PDFパスワードクラック

+大学の課題チート手法

xryuseix

@ryusei_ishika

1回生が入ったので，自己紹介

- 名前：石川琉聖(ID: xryuseix)
- 三回 情理 SNコースです
- セキュリティとアルゴリズムをやります
- いろんなイベントに出没します
- RiST元副団体長, RiPPro元団体長です
- C++とPythonをよく書きます

Event

年	内容
2019	セキュリティ・キャンプ全国大会2019 集中開発コース 暗号化通信ゼミ
2020-2021	若手セキュリティイノベーター育成プログラム SecHack365 研究駆動コース
2020	AVTOKYO 2020 Talks 情報通信システムセキュリティ研究会（ICSS） ▼ 研究テーマ
2021	• 「仮想背景を使用したリモート会議映像における秘匿された背景の再構築手法」 ○辻知希，石川琉聖（立命館大）・衛藤将史（NICT）・服部祐一（セキュアサイクル）・井上博之（広島市大） • 「プログラミングコンテストにおけるソースコードの盗作検知手法の実装と評価」 ○石川琉聖（立命館大）・服部祐一（セキュアサイクル）・井上博之（広島市大）・猪俣敦夫（阪大）
2021	ICPC アジア地区横浜大会

Media

年	内容
2021	サイバーセキュリティII 第２回 情報セキュリティ教育と人材育成 BS231ch

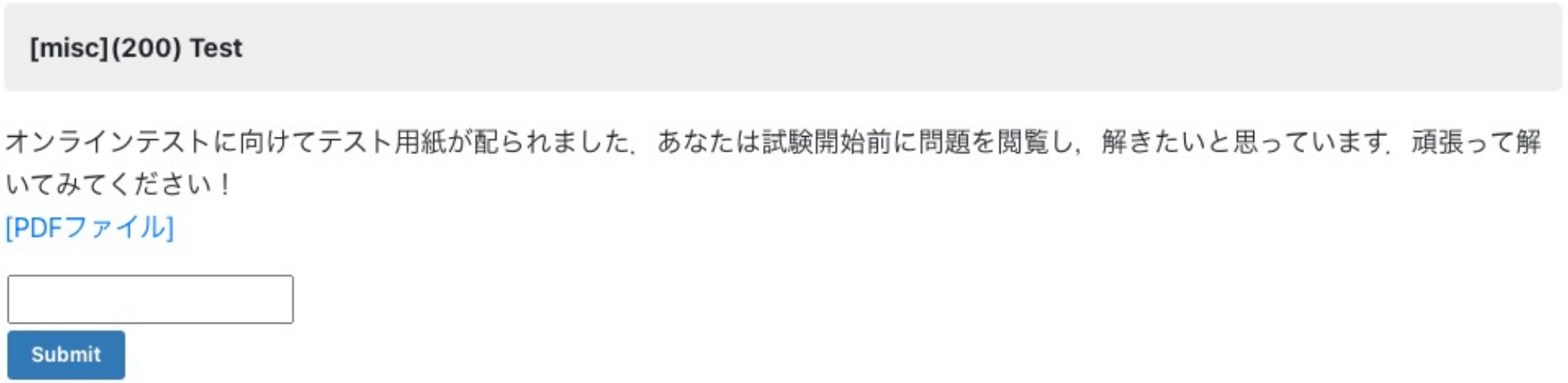
Hack

年	内容
2020-	IPA 脆弱性関連情報届出受理 42件 ▶ 取得番号一覧

https://xryuseix.github.io/

ここからが本題です

- CTF の問題をプレゼント🎉



https://xryuseix.github.io/ctf

問題の背景

概要

- オンラインのテストが行われます.
- 問題ファイルの形式はPDFです.
- 問題は事前に配られ，パスワードは試験開始とともに通達されます.

目的

- パスワードを解除して事前に問題を読みましょう.

補足

- ちなみに難所は二箇所あります.

皆さんが問題を解いている間に(1)

大学の課題チート手法を紹介します！

DeepL

- みなさんご存知の翻訳ツールです.
- 9割以上(体感)の文章に対して違和感のない翻訳ができます.
- 大学回線だと止まりました(泣)

