常葉高校・大学
情報セキュリティ講座

外部公開用

身近なネットの危険を疑似体験しながら学ぶ情報セキュリティ講座

2026年10月14日（水）

©若林遥大 (遠山研究室) All rights reserved.

講師紹介

○ 若林 遥大（わかばやし はると）

▶ 静岡大学 大学院総合科学技術研究科 情報学専攻

→ 情報セキュリティ教育やプログラミング教育などについて研究

▶ 鳥取県出身

→ 高専出身で，大学院から静岡大学に進学（静岡在住半年）

▶ 静岡県警察ヤング防犯ボランティアに登録

→ 本日は，県警・常葉高校 様よりご依頼を受けて講座を実施！

©若林遥大 (遠山研究室) All rights reserved.

本日の内容

1．情報モラルとセキュリティの基本

▶ 自分を守るためのセキュリティとは？

2．身近なサイバー犯罪の手口 とその対策

① 公開された情報から，個人情報を抽出してみよう

② 特定されやすいパスワードって何だろう？

3．おわりに

©若林遥大 (遠山研究室) All rights reserved.

0．講座を始める前に

https://visusec.jp

① 検索サービスで「VISUSEC」と検索してください



©若林遥大 (遠山研究室) All rights reserved.

0．講座を始める前に

② 表示されたページ画面右上，「お知らせ」ボタンを押してください



©若林遥大 (遠山研究室) All rights reserved.

0．講座を始める前に

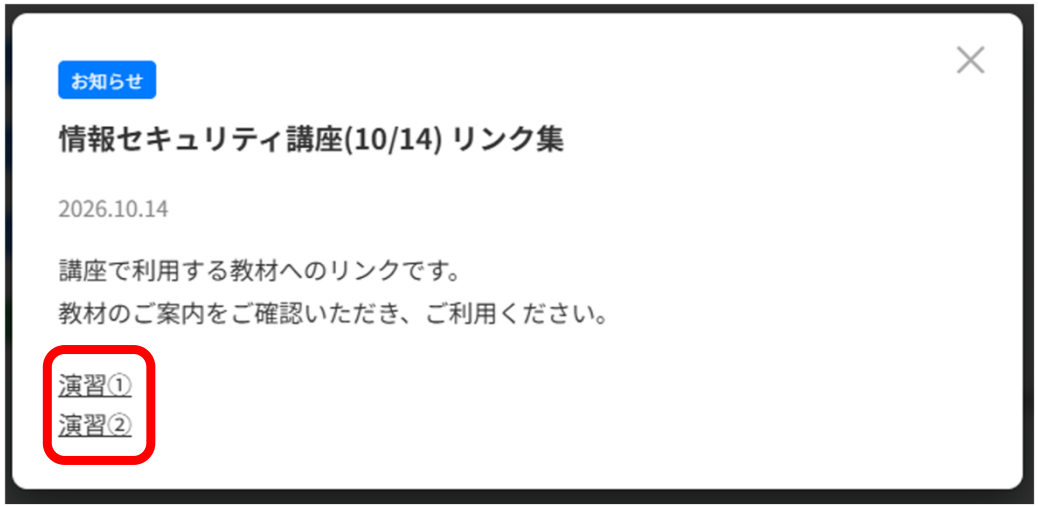
③ 最上部に表示されているお知らせをクリックしてください



©若林遥大 (遠山研究室) All rights reserved.

0．講座を始める前に

④ 利用する際にはご案内しますので，こちらの画面でお待ちください



©若林遥大 (遠山研究室) All rights reserved.

0．講座を始める前に

〇事前アンケート

▶一人で回答してください

さまざまな正解があります．回答は本講座の改善に活用します．

©若林遥大 (遠山研究室) All rights reserved.

1．情報モラルとセキュリティの基本

○ サイバー犯罪に遭わないためにはどうすればいいのだろうか？

▶ スマホなどインターネットにつながる装置を使わない！

→ そんなこと，不可能に近い…

○ 日常的にサイバー空間で生活をしている

▶ 勉強，娯楽，買い物，人との交流がすべてインターネットで出来る

→ 危険だから使わないとは，ならない

▶ その一方で，人が集まるところには犯罪も集まる

→ 正しい知識や行動ができないと悪い人の標的になってしまう

©若林遥大 (遠山研究室) All rights reserved.

