

# プロジェクト研究A 発表資料

## ～フィッシングサイトの現状調査～

---

情報理工学科 1W202060 大西真基久

# 目次

## ～フィッシングサイトの現状調査～

---

1. 動機
2. 行ったこと
3. 調査したフィッシングサイトの紹介
4. 考察
5. 今後の展望
6. 付録

# 1. 動機

---

- ・ショートメッセージに届く怪しいURLが気になった

やまと運輸よりお荷物を発送しましたが、宛先不明です、下記よりご確認ください。  
[http://  
ikifd.yhwnv.com](http://ikifd.yhwnv.com)

お荷物の住所が不明でお預かりしております、確認してください。[http://  
yjfeb.qmecd.com](http://yjfeb.qmecd.com)



調べてみるとフィッシングや詐欺など出てきた

# 1. 動機

---

- ・フィッシングサイトとは

実在する組織を偽った偽サイトで、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった**個人情報**を詐欺するサイト

(フィッシング対策協議会より <https://www.antiphishing.jp/>)

## 2. やったこと

---

時系列順に簡単に述べると

- ・PhishTankからフィッシングサイトのURLを取得し、URLScanを利用してスクリーンショット、ドメインのIPアドレス、証明書などを

調査した(PhishTank:<https://phishtank.org> , URLScan: <https://urlscan.io>)

- ・クローリングプログラムを作成し、自動でスクリーンショット、HTMLを取得できるようにした

- ・フィッシング対策協議会のデータソースから得られたurl

のうち、クローリングしてアクセス可能と判定したサイトに実際にアクセスし、個人情報を入力してみた

### 3.調査したフィッシングサイトの紹介

---

注意 安全性を考えて調査した

- ・フィッシングサイトのデータソースはフィッシング対策協議会のものを利用した
- ・フィッシングサイトへのアクセスは研究室のサーバを利用した
- ・入力に使用したメールアドレスは捨てメアドサイト(<https://temporary-email.com> など)から利用した

# 3.調査したフィッシングサイトの紹介

---

## 調査の流れ

- ・フィッシング対策協議会のデータソースからフィッシングサイトのurlをクロールした

→フィッシングサイトのスクリーンショットとHTMLを取得した

→得られたデータはほとんど空だった(閉鎖)

→フィッシング対策協議会に報告されたサイトはすぐに閉鎖される

### 3.調査したフィッシングサイトの紹介

---

そこで、クローリングによって、まだアクセスできるサイトを探した(体感約150個のurlに対して5個程度しか生きていない)

→アクセスし、**個人情報(メールアドレス、ID、パスワードなど)**を実際に入力した

#### 注意

- ・フィッシングサイトのデータソースはフィッシング対策協議会のものを利用した
- ・フィッシングサイトへのアクセスは研究室のサーバを利用した
- ・入力に使用したメールアドレスは捨てメアドサイト(<https://temporary-email.com> など)を利用した



# 3.調査したフィッシングサイトの紹介

---

実際アクセスしたサイトのうち三種類紹介する

- BIGLOBEの偽サイト(ID, パスワードを詐欺する)

偽物 : <https://www.lycot.in//image/catalog/blog/index.php?em=example@example.or.jp>

偽物 : <https://www.shemco.net/admin/careers/index.php>

本物 : <https://auth.sso.biglobe.ne.jp/mail/>

- smbcの偽サイト(支払い情報を詐欺する)

偽物 : <https://scmcb-cradrs.juanj.cn>

本物 : <https://www.smbc-card.com/mem/index.jsp>

- 楽天の偽サイト(支払い情報を詐欺する)

偽物 : <https://rakuten-sg.shopping/users/login>

本物 : [https://grp01.id.rakuten.co.jp/rms/nid/vc?\\_\\_event=login&service\\_id=top](https://grp01.id.rakuten.co.jp/rms/nid/vc?__event=login&service_id=top)

