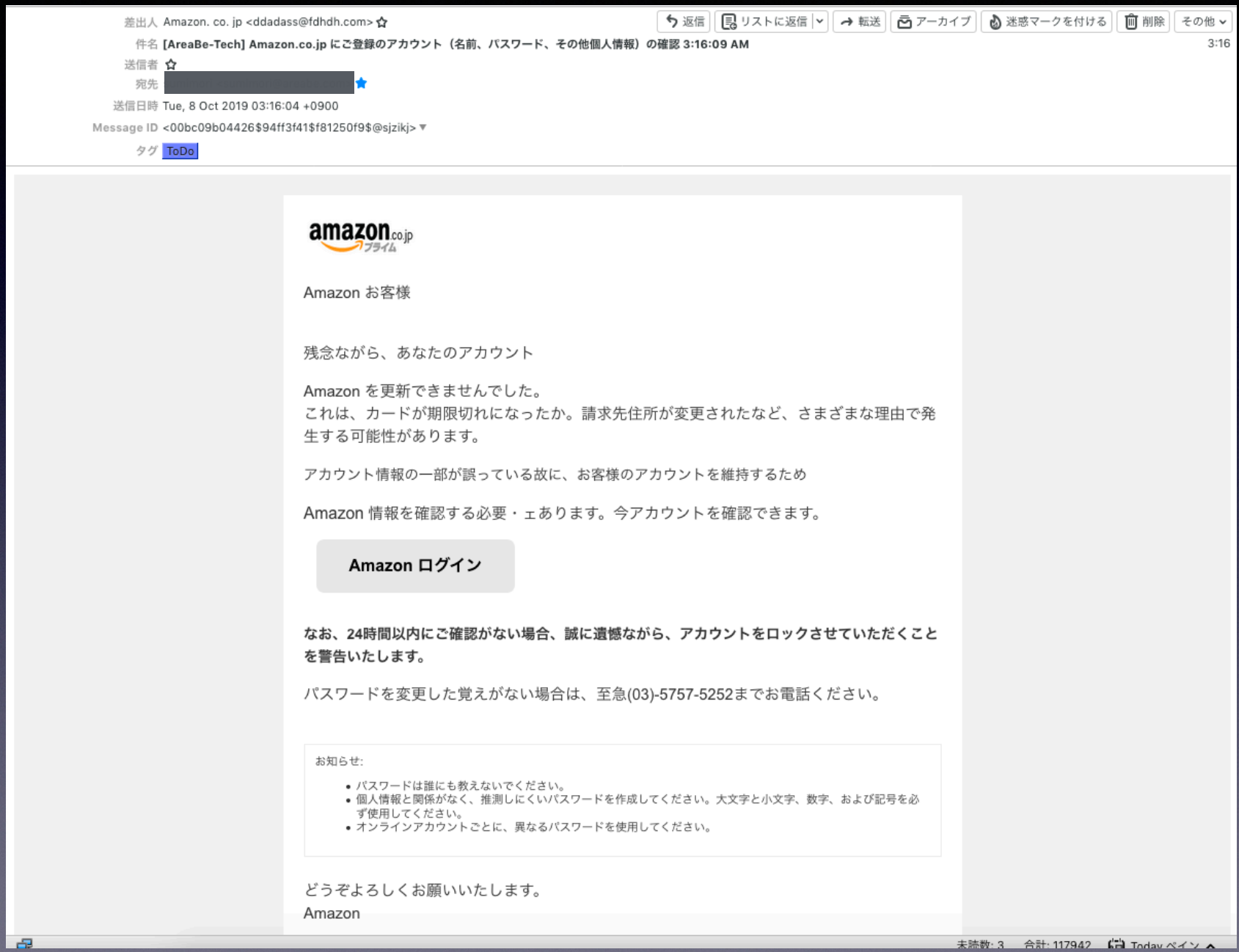
フィッシングの手口を探る

エリアビイジャパン 株式会社
情報処理安全確保支援士
池田貴志

第000074号

ある日こんなメールが届いた



差出人 Amazon. co. jp <ddadass@fdhdh.com>
返信 | リストに返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除 | その他
件名 [AreaBe-Tech] Amazon.co.jp にご登録のアカウント（名前、パスワード、その他個人情報）の確認 3:16:09 AM
3:16
送信者
宛先 [redacted]
送信日時 Tue, 8 Oct 2019 03:16:04 +0900
Message ID <00bc09b04426$94ff3f41$f81250f9$@sjzikj>
タグ ToDo

amazon.co.jp プライム

Amazon お客様

残念ながら、あなたのアカウント

Amazon を更新できませんでした。
これは、カードが期限切れになったか。請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため

Amazon 情報を確認する必要・ェあります。今アカウントを確認できます。

Amazon ログイン

なお、24時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただくことを警告いたします。

パスワードを変更した覚えがない場合は、至急(03)-5757-5252までお電話ください。

お知らせ:

- パスワードは誰にも教えないでください。
- 個人情報と関係がなく、推測しにくいパスワードを作成してください。大文字と小文字、数字、および記号を必ず使用してください。
- オンラインアカウントごとに、異なるパスワードを使用してください。

どうぞよろしくお願いいたします。
Amazon

未読数: 3　合計: 117942　Today ペイン

受信 | 作成 | チャット | アドレス帳 | タグ | クイックフィルター | 検索 <⌘K>

返信 | 全員に返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除 | その他

差出人 Amazon. co. jp <vebikn423@fjnrtfhbdgv.com>

件名 Amazon.co.jp にご登録のアカウント（名前、パスワード、その他個人情報）の確認 7:09:13 AM

2019/09/27 7:09

宛先 [redacted]

送信日時 Fri, 27 Sep 2019 07:09:09 +0900

Message ID <002dcfe9a866$0946e3d2$43444bbe$@troulgm>

タグ 後で

User Agent Microsoft Outlook 16.0

amazon.co.jp プライム

Amazon お客様

残念ながら、あなたのアカウント

Amazon を更新できませんでした。
これは、カードが期限切れになったか。請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため

Amazon 情報を確認する必要・ェあります。今アカウントを確認できます。

Amazon ログイン

なお、24時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただくことを警告いたします。

パスワードを変更した覚えがない場合は、至急(03)-5757-5252までお電話ください。

お知らせ:

- パスワードは誰にも教えないでください。
- 個人情報と関係がなく、推測しにくいパスワードを作成してください。大文字と小文字、数字、および記号を必ず使用してください。
- オンラインアカウントごとに、異なるパスワードを使用してください。

