

令和 7 年 8 月

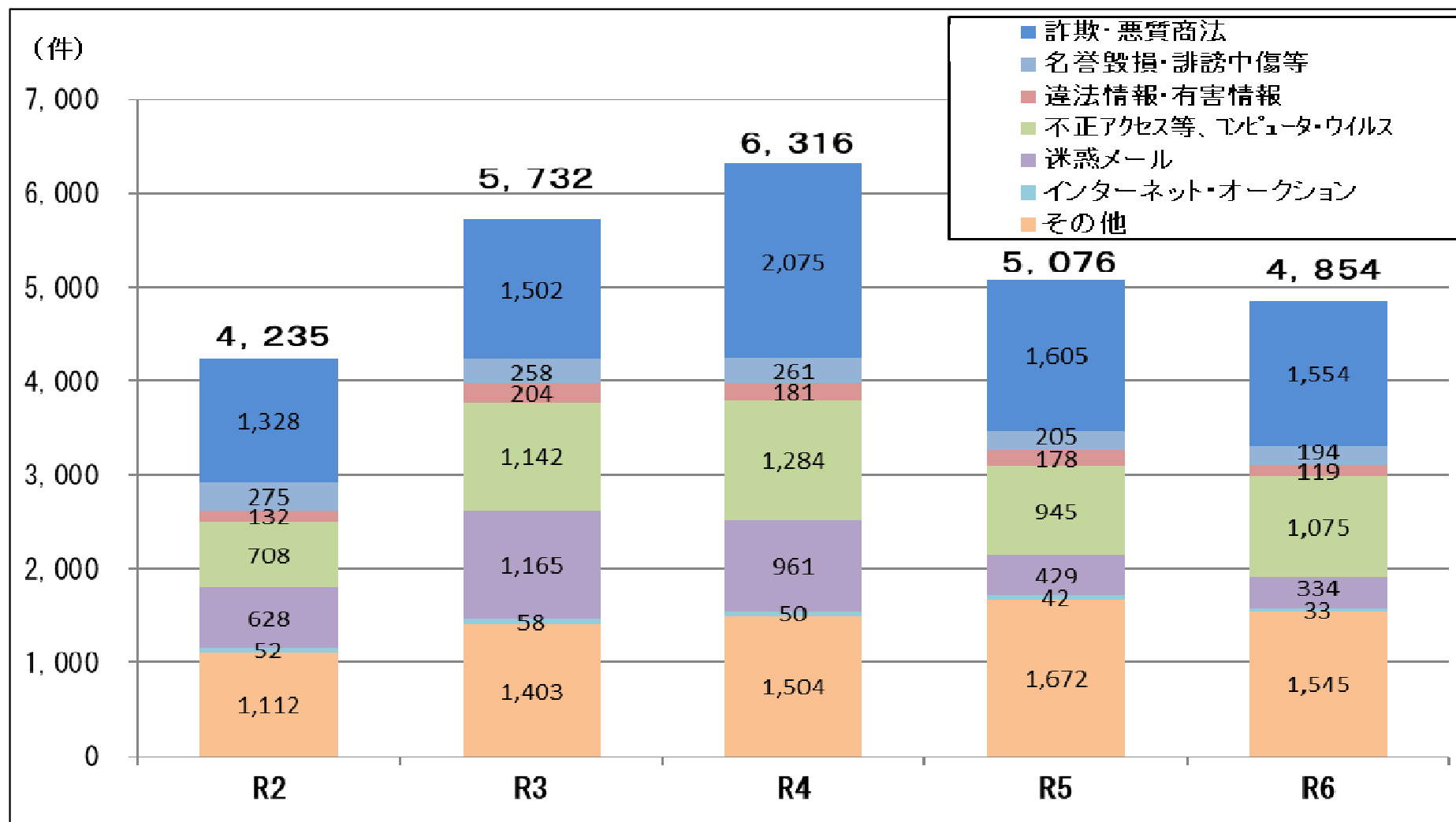
サイバー犯罪の現状と対策

福岡県警察本部サイバー犯罪対策課
サイバー企画・対策係

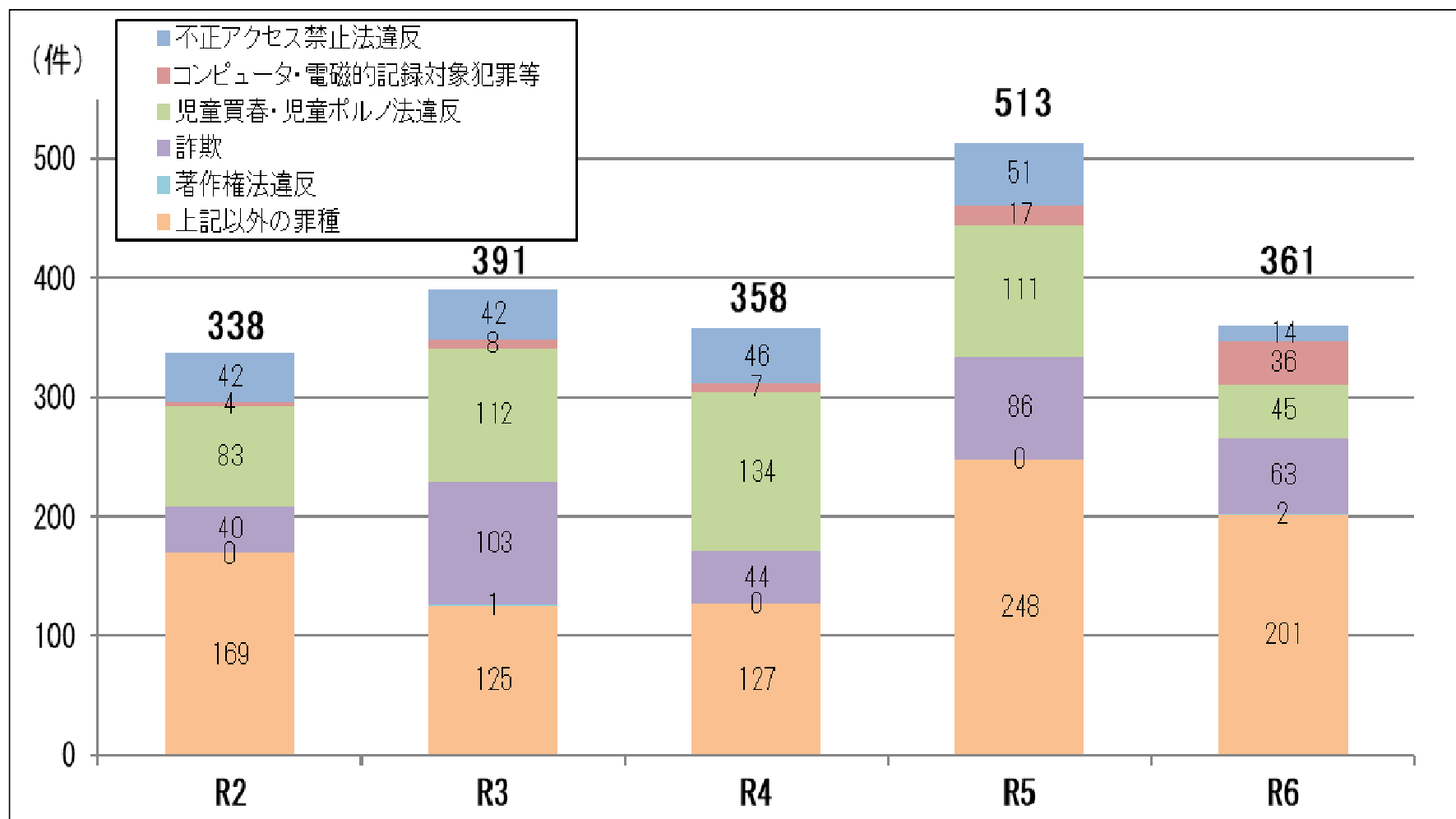
- 1 はじめに（現状）
- 2 サイバー犯罪の手口
 - 偽（詐欺）サイト
 - フィッシング・当選金詐欺
 - サポート詐欺・プリペイドカード（電子マネー）
 - SNS型投資・ロマンス詐欺
- 3 身近にある脅威～SNS編～
- 4 闇バイト
- 5 パスワード（口座）管理
- 6 相談窓口・サイト

1 はじめに (現状)