# 3.調査したフィッシングサイトの紹介

## BIGLOBEの偽サイト

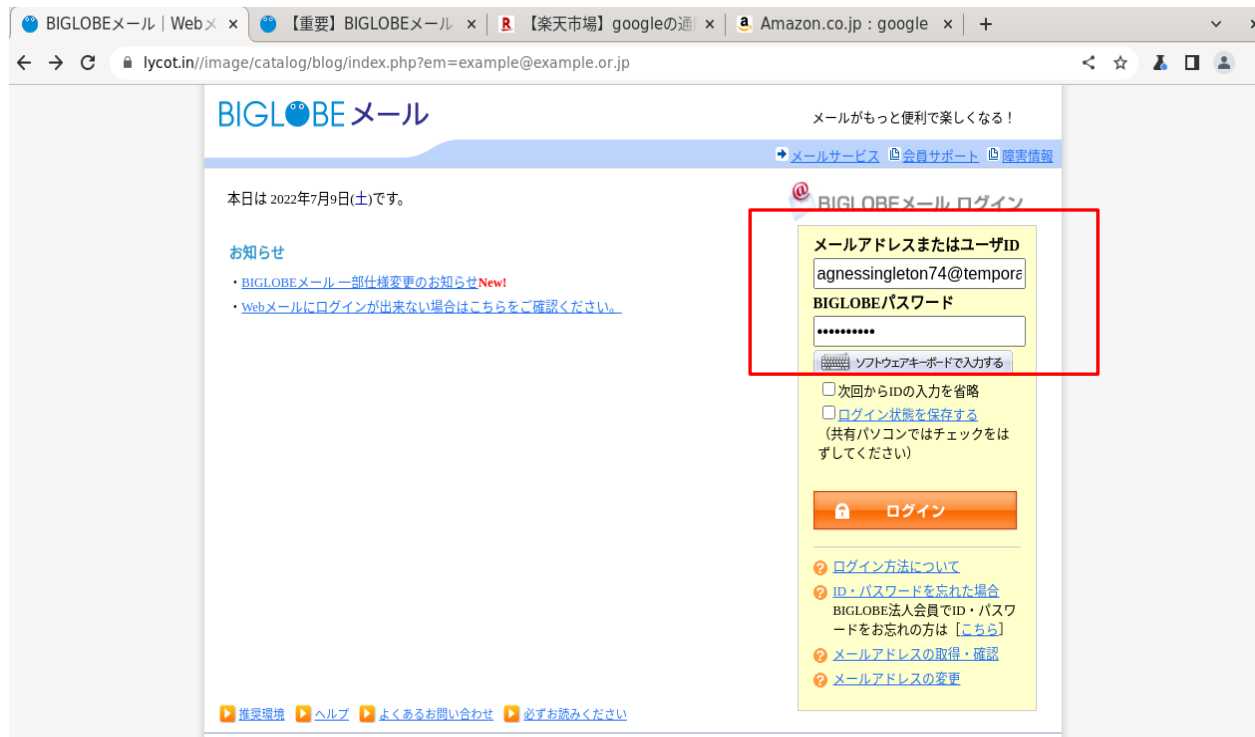


## BIGLOBEの本物のサイト



# 3.調査したフィッシングサイトの紹介

## BIGLOBEの偽サイト



捨てメアドとでたらめなパスワードを入力してみる

# 3.調査したフィッシングサイトの紹介

## BIGLOBEの偽サイト



捨てメアドとでたらめなパスワードを入力してもログインが成功した

# 3.調査したフィッシングサイトの紹介

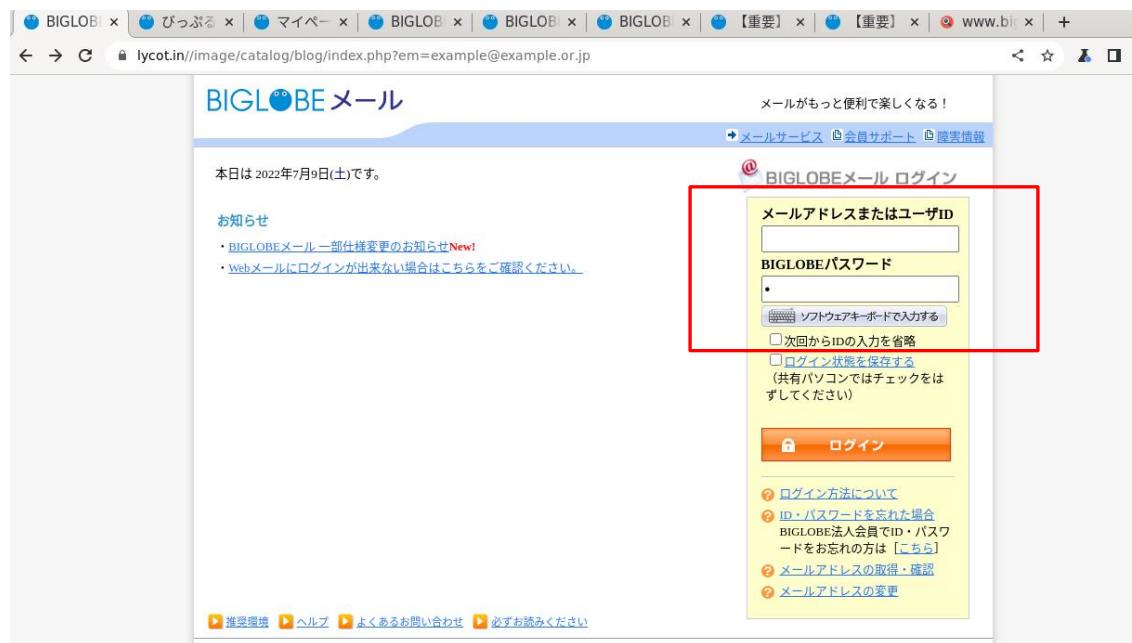
## BIGLOBEの偽サイト



実はログイン後のサイトは**本物のBIGLOBEのサイト**だった(**ログイン未完了状態**)

# 3.調査したフィッシングサイトの紹介

## BIGLOBEの偽サイト



メールアドレスを入力せずとも、パスワードを一文字でも入力するとログインできた

# 3.調査したフィッシングサイトの紹介

## BIGLOBEの偽サイト

The screenshot shows a web browser window with the address bar displaying a URL that appears to be a legitimate BIGLOBE page but is actually a phishing site. The page header says "BIGLOBE メール" and "メールがもっと便利で楽しくなる!". Below this, there are links for "メールサービス", "会員サポート", and "障害情報". The main content area includes a date notice ("本日は 2022年7月9日(土)です。"), a notice section ("お知らせ") with links to updates and login issues, and a login form titled "BIGLOBEメール ログイン". The login form has two input fields: "メールアドレスまたはユーザID" (containing "agnessingleton74@tempore") and "BIGLOBEパスワード". A red rectangle highlights the password field, which has a message "Please fill out this field." below it. Below the password field, there is a link to "ログイン方法について" and a note about saving cookies. At the bottom, there is a "ログイン" button and a list of links: "ログイン方法について", "ID・パスワードを忘れた場合", "BIGLOBE法人会員でID・パスワードをお忘れの方は【こちら】", "メールアドレスの取得・確認", and "メールアドレスの変更". The footer contains links for "推奨環境", "ヘルプ", "よくあるお問い合わせ", and "必ずお読みください".

メールアドレスを入力してもパスワードを入力しなければログインはできない

### 3.調査したフィッシングサイトの紹介

---

#### BIGLOBEの偽サイト

- ・HTMLは**大部分が本物のサイトをコピー**して作られたもの
  - ・他のBIGLOBEの偽サイトのHTMLと比較すると、ログインに使用するinputタグのvalue属性が異なるだけだった
- フィッシングサイト作成ツールで作成された可能性がある



### 3.調査したフィッシングサイトの紹介

---

#### BIGLOBEの偽サイト

- ・ログイン完了後は本物のサイトへ移動する
  - ・カード情報の入力画面は一切なかった
- ログイン情報を盗むことが目的
- ・入力したメールアドレスに怪しいメールが届くことはなかった

# 3.調査したフィッシングサイトの紹介

## smbcの偽サイト



## smbcの本物のサイト



# 3.調査したフィッシングサイトの紹介

## smbcの偽サイト

The screenshot shows a web browser window with a URL that appears to be a legitimate SMBC login page but is actually a phishing site. The page features the SMBC logo and navigation links. The main content area is titled 'Vpassログイン' (Vpass Login). It contains two input fields: 'ID' with the value 'aaa' and 'パスワード' (Password) with masked characters. To the right of these fields are links for '初めてご利用の方' (First-time users), 'Vpassにご登録（無料）' (Register for Vpass (free)), and 'Vpassとは？' (What is Vpass?). Below the input fields is a CAPTCHA puzzle with the instruction: '左のピースを右の画像に移動させて、パズルを完成させてください。' (Move the pieces on the left to the image on the right to complete the puzzle). A 'ログイン' (Login) button is positioned below the puzzle. At the bottom, there is a '重要なお知らせ' (Important notice) section dated 2022年06月20日, mentioning a notice about SMS usage.