1．情報モラルとセキュリティの基本

○ サイバー犯罪って具体的にどんなもの？

▶ 不正アクセスなど，システムを狙った犯罪

→ 他人のIDやパスワードを盗んでログインする

→ データを勝手に書き換えたり，ウイルスをばらまいたりする

▶ インターネットやSNSを悪用した犯罪

→ SNSでの誹謗中傷，他人の個人情報の無断公開

→ 「闇バイト」の募集・応募（特殊詐欺への加担）

©若林遥大 (遠山研究室) All rights reserved.

1．情報モラルとセキュリティの基本

○ 「知らなかった」では済まされない！

▶ 軽い気持ちの投稿やクリックが，犯罪になることがある

→ **中高生が加害者になる事例も少なくない**

○ どうすれば自分の身を守れるのか？

▶「手口」を知ることが一番の対策

→ 知らない手口から自分の身は守れない

▶ 座学に加えて，実際に体験しよう

→ 「攻撃者」も体験してみよう！

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

①公開された情報から，個人情報を抽出してみよう

〇 SNSに旅先の思い出を投稿するとき，どのような注意をすべきか？

楽しかった思い出をみんなに見せたい！投稿する前提で考えよう

→ 演習を通じて近くの人と話し合ってもらいます！

投稿の例



念願の2人旅～～！🎢💗
始発間に合うか心配でマリナート前ダッシュしたし初のお泊まりでちょっとドキドキだったけど，楽しすぎた！！
アヤ，さいこうの誕プレありがとう✨
高校生活最高の思い出💞
#女子旅 #お泊まり #テーマパーク #JK旅 #JKライフ #高校生活 #親友旅 #青春してる #旅行記録 #思い出グラム #余韻 #最高すぎた