http://amazon.co.jp.d3552388b309459e660c07316f65e42423e910bd.xyz/

http://amazon.co.jp.db82b3360519b3824cd0d103f3866062314c6c78.store/

Today ペイン

フィッシングに合わない極意

1　メールの送信元アドレスをチェック

2　メールのリンク先をチェック

3　Google先生に聞いてみる

4　メールのリンクはクリックしない、気になるなら
　　サイトに直接アクセスして調べる

5　メールの画像ダウンロードはオフにする
（通常それが規定値）

6　あわてない

今日はフィッシングに引っかかってみましょう

ただし、ハッカーの手法で

やってはいけない

1　メールのセキュリティ設定を不用意にオフにしてはいけない

自動開封確認や画像のアクセス履歴でフィッシングメールを受け取っていることが相手にわかってしまう可能性がある　→　新たなフィッシングメール

2　家や会社からフィッシングサイトにアクセスしてはいけない

受信者のIPアドレスを相手に教えてしまう　→ 新たな攻撃

3　不用意にリンク先をアクセスしてはいけない

マルウエアがダウンロードされる可能性　→ 二次被害

まず、メールのソースを調べます

次のソース: mailbox:///Users/areabe/Library/Thunderbird/Profiles/zqqcf1el.default/Mail/areabe.com/Inbox?number=118137

```
This is a multi-part message in MIME format.

------=_NextPart_000_0A3D_0139FA23.14C83BB0
Content-Type: text/plain;
    charset="utf-8"
Content-Transfer-Encoding: base64

QW1hem9uLmNvLmpwIOOBq+OBlOeZu+mMsuOBruOCouOCq+OCpuODs+ODiO+8iOWQjeWJjeOAgeOD
keOCueODr+ODvOODieOAgeOBneOBruS7luWAi+S6uuaDheWgse+8ieOBrueiuuiqjS4uLg0K44Gg
44Kl44K+44O0IA0KIA0KDQogIA0KINCQbWF6b24g44GK5a6i5qeYIA0KDQoNCuaui+W/teOBquOB
jOOCieOAgeOBguOBquOBn+OBruOCouOCq+OCpuODs+ODiCANCuODpOOBp+ODi+OCnOOCj+ODoOOC
myANCtCQbWF6b24g44KS5pu05paw44Gn44GN44G+44Gb44KT44Gn44GX44Gf44CCDQrjgZPjgozj
ga/jgIHjgqvjg7zjg4njgYzmnJ/pmZDliIfjgozjgavjgarjgaPjgZ/jgYvjgILoq4vmsYLlhYjk
vY/miYDjgYzlpInmm7TjgZXjgozjgZ/jgarjganjgIHjgZXjgb7jgZbjgb7jgarnkIbnlLHjgafn
mbrnlJ/jgZnjgovlj6/og73mgKfjgYzjgYLjgorjgb7jgZnjgIIgDQoNCg0K44KH44KD44GE44GU
44K344ORIA0KDQrjgqLjgqvjgqbjg7Pjg4jmg4XloLHjga7kuIDpg6jjgYzoqqTjgaPjgabjgYTj
govmlYXjgavjgIHjgYrlrqLmp5jjga7jgqLjgqvjgqbjg7Pjg4jjgpLntq3mjIHjgZnjgovjgZ/j
goEgDQrjgrLjgYbjgYkgDQoNCuOCiOODnOOCk+OCj+OBqCANCtCQbWF6b24g5oOF5aCx44KS56K6
6KqN44GZ44KL5b+F6KaB44O744Kn44GC44KK44G+44GZ44CC5LuK44Ki44Kr44Km44Oz44OI44KS
56K66KqN44Gn44GN44G+44GZ44CCDQrQkG1hem9uIOODreOCsOOCpOODsyANCg0KDQrjgarjgYrj
gIEyNOaZgumWk+S7peWGheOBq+OBlOeiuuiqjeOBjOOBquOBhOWgtOWQiOOAgeiqoOOBq+mBuuaG
vuOBquOBjOOCieOAgeOCouOCq+OCpuODs+ODiOOCkuODreODg+OCr+OBleOBm+OBpuOBhOOBn+OB
oOOBj+OBk+OBqOOCkuitpuWRiuOBhOOBn+OBl+OBvuOBmeOAgg0KDQoNCuOCquOCteODkOOBteOD
tuODgeODliANCg0K44OR44K544Ov44O844OJ44KS5aSJ5pu044GX44Gf6Kaa44GI44GM44Gq44GE
5aC05ZCI44Gv44CB6Iez5oClKDAzKS01NzU3LTUyNTLjgb7jgafjgYrpm7voqbHjgY/jgaDjgZXj
gYTjgIINCg0KDQrjg6Djg43jga7jg5fjgYfjgbrjgbHjgb8gDQrjgYrnn6XjgonjgZs6IOODkeOC
ueODr+ODvOODieOBr+iqsOOBq+OCguaVmeOBiOOBquOBhOOBp+OBj+OBoOOBleOBhOOAgiANCuOD
s+OCr+OCuOODpOOCiSANCuWAi+S6uuaDheWgseOBqOmWouS/guOBjOOBquOBj+OAgeaOqOa4rOOB
l+OBq+OBj+OBhOODkeOCueODr+ODvOODieOCkuS9nOaIkOOBl+OBpuOBj+OBoOOBleOBhOOAguWk
p+aWh+Wtl+OBqOWwj+aWh+Wtl+OAgeaVsOWtl+OAgeOBiuOCiOOBs+iomOWPt+OCkuW/heOBmuS9
v+eUqOOBl+OBpuOBj+OBoOOBleOBhOOAgiANCuOCnODuOOBkCANCuOCquODs+ODqeOCpOODs+OC
ouOCq+OCpuODs+ODiOOBlOOBqOOBq+OAgeeVsOOBquOCi+ODkeOCueODr+ODvOODieOCkuS9v+eU
qOOBl+OBpuOBj+OBoOOBleOBhOOAgg0KDQrjganjgYbjgZ7jgojjgo3jgZfjgY/jgYrpoZjjgYTj
gYTjgZ/jgZfjgb7jgZnjgIIgDQrjgqrjgabjgbzjg6YgDQoNCtCQbWF6b24gDQogDQoNCg0KDQog
DQo=

------=_NextPart_000_0A3D_0139FA23.14C83BB0
Content-Type: text/html;
    charset="shift_jis"
Content-Transfer-Encoding: base64

PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2l0aW9uYWwv
L0VOIj4NCjxIVE1MPjxIRUFEPg0KPE1FVEEgY29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PXNo
aWZ0X2ppcyIgaHR0cC1lcXVpdj1Db250ZW50LVR5cGU+DQo8TUVUQSBuYW1lPUdFTkVSQVRPUiBj
b250ZW50PSJNU0hUTUwgMTEuMDAuOTYwMC4xOTQ2MyI+PC9IRUFEPg0KPEJPRFk+DQo8U1RZTEUg
dHlwZT10ZXh0L2Nzcz4NCi5idXR0b24gew0KICAgIGJhY2tncm91bmQtY29sb3I6ICNlN2U3ZTc7
DQogICAgYm9yZGVyOiBub25lOw0KICAgIGNvbG9yOiB3aGl0ZTsNCiAgICBwYWRkaW5nOiAxNXB4
IDMycHg7DQogICAgdGV4dC1hbGlnbjogY2VudGVyOw0KICAgIHRleHQtZGVjb3JhdGlvbjogbm9u
ZTsNCiAgICBkaXNwbGF5OiBpbmxpbmUtYmxvY2s7DQogICAgZm9udC1zaXplOiAxNnB4Ow0KICAg
IG1hcmdpbjogMTRweCAxMnB4Ow0KICAgIGN1cnNvcjogcG9pbnRlcjsNCiAgICBib3JkZXItcmFk
```

