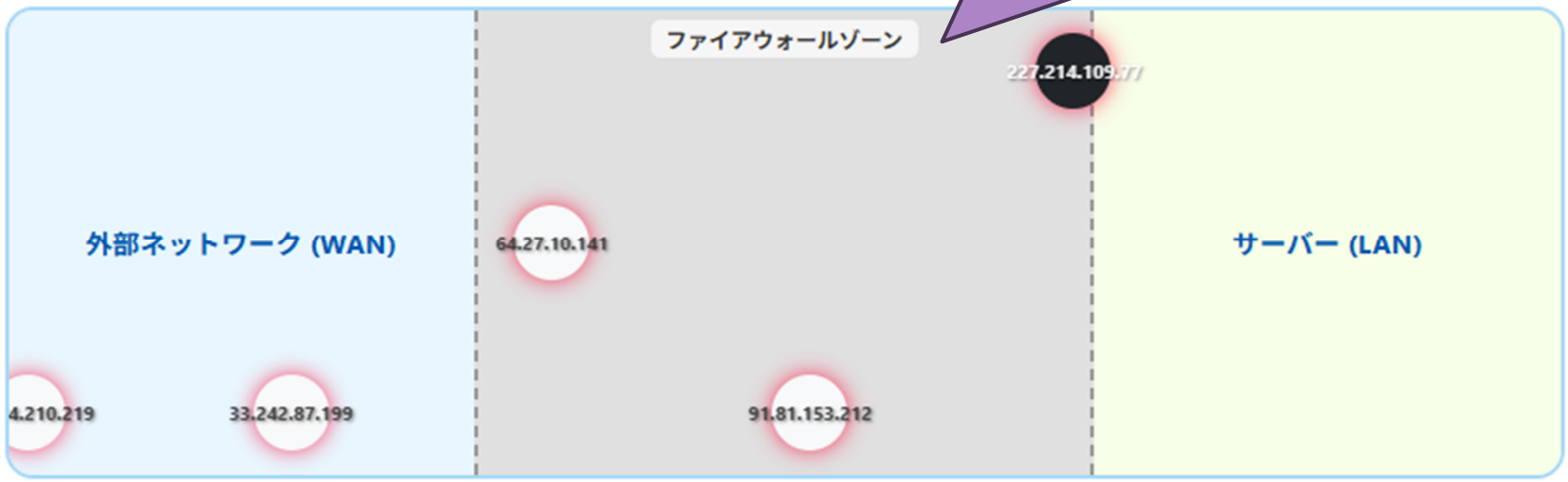
2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう

通信は左から右へ流れていきます.