でたらめなIDとパスワードを入力すると

# 3.調査したフィッシングサイトの紹介

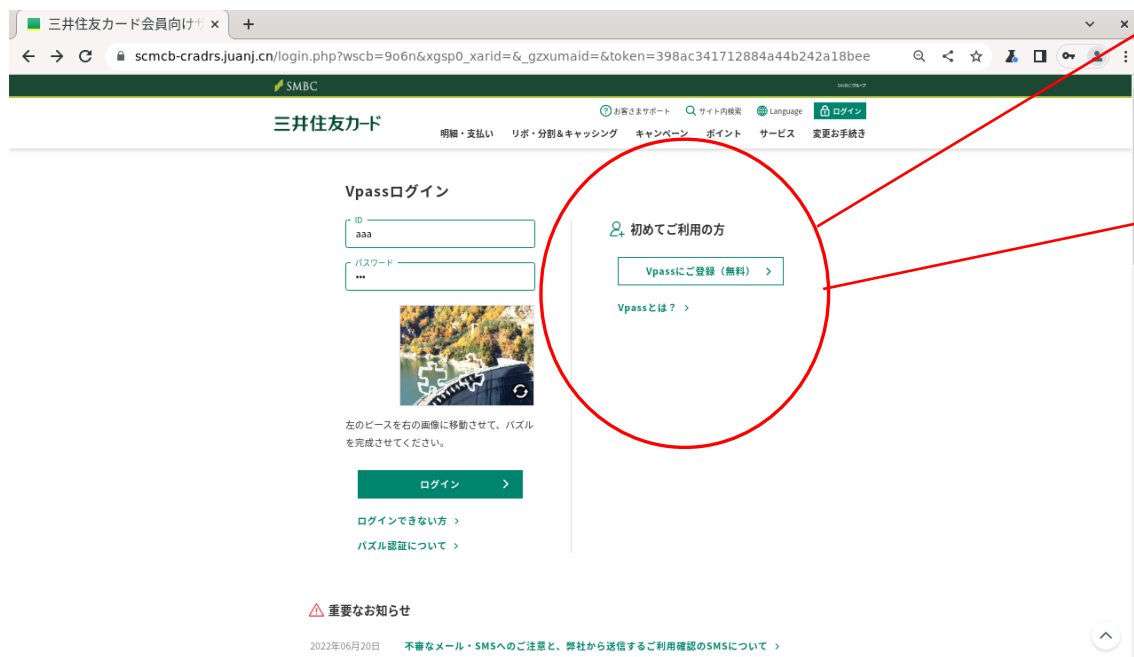
## smbcの偽サイト

The screenshot shows a web browser window with a URL that appears to be a legitimate SMBC site but is actually a phishing site. The page has a green header with the SMBC logo and the text '三井住友カード' (Sanwa Card). Below the header, there is a navigation bar with links like 'お客さまサポート' (Customer Support), 'サイト内検索' (Site Search), 'Translated Page', '会員情報' (Member Information), and 'ログアウト' (Logout). The main content area is titled 'カードご登録内容の照会' (Check Card Registration Information). Below this title, there is a section for '現在操作中のカードについて' (About the card currently being processed), followed by a 'ご注意' (Notice) section with several bullet points. The main form area contains fields for '会員番号' (Card Number) and 'カード有効期限' (Card Validity Period). The '会員番号' field is a 16-digit number, and the 'カード有効期限' field is a date (month/year). There are also small images of credit cards and a '資料請求' (Request for Materials) link.

ログインが完了し、**カード情報**の入力画面へ

# 3.調査したフィッシングサイトの紹介

## smbcの偽サイト



初めてご利用の方

Vpassにご登録（無料）

Vpassとは？

これを押すとどうなるか

# 3.調査したフィッシングサイトの紹介

## smbcの偽サイト

カード情報の入力画面へ移動した(ログイン後の画面と同じ)

# 3.調査したフィッシングサイトの紹介

## smbcの**本物**のサイトで

SMBCグループ

三井住友カード

明細・支払い リボ・分割&キャッシング キャンペーン ポイント サービス 変更手続き

② お客様サポート 🔍 サイト内検索 🌐 Language 🏠 ログイン

### Vpassログイン

ID

パスワード

左のピースを右の画像に移動させて、パズルを完成させてください。

ログイン >

ログインできない方 >

パズル認証について >

👤 初めてご利用の方

Vpassにご登録（無料） >

Vpassとは？ >

これを押すとどうなるか

### 3.調査したフィッシングサイトの紹介

smbcの**本物**のサイトでは、**すぐにカード情報の入力を求められることはない**



ご登録のお手続き





### 3.調査したフィッシングサイトの紹介

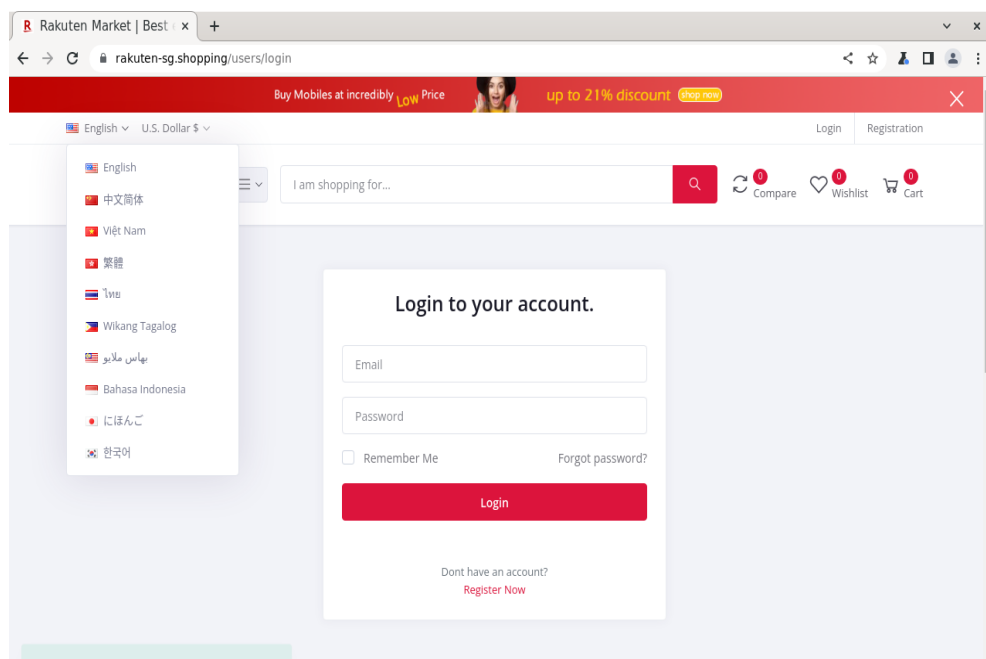
---

#### smbcの偽サイト

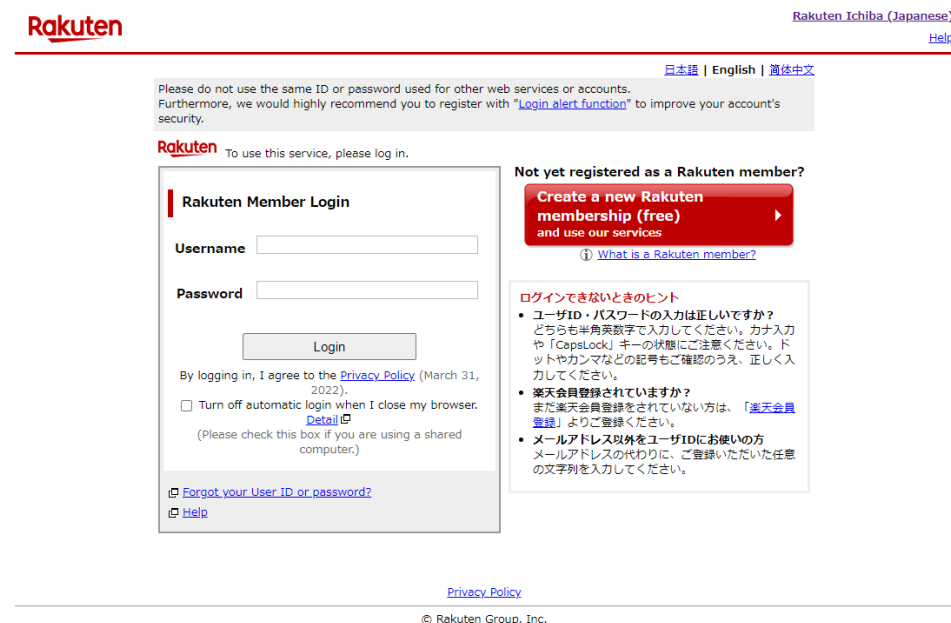
- ・HTMLは**大部分が本物のサイトのコピー**であった
  - トラッカーを消していたり、「Vpassに登録」を押すと飛ぶリンクがログイン完了後の画面と一致していた
  - カード情報を盗むことが目的**

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト(英語)



## 楽天の本物のサイト(英語)



# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト(日本語) 楽天の本物のサイト(日本語)

Rakuten Market | Best

rakuten-sg.shopping/users/login

Buy Mobiles at incredibly **Low** Price up to 21% discount [shop now](#)

にほんご U.S. Dollar \$ ログイン 登録

Rakuten 私はいくつかの... 比較する ウィッシュリスト カート

あなたのアカウントにログイン。

Eメール

パスワード

☒ 私を覚えてますか パスワードをお忘れですか?