サイバー犯罪の相談受理事件数（福岡）

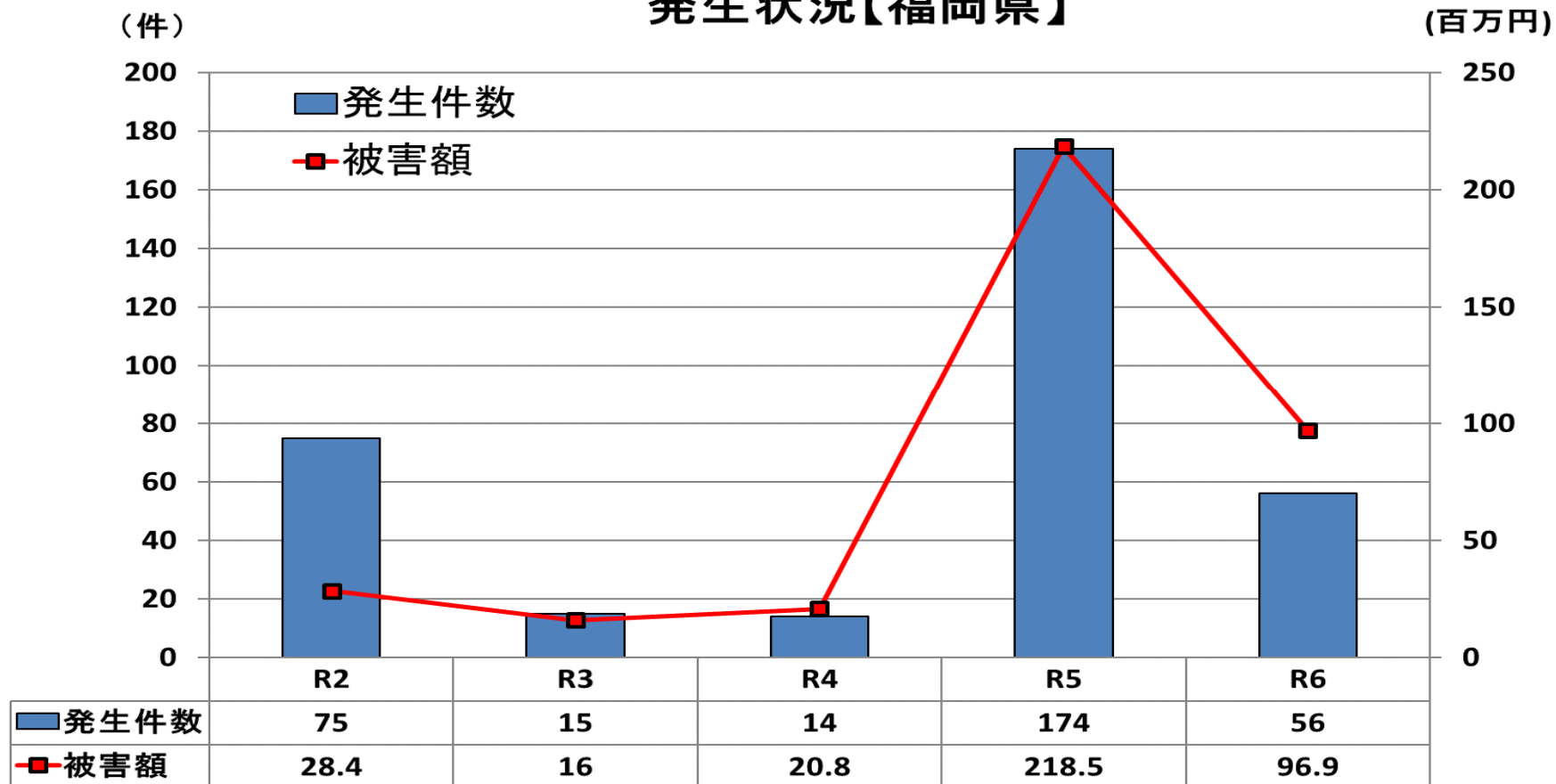


サイバー犯罪の検挙件数（福岡）

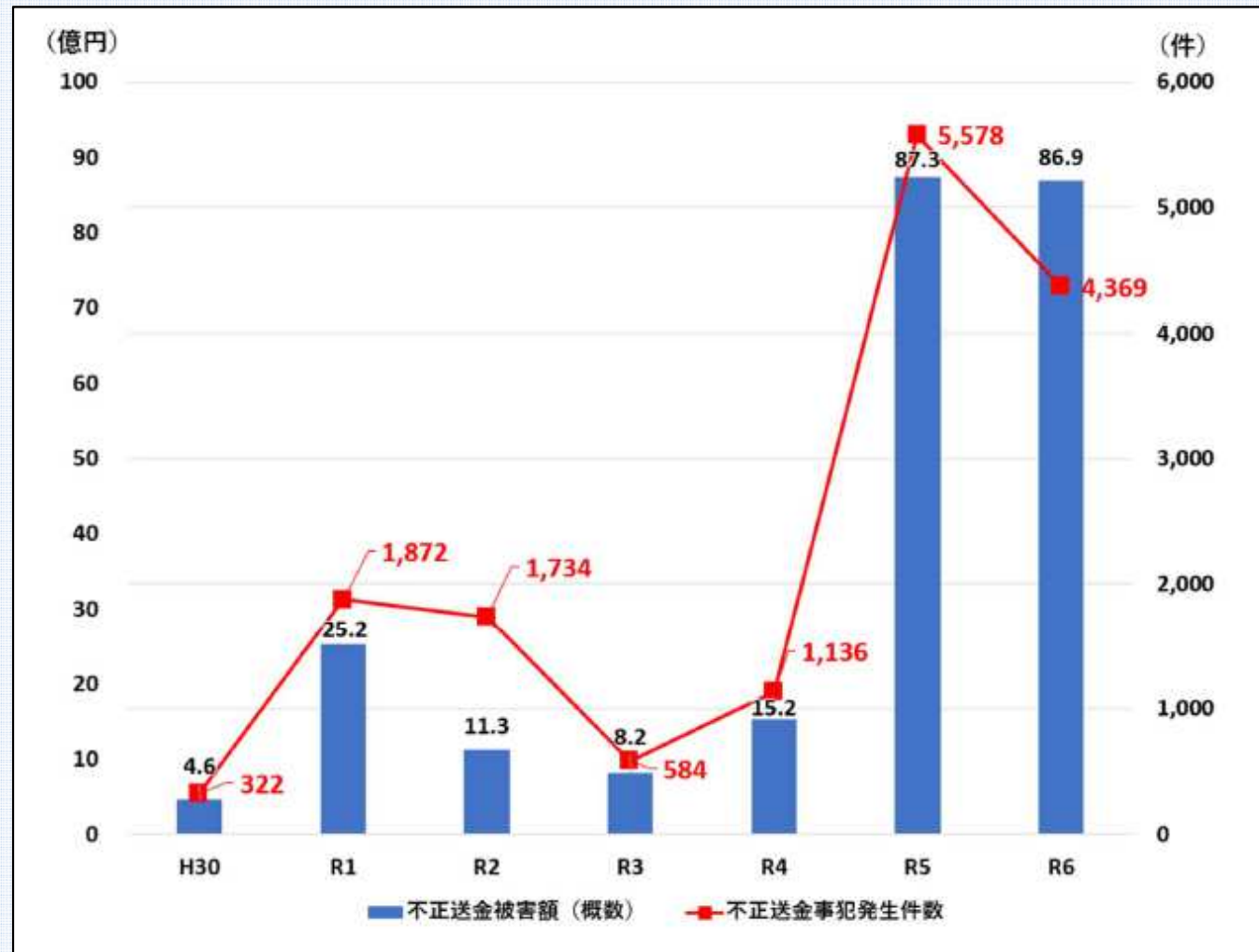


インターネットバンキングに係る不正送金事犯の発生状況（福岡）

発生状況【福岡県】



インターネットバンキングに係る不正送金事犯の発生状況（全国）



出典：警察庁HP 広報資料「令和6年におけるサイバー空間をめぐる脅威の情勢等について」

情報セキュリティ10大脅威2025

個人	順位	組織
インターネット上のサービスからの個人情報の窃取	1位	ランサム攻撃による被害
インターネット上のサービスへの不正ログイン	2位	サプライチェーンや委託先を狙った攻撃
クレジットカード情報の不正利用	3位	システムの脆弱性を突いた攻撃
スマホ決済の不正利用	4位	内部不正による情報漏えい等
偽警告によるインターネット詐欺	5位	機密情報等を狙った標的型攻撃
ネット上の誹謗・中傷・デマ	6位	リモートワーク等の環境や仕組みを狙った攻撃
フィッシングによる個人情報等の詐取	7位	地政学的リスクに起因するサイバー攻撃
不正アプリによるスマートフォン利用者への被害	8位	分散型サービス妨害攻撃（DDoS攻撃）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	9位	ビジネスメール詐欺
ワンクリック請求等の不当請求による金銭被害	10位	不注意による情報漏えい等