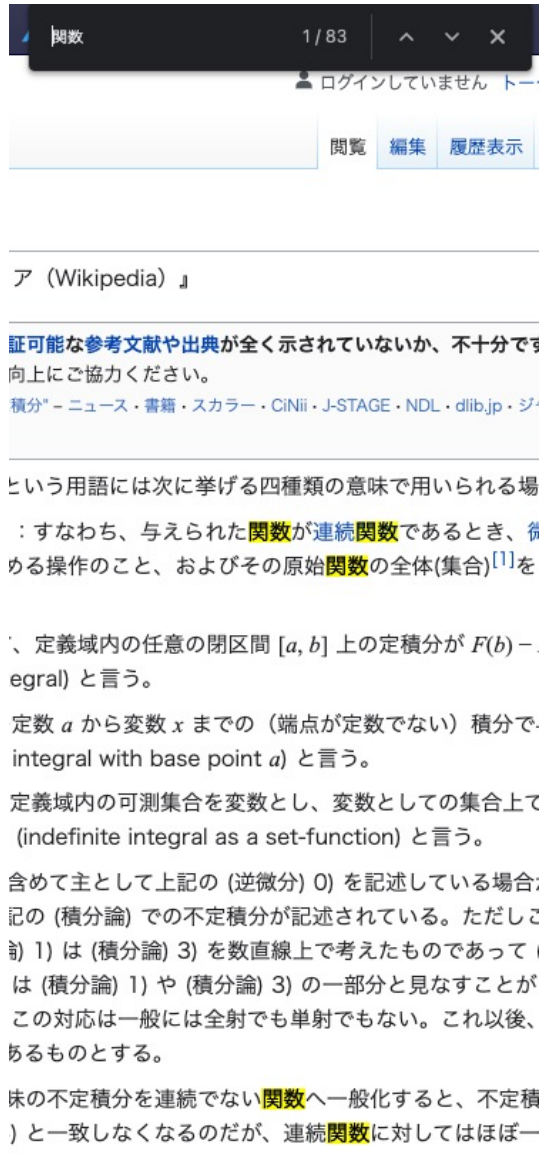
https://www.deepl.com/translator

チートその２

- WolframAlpha 計算知能
  - 数式の計算ができます.
  - 課金すると途中式まで！

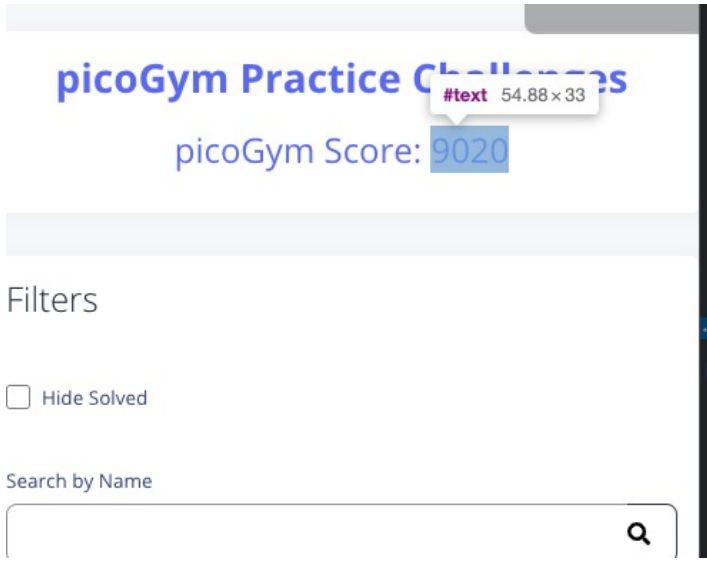
チートその３

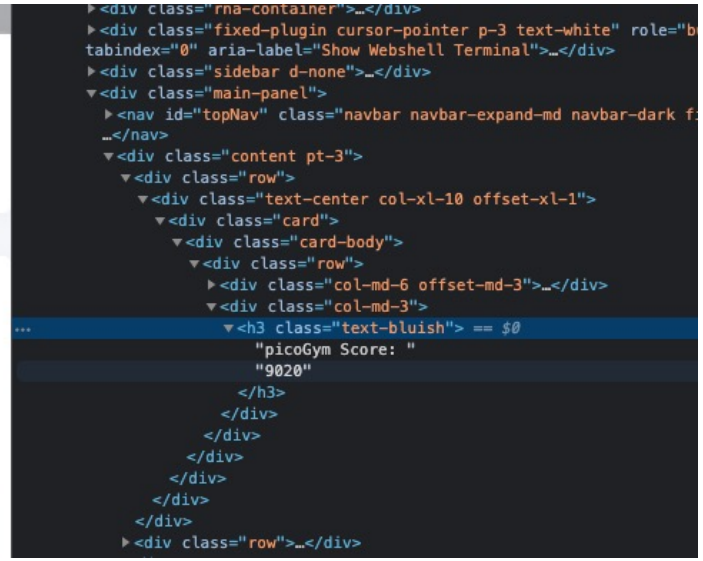
- Web検索
  - みなさんご存知ですが，検索ができます.
  - Webページ内検索はctrl(cmd)+F
  - PDFも当然検索ができます
    - コピーガードに関しては後ほど説明
  - オンラインテスト中にレジュメから探索しよう！

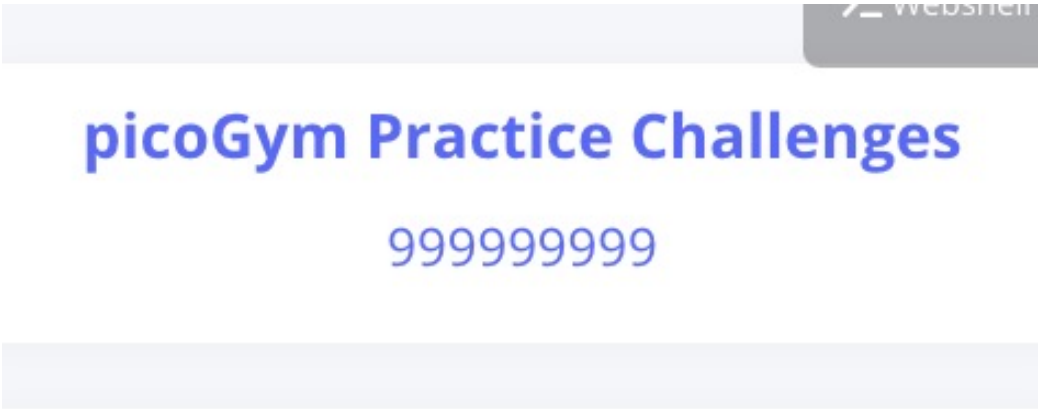


ページ改ざん

- Webサイトを用いた課題でページをスクショする場合
- 改ざんすることで解けたことにできます.