ログイン

アカウントをお持ちではありませんか? [今すぐ登録](#)

Rakuten 楽天市場

日本語 | English | 简体中文

セキュリティ対策を見直しませんか? [詳細はこちら](#)

Rakuten このサービスをご利用になるにはログインしてください。

楽天会員ログイン

ユーザーID <半角英数字>

パスワード <半角英数字>

ログイン

個人情報保護方針に同意してログイン (2022年3月31日改定)  
☐ ブラウザを開くときオートログインを無効にする [詳細](#)  
(共有のコンピュータをお使いの方は選択してください)

[ユーザー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

[① 楽天会員とは?](#)

ログインできないときのヒント

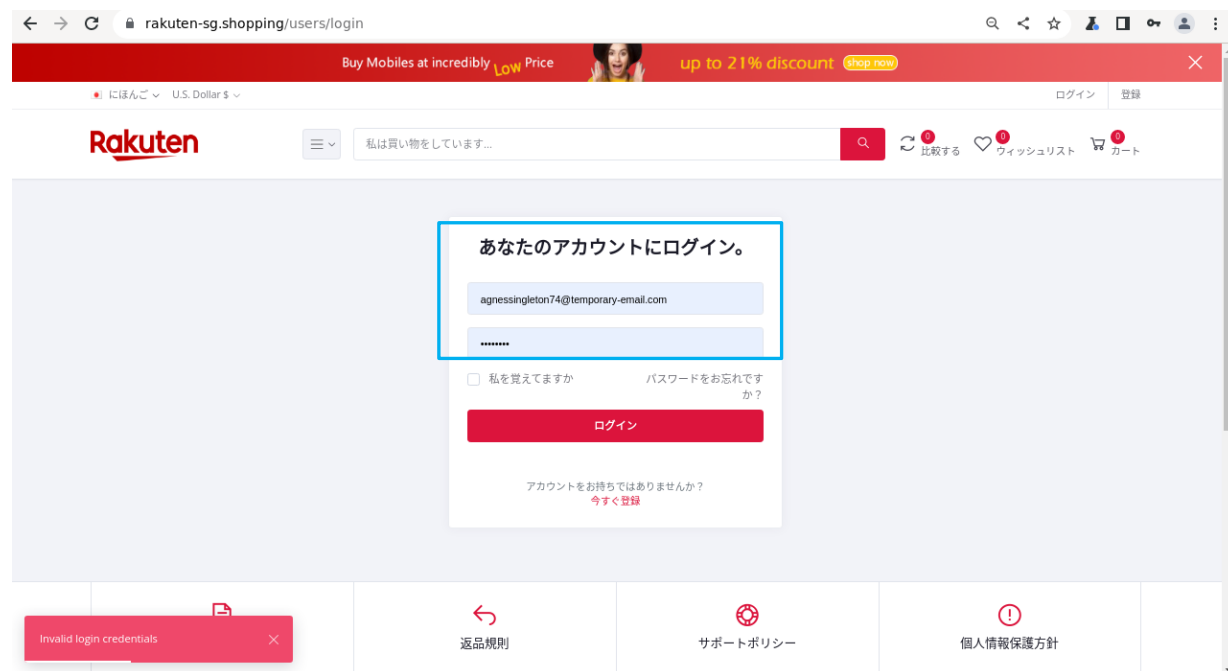
- ユーザーID・パスワードの入力は正しいですか?  
どちらも半角英数字で入力してください。カナ入力や「CapsLock」キーの状態にご注意ください。ドットやカンマなどの記号もご確認のうえ、正しく入力してください。
- 楽天会員登録されていますか?  
まだ楽天会員登録をされていない方は、「[楽天会員登録](#)」よりご登録ください。
- メールアドレス以外をユーザーIDにお使いの方  
メールアドレスの代わりに、ご登録いただいた任意の文字列を入力してください。

個人情報保護方針

© Rakuten Group, Inc.

