



Kanper

チーム名: UN頼み

電気通信大学

岡山 あん(発表者)

池澤 隆人

嶋田 康太

篠崎 佑馬

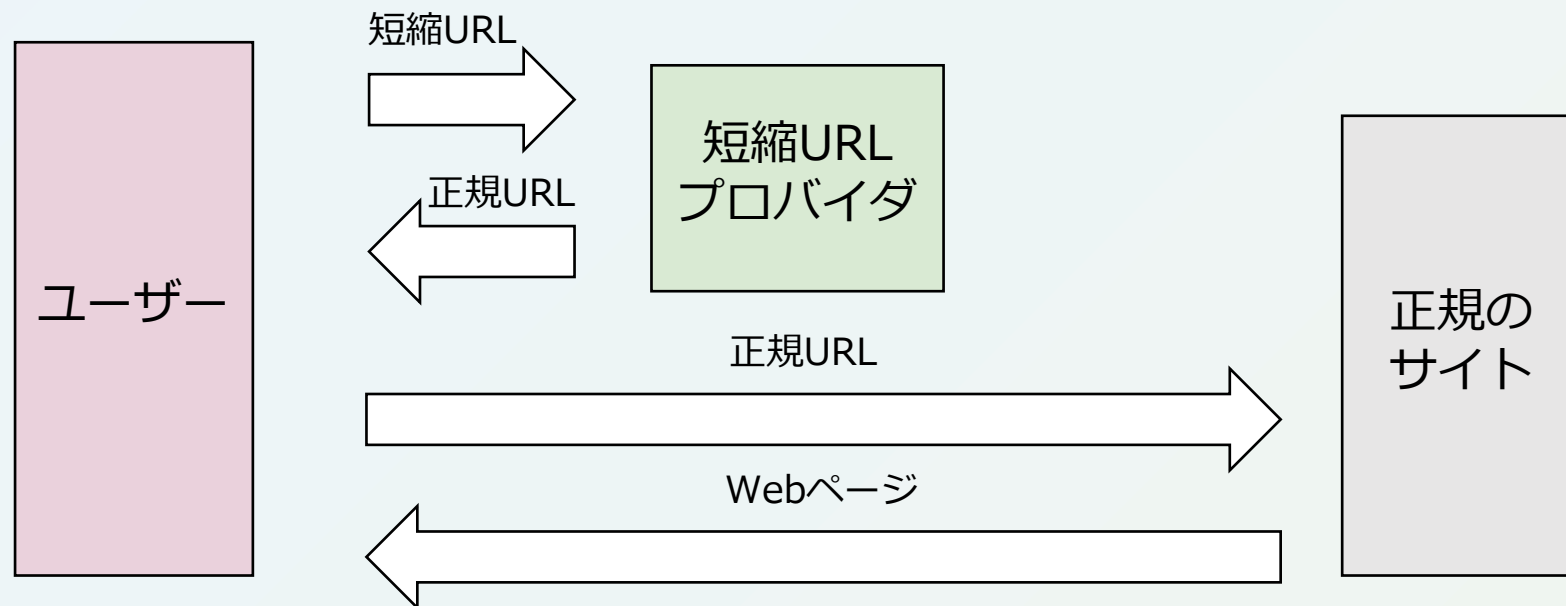
渡邊 祐貴

NTTコミュニケーションズ

大森 敬仁

短縮URLとは

- 正規のURLにリダイレクトされる短めなURLのこと
- BitlyやTinyURLなどの短縮URLプロバイダから提供される
- 文字数の節約を目的にSNSやメールで使用される場合が多い



短縮URLの問題点

- 短縮URLから遷移先のURLが分からない
 - 悪質サイトへのURLが隠されてしまう
- 1つの遷移先に対して複数の短縮URLを簡単に作成可能
 - 迷惑メールフィルタのフィッシングURL検知機能が回避されてしまう

【警視庁】 重要なお知らせ、必ずお読みください。
<https://cutt.ly/> [redacted]

図. 警視庁を語った短縮URLを用いたフィッシング

(参考: <https://diamond.jp/articles/-/309413?page=4>)

ブルートフォース攻撃の餌食に

短縮URLはなぜ「使ってはいけない」といわれるのか？ セキュリティ面から考える




短縮URLは長いURLと比べて安全性が低く、攻撃者にマルウェア拡散の足掛かりを与えかねないという見方がある。それはなぜなのか。

図. 短縮URLの特集記事

(参考: <https://techtarget.itmedia.co.jp/tt/news/1710/02/news03.html>)

短縮URLにアクセスする時に、遷移先を確認する機能が必要！

問題に対する既存の解決ツール

- LinkUnshortener 
- Unshorten.It! 
- ExpandURL 

いずれも短縮URLアクセス時に正規サイトの情報を表示

(遷移先のページの詳細情報・セキュリティチェックサイトのURL・サムネイル)

既存ツールの問題点

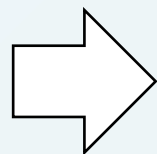
1. 短縮URLにアクセスする度にツールが起動する

- よく訪れるドメインに遷移する場合でも、手動で確認が必要となる

<http://bit.ly/2189pis>

<http://tiny.cc/693zuz>

(良く見るブログサイトの
quota.comの記事に遷移する短縮URL)



確認してから
遷移して!



