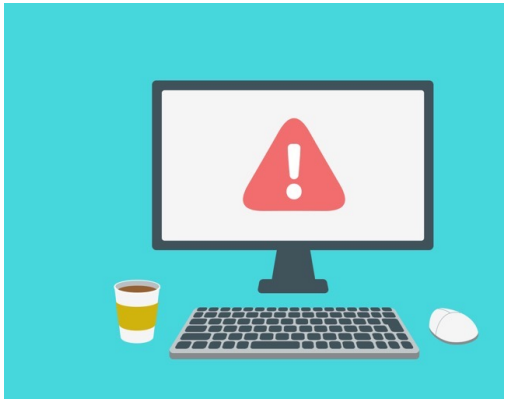
消費者月間記念講演

今ネットの世界で何が起きているのか

～ネット犯罪、トラブルへの対処法～

2023年5月30日（水）
14：00～15：30
WEB110.COM
吉川誠司



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 2023」

https://www.ipa.go.jp/security/10threats/10threats2023.html

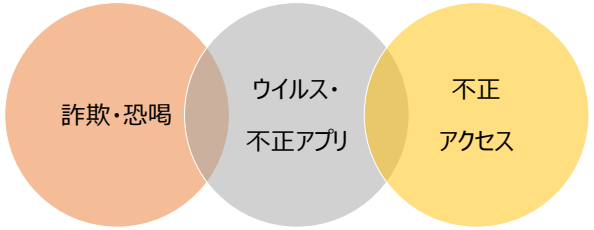
1. フィッシングによる個人情報等の詐取
2. ネット上の誹謗・中傷・デマ
3. メールやSMS等を使った脅迫・詐欺の手口による金銭要求
4. クレジットカード情報の不正利用
5. スマホ決済の不正利用
6. 不正アプリによるスマートフォン利用者への被害
7. 偽警告によるインターネット詐欺
8. インターネット上のサービスからの個人情報の窃取
9. ワンクリック請求等の不正請求による金銭被害

解説

2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案からIPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が審議・投票を行い、決定したもの。

日々ばらまかれているフィッシングメールの状況

金銭被害につながる犯罪の手口・手段



落とし穴である確率が高い３つのパターン

1. 一方的に届いたメールやSMSのリンク先
2. ブラウザに突然表示される「ウイルス感染してるよ」的な偽セキュリティ警告
3. うまい儲け話し

1 一方的に届いたメールやSMSのリンク先

宅配の不在配達通知等を装った偽ショートメッセージ（SMS）の手口

ついクリックしてしまいそうになるショートメッセージ

国税庁をかたる偽SMS

携帯会社をかたる偽SMS

宅配便をかたる偽SMS

国税庁を語る偽SMSのリンクをクリックした場合

偽のWebサイトへ誘導して個人情報、クレジットカード情報などを入力させようとする

スマホのOS別　手口と想定される被害

偽SMS

お荷物のお届けにあがりましたが不在の為持ち帰りました。ご確認ください。http://[redacted].duckdns.org

詐欺　不正アプリ　不正アクセス

Androidの場合

不正アプリをインストールさせようとする

- 同様の偽不在通知の大量送信
- キャリア決済の悪用
- フリマなどのアカウントの無断作成
- Googleアカウントへの不正ログイン

詐欺　不正アクセス

iPhoneの場合

フィッシングサイトで電話番号と認証コード、Apple IDとパスワード、銀行の認証情報等を入力させようとする

- キャリア決済の悪用
- Apple IDへの不正ログイン
- ネットバンキング等への不正ログイン

詐欺　不正アプリ　不正アクセス

Androidの場合

SMSのリンクをタップした後の画面遷移

Androidの場合

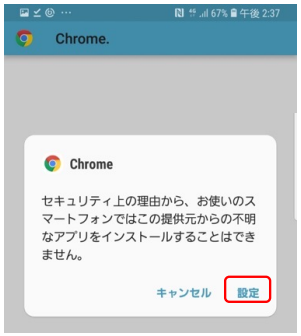
白紙ページでChromeのアップデートを促すパターン

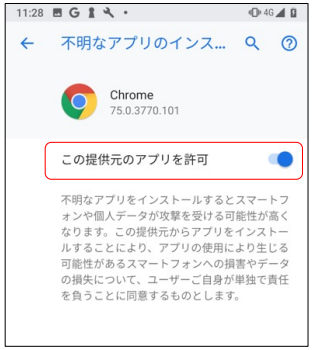
OKを押すと.apkファイルがダウンロードされる

「開く」をタップするとアプリのインストール手順に進む

Androidの場合

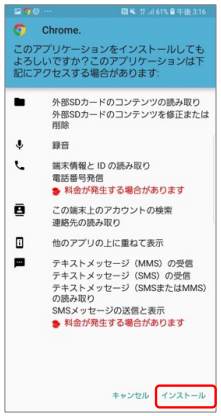
不明なアプリのインストール許可が**OFF**の場合は自分で**ON**にする必要がある
※表示内容は、Androidのバージョンによって異なる





不正アプリをインストールするまでの流れ

Androidの場合



相談者が「インストールはしてないと思う」と言っていても、実際には入れてしまっていることが少なくないので注意

インストールしようとするアプリが求める権限の一覧が表示される

「次へ」をタップすると、「インストール」に変わる

不正アプリをインストール時の挙動例

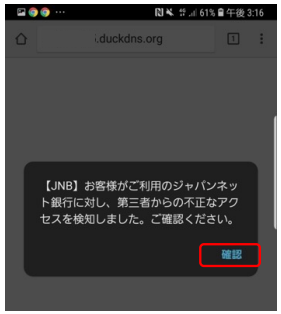
Androidの場合

「はい」をタップすると、既存のメッセージアプリに取って代わる

不正アプリをインストール後のさらなる展開

Androidの場合

アプリのインストール後に偽の警告メッセージが出ることもある



フィッシングサイトで入力するとさらなる被害に繋がる

不正アプリをインストールしてしまった場合の影響

Androidの場合

ショートメール機能の悪用
- 不正アプリをインストールしたスマホから、同じ内容のSMSが多数送信される。
- 送信先は被害端末内に登録されていた連絡先情報（電話番号）ではない。
- SMSを受信した相手から、荷物に関する問い合わせ電話やSMSが複数届く。
- SMS送信に伴う料金が発生する。