# 3.調査したフィッシングサイトの紹介

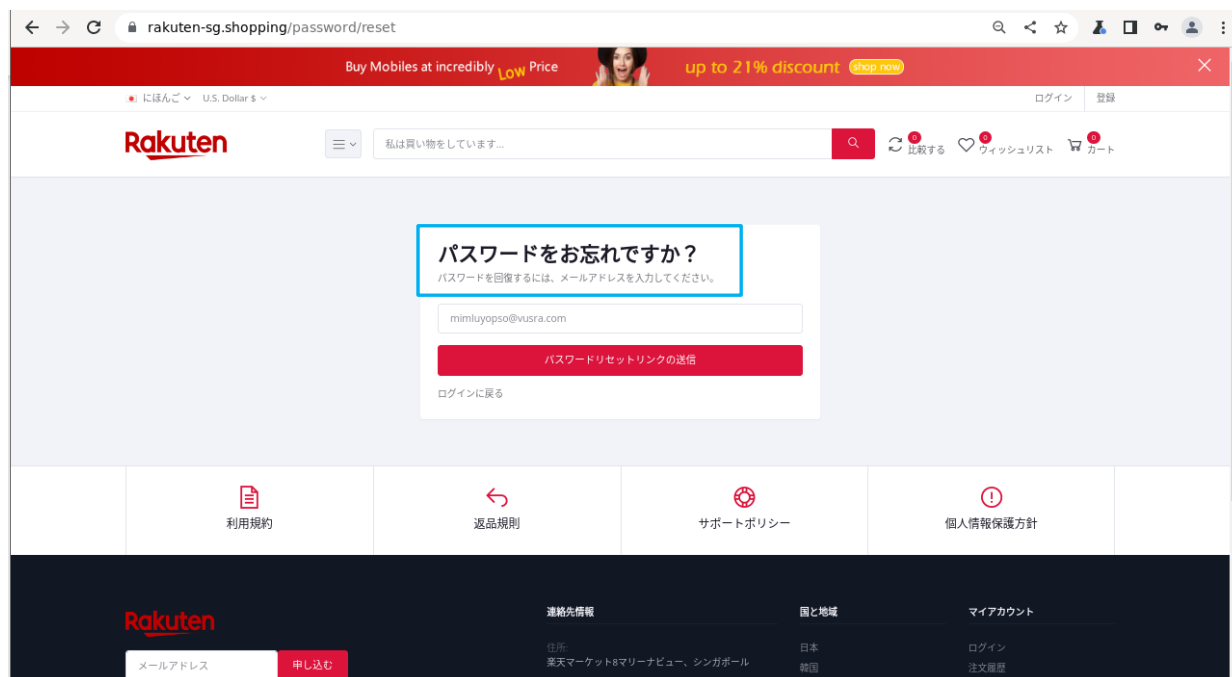
## 楽天の偽サイト



捨てメアドとでたらめなパスワードでは  
ログインできなかった

# 3.調査したフィッシングサイトの紹介

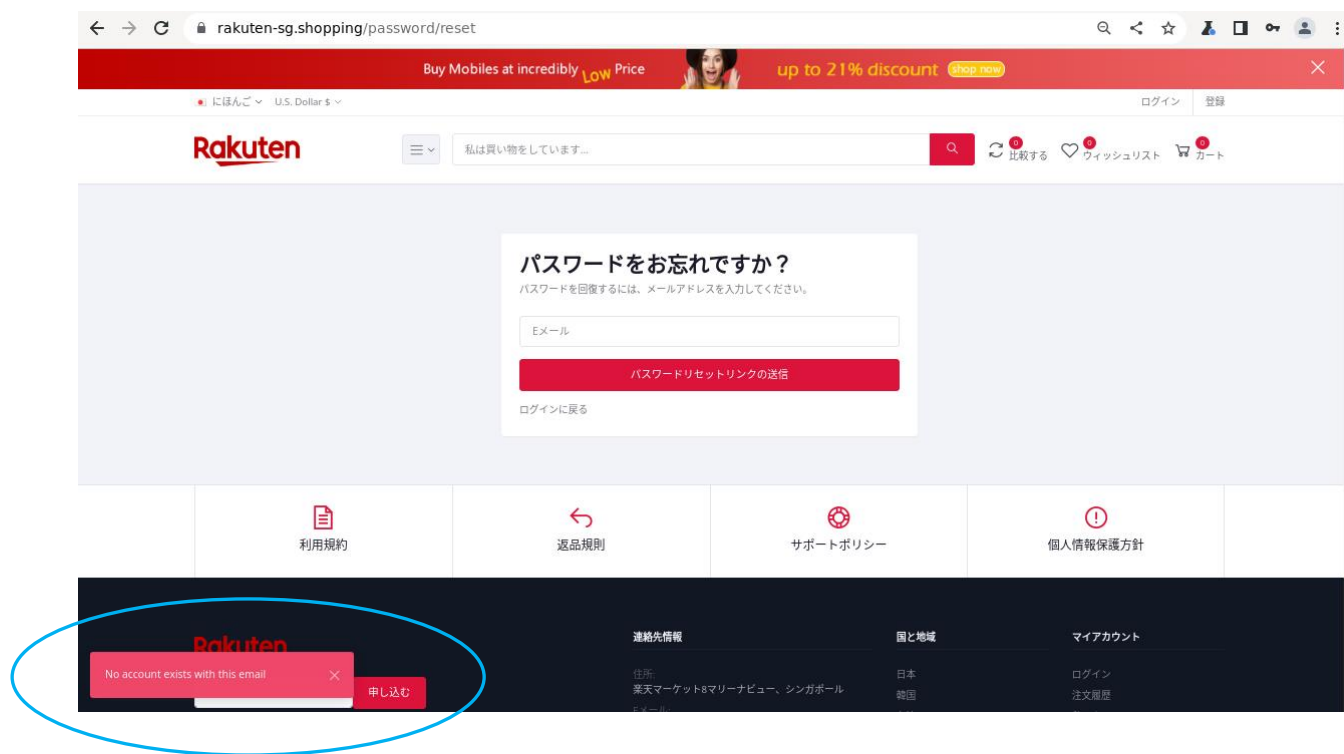
## 楽天の偽サイト



登録していないメールアドレスを入力して  
パスワードの再設定を行おうとすると

# 3.調査したフィッシングサイトの紹介

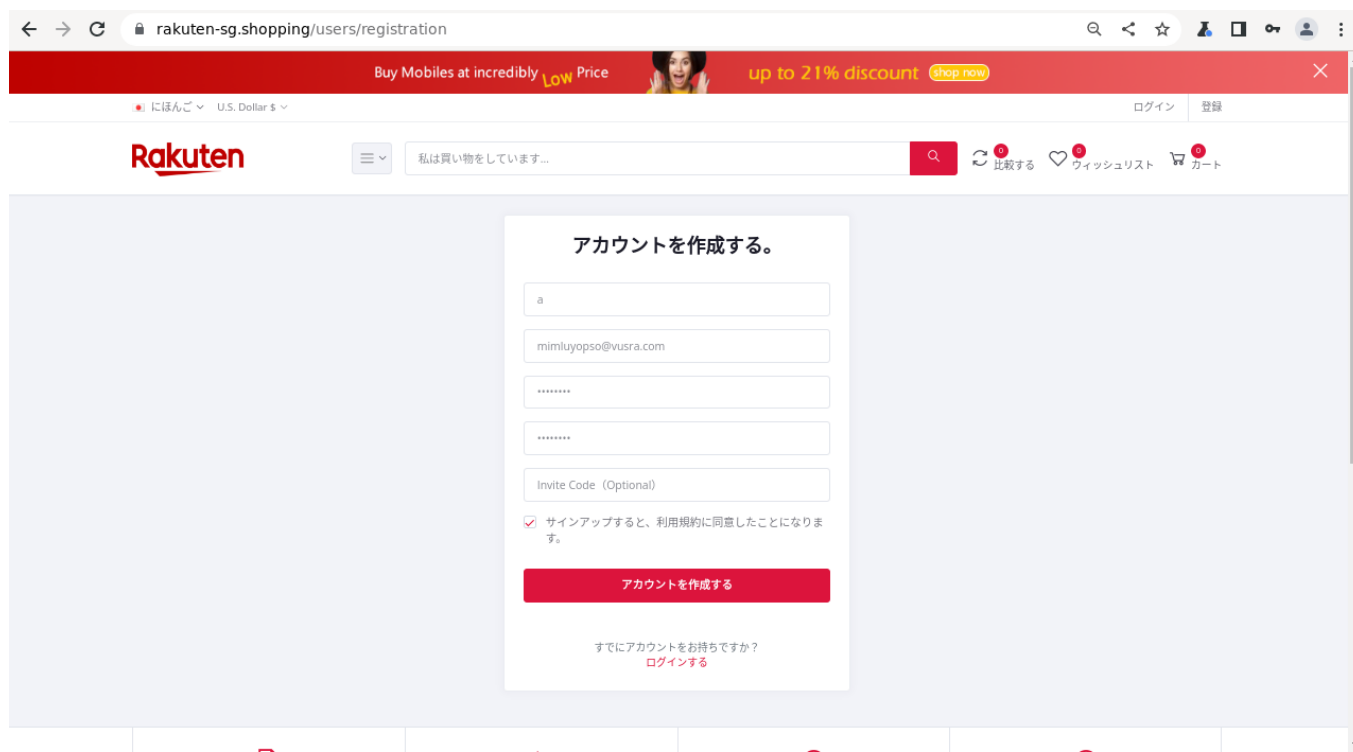
## 楽天の偽サイト



メールアドレスに対応するアカウントが存在しない旨のメッセージが表示される

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト

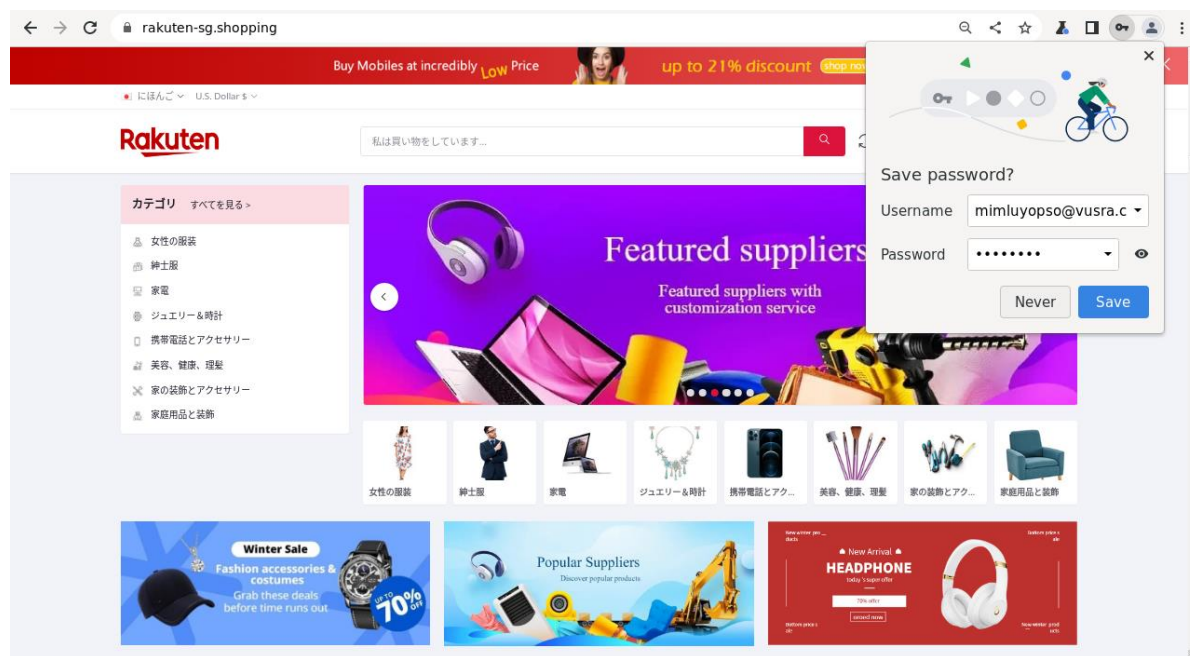


The screenshot shows a web browser window with the URL `rakuten-sg.shopping/users/registration`. The page has a red header with the text "Buy Mobiles at incredibly Low Price" and "up to 21% discount" with a "shop now" button. Below the header, there is a navigation bar with the Rakuten logo, a search bar, and links for "ログイン" (Login) and "登録" (Registration). The main content area is a light blue box containing