よく見るブログサイトだから
自動で遷移して欲しいなあ

2. そもそもツール側のサーバが信頼できるか不明瞭



安全だよ

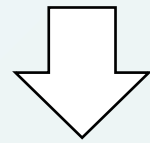


本当?

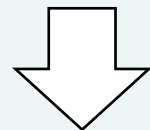
提案ツール: Kanper

- 短縮URLへのアクセス時に遷移先の情報の表示
- ホホワイトリスト・ブラックリスト機能搭載
- アクセス情報などを完全に制御できるセキュア機能

隠された真相(遷移先の悪質URL)を看破する者



看破er



Kanper



① 遷移先情報の表示機能

N段リダイレクトでも
遷移先を特定

短縮URLへのアクセス時に遷移先の情報を表示する

次のページを表示しますか？

CANCEL

OK

ホワイトリストに追加して表示

ブラックリストに追加

ページ情報

ページタイトル

国立大学法人 電気通信大学

URL

https://www.uec.ac.jp/

ページの説明

電気通信大学は、武蔵野の緑溢れる東京都調布市にある国立大学です。「総合コミュニケーション科学」の創造と「Unique & Exciting Campus」の実現を目指します。

安全性チェック

Google透明性レポート ✓

Norton Safe Web ☑

Kaspersky Threat Intelligence Portal ☑



① 遷移先情報の表示機能

表示内容: ページ概要・Google Safe Browsingの結果・サムネイル

アイコンでも結果を表示

次のページを表示しますか？

CANCEL

OK

ホワイトリストに追加して表示

ブラックリストに追加

ページ情報

ページタイトル

国立大学法人 電気通信大学

URL

https://www.uec.ac.jp/

ページの説明

電気通信大学は、武蔵野の緑溢れる東京都調布市にある国立大学です。「総合コミュニケーション科学」の創造と「Unique & Exciting Campus」の実現を目指します。

ページのタイトルや説明文

安全性チェック

Google透明性レポート 

Norton Safe Web

Kaspersky Threat Intelligence Portal

セキュリティチェックの結果



トップページ | 文庫・学内マップ | お問い合わせ | 入試資料請求 | サイトマップ | English | Google Translate (中国語翻訳)

電気通信大学
The University of Electro-Communications

受験生の方 | 在学生の方 | 卒業生の方 | 企業・研究機関の方 | 一般の方

大学案内 | 学域(学部) | 大学院 | 図書館・教育研究センター | 教育・学生生活 | 就職・進路 | 研究・産学連携 | 地域交流・国際交流

「UECウクライナ等国際的人道支援基金」の創設について

UEC Research
電通大の先進的な研究を紹介

「海上漂着の新たな電子資源」電気通信大
「AIとロボットの連携」電気通信大
「人とコンピュータが協働する社会」電大
UEC e-Bulletin

遷移先のサムネイル

②UXのこだわり：ホワイトリスト機能

ホワイトリストにURLを登録すると確認作業なしで遷移できる

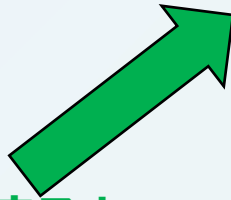


遷移先のドメインがホワイトリストに登録されているため、正規サイトがそのまま表示される
→ 別の短縮URLであっても、遷移先が同じであれば確認画面が発生せず表示

②UXのこだわり：ホワイトリスト登録方法 1

遷移画面上で“**ホワイトリストに追加して表示**”を選択

ここをクリックすると
ホワイトリストに登録
して遷移する



次のページを表示しますか？

ページ情報

ページタイトル
国立大学法人 電気通信大学

URL
<https://www.uec.ac.jp/>

ページの説明
電気通信大学は、武蔵野の緑溢れる東京都調布市にある国立大学です。「総合コミュニケーション科学」の創造と「Unique & Exciting Campus」の実現を目指します。

