

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	<ul style="list-style-type: none"> 「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🎉

[misc](200) Test

オンラインテストに向けてテスト用紙が配られました。あなたは試験開始前に問題を閲覧し、解きたいと思っています。頑張ってください！

[\[PDFファイル\]](#)

Submit

<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！

$y'' + y = 0$

拡張キーボード

アップロード

例を見る

ランダムな例を使う

入力:

$y''(x) + y(x) = 0$

常微分方程式の型:

自律方程式

$y''(x) = -y(x)$

ファン・デル・ポール方程式

$y''(x) + y(x) = 0$

ファン・デル・ポール方程式

常微分方程式の分類:

二階線形常微分方程式

別の形:

$y''(x) = -y(x)$

微分方程式の解:

$y(x) = c_2 \sin(x) + c_1 \cos(x)$

各サンプルの解のプロット

微分方程式

$f(x) = \log(x)/x^2$ の最大値

拡張キーボード

アップロード

例を見る

ランダムな例を使う

最大値は数式の最適化とする | 代わりに 数学 とする

"log" は自然対数関数とする | 或いは 10 を底とする対数 とする

入力解釈:

最大化

$\frac{\log(x)}{x^2}$

log(x) は自然対数です

最大値:

近似値

ステップごとの解説

$x = \sqrt{e}$ のとき, $\max\left(\frac{\log(x)}{x^2}\right) = \frac{1}{2e}$

極大値

0 から π の範囲で $\sin x$ を積分

拡張キーボード

アップロード

例を見る

ランダムな例を使う

定積分:

ステップごとの解説

$\int_0^\pi \sin(x) dx = 2$

積分の視覚的表現:

不定積分:

ステップごとの解説

$\int \sin(x) dx = -\cos(x) + \text{定数}$

積分

このページをダウンロード

Wolfram言語を使っています

2021/6/25

Ritsumeikan Security Team

○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ユメから探索しよう！

関数 1 / 83 ^ v x

ログインしていません トー...

閲覧 編集 履歴表示

ア (Wikipedia) 』

証可能な参考文献や出典が全く示されていないか、不十分で向上にご協力ください。

積分* - ニュース・書籍・スカラー・CiNii・J-STAGE・NDL・dlib.jp・ジ...