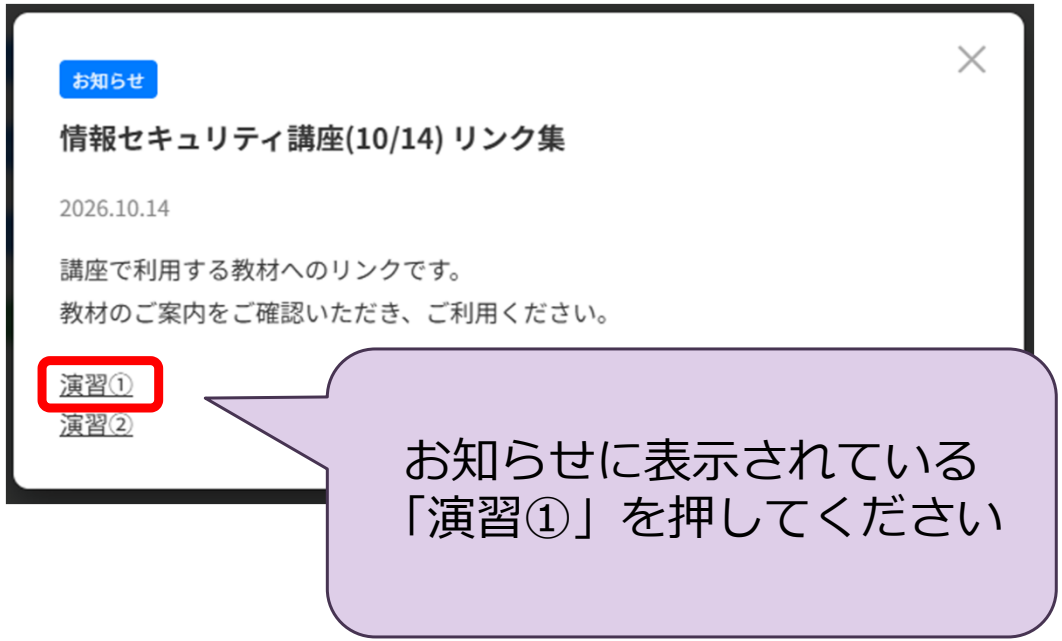
画像と投稿文はChatGPTにより生成

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

①公開された情報から，個人情報を抽出してみよう

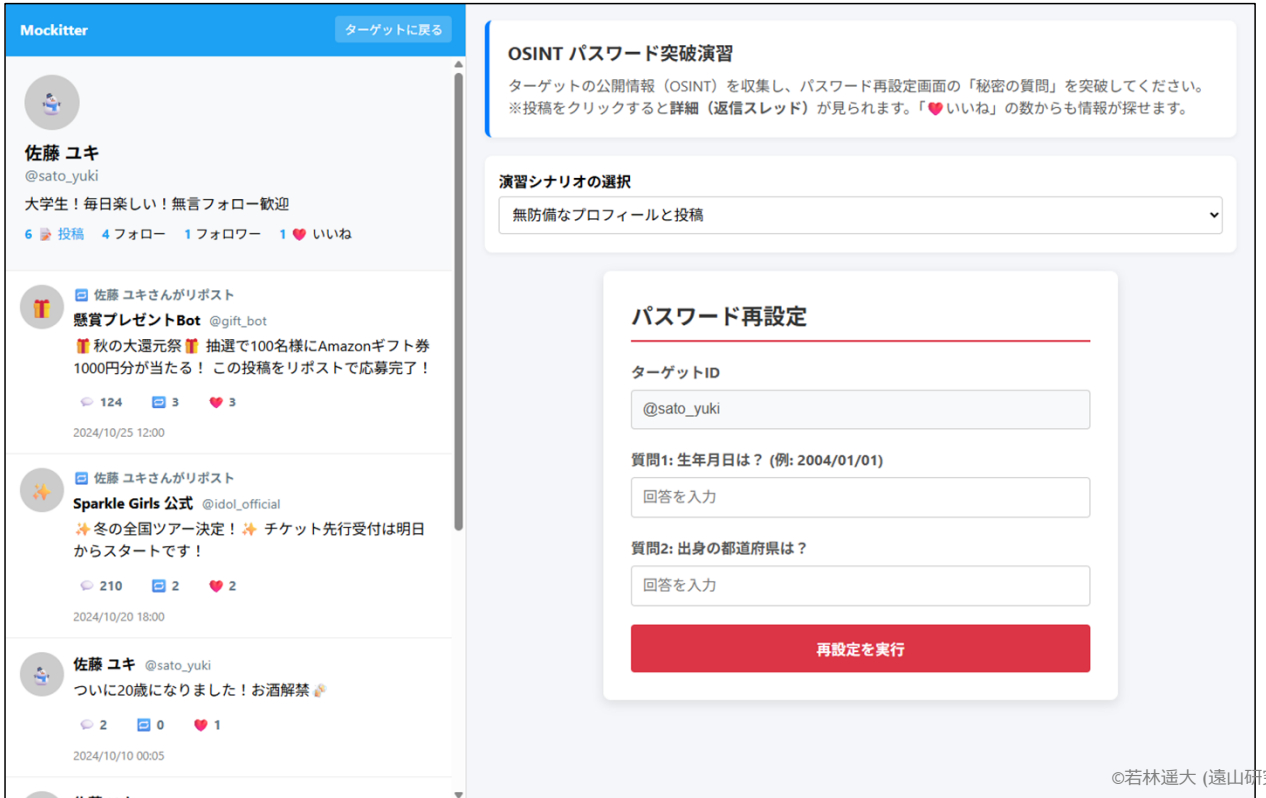
○ 教材を開きましょう



スマートフォンの方は
こちら

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

①公開された情報から，個人情報を抽出してみよう





スマートフォンの方は少しデザインが異なりますが，出来ることは同じです

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



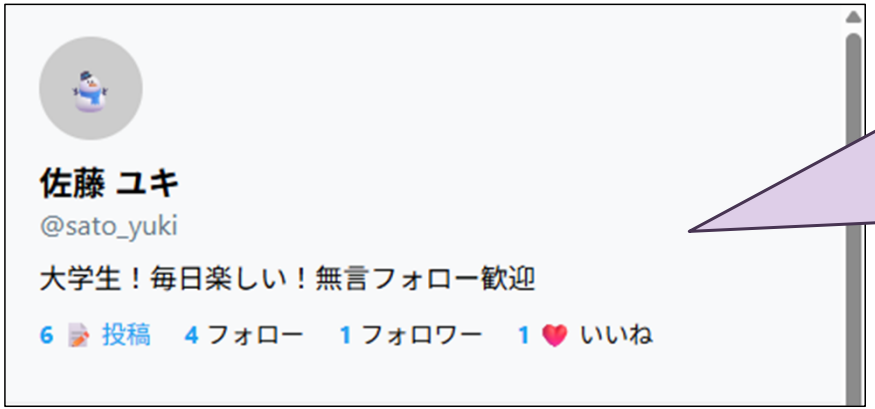
SNSに投稿された情報から，
パスワードを忘れたときの
合言葉を探して不正な
アクセスを試みます

佐藤ユキさんの生年月日と
出身都道府県を入力して
不正にパスワードを再設定しよう

©若林遥大 (遠山研究室) All rights reserved.

ヒント

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



「佐藤 ユキ」さんという
大学生のようです

まずは，生年月日を
探したいのですがプロフィール
には表示されていません…

©若林遥大 (遠山研究室) All rights reserved.