安全性チェック

Google透明性レポート

Norton Safe Web

Kaspersky Threat Intelligence Portal

UEC 電気通信大学
The University of Electro-Communications

「UECウクライナ等国際的人道支援の創設について」

UEC Research
電通大の先進的な研究を紹介

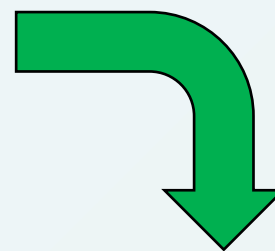
②UXのこだわり：ホワイトリスト登録方法2

画面右上の拡張機能設定から、“今のページをホワイトリストに追加”を選択



②UXのこだわり：ホワイトリストの編集

編集画面で簡単に整理可能



編集画面へ遷移

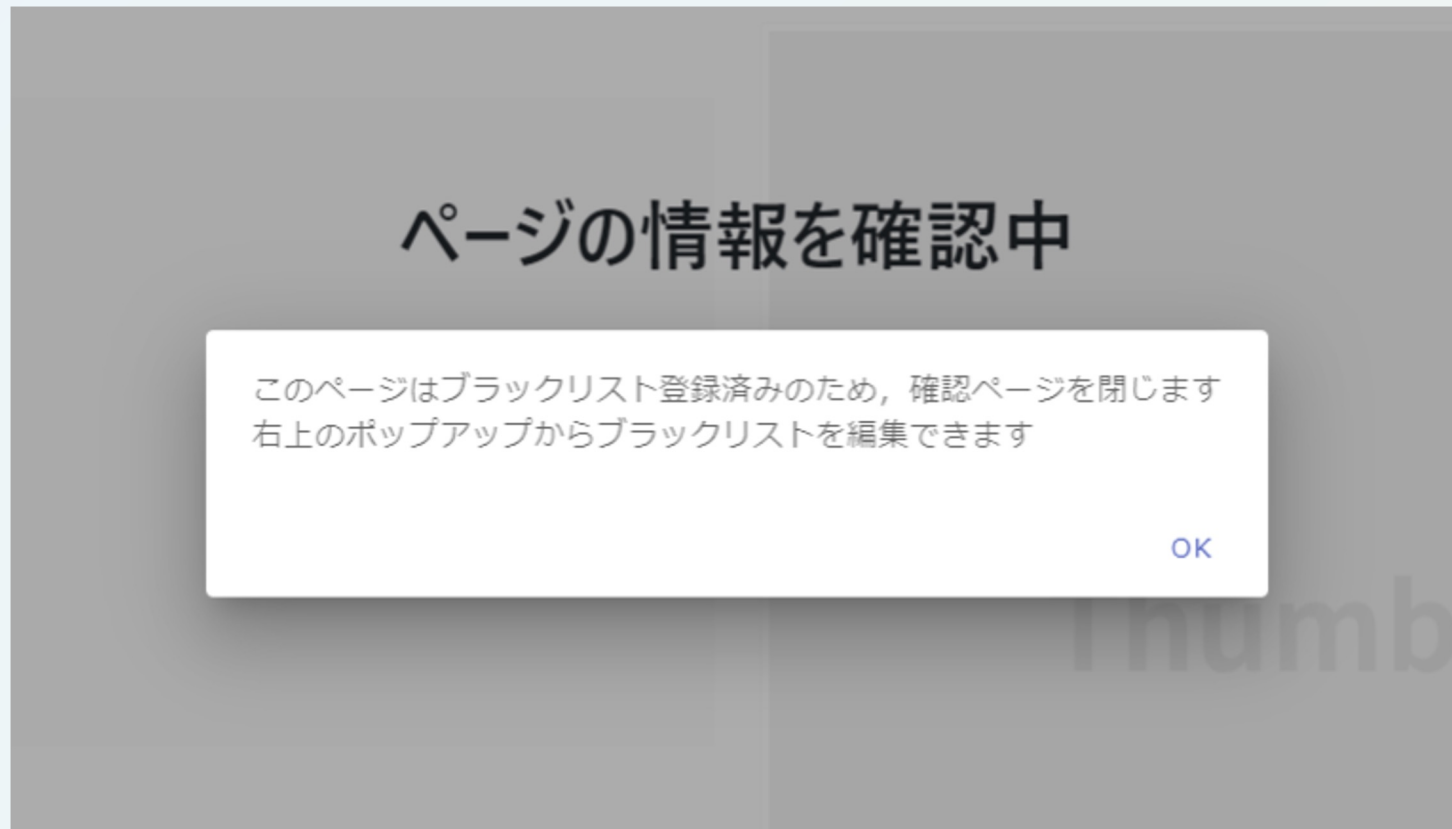
削除ボタンを押すと確認なしで削除されます

タイトル	ドメイン	削除
国立大学法人 電気通信大学	www.uec.ac.jp	
阿部寛のホームページ	abehiroshi.la.coccan.jp	
Wikipedia	ja.wikipedia.org	