という用語には次に挙げる四種類の意味で用いられる場

: すなわち、与えられた関数が連続関数であるとき、微める操作のこと、およびその原始関数の全体(集合)^[1]を

、定義域内の任意の閉区間 $[a, b]$ 上の定積分が $F(b) - \text{egral}$) と言う。

定数 a から変数 x までの (端点が定数でない) 積分で、integral with base point a) と言う。

定義域内の可測集合を変数とし、変数としての集合上での (indefinite integral as a set-function) と言う。

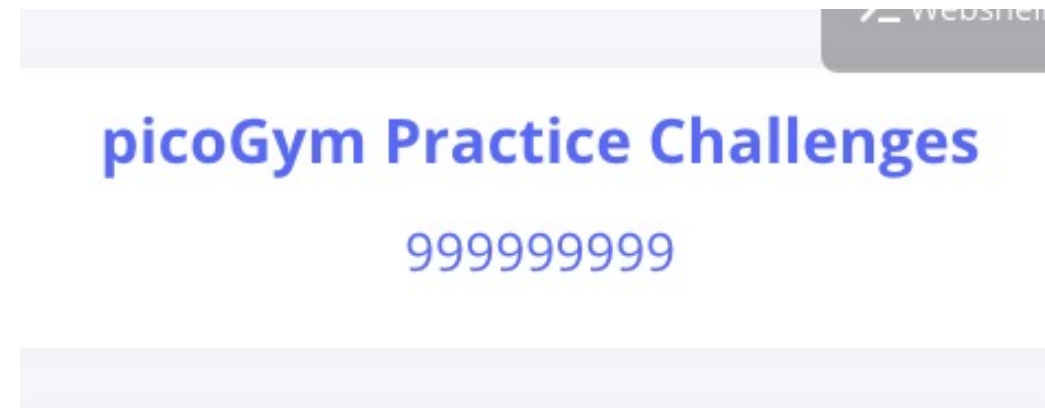
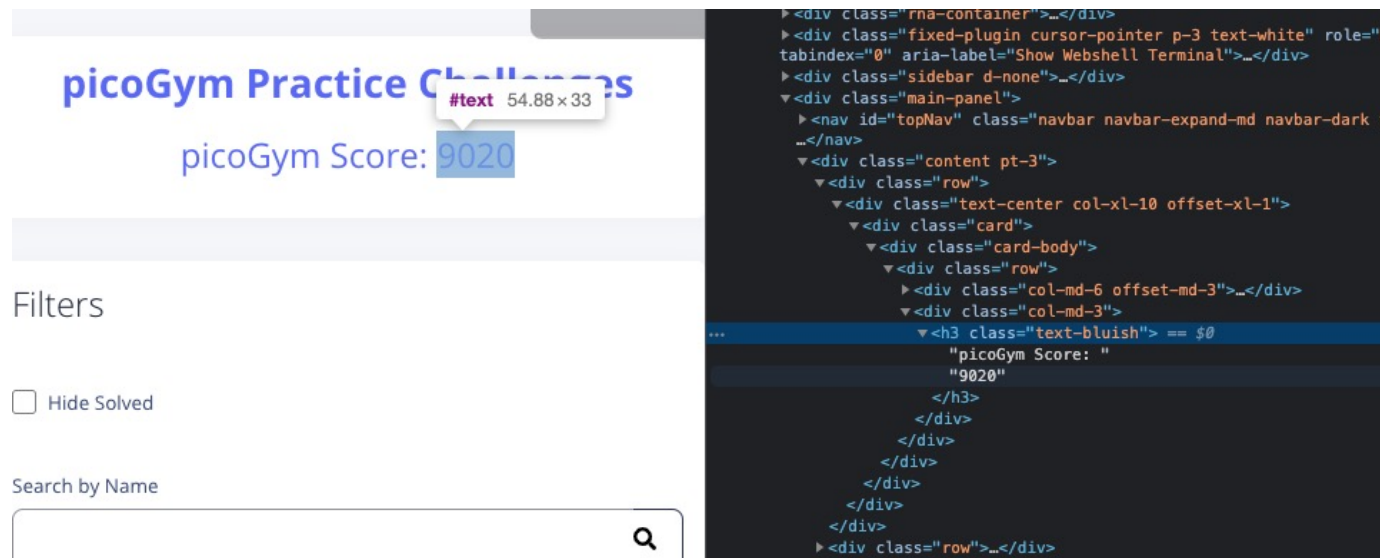
含めて主として上記の (逆微分) 0) を記述している場合; 記の (積分論) での不定積分が記述されている。ただしこ

1) は (積分論) 3) を数直線上で考えたものであって、は (積分論) 1) や (積分論) 3) の一部分と見なすことがこの対応は一般には全射でも単射でもない。これ以後、あるものとする。

味の不定積分を連続でない関数へ一般化すると、不定積分) と一致しなくなるのだが、連続関数に対してはほぼ一

○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`

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のところが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)

```
apple> ~/Desktop > master ↑1 !15 ?36 20:55:24
> perl john-bleeding-jumbo/run/pdf2john.pl problem.pdf > pdf.hash

apple> ~/Desktop > master ↑1 !15 ?36 20:56:17
> cat pdf.hash
```

	File: pdf.hash
1	problem.pdf:\$pdf\$1*2*40*-28*1*16*92f5d0da34ad6847aa21538e2f8184b2*32*8f7bf3e88be262a68e7b9fa5e5b36571ec138d27be757be5ba250e20b2de8006*32*a803d2a01fc11537c56021ef61218acca6a174ff958ec056e41b361aa25f8ba7

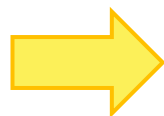
パスワードリストを取得

- 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).