ヒント

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



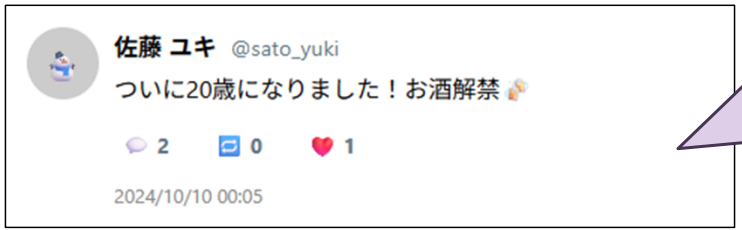
何気ない日常を
投稿しているようですね

誕生日がわかるきっかけは
ないでしょうか？

©若林遥大 (遠山研究室) All rights reserved.

ヒント

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



直接的に生年月日は言っていませんが，20歳になったことを投稿していますね

投稿日から逆算できるのでは？
→ 2004/10/10

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう

〇近くの人と一緒に考えよう！

▶ SNSに旅先の思い出を投稿するとき，どのような注意をすべきか？
投稿する前提で考えてください



フルネームじゃないから大丈夫だよね
旅先だから住所はバレないよね
…本当に大丈夫？

念願の2人旅～～！🚄💗
始発間に合うか心配でマリナート前ダッシュしたし初のお泊まりでちょっとドキドキだったけど，楽しすぎた！！
アヤ，さいこうの誕プレありがとう✨
高校生活最高の思い出🫶
#女子旅 #お泊まり #テーマパーク #JK旅 #JKライフ #高校生活 #親友旅 #青春してる #旅行記録 #思い出グラム #余韻 #最高すぎた

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう

○ SNS上の情報を組み合わせると新たにわかることがある

○「OSINT」(オシント)

▶ Open-Source Intelligence

特定の目的について誰でも入手できる情報を分析してまとめたもの

→ セキュリティ対策や犯罪捜査などポジティブな面でも活用される

→ 一方で，犯罪者の情報収集などに悪用される場合もある

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう

○ 「OSINT」が悪用されると？

▶自宅や学校，通学経路などが特定される可能性がある

▶ 「秘密の質問」を特定される可能性もある

→ 秘密の質問に真面目に答えないことも大切！

○ ネット上に日常を公開するときは，個人が特定される情報には注意！

▶ 今の時代投稿するべきでないとは，言えない

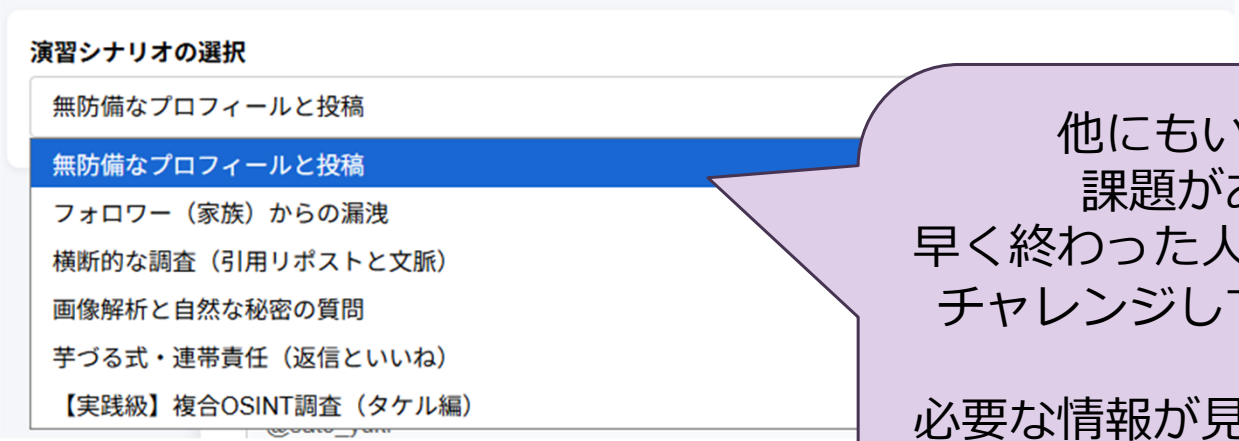
→ 投稿するリスクは事前に理解しておくこと

▶ 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ある

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
①公開された情報から，個人情報を抽出してみよう



他にもいろいろな
課題があります
早く終わった人は他の課題にも
チャレンジしてみてください

必要な情報が見つからないときは，「いいね」の一覧から別のユーザーの投稿を見に行くといいかも

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

①公開された情報から，個人情報を抽出してみよう



何気ない写真にも
たくさん情報がある

文字情報以外に得られ
そうな情報ってある？

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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 パスワードは家の鍵と同じように大事なもの．でも長いと管理が面倒．