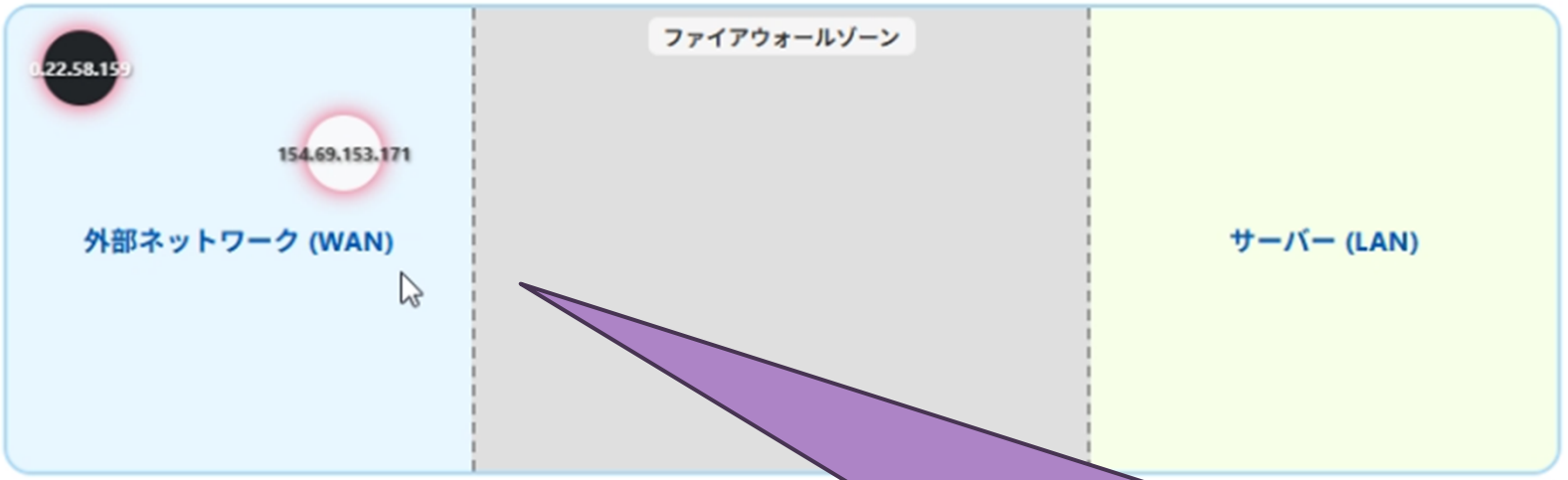
通信を「通過させる」
「通過させない」をファイアウォール
ゾーン内で判断します



2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○実際に体験してみよう



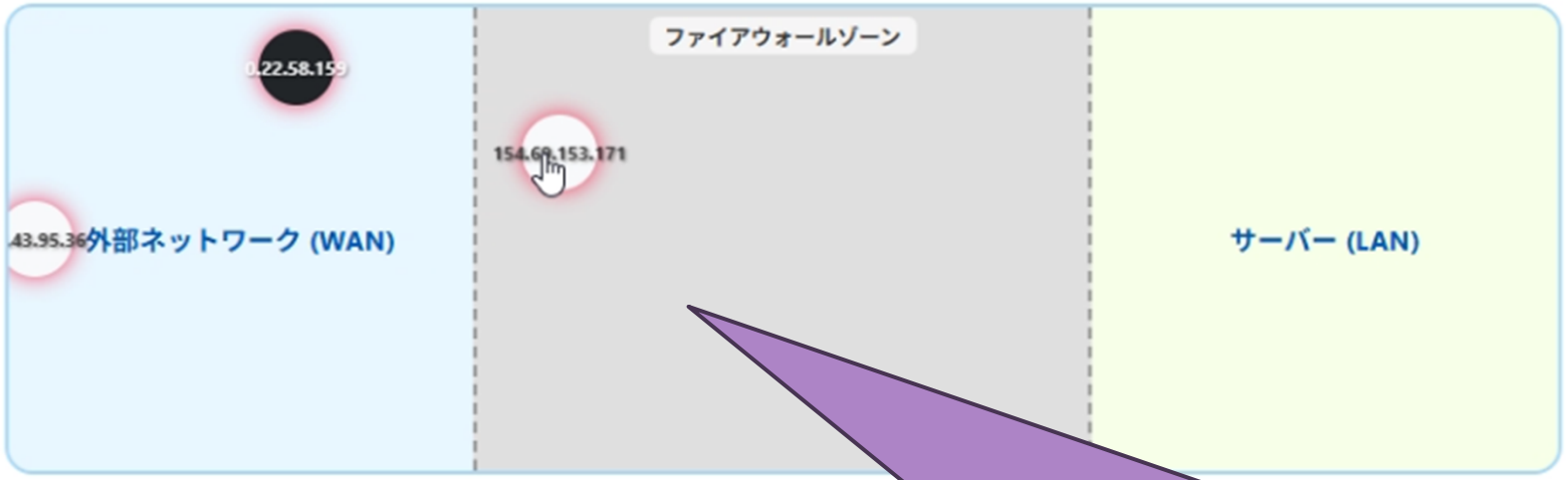
通信は右から左へ流れていきます

左側がインターネットの世界
右端が自分のパソコンと
理解してください

2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう

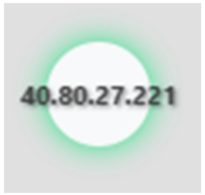


通信を「通過させる」or
「通過させない」をファイアウォール
ゾーン内で判断します

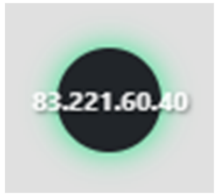
２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

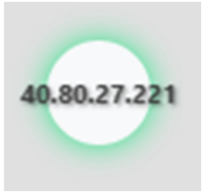
○実際に体験してみよう



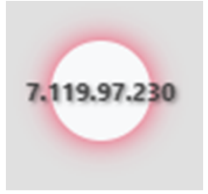
良い通信



悪い通信



通信許可



通信拒否

白色の丸は良い通信ですから
「通信を許可」してください.