解説(1)

~PDF閲覧まで~

パスワードクラックツール John the ripper

概要

- パスワードクラックツールです
- (表向きにはパスワードの強度チェックツールになっているらしい)

ダウンロード

- kali linuxには最初から入っています(推奨)
- Macの人はこれ(Macは作業の途中からサポートできません)(だからkali推奨)
- `wget https://github.com/magnumripper/JohnTheRipper/archive/bleeding-jumbo.zip`
- `unzip JohnTheRipper-bleeding-jumbo.zip`
- `brew install john`

Johnの解読手順

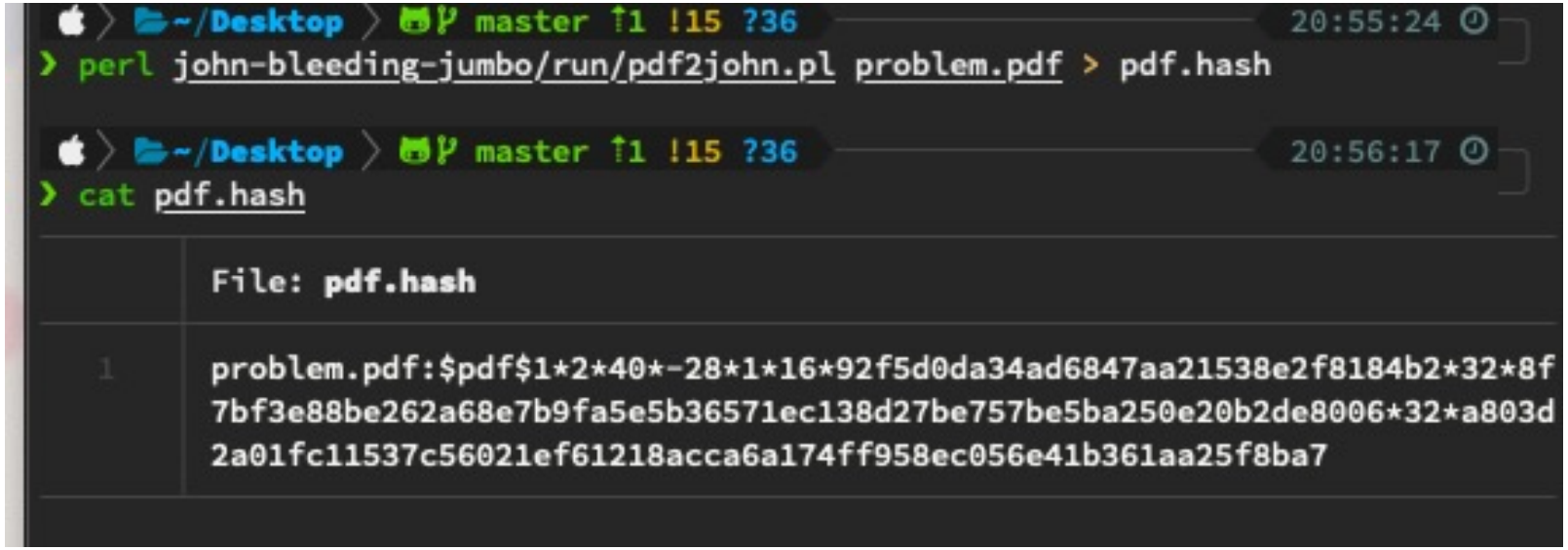
1. 暗号化されたPDFを**ハッシュ化**

2. **パスワードリスト**を入手

3. ハッシュ化したPDFとパスワードリストをJohnに渡すと**パスワードGet!!**

暗号化されたPDFのハッシュを取得

- perlが必要でした．mac, kaliには最初から入ってます
- john-bleeding-jumboのとこがJohnTheRipper-bleeding-jumboとかになってるかもです．
- ハッシュ化するとこんな感じです(多少異なるかもです)