a registration form titled "アカウントを作成する。" (Create an account). The form has fields for a username (containing "a"), an email address (containing "mimiluyopso@vusra.com"), a password (masked with "\*\*\*\*\*"), and a confirm password field (masked with "\*\*\*\*\*"). There is also an "Invite Code (Optional)" field. Below the fields, there is a checkbox labeled "サインアップすると、利用規約に同意したことになります。" (By signing up, you agree to the terms of use.) which is checked. At the bottom of the form is a red button labeled "アカウントを作成する" (Create account). Below the button, there is a link "すでにアカウントをお持ちですか？ ログインする" (Already have an account? Login).

アカウントを作成してみると

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト



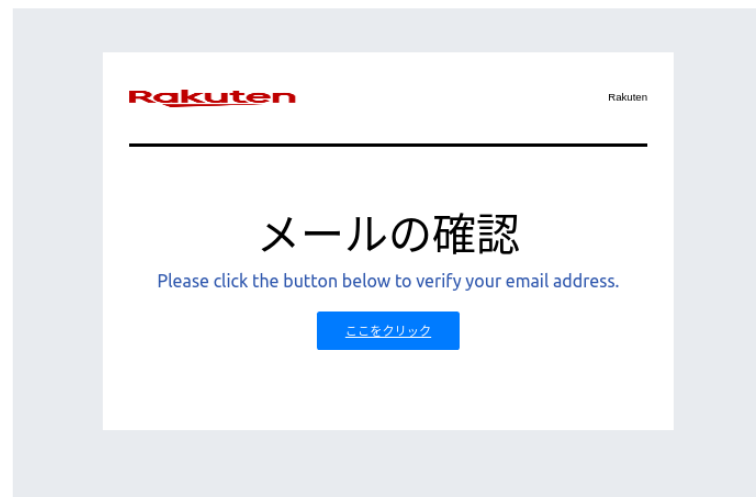
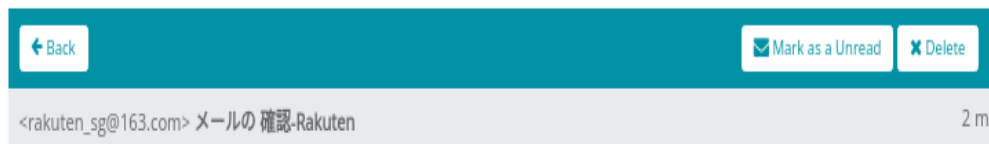
SENDER	SUBJECT	TIME
 rakuten_sg@163.com	メールの 確認-Rakuten	18 s