ホワイトリストの確認・削除を簡単に行える！

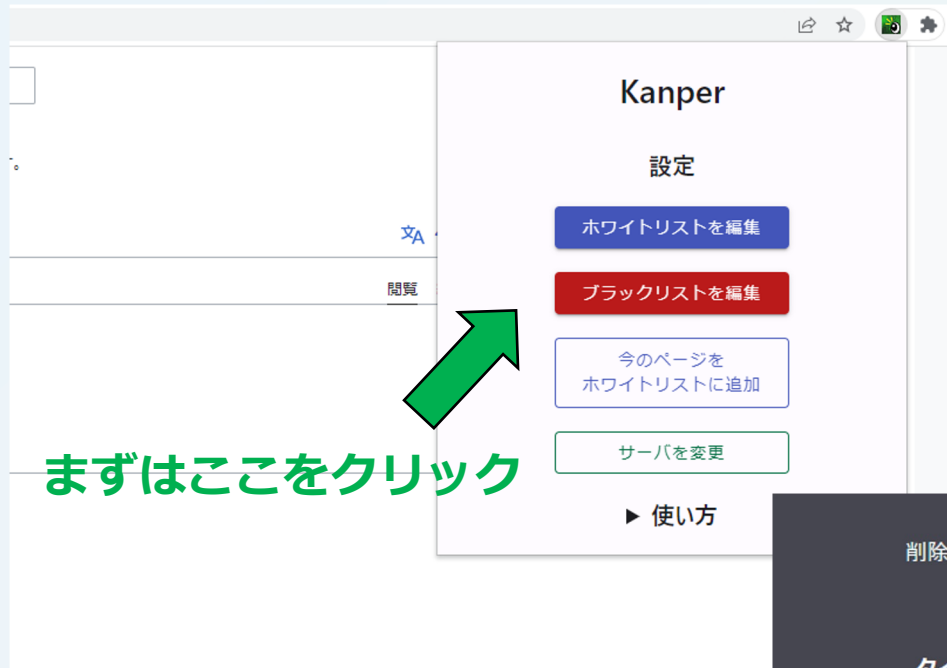
②UXのこだわり：ブラックリスト機能

- ブラックリストにURLを登録することで、確認画面で対象のURLへの遷移を防ぐことができるようになる
- 遷移先のドメインを登録するため、別の短縮URLであっても遷移を防げる