出典：独立行政法人情報処理推進機構 「情報セキュリティ10大脅威 2025」

コミュニケーション手段の**オンライン化**

Web会議 テレワーク

社会全体の**デジタル化**

運転免許証 マイナンバーカード キャッシュレス決済

サイバー空間における**社会・経済活動の拡大**

ネットワークを利用した犯罪

S N S 等に関連する犯罪

2 サイバー犯罪の手口

偽・詐欺サイト

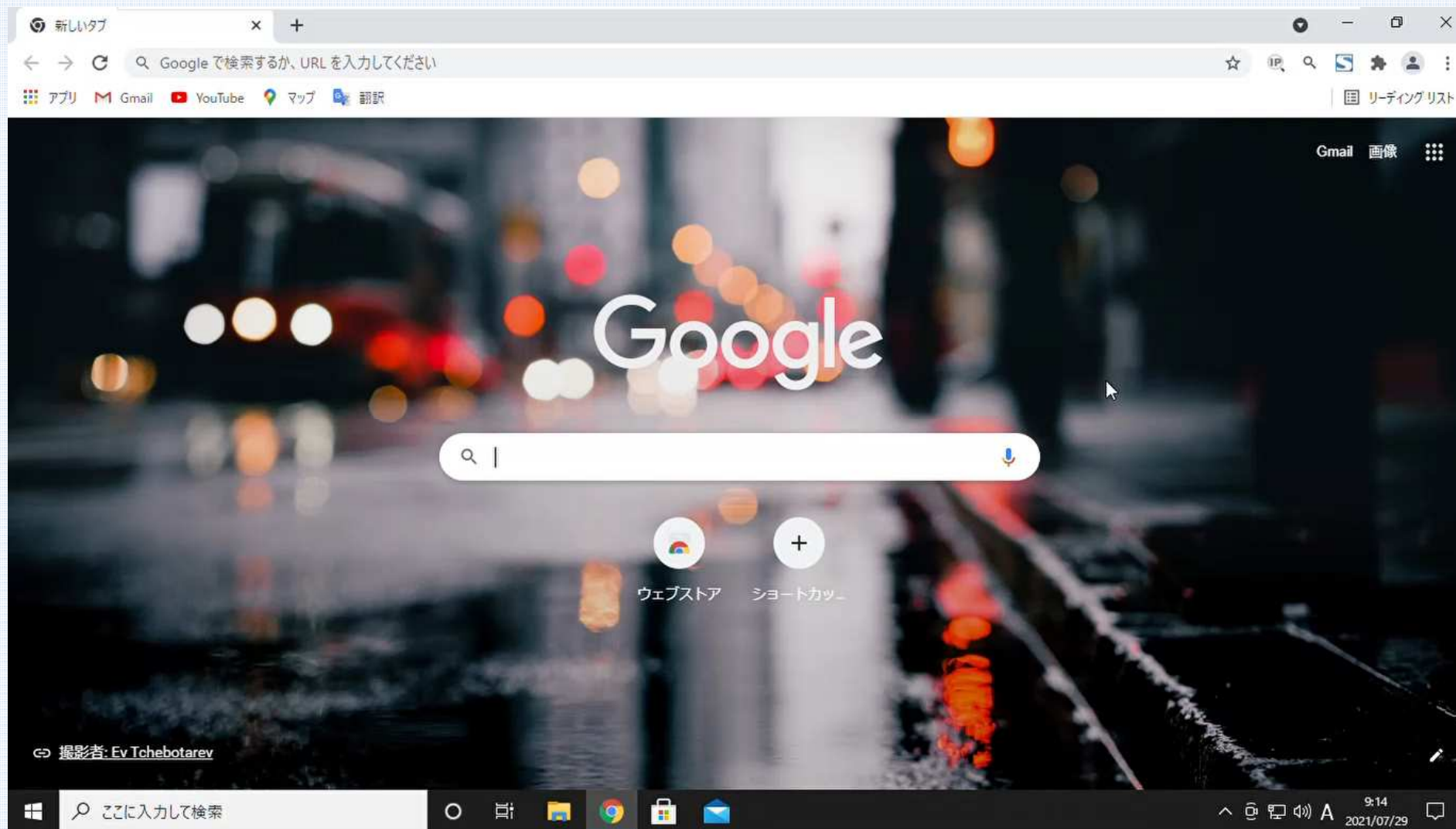


偽・詐欺サイトとは

お金を振り込んでも商品が送られてこない
ショッピングサイト

お金やキャッシュカード情報などが
盗まれます！

偽・詐欺サイト



偽・詐欺サイト

ショッピング IDでもっと便利に 新規取得
ログインしてお買い物するとポイントがたまります

dyson 公式オンラインストア

Yahoo! JAPAN 無料でお店を開こう! ヘルプ

自転車 スマートジョイ > メーカー > パナソニック > 電動自転車 > パナソニック ベロスターミニ BE-ELVS073 2021年モデル 20インチ 外装7段変速 電動アシスト自転車

自転車 スマートジョイ ★★★★★ 4.30 (4,555件) 会社概要

ご利用ガイド 配送・送料 キャンセル規約 返品特約 ※重要なお知らせ 問い合わせ

配送に関するご注意 ■ お盆休みのご案内 8月11～15日は全ての業務がお休みです ■

新型コロナウイルスの影響による パーツ代替えのお知らせ

現在、新型コロナウイルスの影響により自転車パーツの供給が難しい状況となっています。
スムーズに商品を供給するため、各メーカー側で予告なく仕様変更がされるケースが発生しています。

**パーツ代替えの箇所は主にタイヤ（カラータイヤが黒タイヤになる等）ですが、
他の箇所でも仕様変更の可能性がございます**

ベロスター・ミニ *Velo-Star*

ブランド: パナソニック

スポーツモデル 電動自転車 電動アシスト自転車 激安価格

パナソニック ベロスターミニ BE-ELVS073 2021年モデル 20インチ 外装7段変速 電動アシスト自転車

0件の商品レビュー

価格情報

メーカー希望
小売価格
(税込) **109,800 円**

通常販売価格
(税込) **99,800 円** 9% OFF
10,000円引き

東京都は送料4,200円
※条件により送料が異なる場合があります

97,800 円 で購入のチャンス▼

配送情報

【取寄品】欠品時メール連絡 | 在庫確保時→(～08/30までに発送)
※発送予定日はストアにお問い合わせください
すべてのお届け方法とお届け日を確認する>

注文について

・手数料・送料・配送方法について (お買い物ガイド)
・メーカー希望小売価格の価格について
・返品申請の申請をする

シェアする

ボーナス等

1% 還元

998ポイント (1%)
ログインすると獲得できます。

あなたはまだYahoo!ショッピングで
PayPayを利用できません

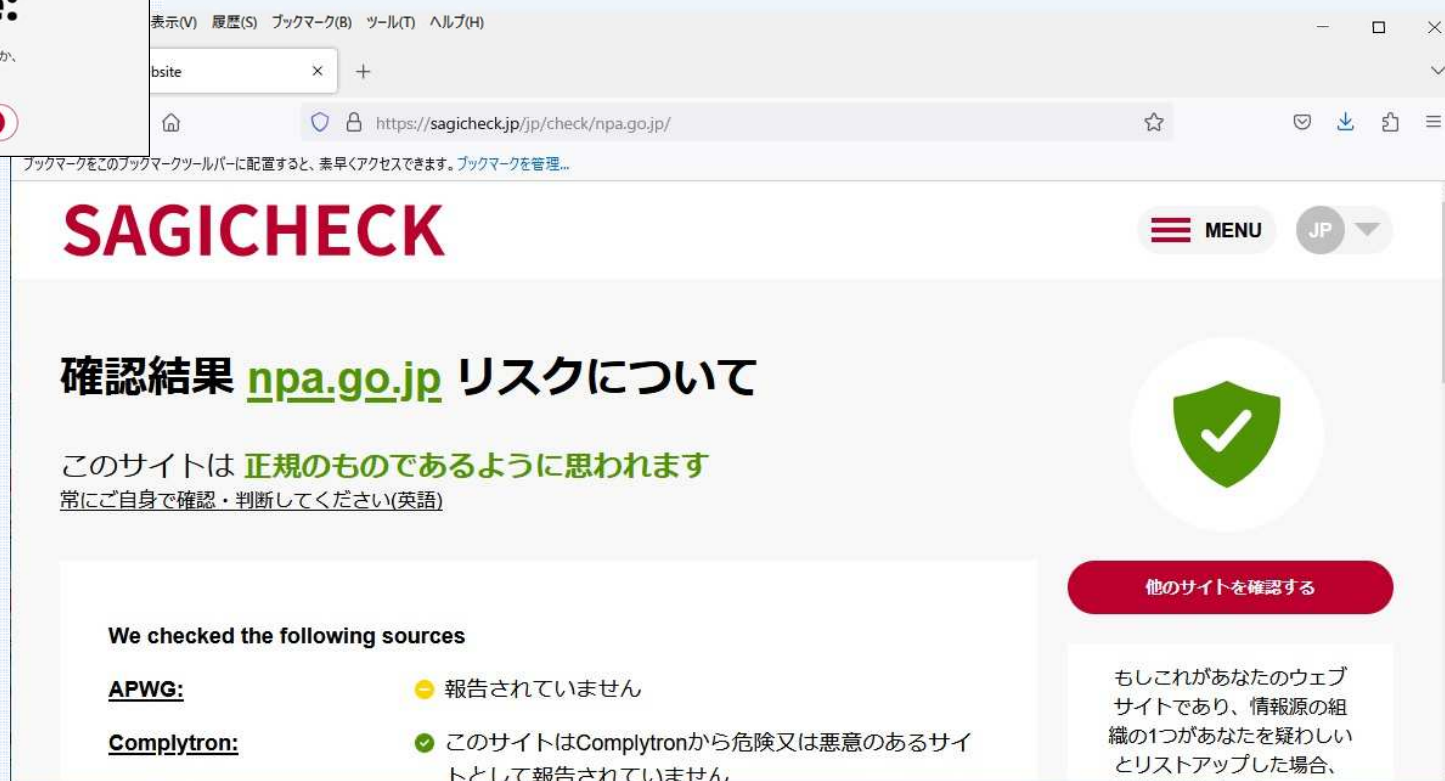
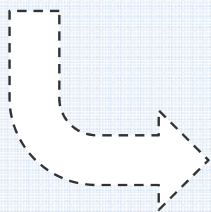
**気軽に始められる
エントリー向け電動バイク**

偽・詐欺サイト



偽サイトの被害防止策

- ・ JC3 が収集した情報を「ScamAdviser」へ情報提供
- ・ ウェブサイトの信ぴょう性を確認できるサービスを開始



サイバー犯罪の手口～偽サイト

偽サイトの被害防止策

その他、ウェブサイトの安全性を無料でチェックしてくれるサイトもありました

詐欺ウォール

詐欺サイト チェッカー

Powered by 詐欺ウォール

詐欺ウォールが収集したブラックリストを元に無料で気になるサイトをチェックします。

ネット詐欺かも・・・ 

<https://olvbec.bonecool.top/>

チェック

 危険なwebサイトです

チェックしたURL：
<https://olvbec.bonecool.top/>

このwebサイトは
違法サイト/詐欺サイトとして
報告されています。

webサイト判定結果変更をリクエストする前に詐欺ウォール（体験版）で精密検査を行ってください。

予防・対策

- ショッピングサイトのドメインを確認する
- 信頼のおけるショッピングサイトを利用する
- 安すぎる価格に騙されない
- 会社概要の住所や連絡先が実在するか確認する
- 支払方法が銀行振込のみだったり、振込先が外国人名や個人名の場合、かなり怪しい
- クレジットカード情報等の個人情報を入力しない

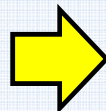
目先の安さよりも見極める力をつける！

フィッシング

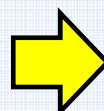
フィッシング

実在する会社等を装ったメールやショートメッセージを送りつけ、メール等に記載されたリンクから本物そっくりの**偽サイトへ誘導**し、ID・パスワード等の個人情報を**入力させて盗み取る**手口