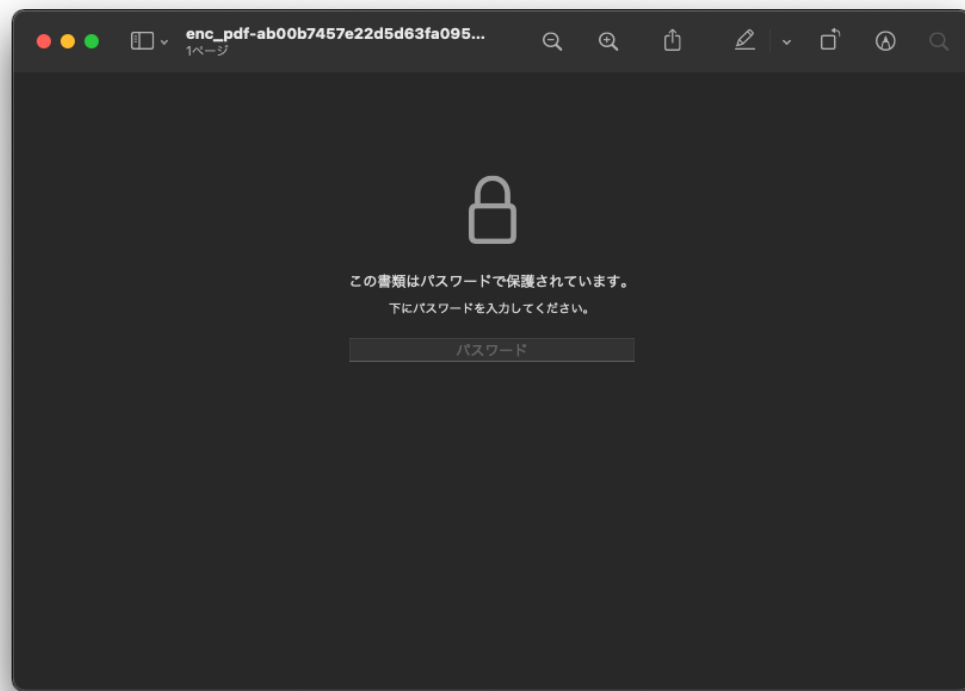
	File: rockyou.txt
1	123456
2	12345
3	123456789
4	password
5	iloveyou
6	princess
7	1234567
8	rockyou
9	12345678
10	abc123
11	nicole
12	daniel
13	babygirl
14	monkey
15	lovely
16	jessica
17	654321
18	michael
19	ashley
20	qwerty
21	111111
22	iloveu
23	000000
24	michelle
25	tigger
26	sunshine
27	chocolate
28	password1
29	soccer
30	anthony
31	friends
32	butterfly
33	purple
34	angel

パスワードを入手する

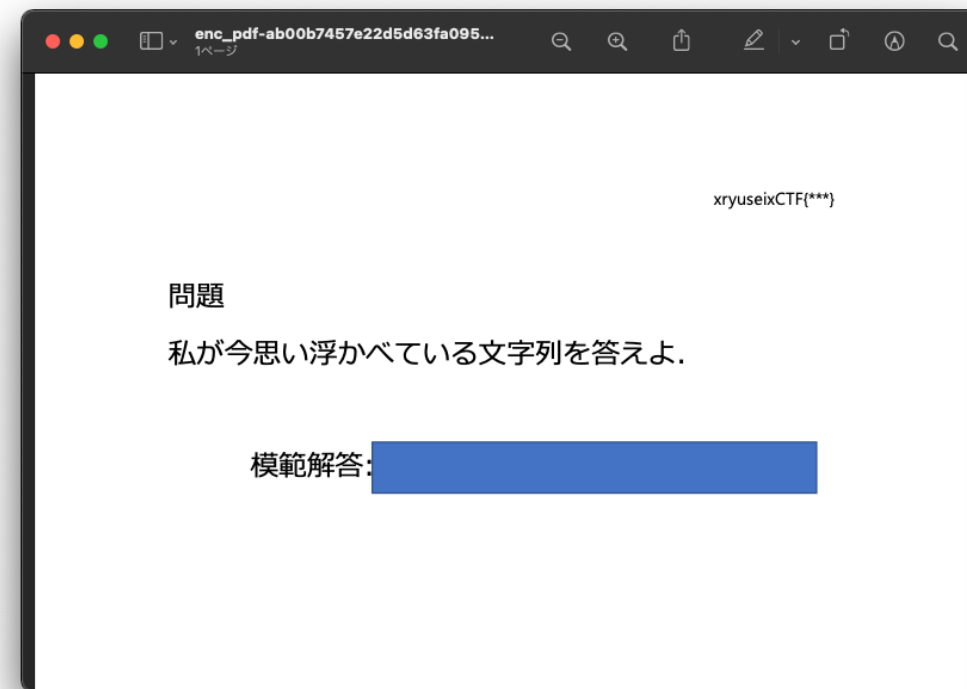
- johnにパスワードリストとハッシュを与えるとパスワード入手できます。
- macはハッシュの形式がおかしいって言われます(僕はよくわかりません><)



```
(parallels@kali-linux-2021-1)-[~/Desktop/Parallels Shared Folders/Home/Desktop]
$ john --wordlist=rockyou.txt pdf.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 2 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password          (problem.pdf)
1g 0:00:00:00 DONE (2021-06-23 21:01) 100.0g/s 25600p/s 25600c/s 25600C/s 123456..free
dom
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed
(parallels@kali-linux-2021-1)-[~/Desktop/Parallels Shared Folders/Home/Desktop]
$
```