中身をデコードして解析

- リンク先の指定は２箇所だけ

  絵のところはhttp://g-ec2.images-amazon.com

  「Amazonログイン」のリンク先は

  http://amazon.co.jp.d3552388b309459e

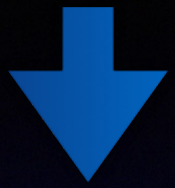
  660c07316f65e42423

  この先を追いかける

- Javascirptのコードはない

- あやしいファイルをダウンロードしたり動かしたりするコードもない

http://amazon.co.jp.d3552388b309459e660c07316f65e42423e910bd.xyz



リダイレクト

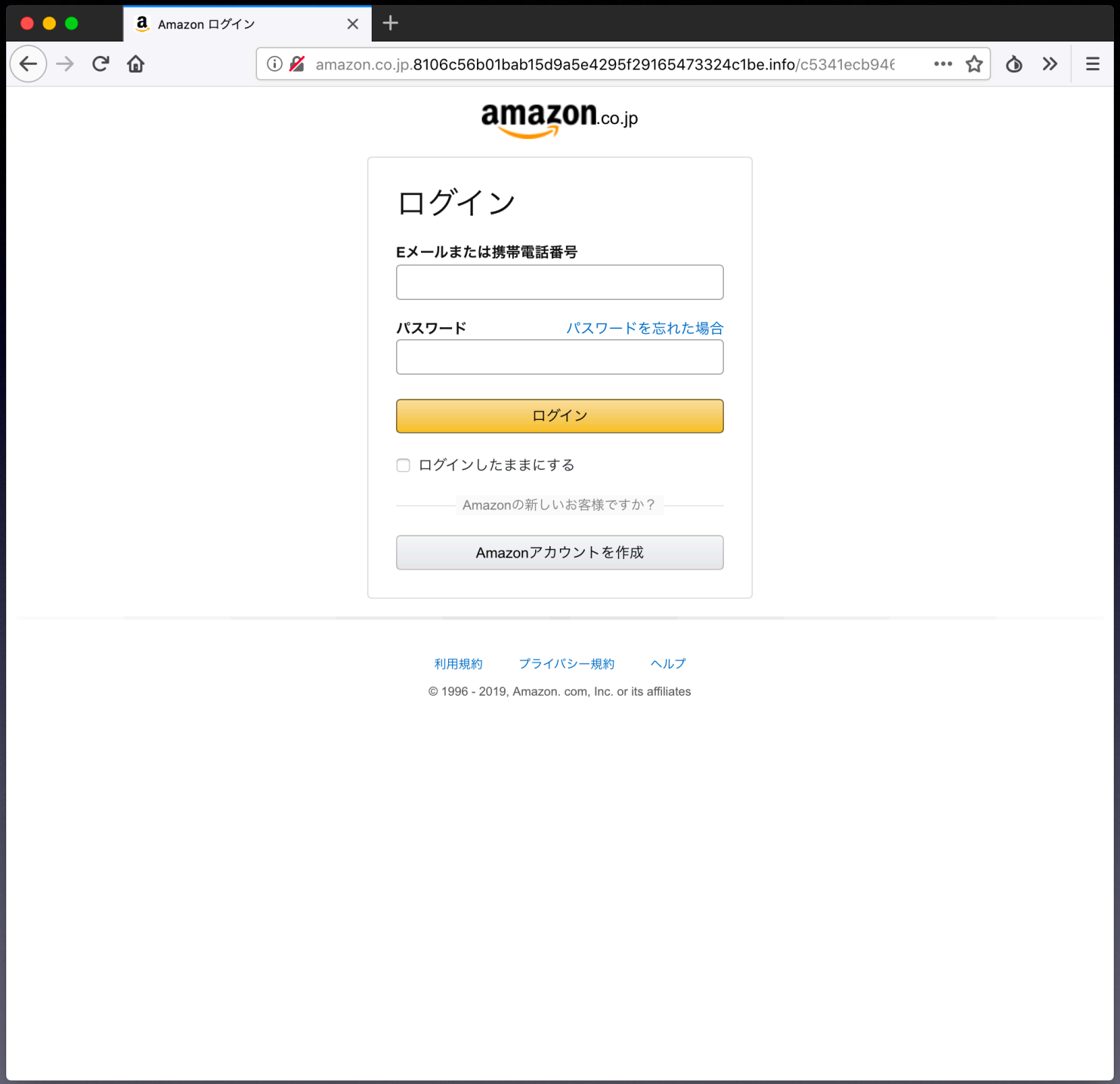
http://amazon.co.jp.8106c56b01bab15d9a5e4295f29165473324c1be.info/

リダイレクト

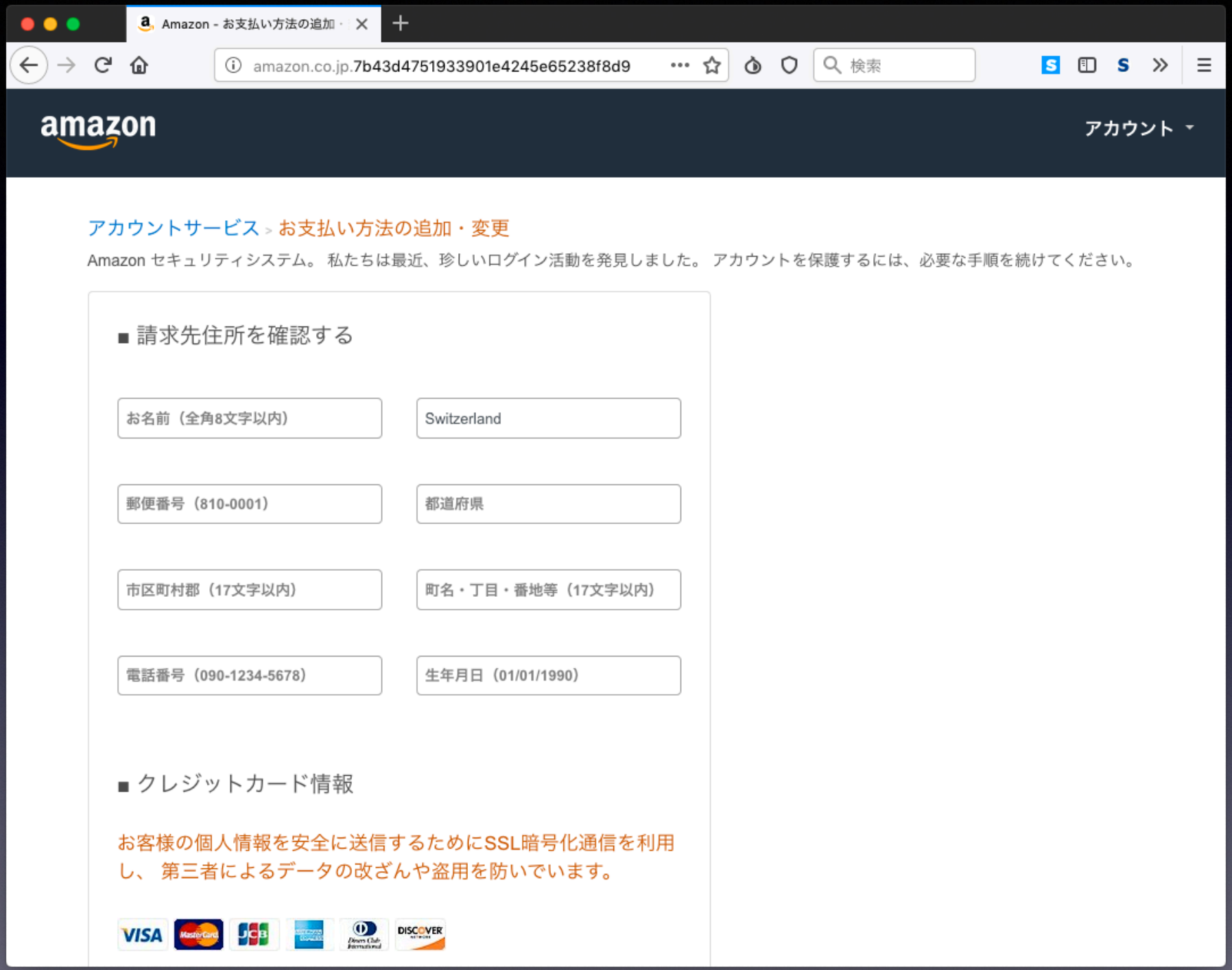
http://amazon.co.jp.8106c56b01bab15d9a5e4295f29165473324c1be.info/
c5341ecb94663eb782118b820ff06cf00315e27db63b7608a4d2f43552f63a5d/
c9eaaa671b79c95e2d25dd30ebb9a86182428eb4810ccad300342c74c694188b/index.php?
country=-\&lang=