メールが届いた

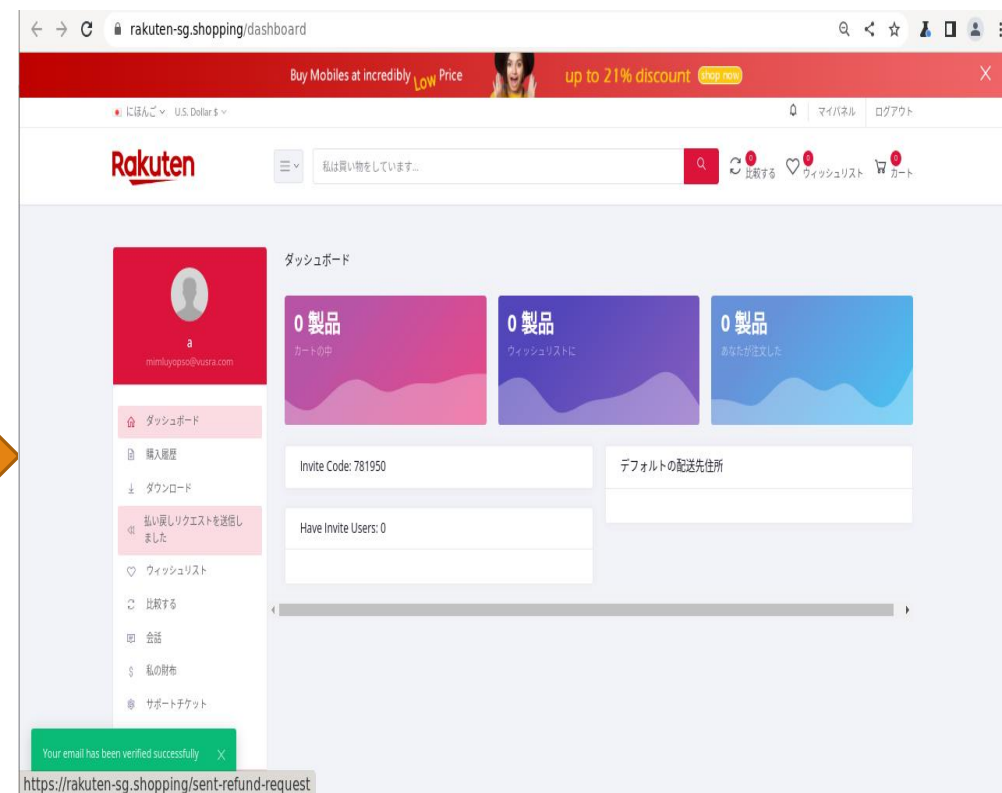


# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト



クリックすると



### 3.調査したフィッシングサイトの紹介

---

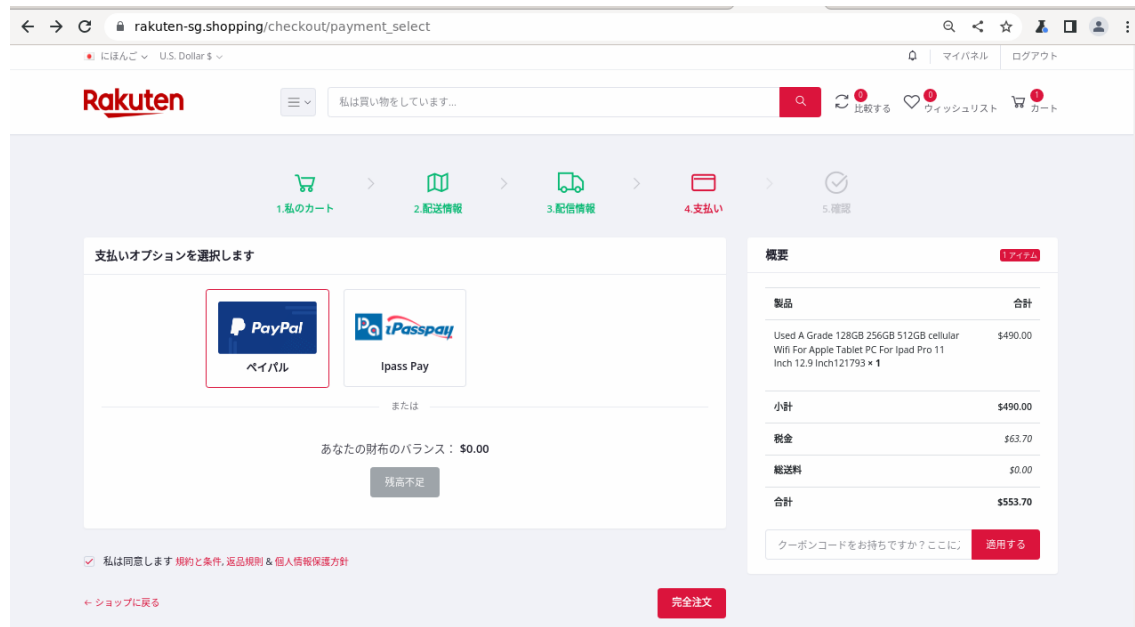
#### 楽天の偽サイト

- ・本物の楽天のサイトとは見た目が大きく異なる
  - 本物のサイトをコピーせず**に攻撃者が作っている
  - E-mail、パスワードを盗むだけならコピーしてログインさせればよい
  - カード情報**を盗むのが目的？