安全で使いやすいパスワードはどうすれば作れるだろう？

→演習の後で近くの人と話し合ってもらいます！

よく聞く話

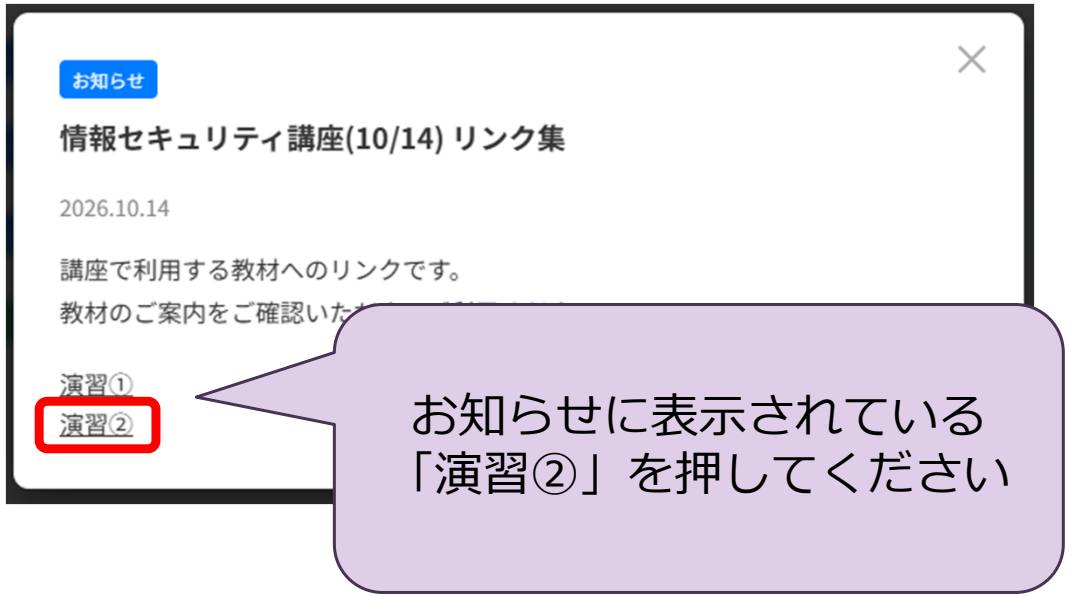
- 「パスワードは8文字以上で，大文字・小文字・数字・記号を混ぜてください」などと言われるけど，いちいち作れません
- 複雑なパスワードは，覚えられません
- 同じパスワードを使い回すのは危険だと聞きながら，短いパスワードを使いまわしています



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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



スマートフォンの方は
こちら

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ 攻撃者が使うようなツールでパスワードを解析してみよう





©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○まずは「toko」で試してみましょう

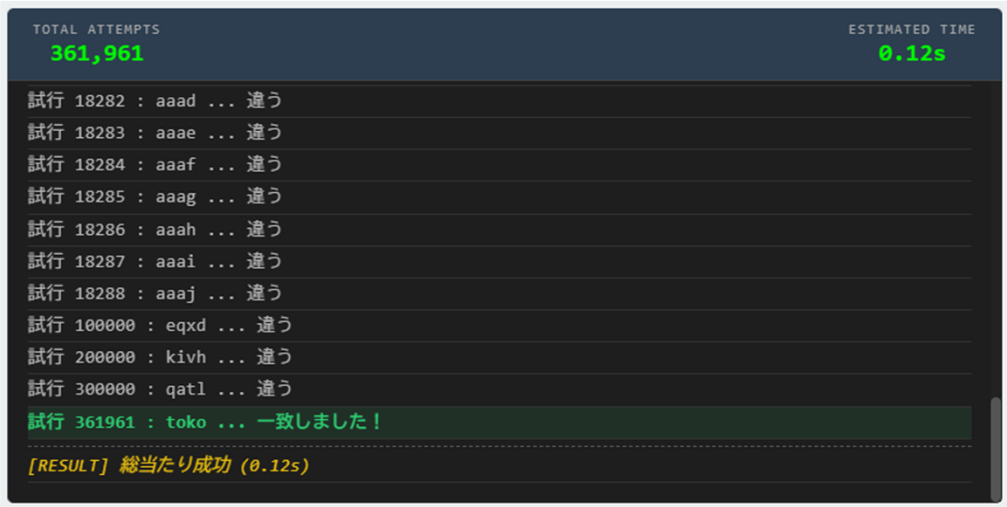


©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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「toko」の場合