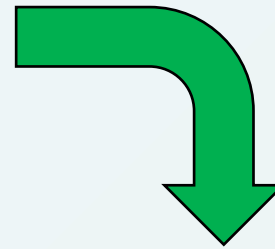


②UXのこだわり：ブラックリストの編集

編集画面で簡単に整理可能



まずはここをクリック



編集画面へ遷移

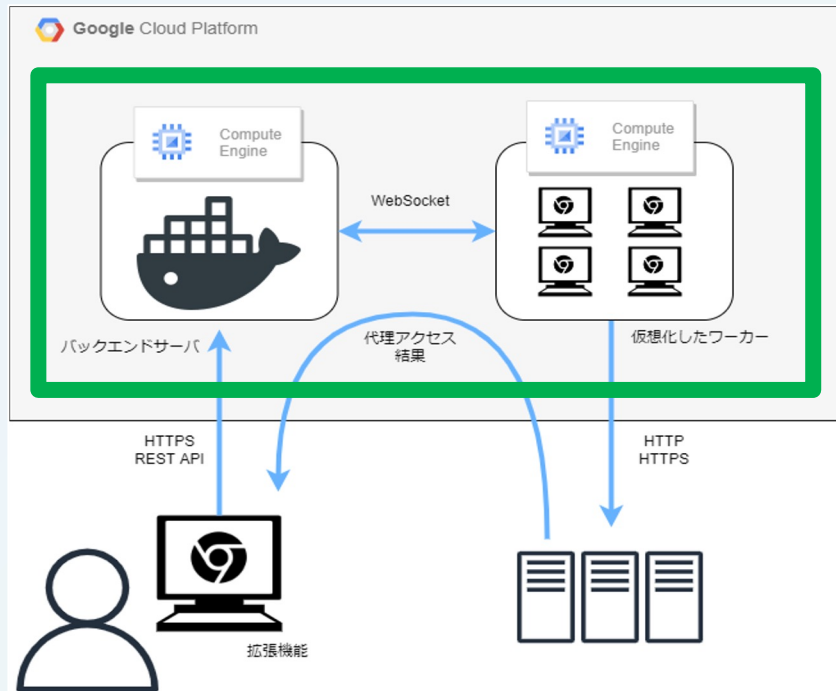


ブラックリストの確認・削除を簡単に行える！

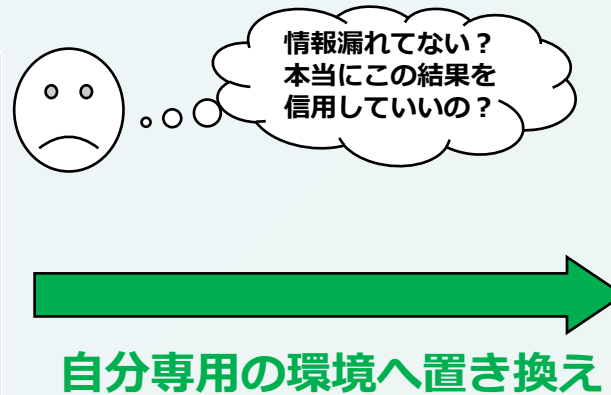
③セキュア機能：サーバの変更

プライバシーなどの懸念点：

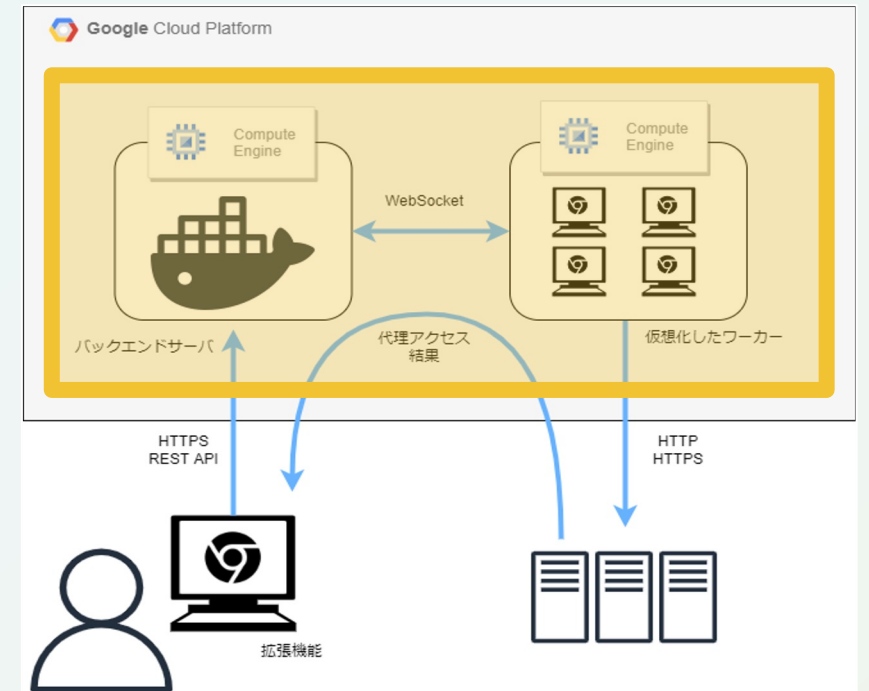
⇒自分の制御下のマシンだけで完結するようにできる



Kanperの構成図



自分専用の環境へ置き換え

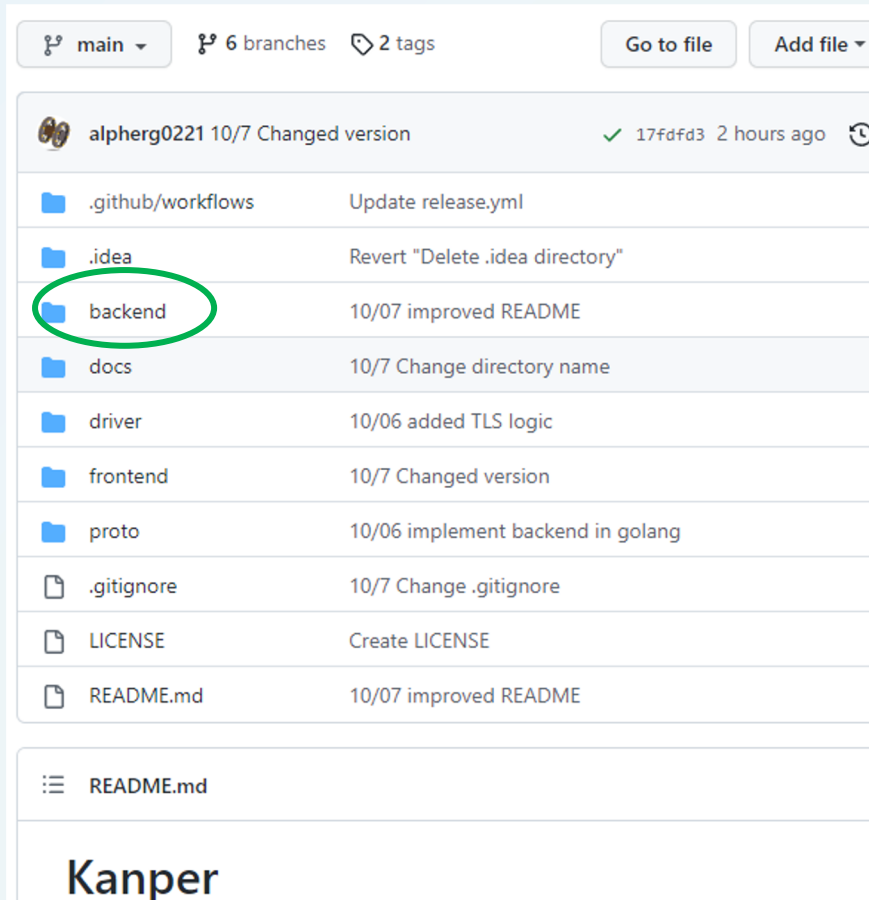


カスタマイズしたKanperの構成図

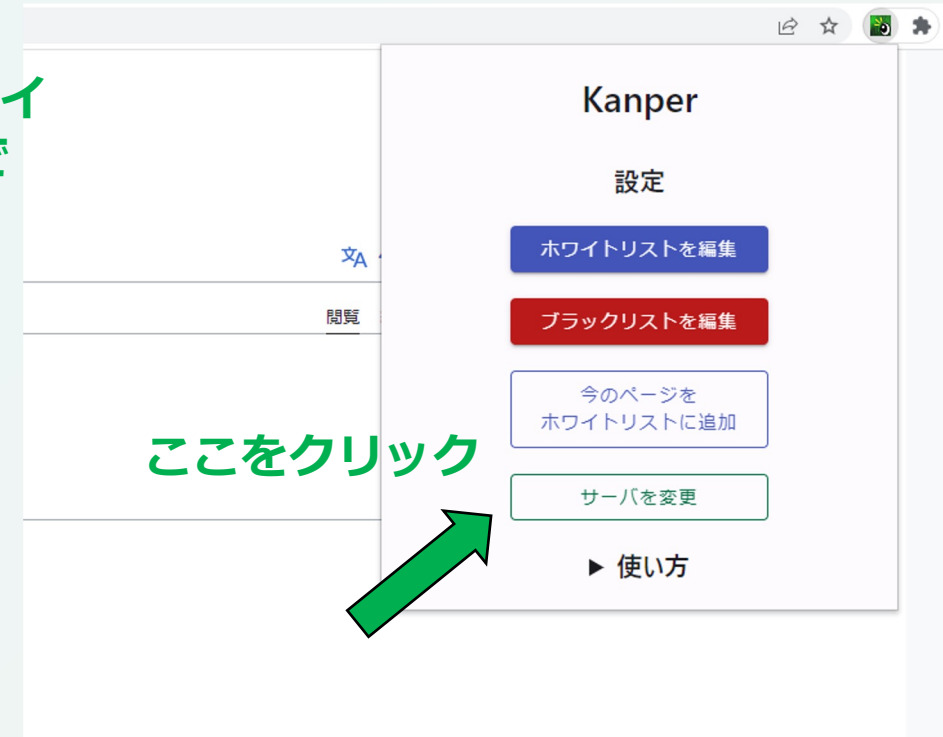