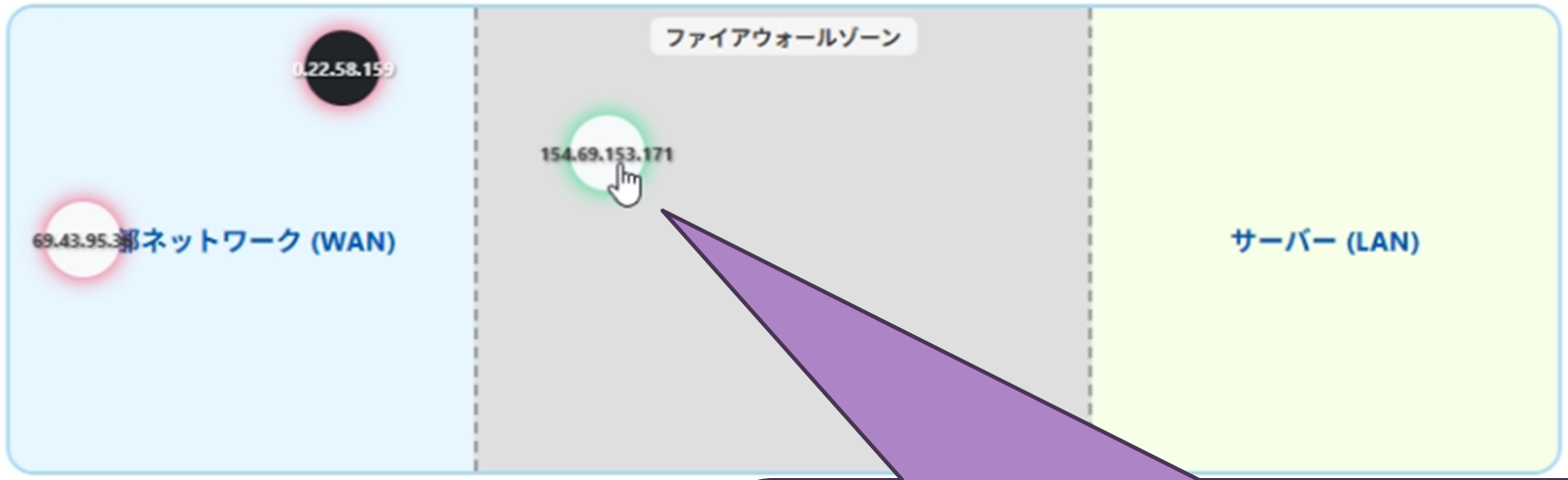
黒色の丸は悪い通信ですから
「通信を拒否」してください.

通信の許可状況は,
丸の周りが緑の場合は「許可」,
赤の時は「拒否」です.