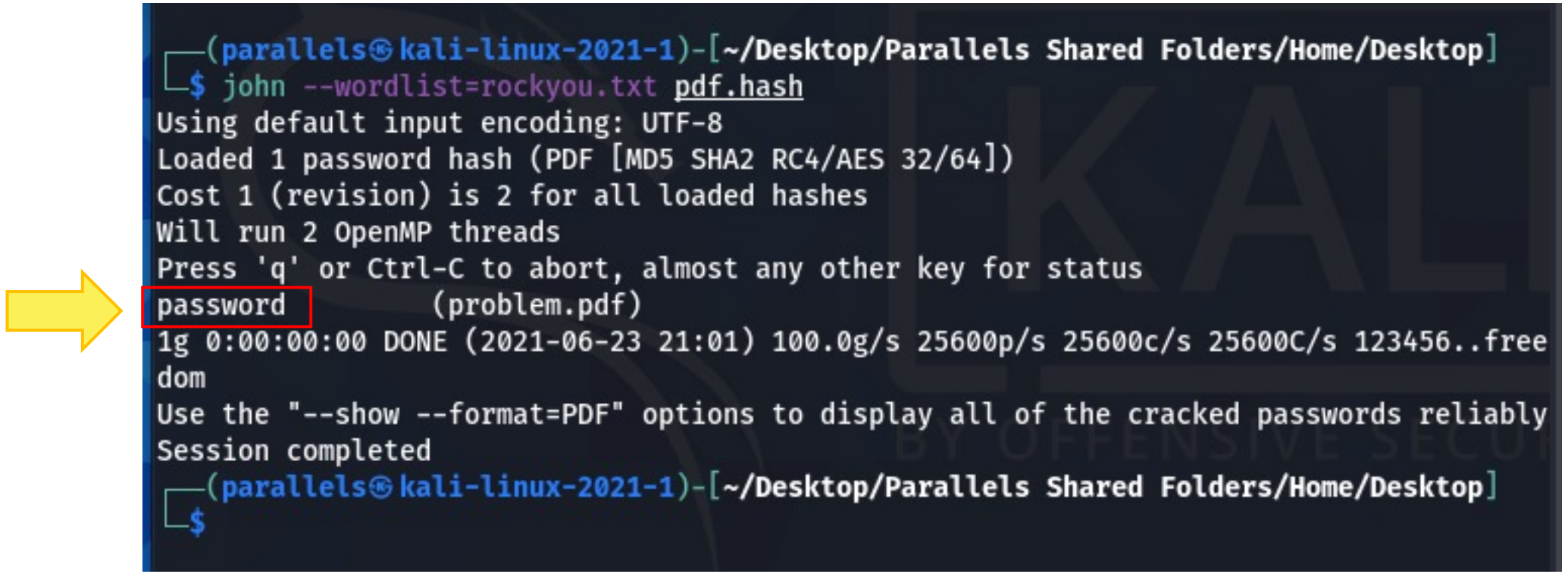


パスワードリストを取得

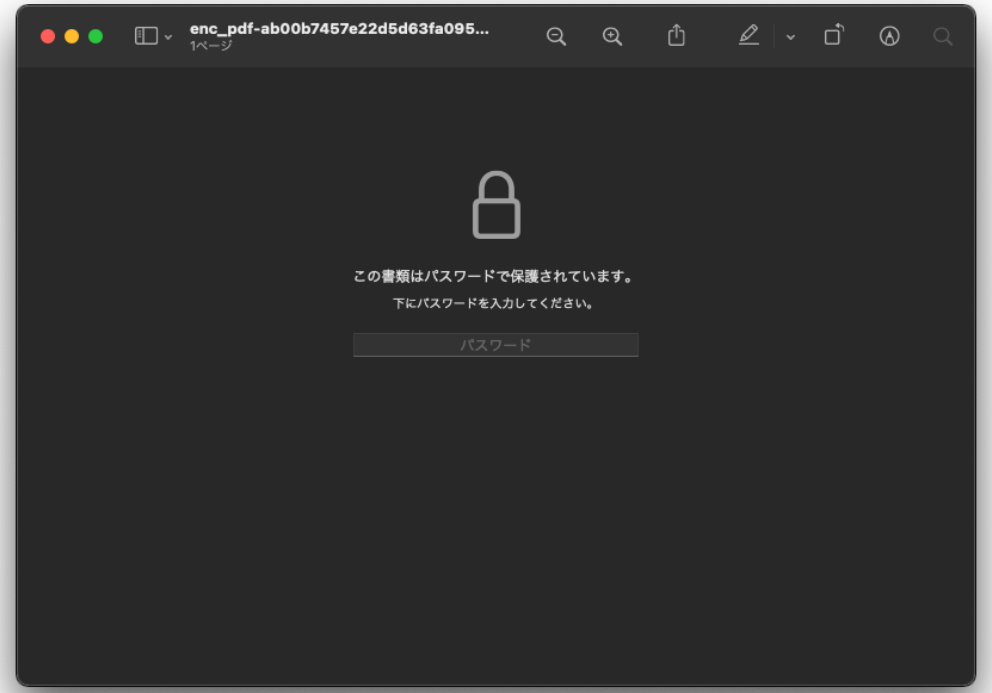
- パスワードリストはなんかいっぱいあります.
- 今回はrockyou.txtっていうのを使いましょう.
- https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt
- ↑このリンクでダウンロードできます(コピーしてdiscordに貼ります).