③セキュア機能：サーバの変更方法 1

すべての機能は自分の制御化のマシンで完結できる

backendを
クローン



Dockerでデプロイ
自動でSSL化まで

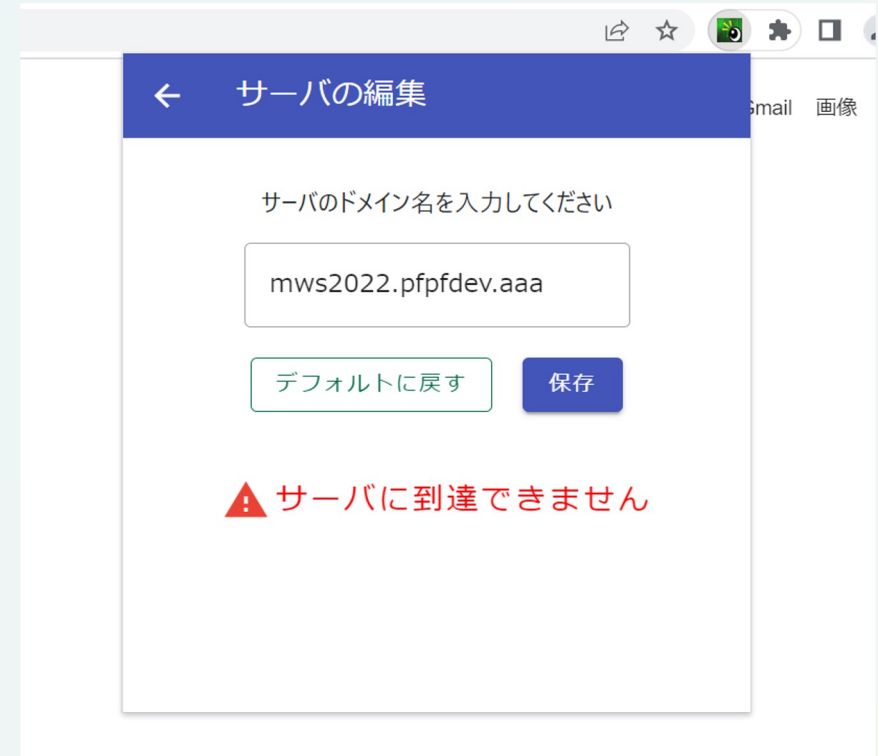


③セキュア機能：サーバの変更方法2

すべての機能は自分の制御化のマシンで完結できる



(無効な値を設定した場合)



UXに抜かりなし！

今回の成果物

- Kanper : 今回開発したツール
- ソースコード : Kanperのソースコード
- カスタムサーバ : セキュア機能を実現するツールなど
- CDパイプライン : githubにpushすると拡張機能ができあがる仕組み
- Swagger : APIのドキュメント・開発用UIページ
- README : Kanperの利用方法・改良方法をまとめた資料
- Loadmap : Kanper開発のこれまでと今後をまとめた資料
- デモページ : Kanperを体験できるページ

開発の流れ(これまで)

Phase1 初期実装

- リダイレクト検知と遷移ブロックロジックの実装
- 遷移確認ページの表示

Phase2 システム化

- サーバーの実装
- ホワइटリスト・ブラックリスト機能の実装

Phase3 UXの改善

- サーバーの改善
- ホワइटリスト・ブラックリストの編集機能の実装
- 安全性評価の表示機能の実装

開発の流れ(今後)

Phase4 追加予定の機能

- 複数端末でのホワイトリスト・ブラックリストの同期機能
- 自作HTTPクライアントの実装

Phase5 改善に向けての取り組み

- 対応する短縮URLの種類拡張
- CI/CDによるサーバ環境の効率化
- How to contributeのドキュメント整備
- サーバ運営をせずにセキュア機能を実現
 - アカウント・トークン管理
 - エンド2エンドの暗号化
 - (運用コストが嵩むので) 収益化の検討