2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう



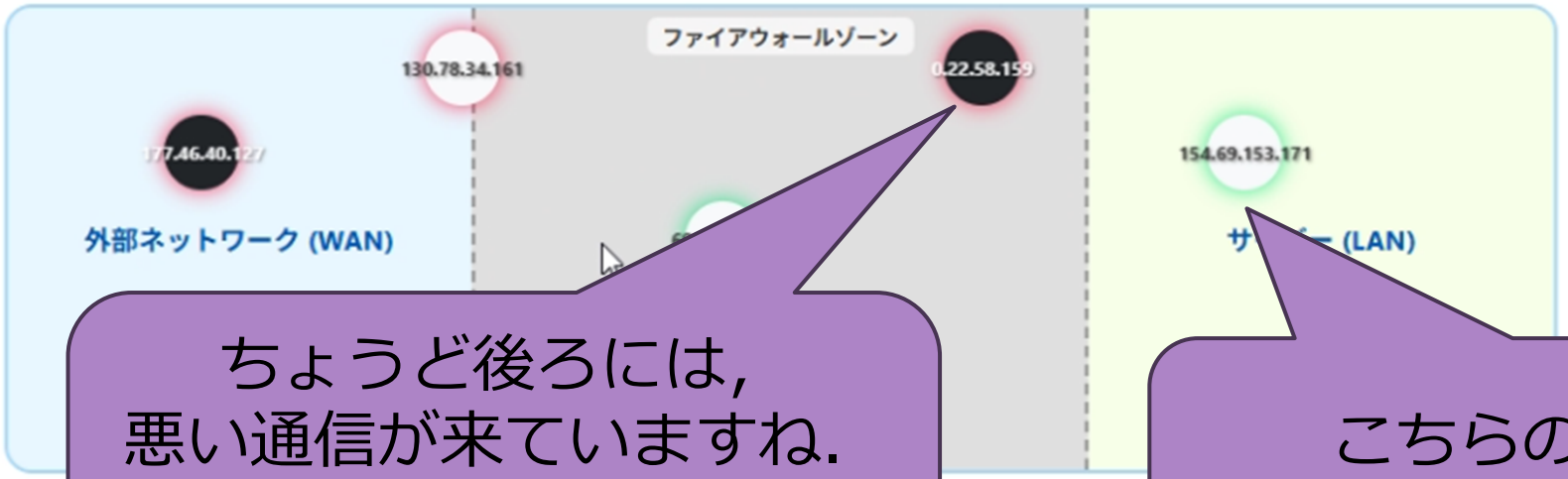
この通信は良い通信ですから
通信を許可しました.

丸の周りが緑色になっています

2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう



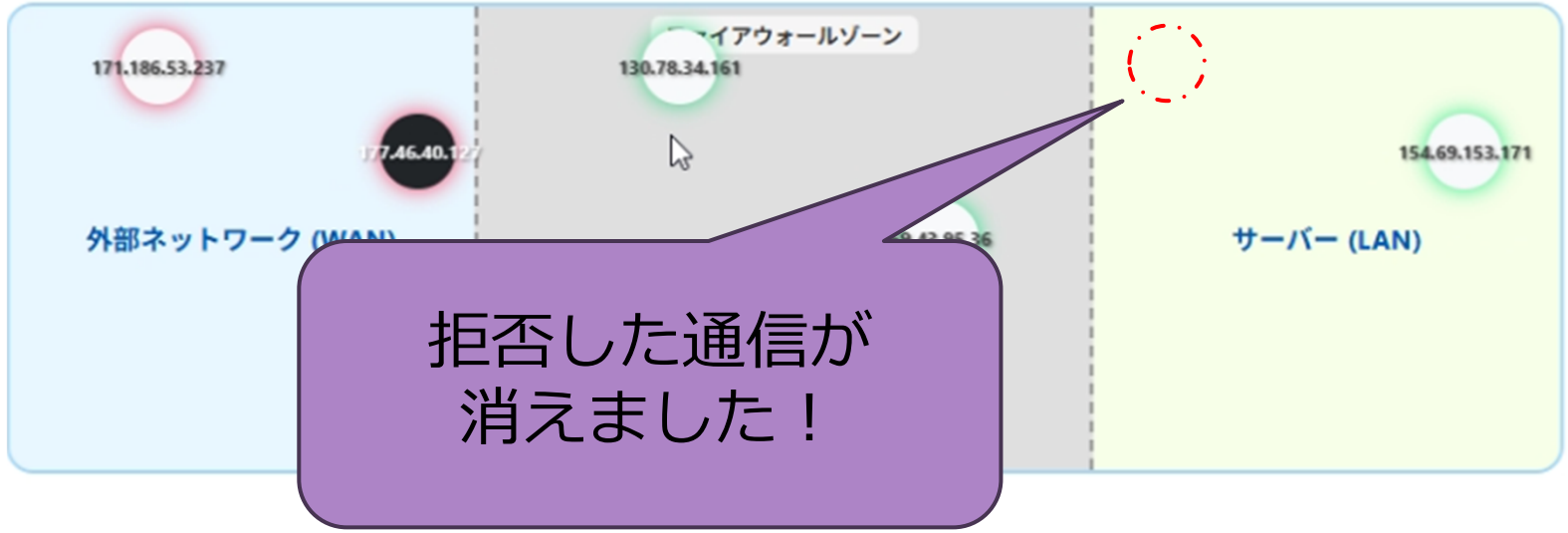
ちょうど後ろには，
悪い通信が来ていますね．
このまま「拒否」でいいの
で赤枠のままです