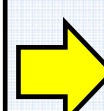
メール
SMS受信



偽サイトへ誘導
ID・パスワードの入力



ID・パスワードなど
情報が盗まれる

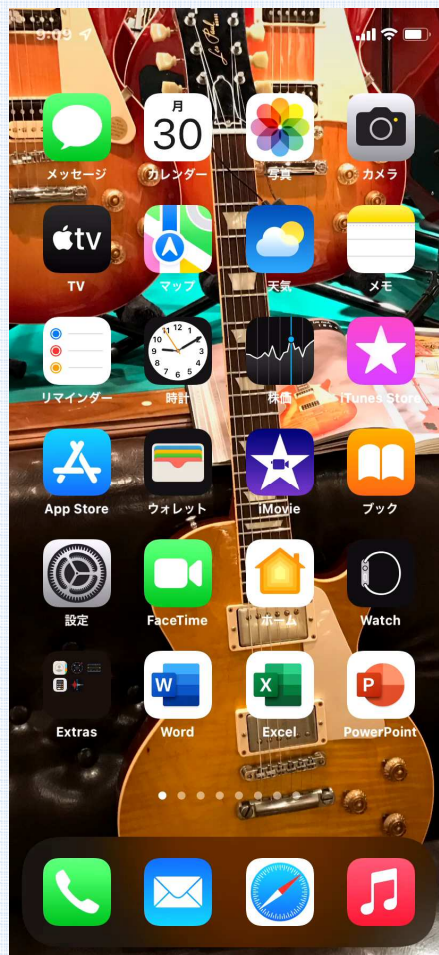


自分の口座から
お金が盗まれる



フィッシング

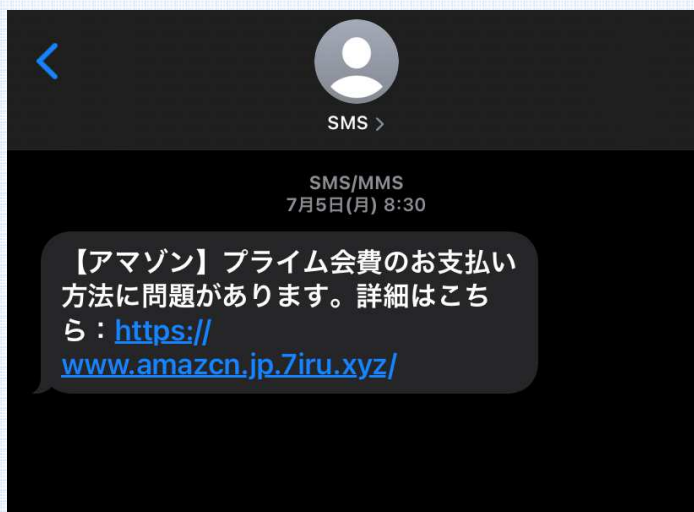
Amazonを装ったSMSからAmazonアカウント情報を盗む手口



フィッシングクイズ

次の画面のうち、正規のSMSはどれでしょう？

A



B



C



正解は . . .



フィッシングクイズ答え合わせ

<  SMS >
フィッシング!!

SMS/MMS
7月5日(月) 8:30

【アマゾン】プライム会費のお支払い
方法に問題があります。詳細はこち
ら: <https://>

www.amazon.jp.7iru.xyz/

騙すために付け加えた文字列

正規URL = <https://www.amazon.co.jp>

フィッシングクイズ答え合わせ

<  MSMKT >
フィッシング!!

SMS/MMS
6月24日(木) 17:29

不正なアクティビティが検知されました為、dアカウントの利用が制限されております。必ずご確認ください。

[docomo.jp/cz.xyz](https://www.nttdocomo.co.jp/cz.xyz)

騙すために付け加えた文字列

正規URL = <https://www.nttdocomo.co.jp>

正規SMS

正規URL = <https://www.amazon.co.jp>

[amazon.co.jp/a/c/r?
k=184a298dfeed4bcc9f3f8e4a4d
7351e6-3bca](https://www.amazon.co.jp/a/c/r?k=184a298dfeed4bcc9f3f8e4a4d7351e6-3bca)

Amazon: 40, JPのサインイン試行。
リンクをタップして対応してください。

よくある騙しパターン

適当な文字列

https://www.●●●co.jp.△△△.xyz/

正規のドメインと同じ文字列

amazon、nttdocomoなど

トップレベルドメインが違う

https://www.●●●.com/

正規のドメインと似た文字列

amazcn、nttdocamoなど

URLやドメインが正規のものか確認してください！

フィッシングクイズ



どっちが本物？

< > SMBCダイレクト
https://smbcezaco.jp.com

SMBC SMBCグループ

三井住友銀行 SMBC
トップ

SMBCダイレクトログイン

第三者に利用される恐れがあります。本人使用じゃない場合、迅速にデバイスロックを実施してください。[くわしくはこちら](#)

SMBCダイレクトの失効やアクセスを通知する当行を騙った不審なショートメッセージにご注意ください。「[くわしくはこちら](#)」

店番号 口座番号

または

契約者番号 -

※契約者番号とは？

10:34 direct.smbc.co.jp

SMBC SMBCグループ

三井住友銀行 SMBC
トップ

SMBCダイレクトログイン

【ご注意ください】
三井住友銀行を偽る、ショートメッセージ(SMS)が多発しています。
絶対に暗証番号・電話番号などを入力しないでください。 SMBC 三井住友銀行

SMBCダイレクトへのログインや電話番号の入力を求める不審なサイトへ誘導するショートメッセージやメールにご注意ください。「[くわしくはこちら](#)」

一部のAndroid端末をご利用のお客様について、W7305のエラーが起きています。「[くわしくはこちら](#)」

[SMBCダイレクトの登録がお済みでないお客さま](#)

店番号 口座番号

または

契約者番号 -

フィッシングクイズ



どっちが本物？

🔒 fuku.vn.com 🔗

本人確認

☐ 本人情報入力

会員番号または申込代表口座番号 必須

☐ 会員番号でログイン

☒ 店番+口座番号でログイン

申込代表口座の「キャッシュカード」に記載された店番、口座番号を入力してください。



🔒 direct.fukuokabank.co.jp 🔗

ログイン情報入力

☐ 初回利用登録がお済みのお客様

会員番号または申込代表口座番号 必須

☐ 会員番号でログイン

☒ 店番+口座番号でログイン

申込代表口座の「キャッシュカード」に記載された店番、口座番号を入力してください。



フィッシングに関する注意喚起動画



予防・対策

- SMSのリンクを絶対に開かない
- 正しいドメイン名か確認する
- 基本的にSMSの内容を信用しない
- なりすましのメールにも注意
- 正規サイトをブックマークに登録し、そこから接続する
- リンクを開いたとしても、ログイン情報やカード情報などを入力しない



どんな文面でもとにかく慌てない！落ち着いて考える！

当选金詐欺

当選金詐欺

★★当選おめでとうございます！
★★2億3000万円！

本サイトをご利用の皆様の中から賞金があたる
恒例の抽選会もう10回目！

今までに9人もの億り人が出ています。今回
は、あなたが見事★★1等★★2億3000万円！！
★を獲得いたしました。おめでとうございます！

賞金をお受け取りいただくため手続きをお願い
します。以下のURLより、当選者専用のウェブ
ページにアクセスし、賞金を振り込む口座など
をご登録ください。

このメールは送信専用となっておりますので、
ご返信やお問い合わせは当選者専用ページから
お願いします。

当選者専用ウェブページはこちら

<https://xxxxxxxxxx.xxx/xxxxx>

本メールは送信専用です



こんなメッセージやメールが来たことはないですか？



当選金詐欺とは？

高額な金額が当選したと嘘のメール等を送り付け、当選金を受け取るには手数料がいるなどと理由をつけてお金をだまし取る手口。
もちろん高額な当選金を受け取れない。

予防・対策

- 世の中そんなうまい話はない
- そもそも勝手に大金が当たるはずがない
- 「もしかしたら？」という欲は捨てる
- 絶対にリンクを開かない
- 連絡先に連絡しない
- 画面が消えない場合は、パソコンの再起動

メッセージを受け取っても無視すれば大丈夫！

サポート詐欺

サポート詐欺

こんなときどうする？



ビービー!

ビービー!



サポート詐欺とは？

パソコン画面に突然「ウイルスに感染した」などと偽のセキュリティ警告を表示させて不安をあおり、表示された電話番号に電話をかけさせ、サポート料金等をだまし取る手口

ファイル(F) 編集(E) 表示(V) VM(M) タブ(T) ヘルプ(H) | [Icons] | [Icons]

Ubuntu 64 ビット

アクティビティ

3月15日 17:51 [Icons]

A [Icons]



新しいタブ

← → ↻ 🏠 🔍 Google で検索、または URL を入力します

🔖 ブックマークをインポ... 🦊 Firefox を使いこなそう

⚙️

Firefox

Google で検索、または URL を入力します

Hotels.com
広告

Trivago
広告

★ @amazon

dolphin-ap...

goldfish-a...

acquainte...

z4r6g9i9.s...

s3.ap-nort...