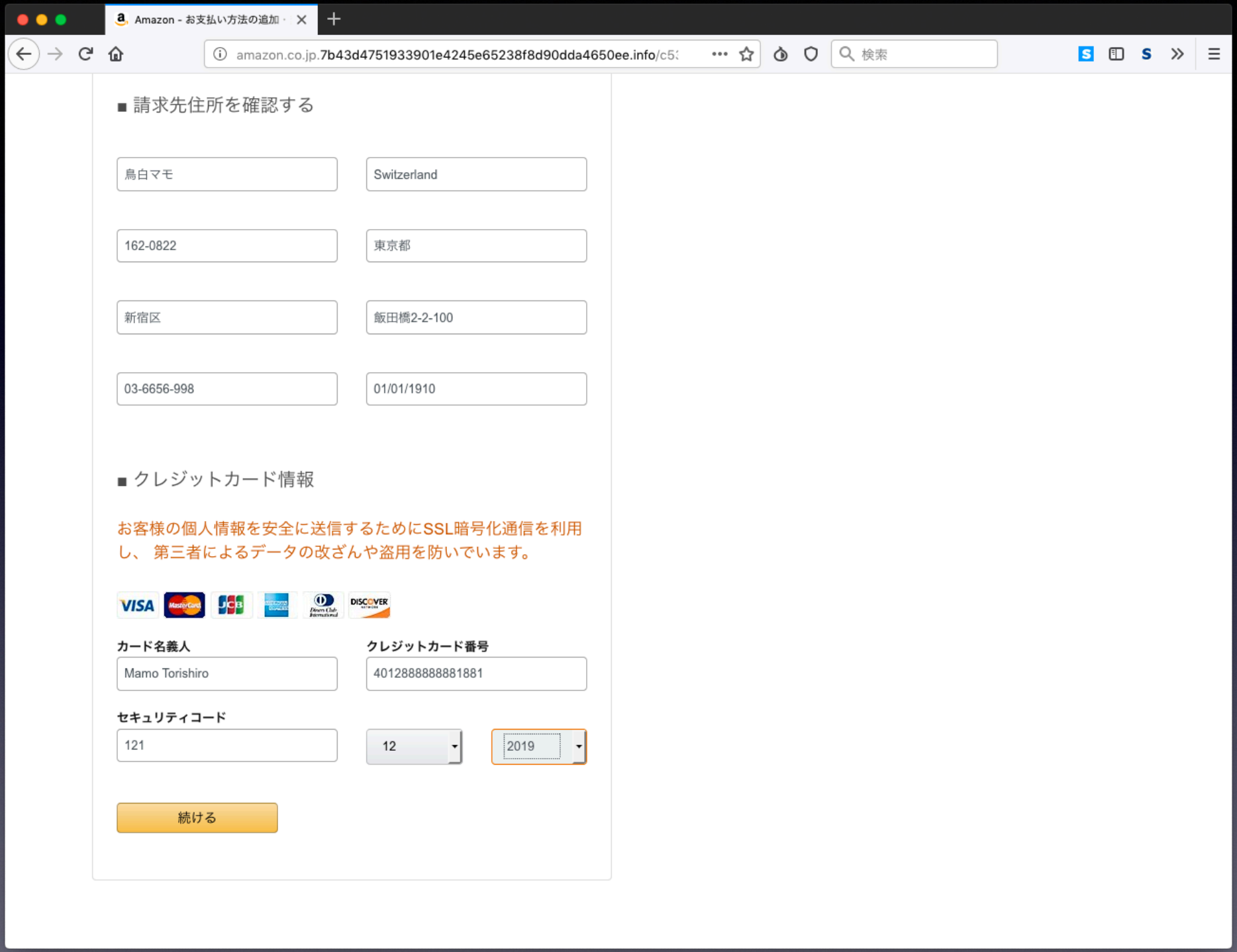
リダイレクト

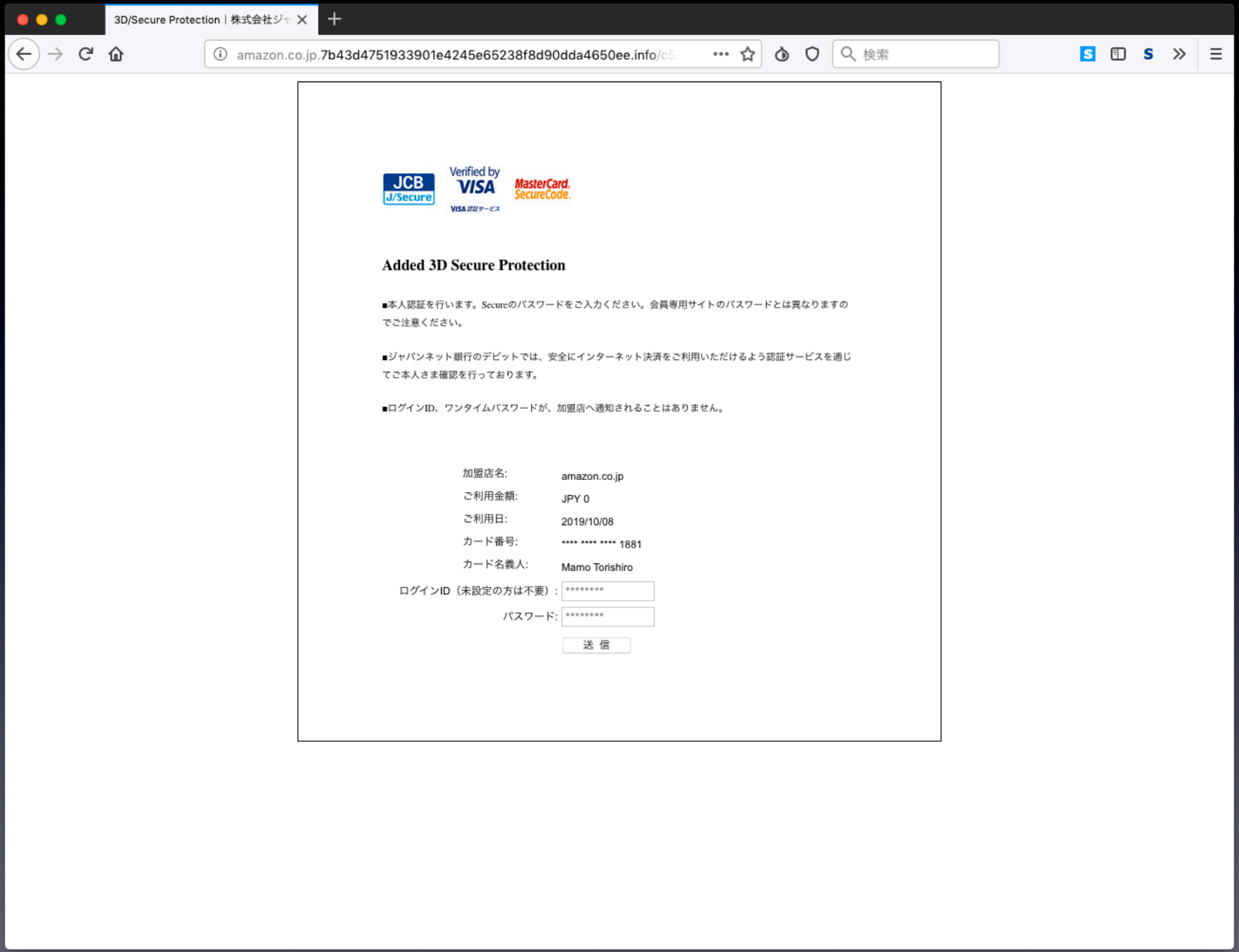
http://amazon.co.jp.8106c56b01bab15d9a5e4295f29165473324c1be.info/
c5341ecb94663eb782118b820ff06cf00315e27db63b7608a4d2f43552f63a5d/
c9eaaa671b79c95e2d25dd30ebb9a86182428eb4810ccad300342c74c694188b/signin.php?
country=JP-Japan%26lang=ja-JP -I