こちらの通信は，
問題なく通過できました

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

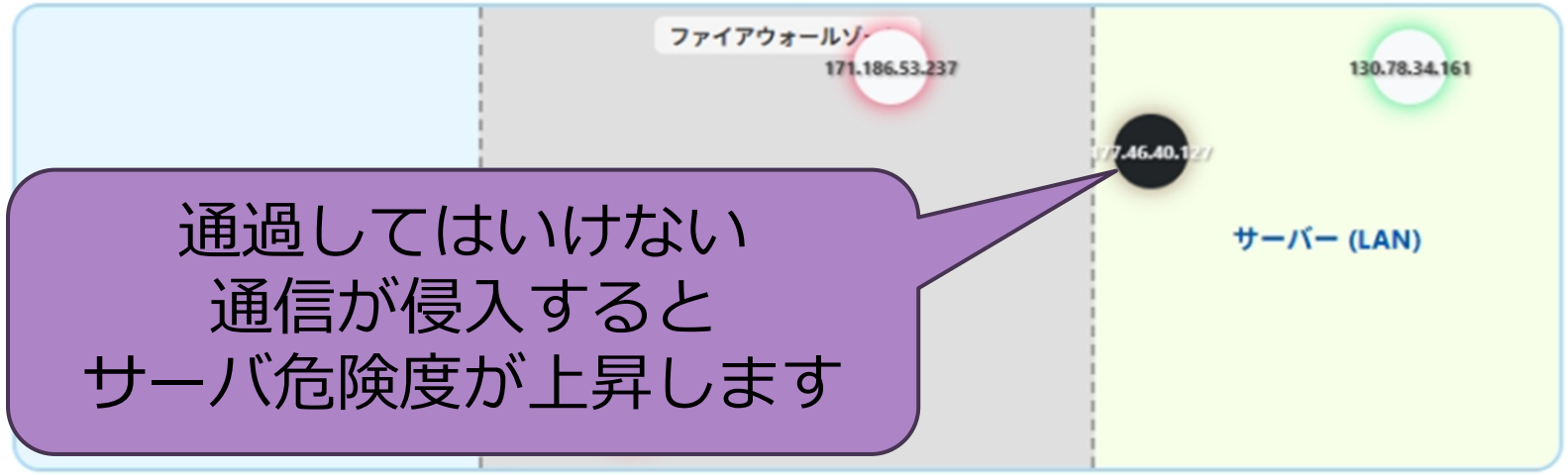
○実際に体験してみよう

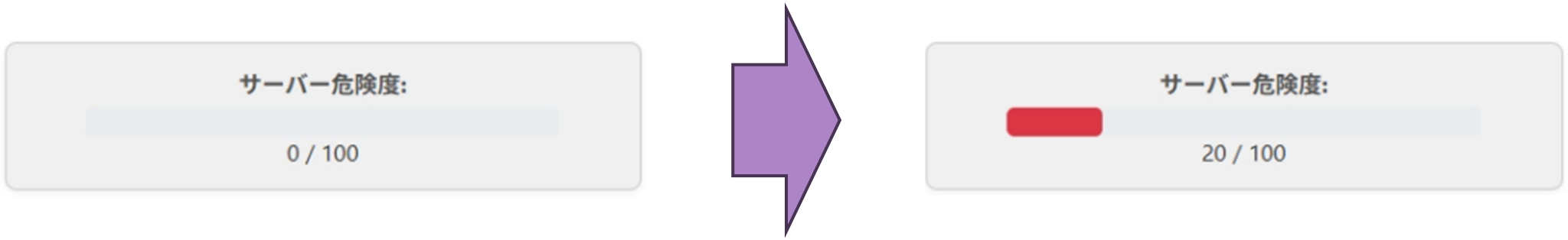


2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○実際に体験してみよう

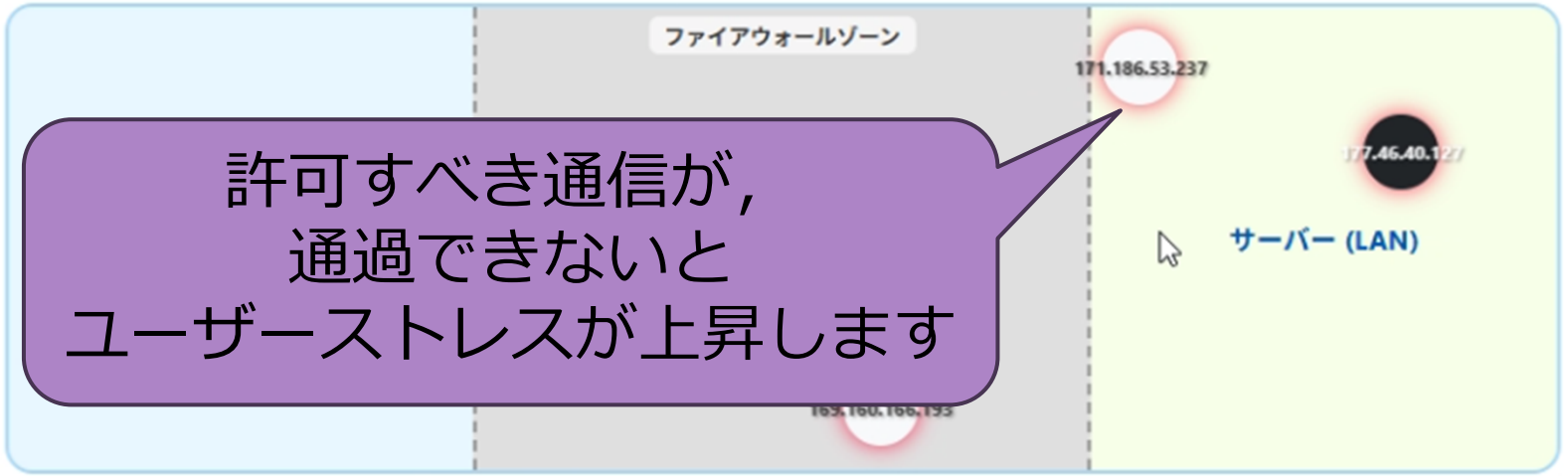


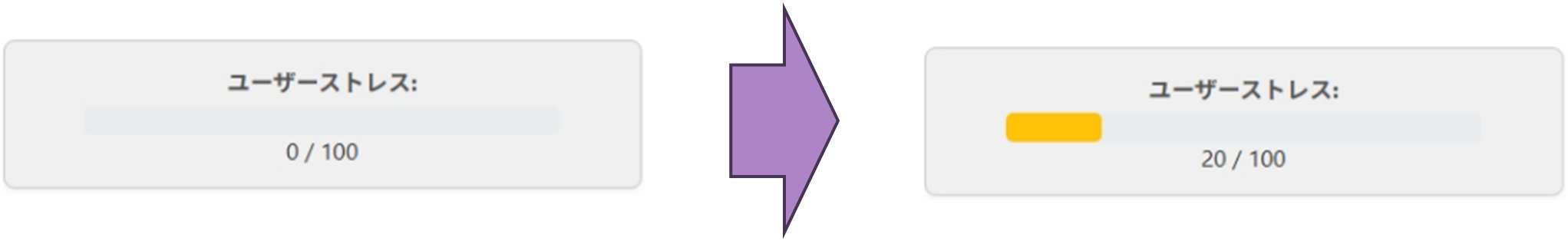


2．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○実際に体験してみよう





２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇実際に体験してみよう

▶今から５分程度時間をとります

→ホワイトリスト方式とブラックリスト方式を両方体験してください

〇ミッション

▶情報にアクセスできる人・できない人を選別する

→不正な通信をしようとしている人の侵入を防いでください

→善良な通信をしようとしている人には絶対に迷惑はかけないこと！

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○皆さんできましたか？

▶どちらも面倒な箇所があったのではないでしょうか？