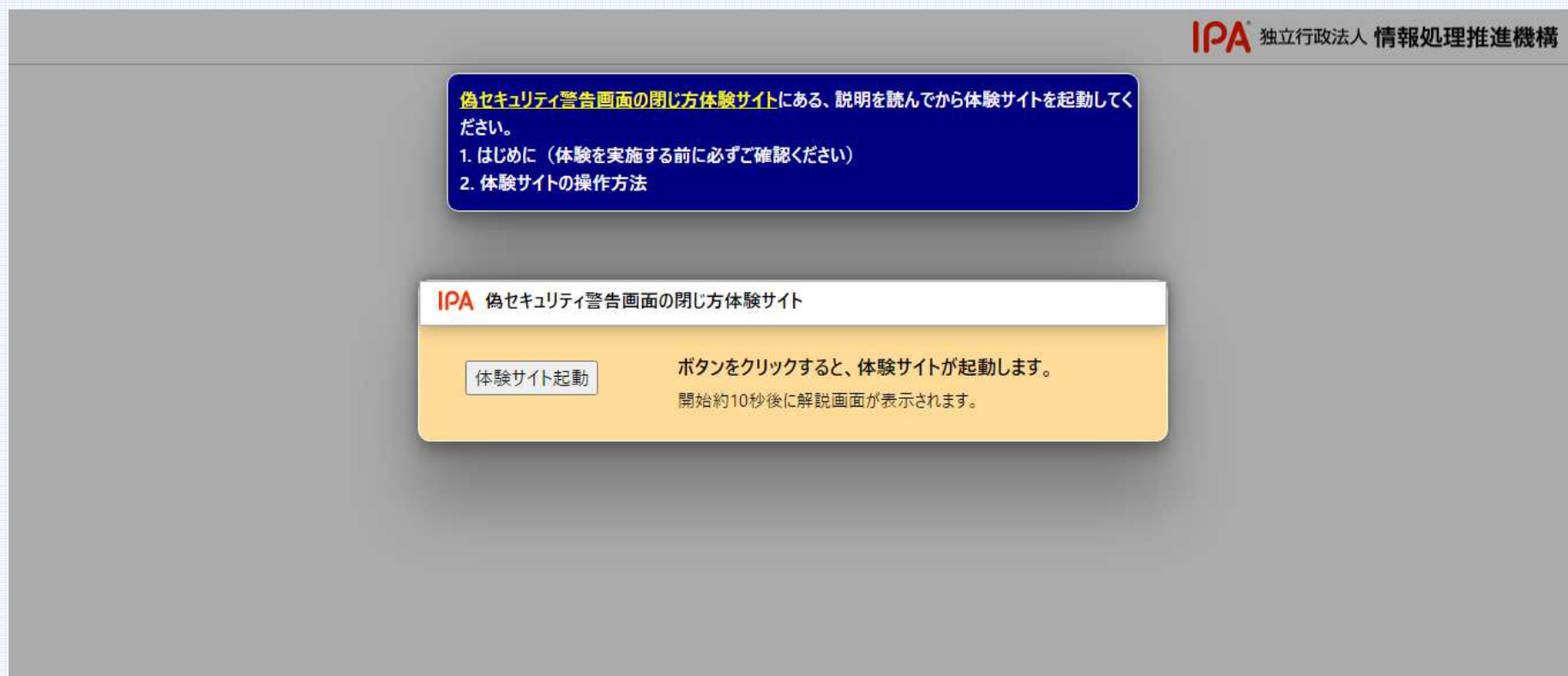
画面に表示の番号に、電話をしました。

警視庁 生活安全部
サイバー犯罪対策課

IPA（独立行政法人情報処理推進機構）

偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト

<https://ipa.go.jp/security/anshin/measures/fakealert.html>



The screenshot shows the IPA website interface for the 'Fake Security Alert Closure Experience Site'. At the top right, the IPA logo and name 'IPA 独立行政法人 情報処理推進機構' are visible. A blue instruction box contains the following text: '偽セキュリティ警告画面の閉じ方体験サイトにある、説明を読んでから体験サイトを起動してください。' followed by a numbered list: '1. はじめに（体験を実施する前に必ずご確認ください）' and '2. 体験サイトの操作方法'. Below this, a white header bar reads 'IPA 偽セキュリティ警告画面の閉じ方体験サイト'. The main content area has an orange background and features a button labeled '体験サイト起動' (Start Experience Site). To the right of the button, text states: 'ボタンをクリックすると、体験サイトが起動します。' and '開始約10秒後に解説画面が表示されます。' (After clicking the button, the experience site will start. The explanation screen will be displayed after approximately 10 seconds).

ちよつと待って！

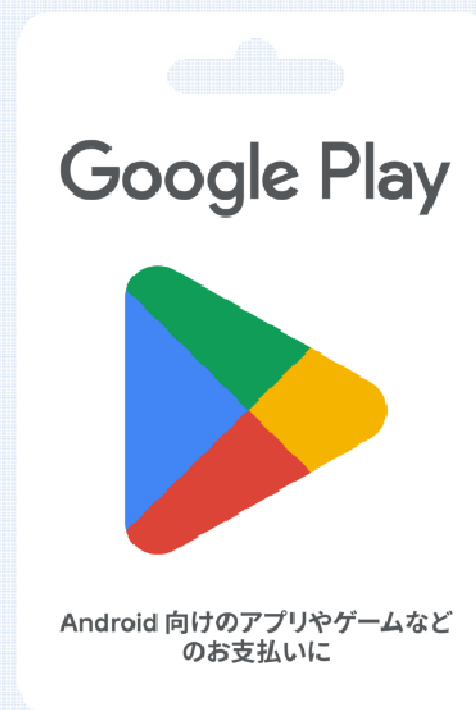


- 慌てない！まず、落ち着いて！
- 画面に書いてある電話番号には**絶対に電話しない！**
- サポート詐欺の画面は「閉じる」や「×」を押しても画面が消えないことが多いので、**ブラウザを閉じるか、パソコンを再起動**しましょう。
- その後、ウイルス対策ソフトなどで**ウイルスチェック**してください。

KEEP OUT KEEP OUT KEEP OUT KEEP OUT KEEP OUT KEEP OUT

プリペイドカード (電子マネー)

プリペイドカード（電子マネー）



コンビニや家電量販店などで販売されています。

ショッピングサイトでの買い物や、音楽、ゲーム等のデジタルコンテンツの購入などに利用されています。

「プリペイドカード（電子マネー） を買ってきて」は詐欺！！

例えば・・・

- サポート詐欺におけるウイルス除去代名目や今後のサポート代名目
- 当選金詐欺における手数料名目
- 出会い系サイトで相手の連絡先を教えてもらうために、言われるがまま次々と購入
・・・など

プリペイドカード（電子マネー）

どのようにしてお金を
だまし取られるの？



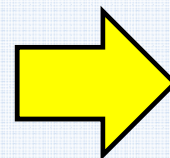
プリペイドカード（電子マネー）

通常利用時

10000円

ギフト券番号：





自分のアカウント

ギフト券を登録

ギフト券番号を入力

ABCD-1234EF-5GHIJ

ギフト券の残高： **10000円**

プリペイドカード裏面の銀色部分をコインで削ってギフト券番号を確認

登録用ページでギフト券番号を入力すると、金額が反映され、利用できるようになる

プリペイドカード（電子マネー）

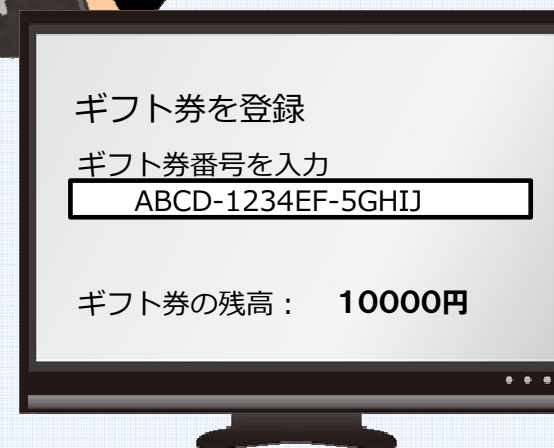
詐欺の場合



②ギフト券番号を教える
よう仕向ける



①様々な理由をつけてプリ
ペイドカードを買わせる



③入手したギフト券番号を、犯罪者
のアカウントで登録
登録された金額をすぐに使用

もう一度言います

「プリペイドカード（電子マネー）を買ってきて」は
詐欺！！

ギフト券番号は絶対に他人に教えない！！

SNS型投資詐欺



ある日、才場さんのフェイスブックにマリアという外国人女性から友達申請がありました。

その後、友達になり、LINE上でメッセージのやり取りをしていました。

マリアとしばらくやり取りしていると、マリアが「私は投資をされていて、かなり儲かっている。あなたも投資をやってみない」と言いました。





元々投資に興味があった才場さんは、物は試しと思い、マリアが勧める投資アプリに登録して、マリアが指定する口座にひとまず10万円を入金しました。

すると、数日で投資した10万円が15万円になったので、これならもっと儲けることができると思った才場さんは、マリアにもっと入金したいと伝え、指定の口座にさらに500万円を入金しました。

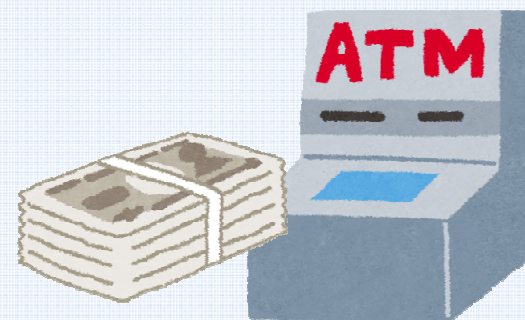




2か月後、アプリで儲けを確認してみると、残高が900万円にもなっていました。才場さんは、早速利益分の400万円を引き出そうと思い、マリアに400万円引き出して欲しいと頼みました。

すると、マリアは「海外口座なので、お金を引き出すには手数料が100万円必要です。」と言いました。

才場さんは、高いなと思いながらも、手数料分を差し引いても利益が出ていたので手数料として100万円入金しました。



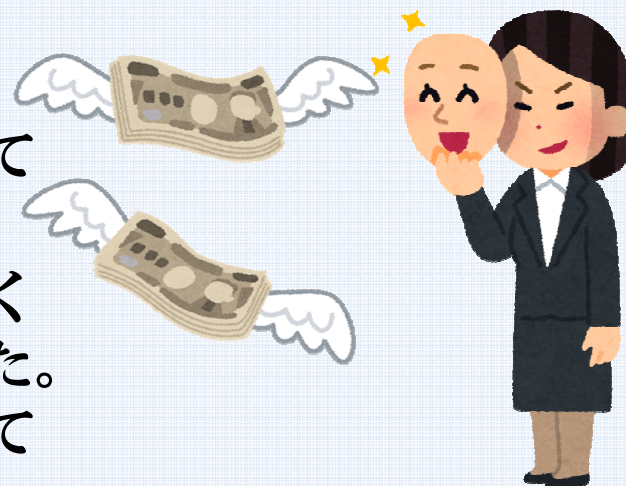


ところが、数日後、香港の捜査機関と名乗るところから連絡があり、「口座をマネーロンダリングの疑いで差し押さえた。100万円払わないと全部没収の上、逮捕されるかもしれない。」と言われました。