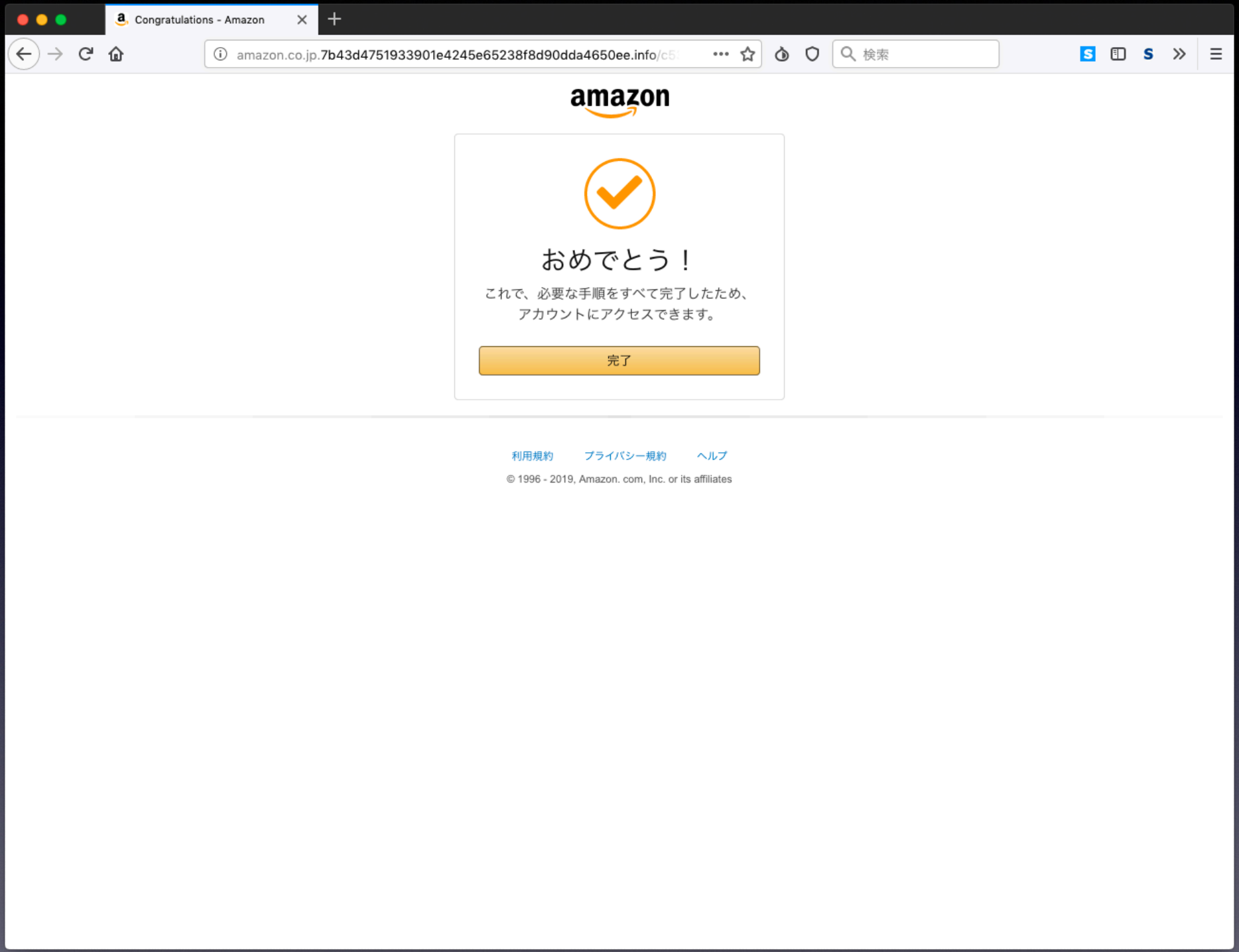

Amazon ログイン
amazon.co.jp.8106c56b01bab15d9a5e4295f29165473324c1be.info/c5341ecb94
amazon.co.jp
ログイン
Eメールまたは携帯電話番号
パスワード
パスワードを忘れた場合
ログイン
ログインしたままにする
Amazonの新しいお客様ですか？
Amazonアカウントを作成
利用規約
プライバシー規約
ヘルプ
© 1996 - 2019, Amazon. com, Inc. or its affiliates

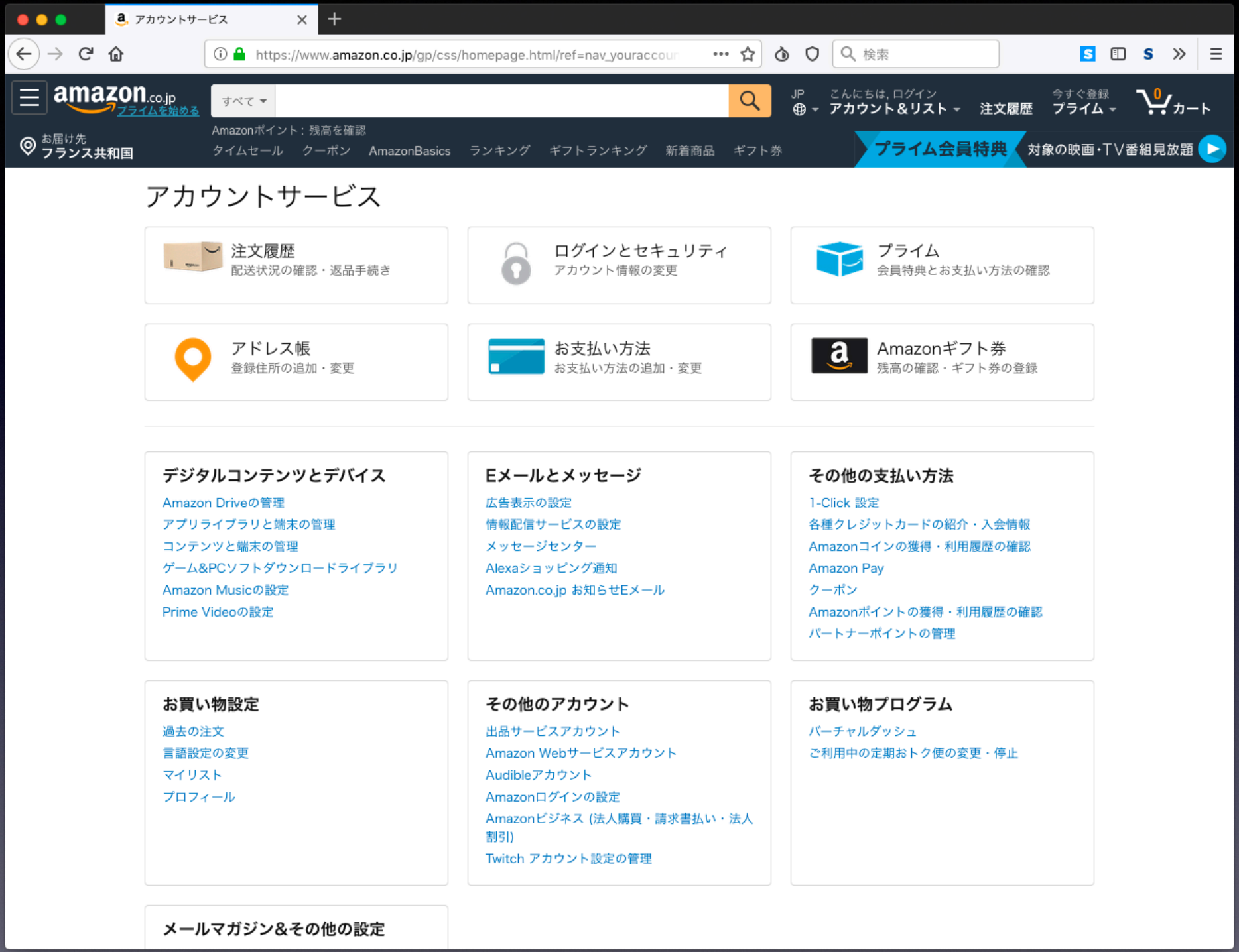

Amazon - アカウントサービス
amazon.co.jp.7b43d4751933901e4245e65238f8
検索
amazon
アカウント
アカウントサービス > お支払い方法の追加・変更
Amazonのセキュリティシステム。 私たちは最近、珍しいログイン活動を発見しました。 アカウントを保護するには、必要な手順を続けてください。
お支払い方法を更新してください！
中断して申し訳ありませんが、お支払い方法の認証に問題があります. お客様の情報を保護するため、お客様の情報が当社のシステムに対して検証されるまで、当社のシステムは一時的にお客様のアカウントに制限を設けています. この手順を完了した直後にアカウントを元に戻すことができます.
続ける


Amazon - お支払い方法の追加
amazon.co.jp.7b43d4751933901e4245e65238f8d9
検索
amazon
アカウント
アカウントサービス > お支払い方法の追加・変更
Amazon セキュリティシステム。 私たちは最近、珍しいログイン活動を発見しました。 アカウントを保護するには、必要な手順を続けてください。
■ 請求先住所を確認する
お名前（全角8文字以内）
Switzerland
郵便番号（810-0001）
都道府県
市区町村郡（17文字以内）
町名・丁目・番地等（17文字以内）
電話番号（090-1234-5678）
生年月日（01/01/1990）
■ クレジットカード情報
お客様の個人情報を安全に送信するためにSSL暗号化通信を利用し、 第三者によるデータの改ざんや盗用を防いでいます。


Amazon - お支払い方法の追加
amazon.co.jp.7b43d4751933901e4245e65238f8d90dda4650ee.info/c5
検索
■ 請求先住所を確認する
鳥白マモ
Switzerland
162-0822
東京都
新宿区
飯田橋2-2-100
03-6656-998
01/01/1910
■ クレジットカード情報
お客様の個人情報を安全に送信するためにSSL暗号化通信を利用し、 第三者によるデータの改ざんや盗用を防いでいます。
VISA
MasterCard
JCB
DISCOVER
カード名義人
Mamo Torishiro
クレジットカード番号
4012888888881881
セキュリティコード
121
12
2019
続ける