“password”
を入力



ここで一段階目クリアです！

○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.

xryuseixCTF{***}

問題

私が今思い浮かべている文字列を答えよ.

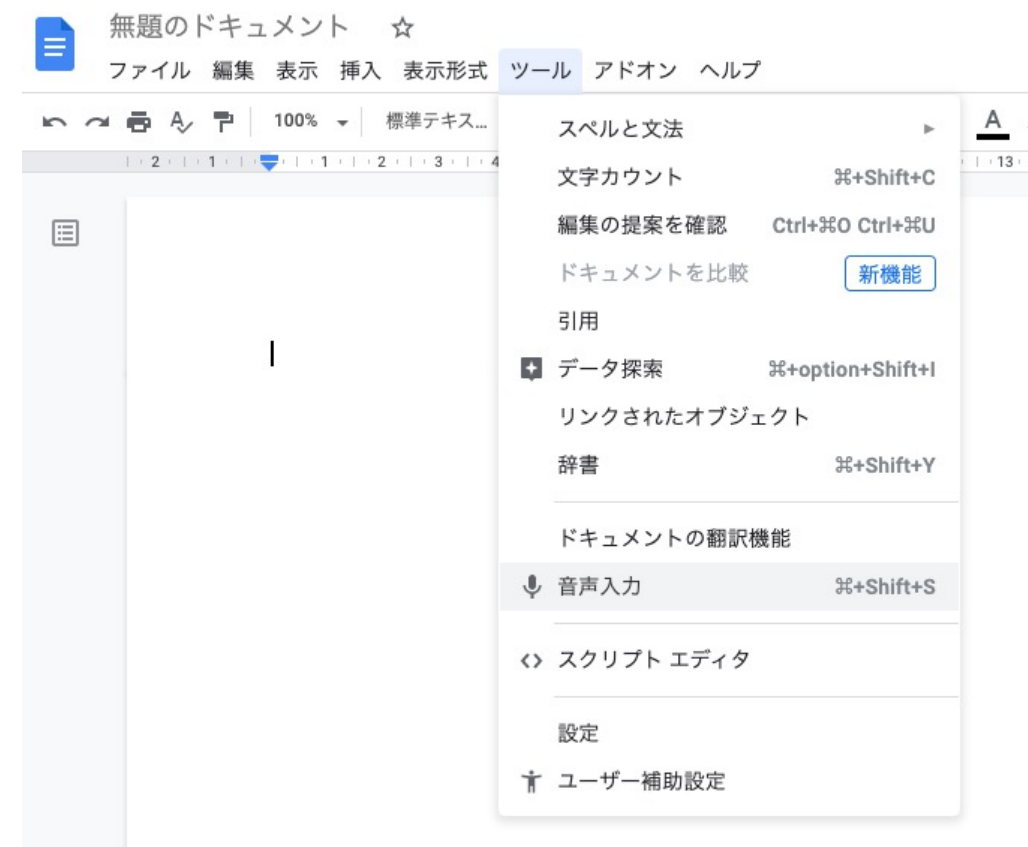
模範解答:

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！

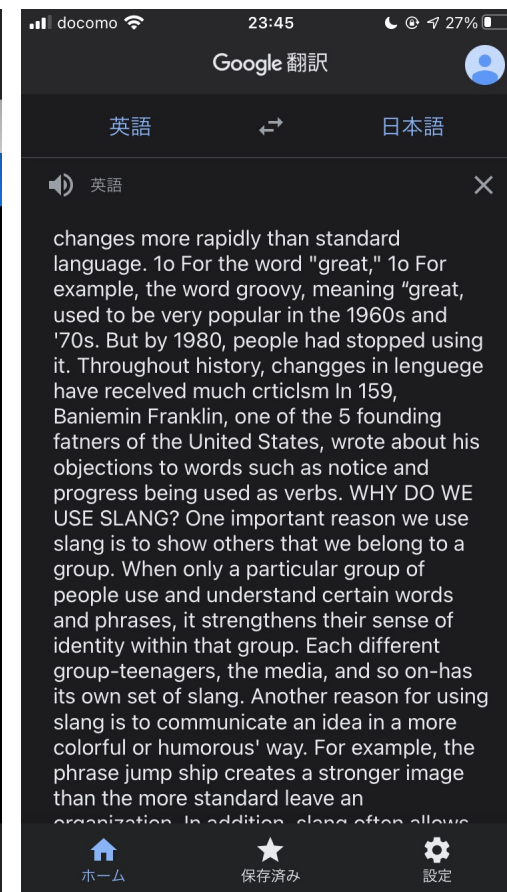
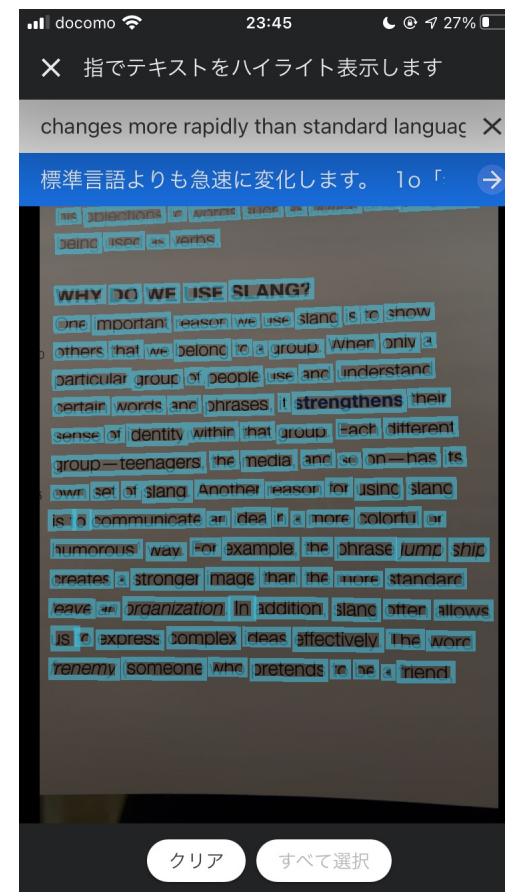
○リスニングは文字起こし+DeepL

- Google Documentを使って文字起こし



○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



○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～

まず考えること

- 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。

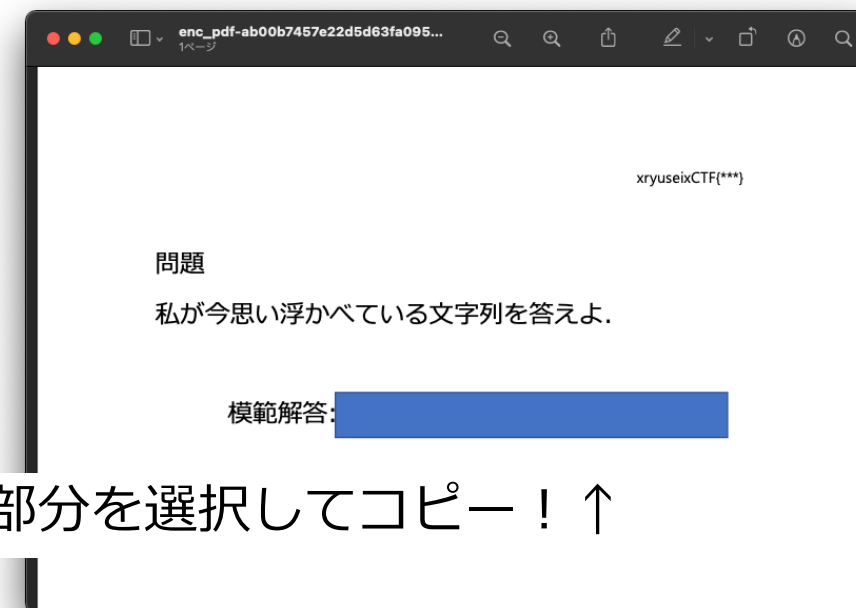


解法その1

- 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.