パスワードを入手する

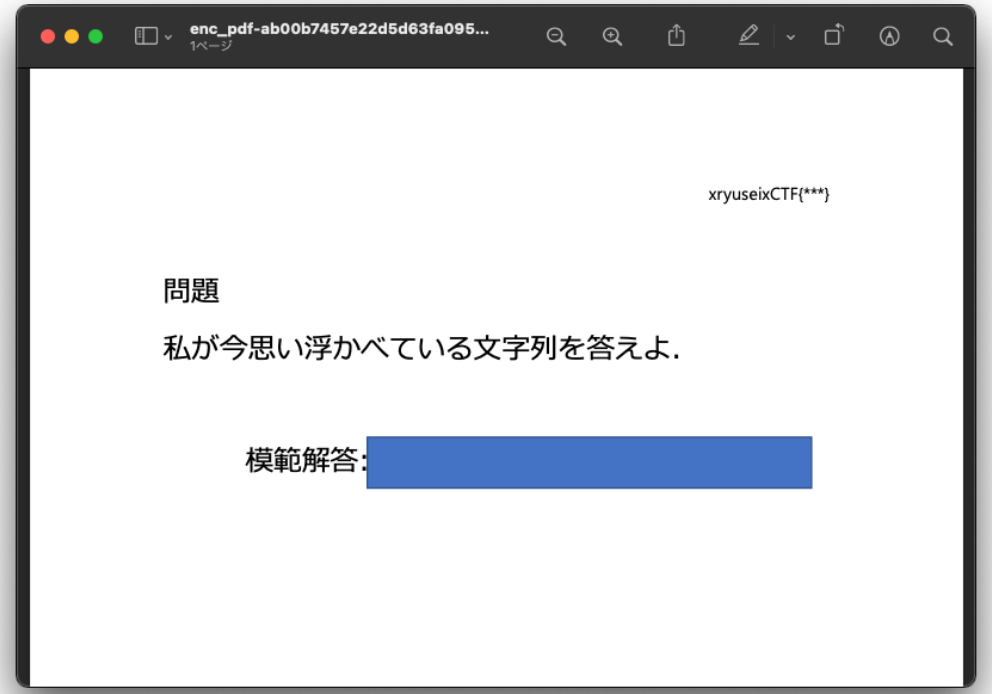
- johnにパスワードリストとハッシュを与えるとパスワード入手できます.
- macはハッシュの形式がおかしいって言われます(僕はよくわかりません><)



テスト問題を閲覧する



“password”
を入力



ここで一段階目クリアです！

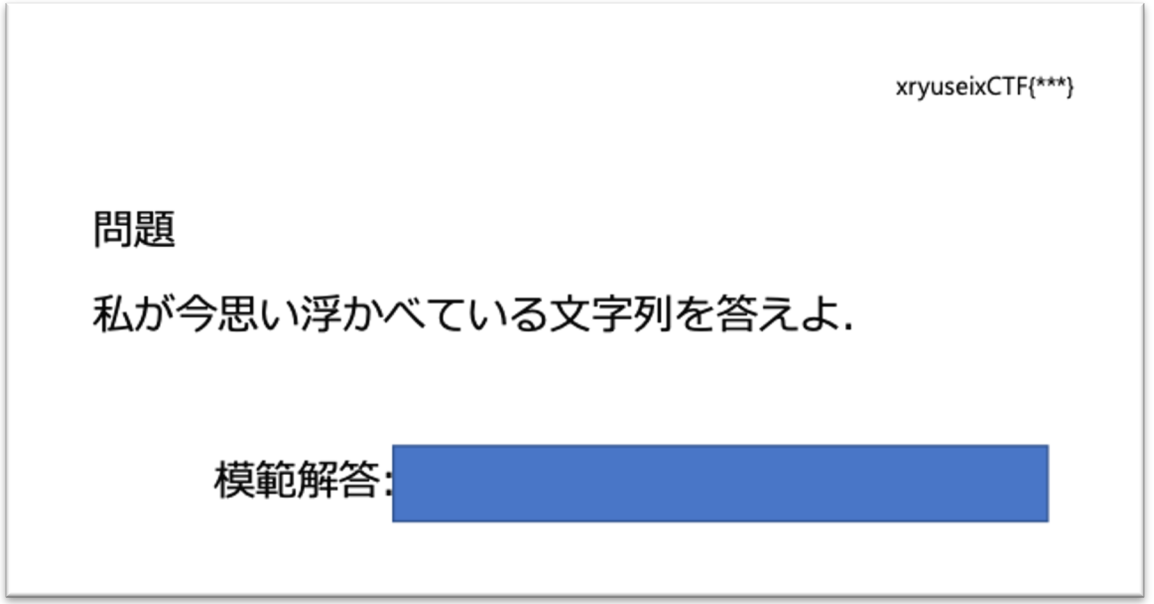
問題の背景 その２

概要

- オンラインで課題が与えられました.
- しかし，残念ながら答えの箇所は塗りつぶされています.
- 塗りつぶしはWordの図形を用いて行われていそうです.