3D/Secure Protection | 株式会社ジャ
amazon.co.jp.7b43d4751933901e4245e65238f8d90dda4650ee.info/c5
検索
JCB J/Secure
Verified by VISA
VISA 認証サービス
MasterCard SecureCode
Added 3D Secure Protection
■本人認証を行います。Secureのパスワードをご入力ください。会員専用サイトのパスワードとは異なりますのでご注意ください。
■ジャパンネット銀行のデビットでは、安全にインターネット決済をご利用いただけるよう認証サービスを通じてご本人さま確認を行っております。
■ログインID、ワンタイムパスワードが、加盟店へ通知されることはありません。
加盟店名: amazon.co.jp
ご利用金額: JPY 0
ご利用日: 2019/10/08
カード番号: **** **** **** 1881
カード名義人: Mamo Torishiro
ログインID（未設定の方は不要）: ********
パスワード: ********
送 信


Congratulations - Amazon
amazon.co.jp.7b43d4751933901e4245e65238f8d90dda4650ee.info/c5
検索
amazon
おめでとう！
これで、必要な手順をすべて完了したため、
アカウントにアクセスできます。
完了
利用規約
プライバシー規約
ヘルプ
© 1996 - 2019, Amazon. com, Inc. or its affiliates


アカウントサービス
https://www.amazon.co.jp/gp/css/homepage.html/ref=nav_youracc
検索
amazon.co.jp
プライムを始める
すべて
JP
こんにちは, ログイン
アカウント＆リスト
注文履歴
今すぐ登録
プライム
0
カート
お届け先
フランス共和国
Amazonポイント：残高を確認
タイムセール
クーポン
AmazonBasics
ランキング
ギフトランキング
新着商品
ギフト券
プライム会員特典
対象の映画・TV番組見放題
アカウントサービス
注文履歴
配送状況の確認・返品手続き
ログインとセキュリティ
アカウント情報の変更
プライム
会員特典とお支払い方法の確認
アドレス帳
登録住所の追加・変更
お支払い方法
お支払い方法の追加・変更
Amazonギフト券
残高の確認・ギフト券の登録
デジタルコンテンツとデバイス
Amazon Driveの管理
アプリライブラリと端末の管理
コンテンツと端末の管理
ゲーム&PCソフトダウンロードライブラリ
Amazon Musicの設定
Prime Videoの設定
Eメールとメッセージ
広告表示の設定
情報配信サービスの設定
メッセージセンター
Alexaショッピング通知
Amazon.co.jp お知らせEメール
その他の支払い方法
1-Click 設定
各種クレジットカードの紹介・入会情報
Amazonコインの獲得・利用履歴の確認
Amazon Pay
クーポン
Amazonポイントの獲得・利用履歴の確認
パートナーポイントの管理
お買い物設定
過去の注文
言語設定の変更
マイリスト
プロフィール
その他のアカウント
出品サービスアカウント
Amazon Webサービスアカウント
Audibleアカウント
Amazonログインの設定
Amazonビジネス (法人購買・請求書払い・法人割引)
Twitch アカウント設定の管理
お買い物プログラム
バーチャルダッシュ
ご利用中の定期おトク便の変更・停止
メールマガジン&その他の設定

このドメインのIPアドレスを調べてWhois検索してみると

Quick Stats

IP Location	United States Mountain View Google Llc
ASN	AS15169 GOOGLE - Google LLC, US (registered Mar 30, 2000)
Resolve Host	238.133.94.34.bc.googleusercontent.com
Whois Server	whois.arin.net

差出人 Mitsubishi UFJ Financial Group <no-reply@mufg.jp>
件名 通知 - 払い戻し保留中の情報
宛先 [redacted]
送信日時 Sat, 29 Jun 2019 04:06:29 +0800
Message ID <VPS51VOmmuoqfyH6k0n0003facc@vps5>
タグ ToDo
X-Account-Key account3

返信 | 全員に返信 | 転送 | アーカイブ | 迷惑マークを付ける | 削除 | その他

2019/06/29 5:06

あなたの情報を保留している返金があります。

この払い戻しは3-5日以内にあなたの銀行口座に送られます。

下のリンクをクリックしてこのフォームに記入してください。

払い戻し情報フォーム

このリンクは24時間以内に期限が切れます。

敬具,

https://mufg-co-jp.com/

未読数: 4 合計: 118063 Today ペイン

現在はmufg-co-jp.comは”まともな”応答をしない

メールを受信した6月時点ではフィッシングサイトが動いていた

SSL証明書も正しく入っていた

あるアメリカのWordPressのサイト内にフィッシングサイトが作られていた

↓

https://xxxx/wp-admin/css/cabb129696bcbc6ae8796f2ff11fa39e/index1.html

サイト管理者にメールし削除してもらった

フィッシングサイトは乗っ取りで作られてしまう

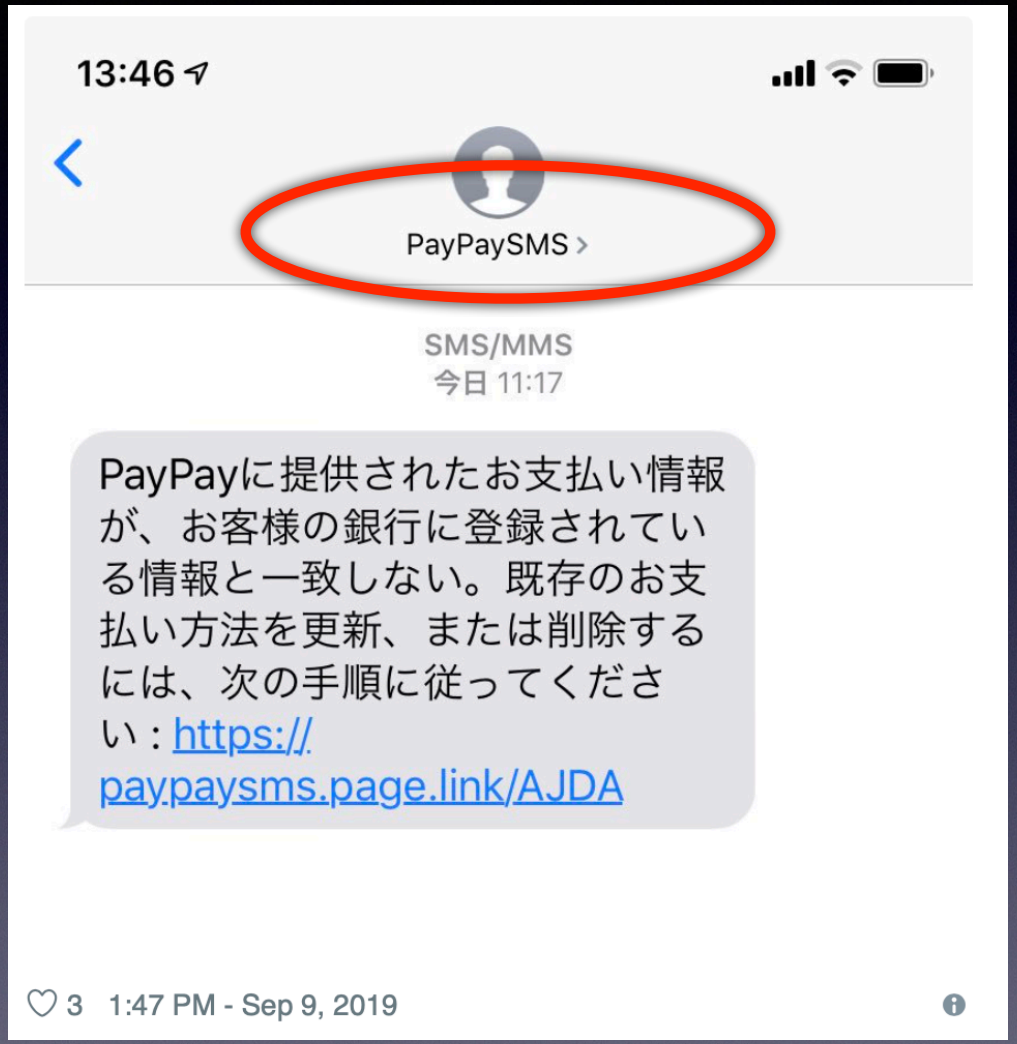
サイト管理者に気がつかれないようにこっそりと

管理が放置されている野良サーバは要注意

スミッシング

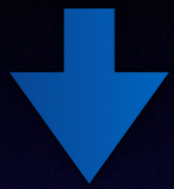
携帯電話・携帯端末などで用いられるSMSに、銀行・企業などを騙ってメッセージを送り、特定のサイトへ誘導・課金する手法

https://www.jc3.or.jp/topics/smscert.html


13:46
PayPaySMS
SMS/MMS
今日 11:17
PayPayに提供されたお支払い情報が、お客様の銀行に登録されている情報と一致しない。既存のお支払い方法を更新、または削除するには、次の手順に従ってください：https://paypaysms.page.link/AJDA
3 1:47 PM - Sep 9, 2019