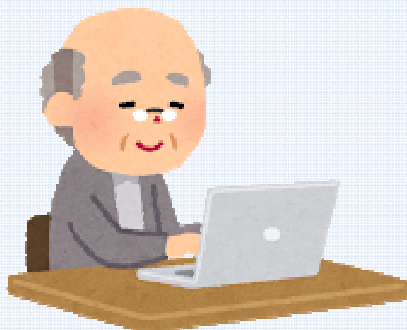
才場さんは、大変なことになったと思って急いで100万円を入金しました。

しかし、それ以降マリアと連絡がつかなくなり、登録したアプリも偽物とわかりました。

もちろん、これまで入金したお金は返ってきませんでした。



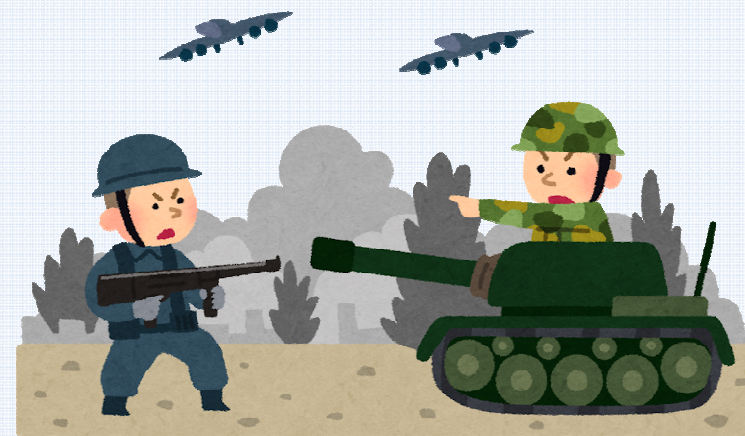
SNS型ロマンス詐欺



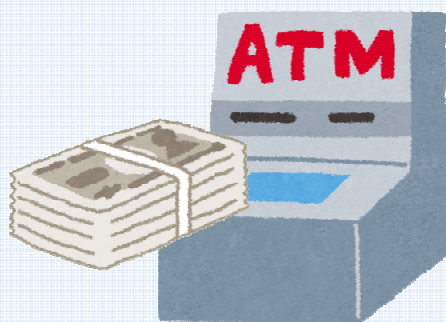
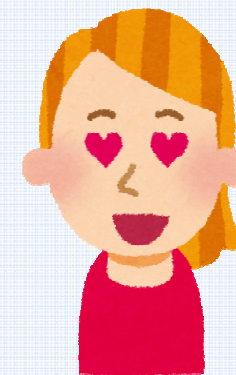
ある日、才場さんのフェイスブックにマリアという外国人女性から友達申請がありました。

何気に友達になり、その後メッセージのやり取りをしていました。

マリアとしばらくやり取りしていると、マリアが「私は米軍人で今シリアにいる。まもなく軍を除隊するから、日本に行ってあなたと結婚したい。除隊する際に報奨金として500万ドル（約5億5000万円）もらえるから、その一部をあなたに受け取ってほしい。」と言いました。



さらに、マリアは「これからあなたのところへ荷物とお金を送ります。だけど、シリアでは私の口座からはお金を引き出すことができないので、荷物の送料の40万円を出して欲しい」と言いました。

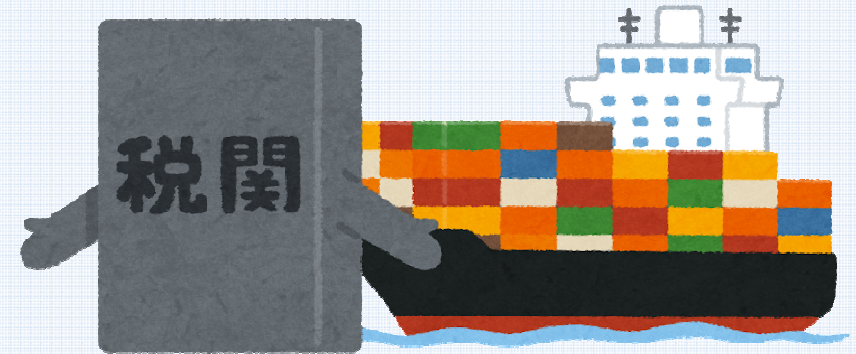


才場さんは、マリアに恋愛感情を抱いていたので、マリアと結婚するために送料を出してあげることになりました。

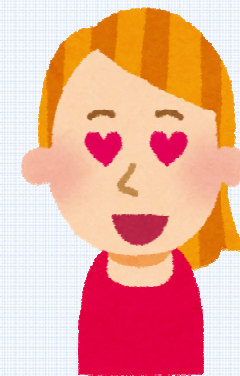
そして、マリアから指定された外国人名義の銀行口座に40万円を振り込みました。

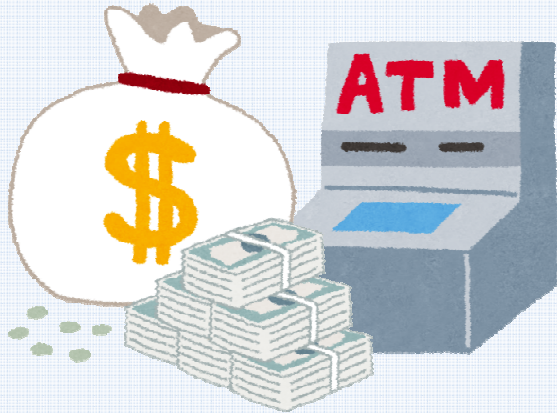
ロマンス詐欺

すると、後日マリアから「荷物を送ったが、大金が入っていたため税関で止められてしまった。税関を通すためには、手数料として8万ドル（約880万円）払わないといけない。荷物が届けばその中にお金が入っているから、とりあえず立て替えておいてほしい。」と言いました。



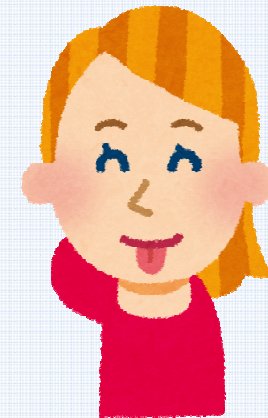
さらに、マリアは「これからシリアを出て日本に行く。だけどクレジットカードも使えないから飛行機代を出して欲しい」と言いました。





才場さんは、早くマリアに会いたい一心で、荷物の手数料と飛行機代として85,000ドル（約930万円）を指定された外国人名義の銀行口座に振り込みました。

ところが、その後マリアとは連絡がつかなくなり、大金が入っているはずの荷物も届くことはありませんでした。



予防・対策

- SNSで知らない人と簡単に友人にならない
- 会ったこともない人を信用しすぎない
- 相手が誰かもわからないのにお金を入金しない
- 儲け話を他人にするはずがない
- 海外口座への入金はしない
- 投資先やアプリの真偽をネットで検索してみる

旨い話には必ず罠がある！

LINEによる被害勧誘の遮断措置

～ 犯人側から一方的に送られてくる投資話の持ちかけ（宣伝広告）や グループ招待が届かないようにするための設定方法 ～



設定方法

[ホーム]>[設定]>[プライバシー管理]をタップ→[メッセージ受信拒否]をオン

メッセージ受信拒否を オンにする

【効果】

登録している友だち以外からのメッセージの受信が拒否されるため、犯人側から一方的に送られてくる投資話が届かなくなります。





LINEによる被害勧誘の遮断措置



設定方法

[ホーム]>[設定]>[友だち]をタップ→[友だちへの追加を許可]をオフ

友だちへの追加を許可をオフにする

【効果】

何らかの経緯で、あなたの電話番号を保有しているLINEユーザー（犯人側）であっても、自動的に友だちに追加（グループへの招待）することができなくなります。

注意！ この方法は、犯人側からの一方的な送り付けを遮断するものです。

投資等に興味を抱き、自ら宣伝広告等を検索して相手LINEアカウントに勧誘される場合には、自分でそれを拒否する以下方法がないので注意してください。

- ※ 上記を設定するとLINEの「友だち」以外からの不審なメッセージは届きません。
- ※ 上記の方法で新たに「友だち」追加したい場合や「友だち」以外のメッセージを受け取りたい場合は、再度設定を変更する必要があります。
- ※ 設定はいつでも変更できます

出典：LINE みんなの使い方ガイド「投資に勧誘された…それ、詐欺です！」

サイトURL：<https://guide.line.me/ja/security/investmentfraud.html>

3 身近にある脅威

～SNS編～

場所を特定できる何気ない投稿

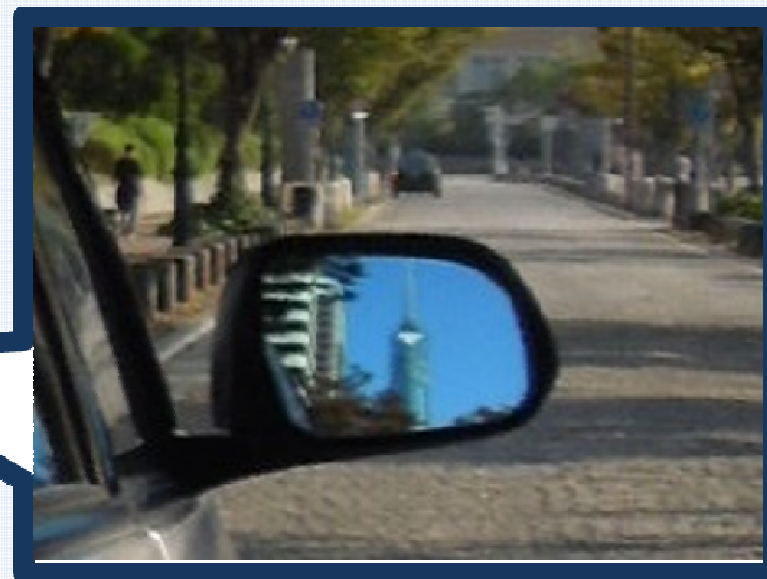


うらめし子 @uramesiko318 • 21分

今日はお出かけ♪



場所を特定できる何気ない投稿



場所を特定できる何気ない投稿



写りこみによる特定の事例

アイドルへのわいせつ事件で逮捕の男 SNS投稿の「瞳の景色」で住所特定か

[2019年10月8日 22:28]