▶ ツールは**361,961**通りのパスワードを試して，突破しました



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

〇次は「tokoh」で試してみましょう



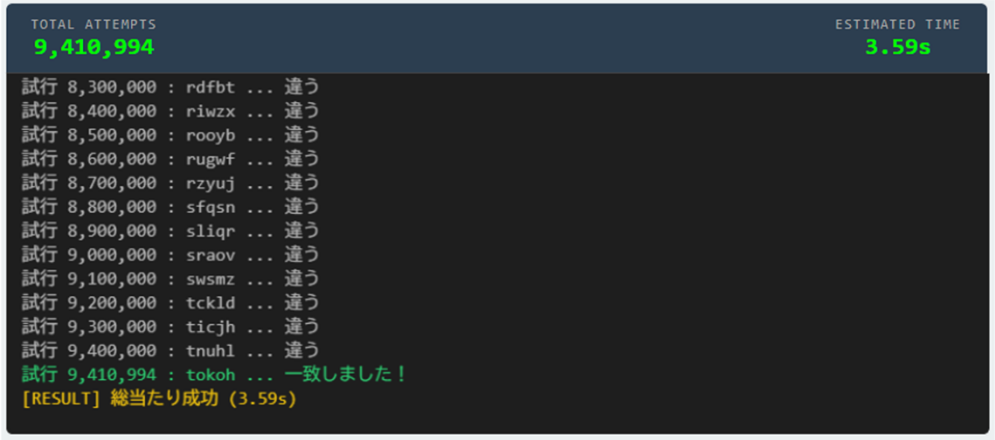
©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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「tokoh」の場合

▶ツールは**9,410,994**通りのパスワードを試して，突破しました

「toko」では**361,961**通りでした



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ 試行回数を比べてみましょう

パスワード	試行回数	実行時間[秒]
toko	361,961	0.12
tokoh	9,410,994	3.59
tokoha	244,685,845	99.57

○ パスワードが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すぐに突破されてしまう！

→ パスワードの桁数は多いほうがいい

※実行時間は，若林の環境での実測値（環境によって異なります）

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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？