出典元：https://akaki.io/2019/sms_spoofing.html

https://paypaysms.page.link/AJDA



リダイレクト

https://t.co/pHw0rDS3GF?amp=1

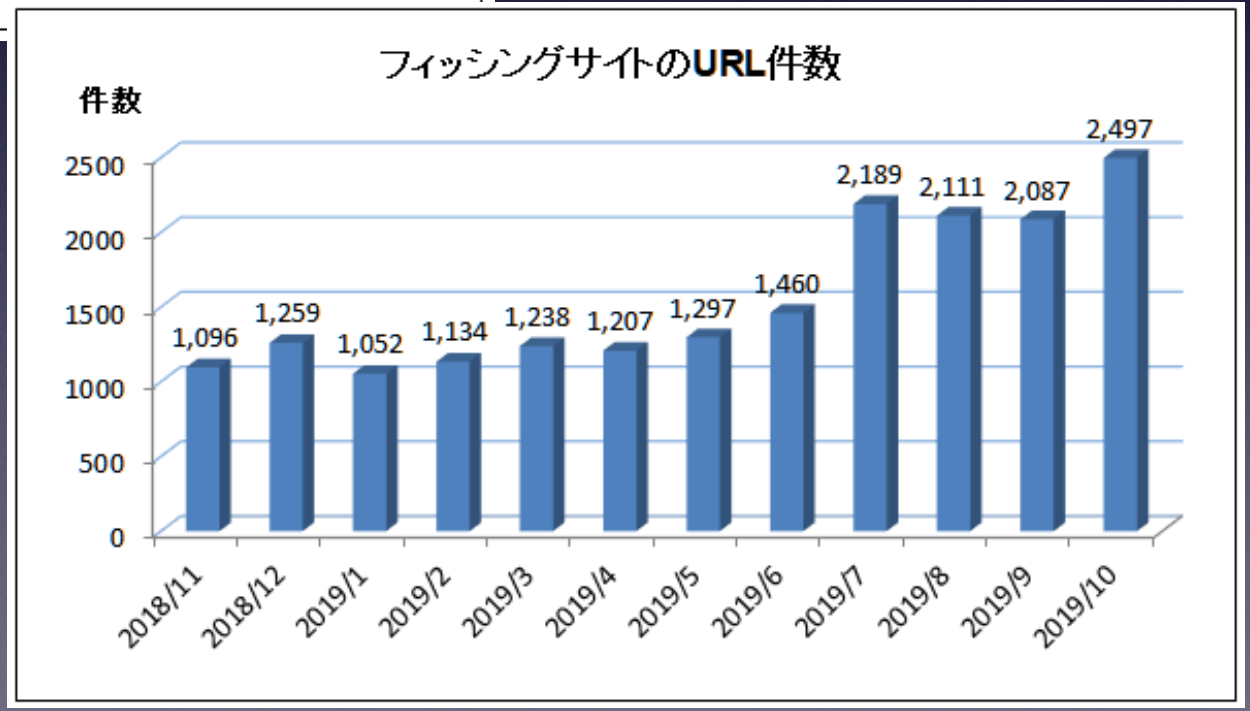
リダイレクト

https://payaapay-jp.com/sign-app-home-ab0304b304c3042306a305f306e004100.php?set=0571061d03e850434c5db6b680ec1c98


受信
作成
チャット
アドレス帳
タグ
クイックフィルター
検索 <⌘K>
差出人 Amazon <account-update@amazon.co.jp>
件名 1回限りの Amazon アカウント仮パスワード
宛先 (自分)
送信日時 Wed, 9 Oct 2019 08:29:48 +0000
Message ID <0101016dafa376f8-888a23b4-d77f-4576-a055-771051a28548-000000@us-west-2.amazonses.com>
タグ ToDo
X-Account-Key account4
返信
転送
アーカイブ
迷惑マークを付ける
削除
その他
2019/10/09 17:29
Amazon.co.jpをご利用いただき、ありがとうございます。
お客様のAmazonアカウントへ、端末またはアプリから登録が試みられました。
セキュリティ上の理由により、端末またはアプリの登録を一度解除した後で、再度登録しようとするとエラーメッセージが表示されます。お手数ですが以下の仮パスワードを使用して登録を行ってください。
507150
仮パスワードには発行から10分間の使用期限があります。失効後は仮パスワードの再発行が必要になりますので、アプリより再度サインインを行ってください。仮パスワードが再度発行されます。
仮パスワードは、Amazonアカウントでお使いのパスワードとは異なります。仮パスワード入力後に、Amazonアカウントでお使いのパスワードを入力してください。
Amazonアカウントでお使いのパスワードは変更されませんので、引き続きご使用いただけます。
なお、端末またはアプリの最新バージョンをインストールすることで、仮パスワードの入力が不要になる場合があります。
今回の登録の試みがお客様ご自身によるものでない場合には、パスワードのリセットを行ってください。
アカウント設定の変更については、以下のURLよりヘルプページをご覧ください。
https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201391470
ご不明な点がありましたら、いつでもご遠慮なくお問い合わせください。
このEメールアドレスは配信専用です。ご不明な点は、下記のURLからカスタマーサービスまでお問い合わせください。
https://www.amazon.co.jp/contact-us/
今後ともAmazon.co.jpをよろしくお願いいたします。
Today ペイン

こんな時の対処法

- サイトに直接ログインして、メッセージが来ていないか確認する
- 不審な取引がないか確認する
- 必要に応じて、パスワードを変更する（パスワードの使い回しをしているような場合は特に）
- ひとまず放置する



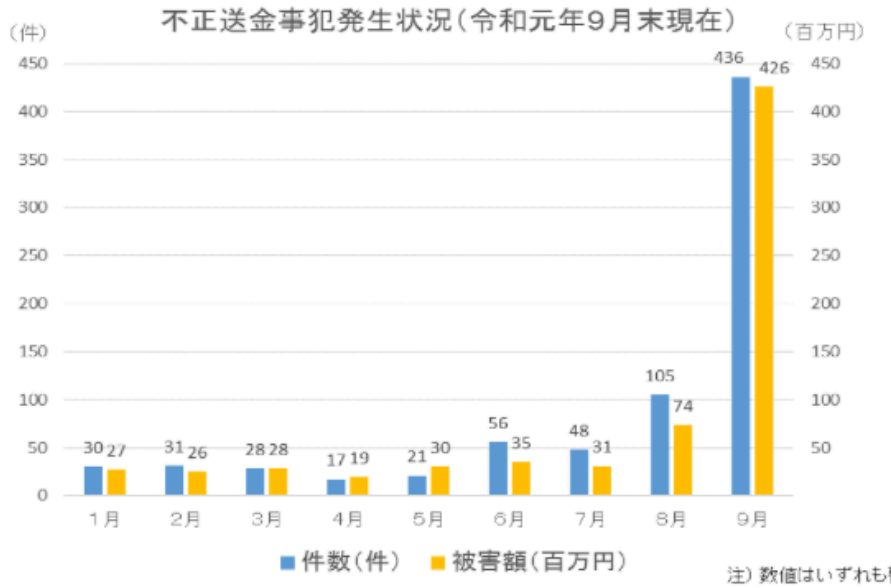
引用元　フィッシング対策協議会：https://www.antiphishing.jp/report/monthly/201910.html