いいね! 0

シェアする

ツイートする

アイドル活動をする20代の女性にわいせつな行為をしたとして警視庁が逮捕した男が、被害者の住所を特定するため、会員制交流サイト（SNS）に投稿された女性の顔写真から「瞳に映った景色を手掛かりにした」と供述していることが8日、捜査関係者への取材で分かった。

捜査関係者によると、男はさいたま市の無職の26歳の男で、SNSの女性の顔写真で瞳に映った駅の景色を確認し、検索大手グーグルのサービス「ストリートビュー」で特徴が似た駅を発見して待ち伏せ、後をつけて自宅マンションを割り出したという。

さらに女性が投稿した動画を見て、室内の様子などから部屋の位置まで突き止めたとされる。容疑者は女性の熱狂的なファンで、コンサートによく足を運んでいた。

警視庁は9月17日、東京都内にあるマンションの敷地で女性の体を触り、軽傷を負わせたとして強制わいせつ致傷などの疑いで逮捕。東京地検は8日に起訴した。

配信による特定の事例

高田馬場で女性刺され死亡 男逮捕、ナイフ2本所持一ネット ライブ配信中か・警視庁

時事通信 社会部

2025年03月11日13時10分 配信



女性が刺された現場を調べる警視庁の捜査員ら＝11日午前、東京都新宿区

11日午前9時50分ごろ、東京都新宿区高田馬場の駅前の路上で、20代ぐらいの女性が刃物で刺され、病院に運ばれたが間もなく死亡した。警視庁は殺人未遂容疑で、現場にいた40代の男を現行犯逮捕。「殺そうとは思っていませんでした」と話しているといい、同庁は今後、容疑を殺人に切り替え、刑事責任能力の有無を含め、動機などを詳しく調べる。

「駅に着いたとの配信を見て周囲を探した」旨供述している！

投稿する場合

- 自宅や職場、その周辺など**場所を特定されるような情報**がないか確認して投稿する
- 投稿内容は、**不特定多数の人に見られている**ことを想定する
- 他人を傷つけたり、馬鹿にする内容の投稿はしない
- **匿名だとしても必ずバレます**

画面の先にも「ひと」がいることを考える！

閲覧・拡散する場合

- ◆ 情報元は**信頼できる**か確認する。
- ◆ 投稿内容は、**いつの時点の情報か**確認する。
- ◆ 投稿内容は、誰かの**プライバシーや名誉を侵害**している内容ではないか考える。
- ◆ 拡散する必要がある情報か、そして「自分」が**拡散すべき情報**か考える。

リポストにも投稿者としての責任がある！

トラブルに巻き込まれないために

- ◆ 住所などの**個人情報**を公開しない
- ◆ **本人の許可なく**、友人、知人の情報を書かない
- ◆ 仕事の内容など**守秘義務**のある情報を書かない
- ◆ 事実と異なる内容、**デマ**を書かない
- ◆ 見知らぬ人物の「友達リクエスト」を承認しない
- ◆ S N S で知り合った人を安易に信用しない

リアルな世界でできないことはしない！

4 闇バイト

闇バイト



闇バイトとは

SNSや掲示板などで、**短時間で高収入**が得られるなど**甘い言葉で募集**し、それに応募すると、詐欺の受け子や出し子、強盗の実行犯などの**犯罪組織の手先**として利用され犯罪者となってしまいます。

ルフィ事件

2022年から全国各地で発生した強盗・強盗殺人等の事件は、“ルフィ”を名乗る人物が、SNSを通じて実行犯を募り、スマホで指示を出して犯行を行わせたとされるもの。

事件は、全国14都道府県で発生したと言われ、SNSに掲載された異常に高収入なアルバイト＝“闇バイト”に申し込んだ者が、テレグラムにより指示を受けていたという共通点があると言われています。