目的

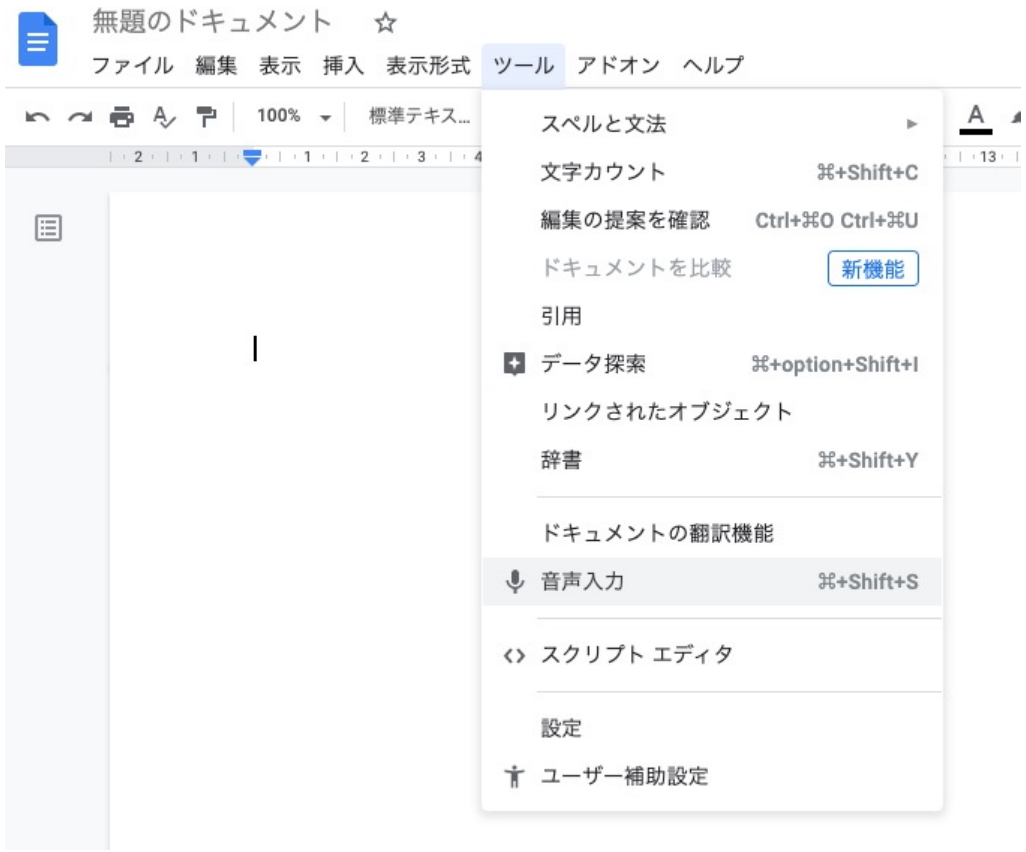
- 問題の答えを入手しましょう.
- フラグ形式はxryuseixCTF{***}です.



皆さんが問題を解いている間に(2)

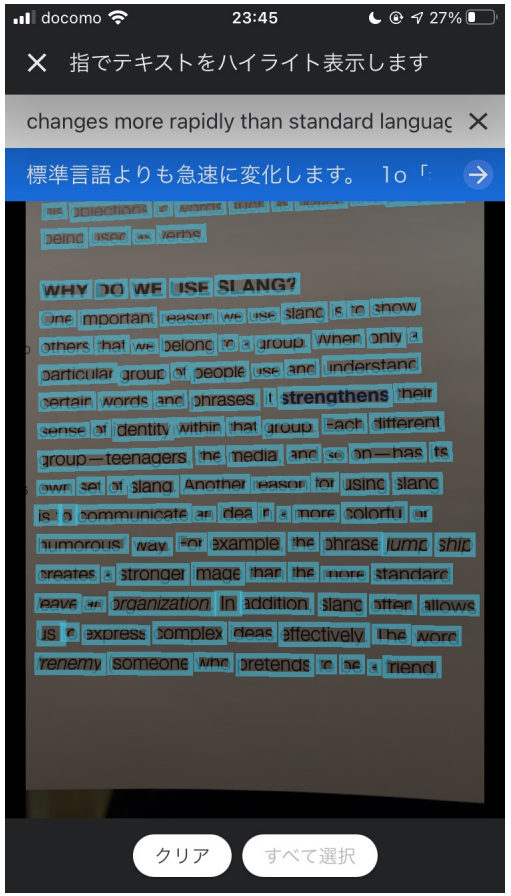
大学の課題チート手法を紹介します！

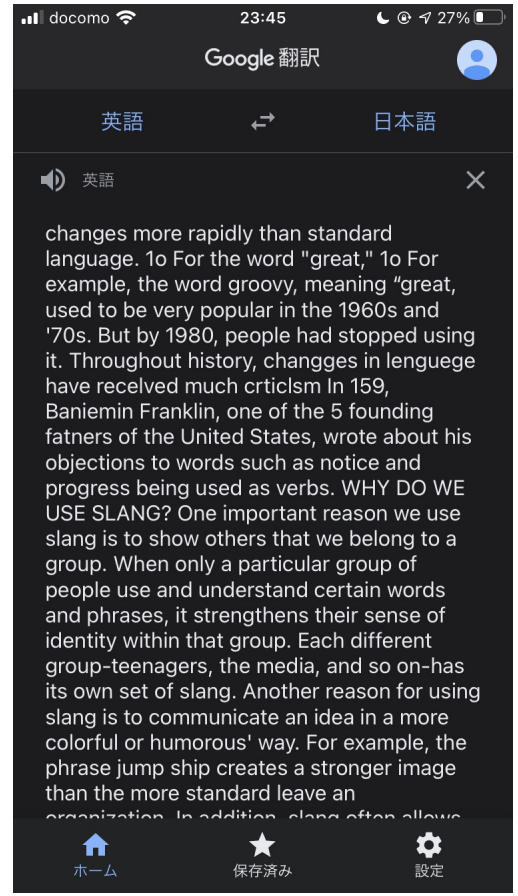
- リスニングは文字起こし+DeepL
  - Google Documentを使って文字起こし