ホーム > お金を預けている方へ

令和元年11月19日更新
金　融　庁

インターネット・バンキングによる預金の不正送金事案が多発しています。

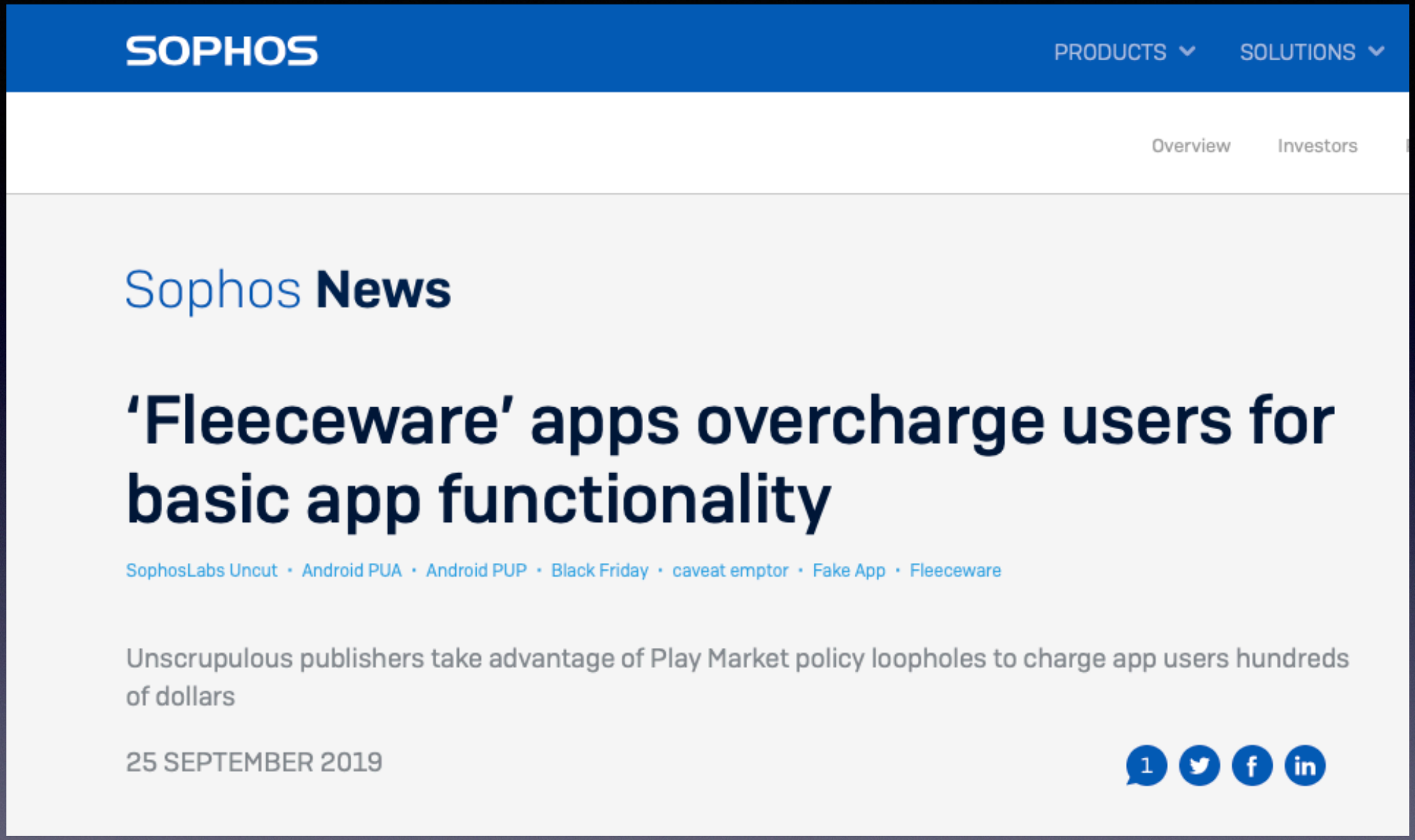
メールやショートメッセージ（SMS等）を用いたフィッシングや、スパイウェア等の不正プログラムを用いた手口により、インターネット・バンキング利用者のＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発しています。



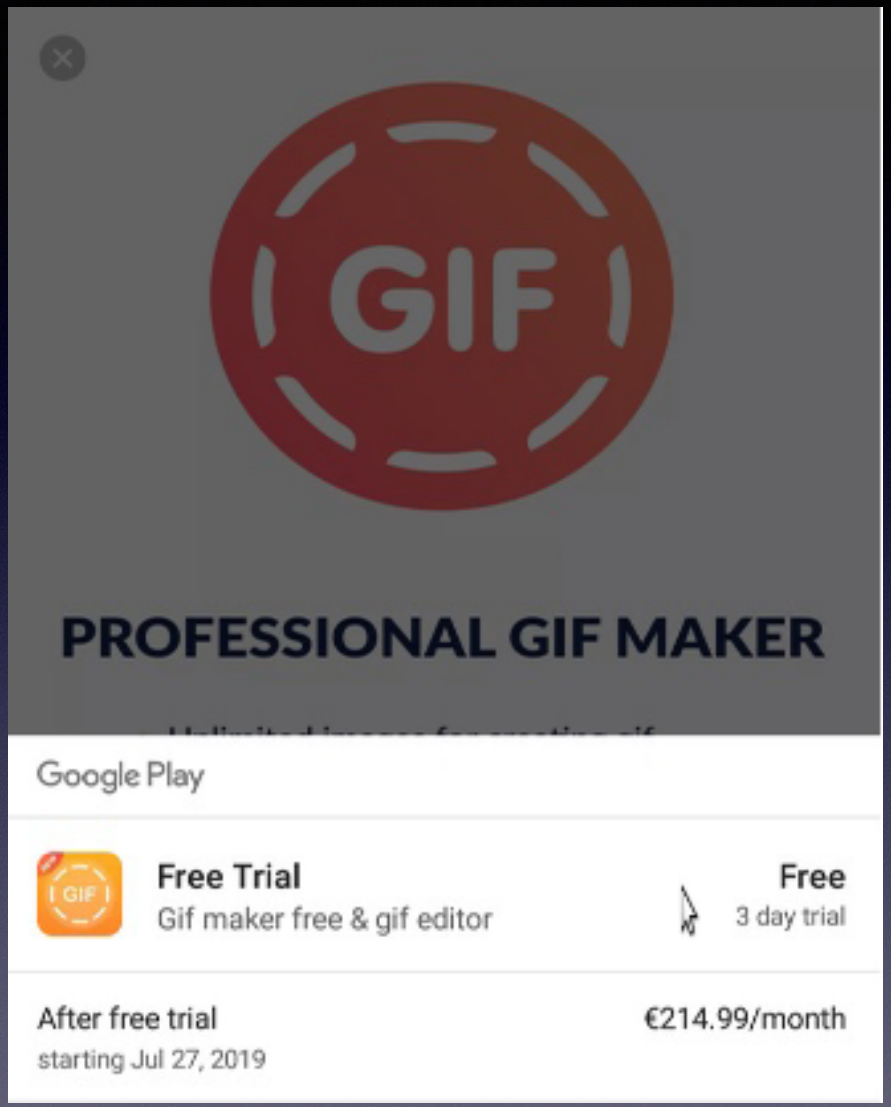
(出典：警察庁HP「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」)

金融庁：https://www.fsa.go.jp/ordinary/internet-bank_2.html

フリースウエア
(fleeceware)



出典： https://news.sophos.com/en-us/2019/09/25/fleeceware-apps-overcharge-users-for-basic-app-functionality/



ユーザは３日間の試用期間の間にアプリを削除した

試用期間経過後に214.99ユーロの支払い請求が届いた（２万5千円から２万6千円くらい）

使用料がべらぼうに高い

意図的に短い試用期間が設定されている

アプリの削除だけでは使用キャンセルにならない

試用期間後の利用契約は自動更新になっている