▶ホワイトリスト方式は，良い通信すべてに許可をする必要がある
→正しく許可されないと利用者の不満につながる可能性が…

▶ブラックリスト方式は，悪い通信を常に監視する必要がある
→悪い通信を通過させると情報流出などのリスクが…

○結局どちらがいいのか？

▶提供するサービスの性質やセキュリティレベルによる
→すごい抽象的な考え方…

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

○ホワイト・ブラックリスト方式どちらがいいかな？

▶会社の関係者のみがアクセスするWebサイト

→ホワイトリスト方式

▶ゲームで不正をした人のアクセスを禁止したい

→ブラックリスト方式

▶不特定多数の登録をした人だけがアクセスできるWebサイト

→ホワイトリスト方式で，できないわけではない

→この場合は，アカウント認証のほうがいいかも

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

OSNSの公開設定について

▶公開設定を適切にできないと，プライベートが筒抜けに

→ストーカーなどの原因になることも…

▶本当に公開してもいい情報ですか？

→マンホールや電柱などが映り込むだけでも住所などを特定される

▶鍵アカウントでは何を投稿してもいい？

→身近な人が，信頼できると思っていた人が流出させる可能性も

→誹謗中傷や名誉棄損など鍵アカウントでもNG

２．不正アクセスとその対策

③情報にアクセスできる人を決める？できない人を制限する？

〇考えてみよう