チートその６

- リーディングも文字起こし+DeepL
  - Google翻訳(スマホアプリ版)を使って文字起こし





チートその7

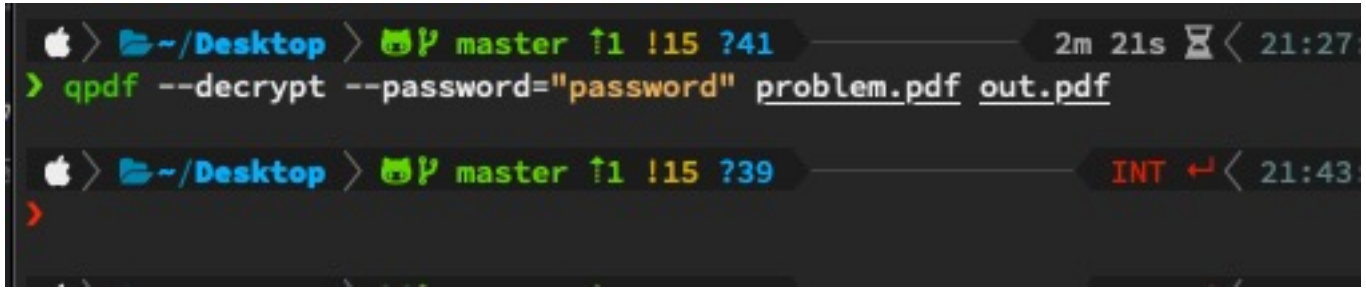
- Webアプリケーションにおける指定時間閲覧しないといけない課題
  - タブを複数開くとWebページ側からは全て閲覧していることになります
    - XReading, EnglishCentral
- 一般企業が作成する音声認識の精度はあまり高くありません
    - EnglishCentral
- ページに含まれる文章は必ずHTML(またはJS, CSS)内に含まれます
  - コピーができます
    - XReading, EnglishCentral

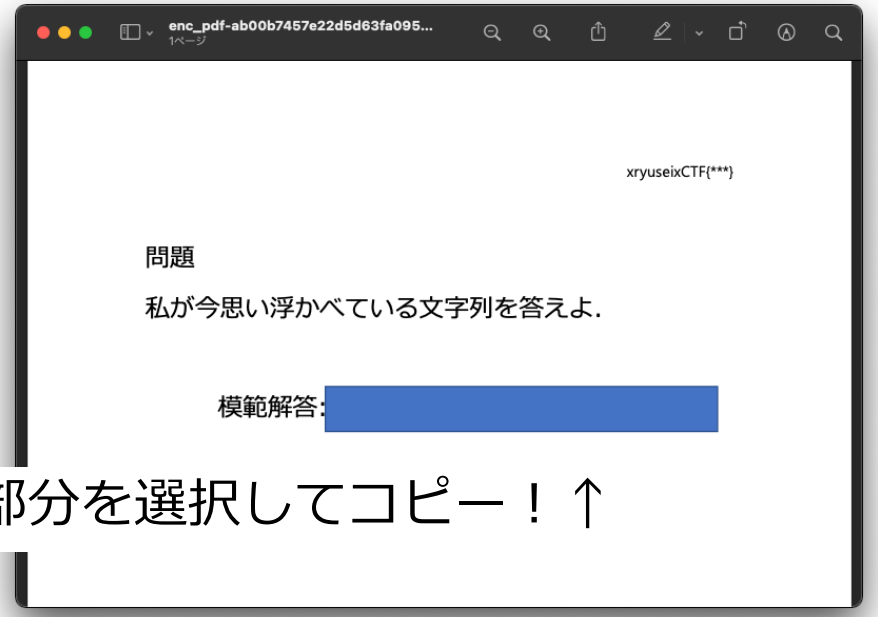
解説(2)

~フラグ取得まで~

- 隠れてても情報が残っているならコピーできませんか？
- って思って僕は抽出を不可でPDF作成しました^^
- 爪が甘い教授(med教授など)だとこれでいけます.