▶ 「toko」を徐々に変化させます

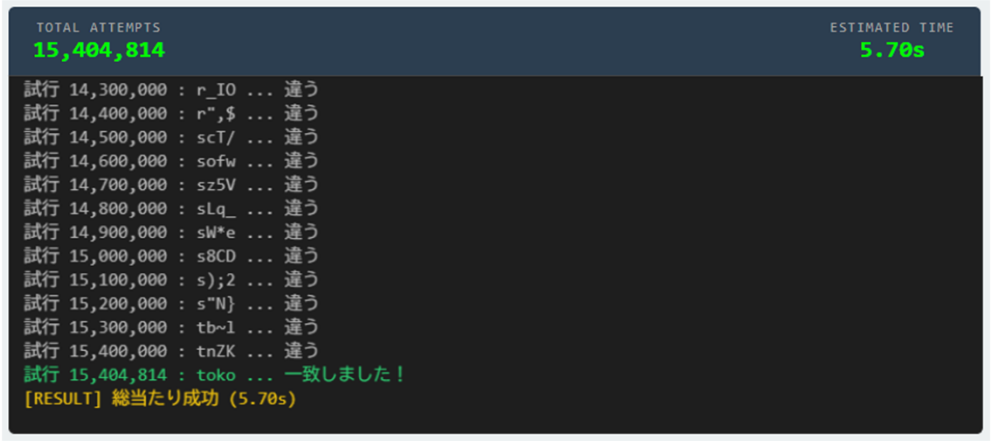


©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ シナリオB「toko」の場合

▶ツールは**15,404,814**通りのパスワードを試して，突破しました



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○「Toko」で実行してみましょう

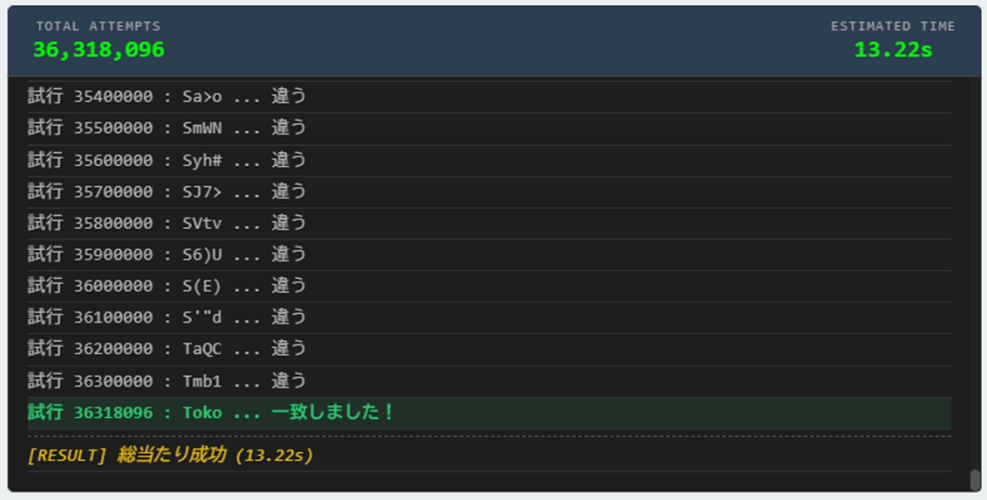


©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ シナリオB「Toko」の場合

▶ツールは**36,318,096**通りのパスワードを試して，突破しました



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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
toko	15,404,814
Toko	36,318,096

〇 文字の種類が1種類増えるだけでも試行回数が大きく違う！

▶ 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

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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（ブルートフォースアタック）とは

▶ パスワードとしてありうる文字の組み合わせを，端から順に全パターン試す手法

→ 桁数が増えたり，文字の種類を組み合わせたりすると，突破されにくくなる

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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「tokoha」で試してみましょう

→ 総当たり攻撃では，244,685,845通り試行しました

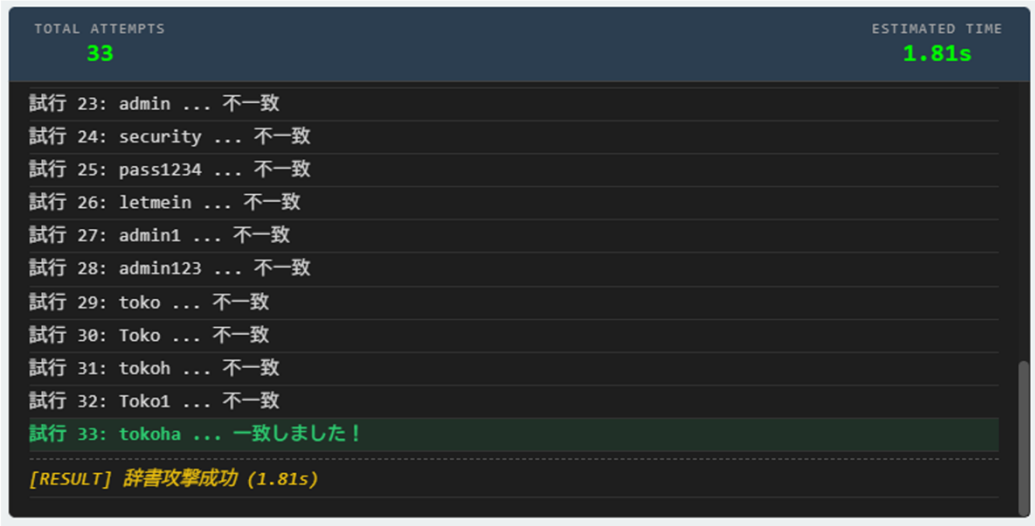


©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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「tokoha」の場合

▶ たったの**33**通りで解析が終わりました…



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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の比較

パスワード	試行回数
総当たり攻撃	**244,685,845**
辞書攻撃	**33**

〇 今回の辞書（攻撃リスト）には「tokoha」が登録されています

▶攻撃者は身近な人の可能性もあります

→個人属性から推測されやすいパスワードは避けましょう

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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 辞書攻撃とは

▶パスワードとして使われやすい文字列で「辞書」を作っておき，辞書に載っていることばを順番に試して，その人のパスワードを割り出す

辞書に載りやすいことば：

- よく使われるパスワード（次ページ）
- ターゲット(被害者)に関する情報
- OSINTで収集したことば

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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

ランキング	世界	日本
1	123456	admin
2	admin	123456
3	12345678	password
4	123456789	Freemima123
5	12345	12345678
6	password	yamamoto2580
7	As123456	Chan8899
8	1234567890	rosycash
9	Pass@123	102030Abcd
10	admin123	mokariku

Top 200 Most Common Passwords - Nord Security (2025)
https://nordpass.com/most-common-passwords-list/