Ｑ５．ホワイトリストの設定を間違うと，どんな問題が起きる？

Ｑ６．ブラックリストの設定を間違うと，どんな問題が起きる？

Ｑ７．ホワイトリストとブラックリスト，管理はどちらが面倒？

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

▶不正にアクセスされる原因はなるべく取り除く

→玄関の扉を全開にして外出しないよね

→でも，手作業で管理するのは大変だったよね…

▶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…

▶情報にアクセスできる人は適切に管理しないといけない

→SNSの公開設定を間違えるとあなたの身も危険にさらすことに

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

○アンケートにご協力ください

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

０．おまけ
パスワードが流出したときの保険 = ハッシュ化

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

0．おまけ
パスワードが流出したときの保険 = ハッシュ化

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

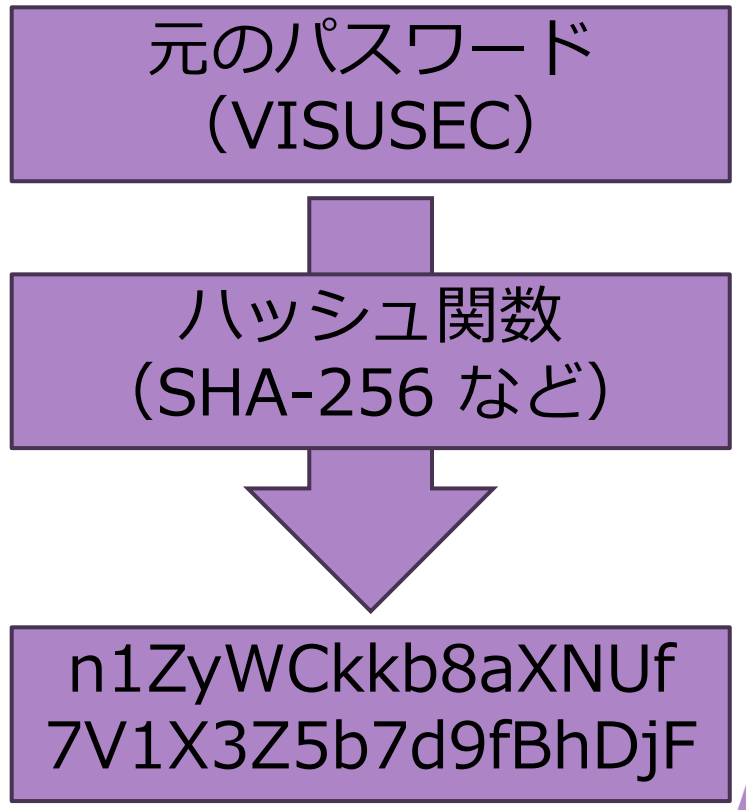
〇暗号化との違い

▶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