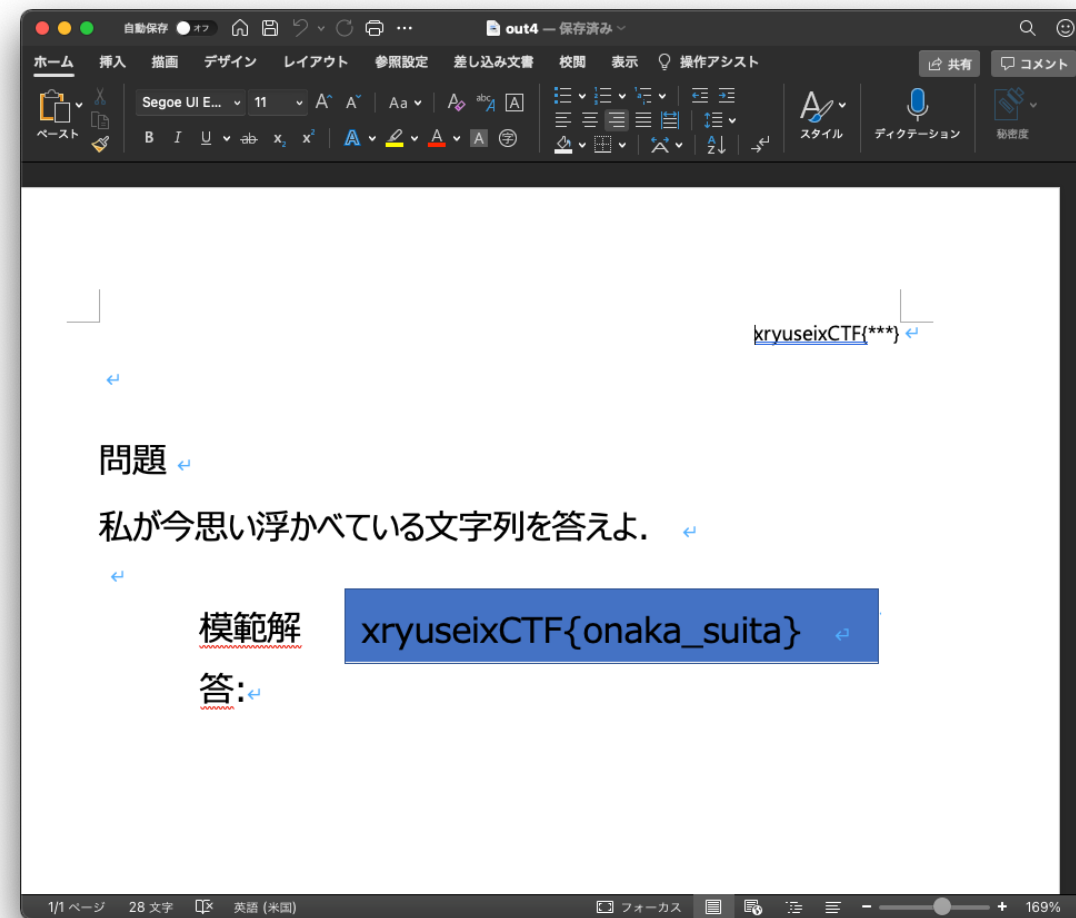
```
Apple > ~/Desktop > master ↑1 !15 ?41 2m 21s < 21:27
> qpdf --decrypt --password="password" problem.pdf out.pdf

Apple > ~/Desktop > master ↑1 !15 ?39 INT ↵ < 21:43
>
```



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
これが圧倒的に楽！



- 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>

ホーム > 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。