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

②特定されやすいパスワードって何だろう？

○ パスワードは家の鍵と同じように大事なもの．でも長いと管理が面倒．
安全で使いやすいパスワードはどうすれば作れるだろう？

複雑にしないと危険…
でも，覚えられないと意味がない
パソコンはどんどん性能が上がる…



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ 考えたパスワードがどのくらい強力か確かめたい人へ



ここを押すと，
推定の処理時間と
処理回数を見ることが
できます！

実際に動かすと
時間がかかるので、
活用してください

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策

②特定されやすいパスワードって何だろう？

○ 安全なパスワードを作るために大切なこと

- ▶ 桁数を多くする
- ▶ 大文字・小文字・数字・記号などを組み合わせる
- ▶ 身近な情報やSNSに公開しているような情報は避ける

○ パスワードがつきとめられる恐怖

- ▶ 不正侵入や乗っ取りをされてしまう！
  アカウントが犯罪に使われる→犯罪の責任を負わされる
  銀行などから不正にお金を引き出される

InstagramやTikTokの
IDとパスワードを
共通にしてない？

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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 将来

- ▶ パスワードを人が記憶する時代は終わるのかもしれない
  → パスキーやワンタイムパスワードの活用例が多くなってきた

- ▶ 人間の記憶には限界がある
- ▶ システムが多いので適切に管理する負担が大きい

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 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 シミュレータ（=総当たり攻撃）の限界（おまけ）

▶ 処理が終わるのを待てるか & お金の問題（リターンが小さすぎる）

→ 桁数や文字種が増えるほど処理時間が指数関数的に増加する

→ 処理時間が端末の性能に依存する

→ 端末の性能が良ければ，その分電気代がかかる

→ 総当たり攻撃がそもそもできないように対策されている

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ シミュレータの秘密（おまけ）

▶ パスワードの桁数や文字数の違いでの違いを体感することが目的
→ 処理速度を意図的に落としたり，一部処理を省略している

▶ 同じ処理をPCやスマホで出来るぎりぎりの速度でやりたい人は…
→ 「解析開始（高速）」を押してみてください

▶ 6桁以上になると，すごく時間がかかります…（処理が重くなる）

パスワード	実行時間[秒]
tokoha（通常）	**99.57**
tokoha（高速）	**12.28**



©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ シミュレータの秘密（おまけ）

▶ 同じ文字数でも処理回数に大きく差が出ることがある
→ シナリオB: 文字種優先特有の問題…

▶ なぜ起きるか考えてみてください！
→ ある意味，解析の仕方によって大きく変わるわけだ

→ 実際の攻撃者も，効率は考えている

©若林遥大 (遠山研究室) All rights reserved.

2．身近なサイバー犯罪の手口 とその対策
②特定されやすいパスワードって何だろう？

○ パスワードを強くするための制限は本質的なのだろうか？（おまけ）

▶ パスワードの桁数・複数の文字種を強制することは良いことか？
→ セキュリティを強化するためには必要であることは否定しない

▶ 実はパスワードを解読するためのヒントにならないか？
→ 少なくとも8桁以上だとか…
→ 制限を突破するために，aを@に変えているんじゃないかとか…

▶ 利便性を損なっていないだろうか
→ いくら安全だからって，不便で良いと感じる人がいるのか？
→ 面倒なことって，何とかして避けようとするのが人間じゃないか

©若林遥大 (遠山研究室) All rights reserved.

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！！！**

▶ 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）

©若林遥大 (遠山研究室) All rights reserved.

3．おわりに

〇 本日のまとめ

▶ ① 自分の情報は自分でコントロールする

→ 投稿する前に一度立ち止まって，確認する！

→ 何気ない写真1枚でも，背景や情報が組み合わされば特定される

▶ ② パスワードは「家の鍵」，使い回しは絶対にしない

→ システムをうまく頼って，強固な鍵を作る

→ 被害を最小限に抑えることを意識する

©若林遥大 (遠山研究室) All rights reserved.

3．おわりに

○ もっと詳しく学びたいと思ったら

▶ 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

▶ IPA（独立行政法人 情報処理推進機構）

→ 最新のセキュリティー事情や注意喚起などを提供している

→ https://www.ipa.go.jp/security/index.html

▶ VISUSECでも様々な教材を提供中！

→ https://visusec.jp/app/

©若林遥大 (遠山研究室) All rights reserved.

3．おわりに

○ 講座の内容・教材に関するお問い合わせ先

▶ 静岡大学 大学院総合科学技術研究科 情報学専攻

若林 遥大（ワカバヤシ ハルト）

Mail：wakabayashi.haruto@whr.jp

©若林遥大 (遠山研究室) All rights reserved.