０．おまけ
パスワードが流出したときの保険 ＝ ハッシュ化

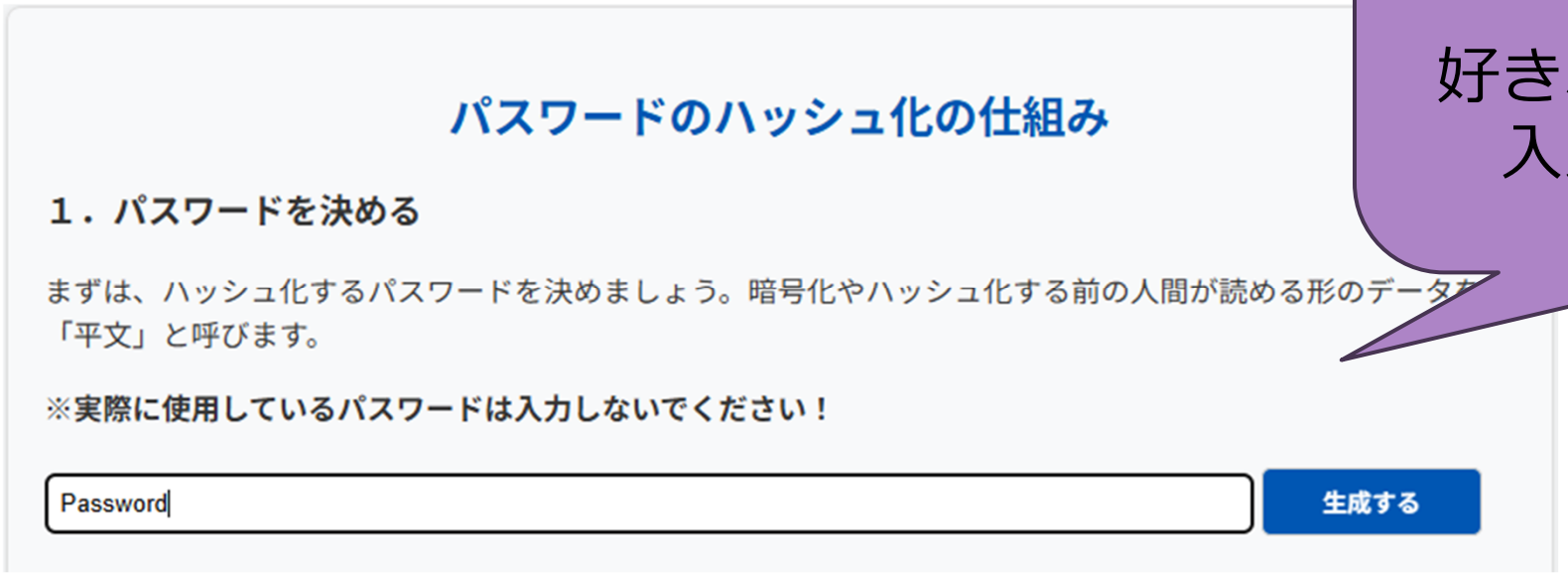
○教材を配信します

０．おまけ
パスワードが流出したときの保険 ＝ ハッシュ化

○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.



0．おまけ
パスワードが流出したときの保険 = ハッシュ化

○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

0．おまけ
パスワードが流出したときの保険 = ハッシュ化

○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

0．おまけ
パスワードが流出したときの保険 ＝ ハッシュ化

○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

0．おまけ
パスワードが流出したときの保険 = ハッシュ化

○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

０．おまけ
パスワードが流出したときの保険 ＝ ハッシュ化

○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

０．おまけ
パスワードが流出したときの保険 ＝ ハッシュ化

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