若い世代が“闇バイト”に多数申し込んでいた

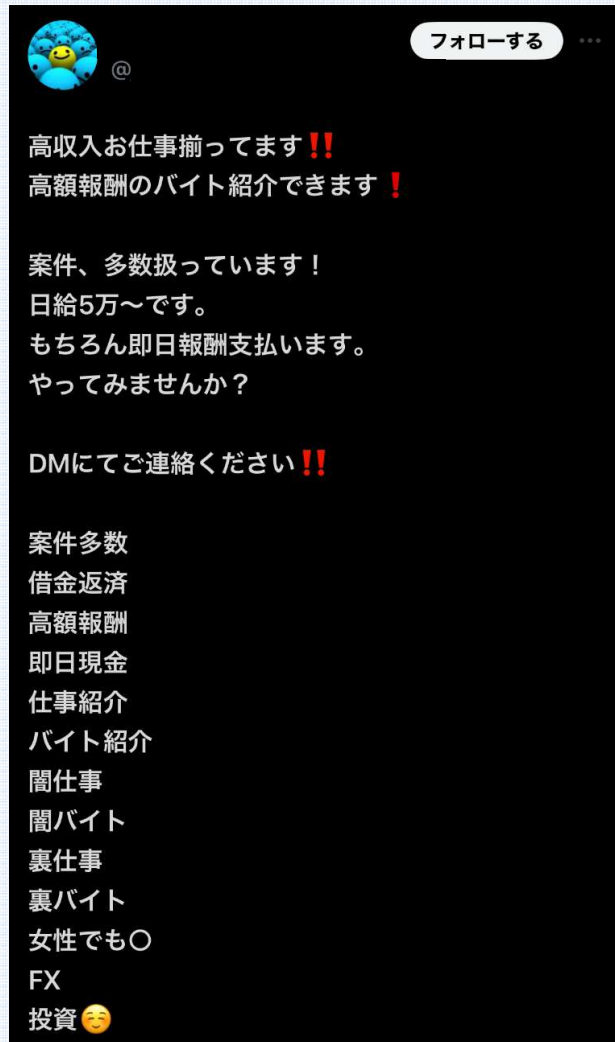
福岡県でも・・・

福岡市内の高校に通う少女（18歳）が窃盗罪で逮捕されました。

少女は、福岡市内の80代の女性のキャッシュカードを不正に入手し、コンビニのATMで3回にわたって、あわせて50万円を引き出したとされています。

少女は、「SNSで調べていたら自分にもできそうな仕事があったので応募した」と話し、闇バイトとみられます。

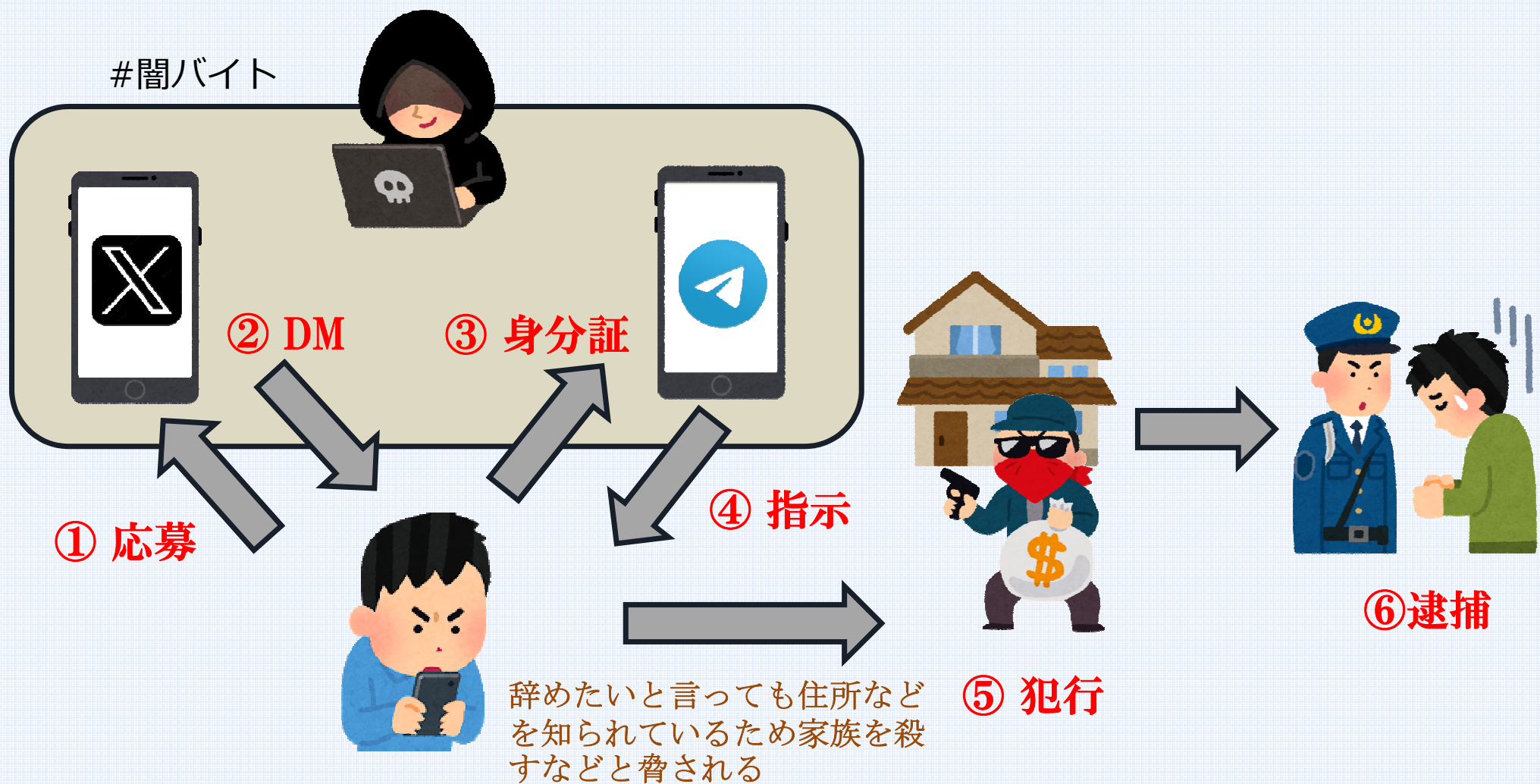
「バイト」という名前が罪の意識をなくしている？



主な犯罪

- 振り込め詐欺
 - 強盗
 - 名義貸し
 - 薬物の運び屋
 - 盗品等の受け子
 - 他人口座の出し子
 - 売春
- ・・・等

闇バイト



特徴

- 主に**SNS**（XやInstagram）で募集
- 具体的な仕事内容を記載していない
- 「**初心者大歓迎！**」「**高額報酬**」などの文言
- SNSのDMで連絡を取り、その後**Telegram**などでやり取り
- **身分確認**と称し免許証などのデータを送らせる
- **保証金**が必要として数万円～数十万円を要求される
- やめたいと言うと「身元をバラす」などと**脅される**

一度やってしまうと抜けられない！

闇バイト

福岡県警察 × 警視庁

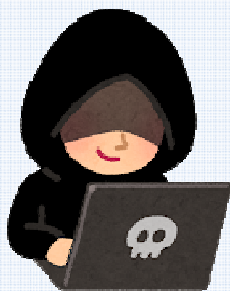
5 パスワード（口座）管理

手口を知る

リスト型攻撃・・・流出したパスワードの**リスト**を使って、
他のサービスでログインを試みる攻撃

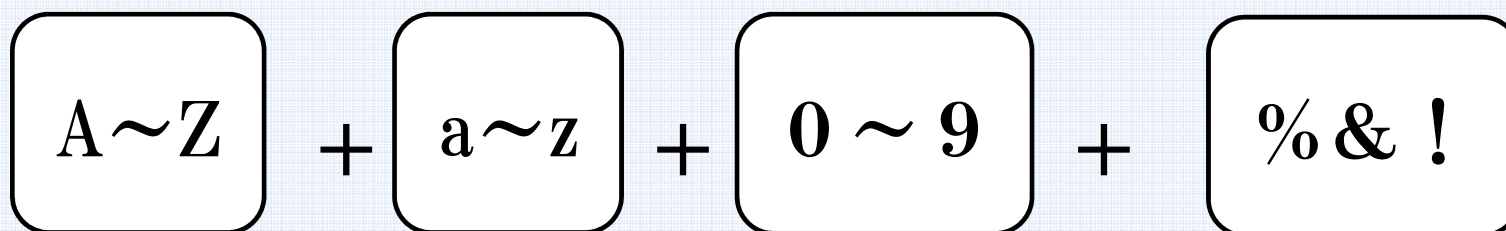
総当たり攻撃・・・全ての文字などの**組み合わせ**を試す攻撃

辞書攻撃・・・パスワードによく使われる**文字列を集めて辞
書化**したものを使い、不正にログインできな
いかを試みる攻撃



パスワードを設定する場合の留意事項

ログイン用パスワードは、
英大文字小文字＋数字＋記号で10桁以上



26種類

26種類

10種類

26種類

探し当てるまでに膨大な時間がかかるようにする！

パスワードを設定する場合の留意事項

	〇〇サイト	〇〇銀行	〇〇ペイ	〇〇クレジット
使い回し	password	password	password	password
おしりだけ 違う	password1	password2	password3	password4
法則性あり	〇〇pass	〇〇pass	〇〇pass	〇〇pass

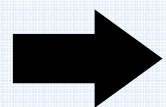
サービス間でのパスワードの使い回し等はしない！

パスワード管理

パスワードを適切に保管する



password



パスワードを書いた付箋

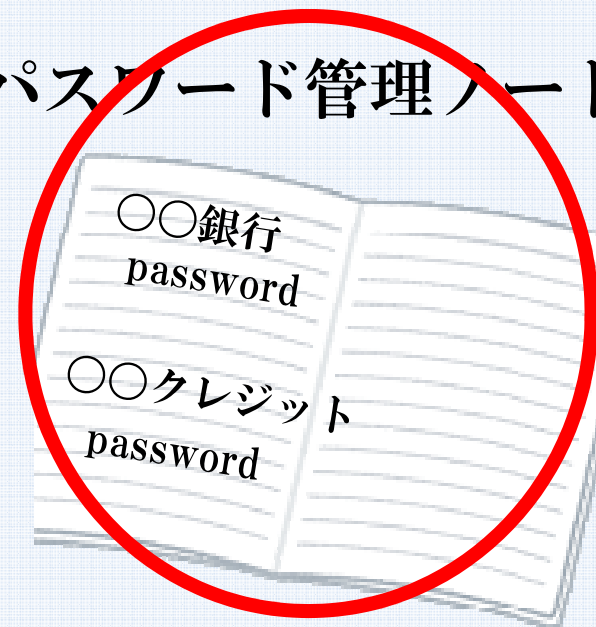
①IDパスワードを
記録しますか？

③次回以降
自動入力



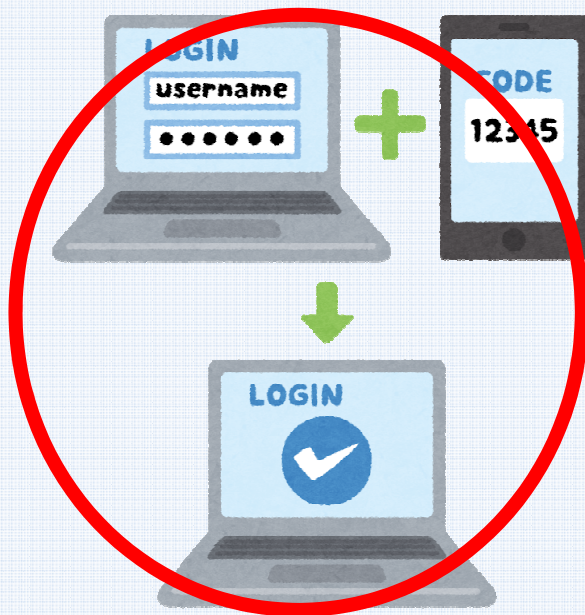
②入力が面倒だから
「Yes」と

パスワード管理ノート



多要素認証を利用する

二段階認証



顔認証



指紋認証



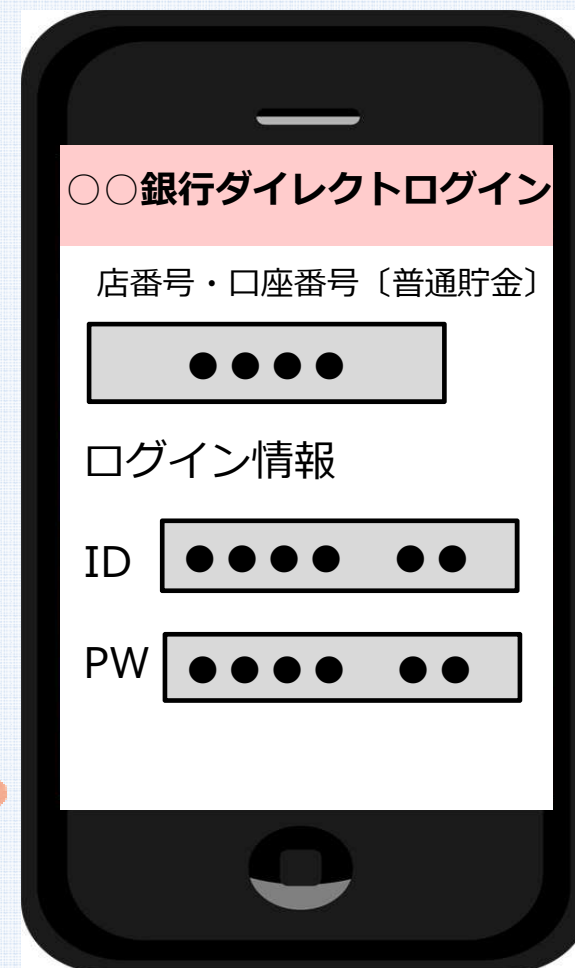
口座譲渡は犯罪です

- ・ 自分や他人名義の通帳・キャッシュカードを譲り渡す（譲り受ける）行為
- ・ ネットバンキングのログインID・パスワードの情報を譲り渡す（譲り受ける）行為

犯罪収益移転防止法違反！

1年以下の懲役

100万円以下の罰金



6 相談窓口・サイト

サイバー犯罪に関する相談窓口

サイバー犯罪被害の届出や相談

最寄りの警察署へご相談ください。

<https://www.police.pref.fukuoka.jp/keisatsusyo/>



サイバー犯罪に関する情報提供の受付

いただいた情報は、警察活動に反映させていただきます。

いただいた情報への返信は行っておりません。

<https://www.police.pref.fukuoka.jp/somu/koho/joho-hitec.html>



サイバーセキュリティに関するサイト

福岡県警察サイバー犯罪対策課

<https://www.police.pref.fukuoka.jp/seian/cyber/>



独立行政法人 情報処理推進機構

<https://www.ipa.go.jp/security/>



日本サイバー犯罪対策センター

<https://www.jc3.or.jp/>



フィッシング対策協議会

<https://www.antiphishing.jp/>



迷惑メール相談センター

<https://www.dekyo.or.jp/soudan/>





fukkei_cyber



@fukkei_cyber



ご清聴、
ありがとうございました！