まとめ

● 新規性

- UXを損なわないホワイトリスト・ブラックリスト機能
- アクセス情報などを完全に制御できるセキュア機能

● 実用性

- 短縮URLで隠蔽された危険なサイトへの有効的な対策
- デモページ・Releasesなど実際のユーザの導線を意識した成果物

● 継続性

- Githubなどを十二分に活用した開発支援・ドキュメント化
- ロードマップによる今後の開発計画の可視化

まとめ

● 貢献

- 短縮URL付フィッシングメールへの対策
- 短縮URLのリスクを考慮して使用を控える人に対する利用障壁を下げる

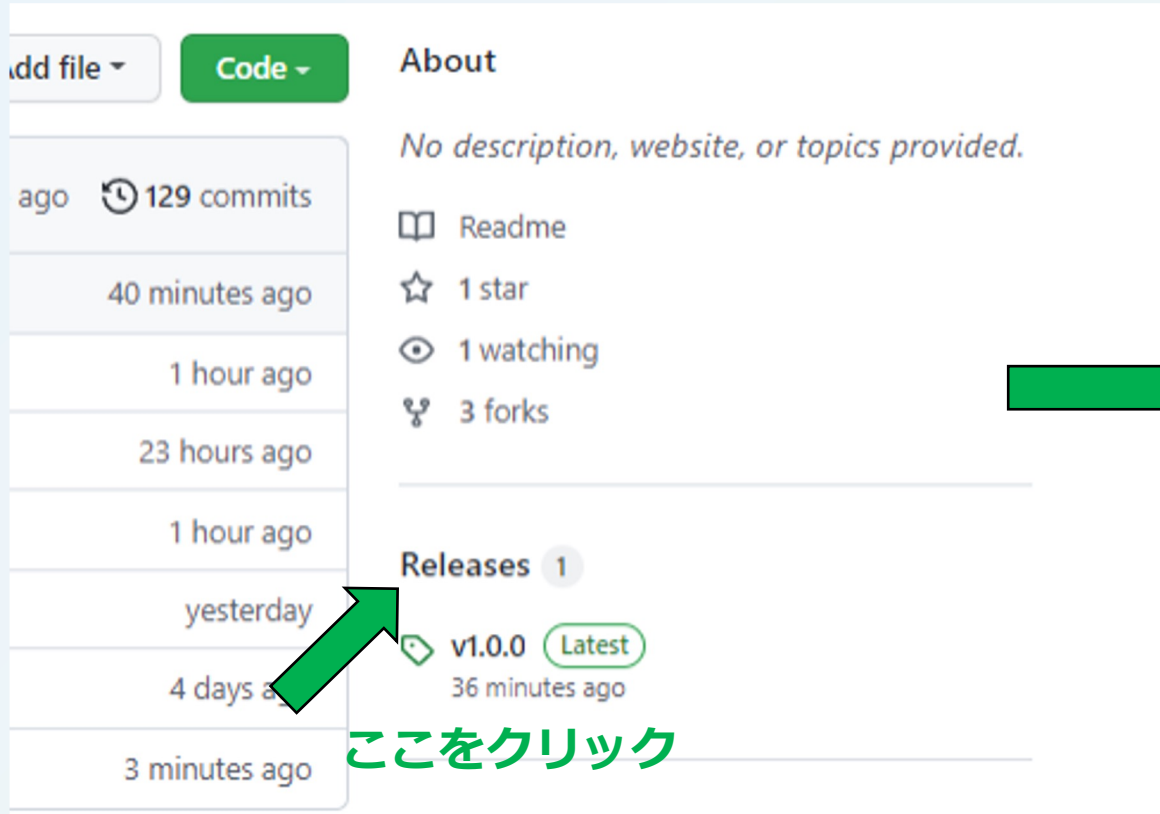
担当箇所

Github, Slack, Discord, Zoom, HackMDを活用して, 下記の分担で作業した

- 篠崎: フロントエンド, アイディアの提案
- 渡邊: フロントエンド
- 池澤: バックエンド
- 岡山: バックエンド, スライド作成, 発表
- 嶋田: バックエンド, スライド作成
- 大森: アイディアの提案, レビュー

[補足] 導入方法

GithubのReleasesからダウンロードし, chromeの拡張機能に設定



add file ▾ Code ▾ About

No description, website, or topics provided.

Readme

1 star

1 watching

3 forks

Releases 1

v1.0.0 Latest
36 minutes ago

ここをクリック



▼ Assets 3

release.zip

Source code (zip)

Source code (tar.gz)

release.zipをダウンロード

[補足] 遷移先情報の表示機能

確認画面で怪しいサイトだと判断することができる

危険なサイトであることを
サイトへの遷移前に確認できる

次のページを表示しますか？

CANCEL

OK

ホワイトリストに追加して表示

ブラックリストに追加

ページ情報

ページタイトル

【楽天】ログイン

URL

https://ntagoi-jp.wyjluug.cn/login.php

ページの説明

安全性チェック

Google透明性レポート

Norton Safe Web

Kaspersky Threat Intelligence Portal



Rakuten Card
楽天e-NAV

セキュリティ対策を怠りませんか？ 詳細はこちら

Rakuten

⚠ ユーザID使用制限 情報を確認して制限を解除してください。

- ・不明なデバイスでログインが発生したかどうか？
- ・お客様のアカウントを他人に譲渡して使用しないください。

楽天会員ログイン

ユーザID

パスワード

ログイン

- 個人情報を第三者に開示してログイン (2017年10月1日改定)
- アプリケーションを使用するときオートログインを無効にする (詳細)

ユーザID・パスワードを忘れた場合

ヘルプ

まだ楽天会員に登録されていない方

楽天会員に新規登録 (無料) して
サービスを利用する

楽天会員とは？

ログインできないときのヒント

- ・ユーザID・パスワードの入力は正しいですか？
どちらか半角英数字で入力してください。カタ入力や「CapsLock」キーの状態にご確認ください。ドットやカンマなどの記号も、よくご確認のうえ、正しく入力してください。
- ・メールアドレスは先をユーザIDにお使いの方
メールアドレスの代わりに、ご登録いただいた任意の文字列を入力してください。
- ・楽天会員登録されていますか？
まだ楽天会員登録をされていない方は、「楽天会員登録」よりご登録ください。

個人情報保護方針

© Rakuten Group, Inc.