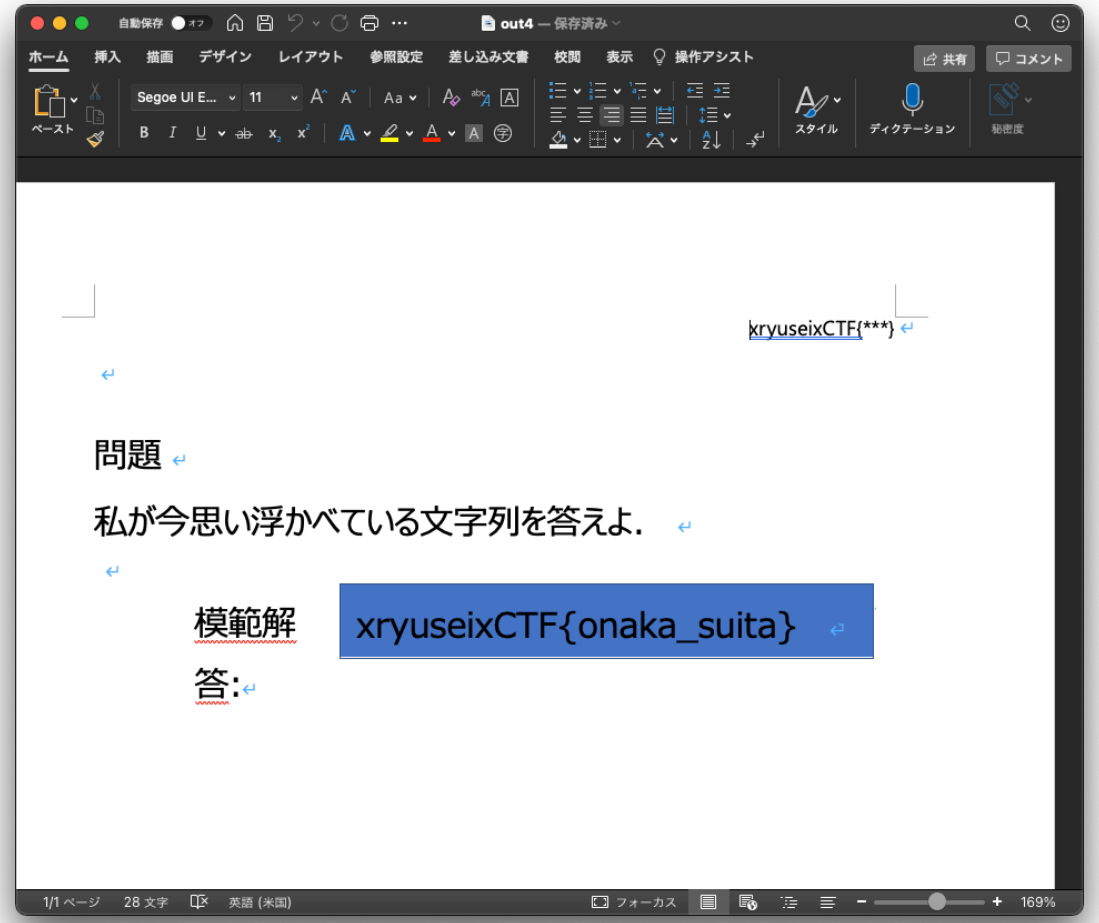
- qpdfコマンド
- brew install qpdfでダウンロードできます(Ubuntuならapt).
- パスワードを指定すると制限を全て解除します.





ここの部分を選択してコピー！↑

- 文字が見えた方が良く無いですか？(=図形を消したく無いですか？)
- パスワードを解除した状態で
  Wordに読み込ませます.
- PWがついてないファイルなら
  これのが圧倒的に楽！



まとめ

- 実はWordでPDFを作成するのは結構危ない
- 実際に情報漏洩したケースもあります
- もしも黒塗りしたい場合は
  黒塗り状態でスクリーンショット
  が一番安全です！気をつけて！

https://scan.netsecurity.ne.jp/article/2020/07/07/44290.html

› インシデント・事故 › インシデント・情報漏えい › 記事

インシデント・事故 ／ インシデント・情報漏えい　2020年7月7日（火） 08時00分

情報漏えいにつながる危険な PDF 利用 － Microsoft Word 網掛け機能誤解、情報公開し注意喚起（大船渡市）

岩手県大船渡市は7月2日、同市Webサイト上で掲載した資料について個人情報が漏えいする可能性のある形式で公開されたことが判明したと発表した。

岩手県大船渡市は7月2日、同市Webサイト上で掲載した資料について個人情報が漏えいする可能性のある形式で公開されたことが判明したと発表した。

これは同市Webサイト上で市選挙管理委員会が掲載した議案資料と会議録について、住所、氏名等の個人情報部分を黒塗りした上でPDF形式で公開していたところ、6月29日午前11時に外部から、特定の方法で黒塗りした部分から個人情報が抽出可能である旨の連絡があり、公開停止したというもの。

同市では、黒塗りで公開していた資料36件の内、告示済みの27件については既に一般に周知されているため同サイトで公開しても差し支えがないと判断した。告示していないものは以下の9件（7人分）の個人情報。

・2018年11月公開開始：3件（住所、氏名）
・2019年7月公開開始：3件（住所、氏名、生年月日、本籍）
・2019年8月：2件（住所、氏名、生年月日、本籍）
・2019年11月：1件（住所、氏名、生年月日、本籍）

同市では該当者に説明と謝罪を行っている。

ScanNetSecurityの取材に対し同市選挙管理委員会の担当者は「本資料はマイクロソフト社のWordで作成し、伏せるべき個人情報には同ソフトの機能である網掛けを使用した。見かけ上は黒塗りしているように見えたため、そのままPDF化し公開したが、文字情報は残っているためコピーすれば、伏せたはずの情報が分かる状態となっていた。私共以外にも、こういったミスをしている自治体等があるかもしれないので、啓発の意味もこめて情報公開を行った。今回の例を広く注意喚起できたらと思います。」と述べた。

あなたが公開したPDF文書は大丈夫？情報漏えい対策に効く、「墨消し」と「非表示情報の消去」の方法 （Adobe Blog）

トップページ

リリース（市ホームページにおける選挙管理委員会の不適正な情報の取扱について）

リリース（公開状況）

シェア　ツイート

記事一覧：顧客情報流出 , 個人情報漏えい

埋蔵文化財発掘届を撮影 201件の個人情報記録した…

EPARKサイトで他の会員情報が誤表示、機能追加…

ExcelをマスキングしPDF変換、コピー＆ペースト…

編集部にメッセージを送る