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト

- ・実際に商品の注文画面へ進んでみた



支払い方法は  
**PayPal**と**IPasPay(クレジット決済)**  
が選択できる

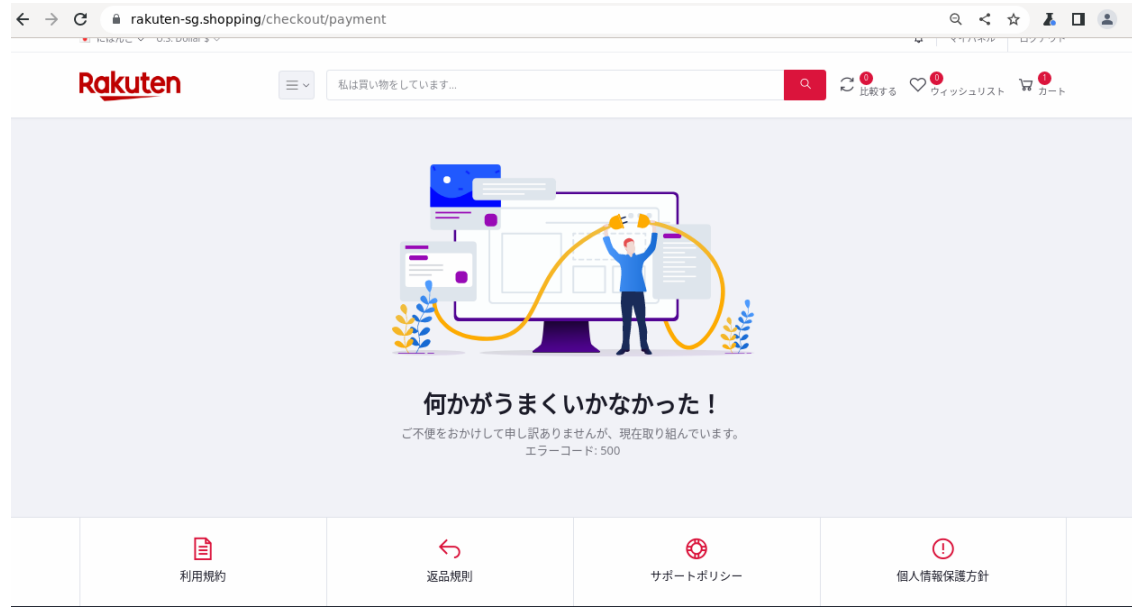


しかし実際には**PayPal**は使用  
できなかった

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト

- ・実際に商品の注文画面へ進んでみた

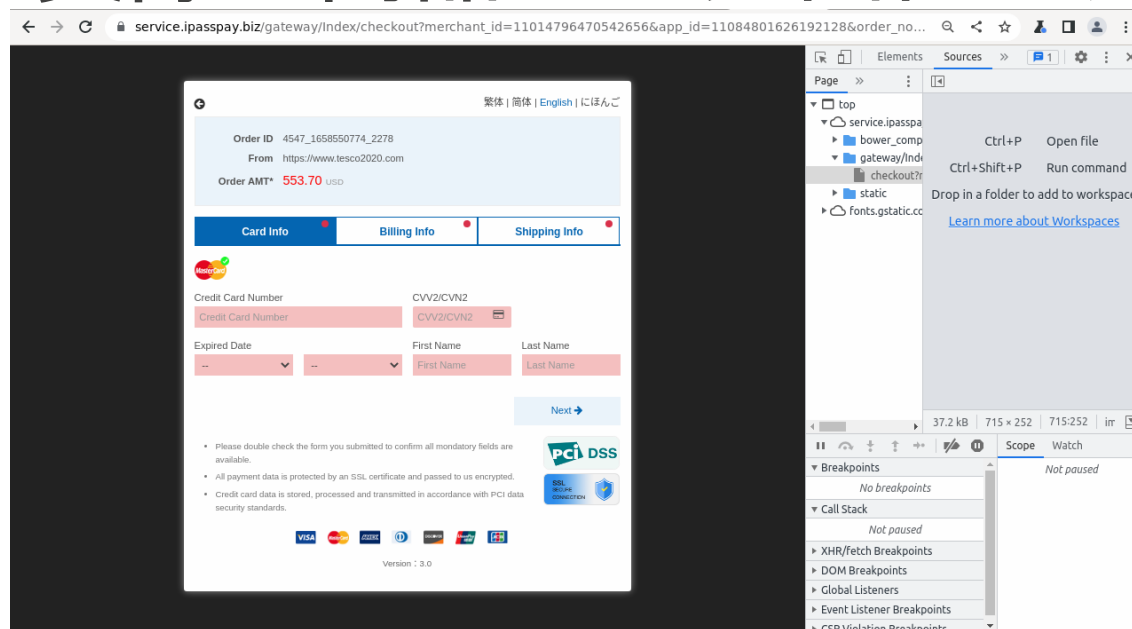


**PayPal**を選択すると何度試しても  
この画面が表示される

# 3.調査したフィッシングサイトの紹介

## 楽天の偽サイト

- ・実際に商品の注文画面へ進んでみた



一方、IpassPay(クレジット決済)は選択できた



カード情報を盗むのが目的

## 4. 考察

---

スクリーンショットおよびアクセスして分かったこと

- ・ほとんどのフィッシングサイトは本物と見た目がそっくりだった

- ・フィッシングサイトによって目的が異なっていた

→**ログイン情報**を盗みたい、**カード情報**を盗みたいなど

- ・使用したメールアドレス(捨てアド)にメールが届くことはなかった  
(楽天の会員登録を除く)

## 4. 考察

---

HTMLからわかったこと

- ・フィッシングサイトによって作り方がさまざまであった

→ 大部分を本物のサイトからコピーしているものやそうでないもの

→ コピーするものは作成ツールを使用したのかも

→ BIGLOBEの偽サイト二つのHTMLを比較すると違いはログインに使用するinputタグのvalue属性が異なるだけだった

- ・コピーして作ったものではトラッカーが消されていた

→ 本物のサイトに知られたくないから

## 4. 考察

---

HTMLからフィッシングサイトを検出できるのか

→HTMLのみを利用してフィッシングサイトを検出するのは難しそう

フィッシングサイトのHTMLについてわかっていること

- ・大部分を本物のサイトからコピーする
- ・個人情報を入力するページやリンクを書き換えている
- ・トラッカーの部分を消している

→本物のサイトと偽物のサイトとではコピーされている部分が多い

→HTMLを比較し、同じ部分が多いあればフィッシングサイトである可能性が高い



## 4. 考察

---

ドメイン名とHTMLを組み合わせて考えるのはどうか？

→ 代表的な組織のドメイン名をあらかじめ記憶する。検知したいサイトのドメインと類似するドメインがあれば、それらのHTML同士を比較する

→ コピーされている部分が多く見つければ、検知中のサイトはフィッシングサイトである可能性が高いと判定できる

だが、そもそも類似するドメインの時点で怪しいのでは？

それにフィッシングサイトの中にはドメインを本物のドメインに似せていないものもあるため、それらの検出はできない

## 5. 今後の展望

---

フィッシングサイトを検知するための具体的な手法を模索したい

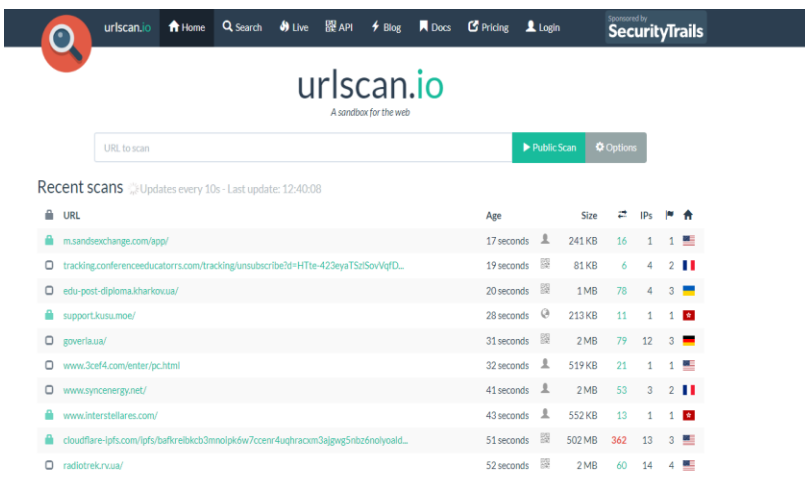
→そのためにより多くのフィッシングサイトを調べたい

→HTMLの観点だけでなく、URLの観点からも考えたい

ご清聴ありがとうございました

# 6.付録

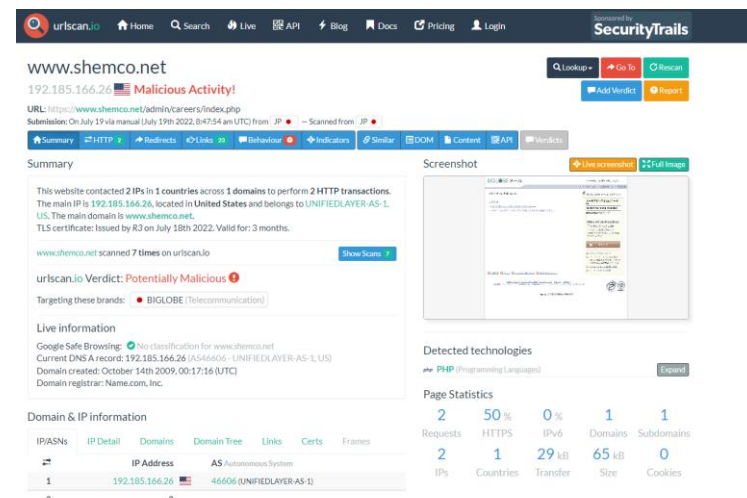
URLScan: <https://urlscan.io>



The screenshot shows the URLScan.io homepage. At the top is a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. Below the navigation bar is the URLScan.io logo and a search bar. A "Public Scan" button is visible. Below the search bar is a table of recent scans.

URL	Age	Size	IPs	Flags
ms.sandvexchange.com/app/	17 seconds	241 KB	16	1
tracking.conferenceeducators.com/tracking/unsubscribe?Ht=423eyaTSotSovVifD...	19 seconds	81 KB	6	4
edu-post-diploma.kharkov.ua/	20 seconds	1 MB	78	4
support.kusu.moe/	28 seconds	213 KB	11	1
govveria.ua/	31 seconds	2 MB	79	12
www.3cef4.com/enter/pc.html	32 seconds	519 KB	21	1
www.syncenergy.net/	41 seconds	2 MB	53	3
www.interstellares.com/	43 seconds	552 KB	13	1
cloudflare-lpts.com/lpts/bafkrelibkcb3mmolpkdw7ccent4ughracxm3ajgw5nibz6nolyoald...	51 seconds	502 MB	362	13
radiotrek.ru/va/	52 seconds	2 MB	60	14

Scan



The screenshot shows the URLScan.io scan results page for the URL <https://www.shemco.net>. The page displays a summary of the scan, including the URL, the main IP (192.185.166.26), and the detected technologies (PHP). The scan results show that the website contacted 2 IPs in 1 country across 1 domain to perform 2 HTTP transactions. The main IP is 192.185.166.26, located in the United States and belongs to UNIFIEDLAYER-AS-1, US. The main domain is www.shemco.net. The TLS certificate is issued by R3 on July 18th 2022, valid for 3 months. The scan results also show that the website is targeted by BIGLOBE (Telecommunications). The page statistics show 2 requests, 50% HTTPS, 0% IPv6, 1 domain, and 1 subdomain. The page size is 65 kB and there are 0 cookies.