アプリによるアクセス権限の不正使用
- キャリア決済サービスにて、身に覚えのないiTunesカード等の請求が発生したという相談を確認している。
- アドレス帳データが外部に送信されている可能性がある。
- フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等にアカウントを勝手に作成され、不正使用されたという相談を確認している。

スマホと紐づくアカウントの不正使用の可能性
- Googleアカウントに身に覚えのないアクセス履歴があったという相談を確認している（アプリとの関連性は不明）。

私のiPhoneにも届いたので、
IPA安心相談窓口と注意喚起ページを教えてみた。

不正アプリをインストールしてしまった場合の対処

Androidの場合

➢ スマホを機内モードにする
- SMSが勝手に送信されないための応急処置としてオフラインにする

➢ 不正アプリのアンインストール
- 相談例では、Chromeアプリに扮しているケースが多い

➢ スマホの初期化
- 不正アプリによる端末本体への影響範囲が不明のため、より安全な対処として初期化を行う

➢ キャリア決済の請求確認
- 身に覚えがないキャリア決済が発生していないか、携帯電話会社に問い合わせる

➢ アカウントサービス等の不正使用確認
- 不正アプリのインストール以降、携帯電話会社、フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等から登録や変更に関するメールやSMS等が届いていた場合は、当該サービス提供会社へ不正使用が発生していないか等を確認してください。

➢ アカウントのパスワード変更
- 初期化後に念のため、スマホに登録しているアプリやインターネットでログインするサービスのパスワードを変更する

インストールした不正アプリの削除方法

Androidの場合

ダウンロードした不正アプリの削除方法

<Android10の例>

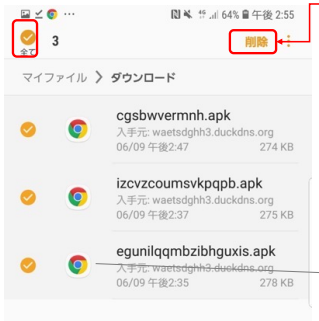
Androidの場合

※不正アプリをインストールしたことが確実な場合は最終的に初期化することになるので、このステップは不要

ダウンロードした不正アプリの削除方法

Androidの場合

※不正アプリをインストールしたことが確実な場合は最終的に初期化することになるので、このステップは不要



必ず削除ボタンかゴミ箱アイコンで削除する

※削除できたはずなのにアイコンが消えない場合は、端末を再起動すれば消える。

このアイコンをタップすると、インストール確認画面になってしまうので触らない！

iPhoneの場合

a. フィッシングサイトに誘導し、アカウント情報とギフト券番号を入力させる手口

iPhoneの場合

① 偽SMSを受信し、記載のURLをタップして、フィッシングサイトにアクセスする。
②～⑤ au IDとパスワードを入力すると、未払い料金を請求する偽のメッセージと偽の請求額が表示される。

次のスライドへ

iPhoneの場合

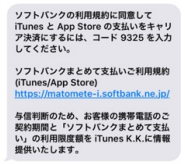
⑥～⑨ iTunesギフトカードのシリアル番号（ギフトカード番号、PINコードともいう）を入力する

b. フィッシングサイトに誘導し、アカウント認証情報とクレジットカード情報を入力させる手口

iPhoneの場合

①携帯電話番号を入力

②携帯電話会社から認証コードがSMSで届く



③届いた認証コードを入力と被害に繋がる

フィッシングサイトにアクセスしてしまった場合の対処

iPhoneの場合

サイトにアクセスしただけなら大丈夫

- フィッシングサイトが表示された場合は、画面を閉じる。
- フィッシングサイトに情報を入力をしていなければ、被害にはつながらない。

Apple IDとパスワードを入力した場合

- 速やかにパスワードの変更を実施。
- Apple IDで不正な購入がないかを確認する。

携帯電話番号と認証コードを入力した場合

- 身に覚えがない購入通知メールがキャリアから届いていないか確認。
- 身に覚えがないキャリア決済が発生していないか、携帯電話会社に問い合わせる。

被害低減に有効と思われる対処・対策

Android　iPhone

1. Apple サポートへの連絡
   キャリアから身に覚えのない決済完了のお知らせメール（呼び方はキャリアにより異なる）が届いたら、すぐにApple サポートに電話をして、本件が不正に購入されたものであることを伝える。

   Apple サポート電話番号：0120-277-535

2. キャリア決済の限度額の変更
   今後の被害低減のために、キャリア決済の限度額を低く設定しておく。

   ※ドコモのように利用規約の改正で限度額が引き上げられるということもあるので、自身の限度額は確認しておくべき。

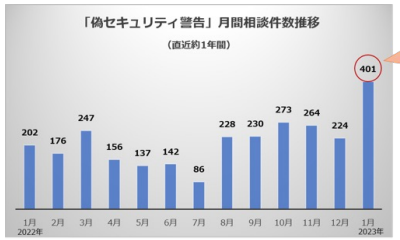
2　**ブラウザに突然表示される「ウイルス感染してるよ」的な偽セキュリティ警告**

詐欺

通称：サポート詐欺

偽セキュリティ警告

IPA安心相談窓口の相談件数が過去最多



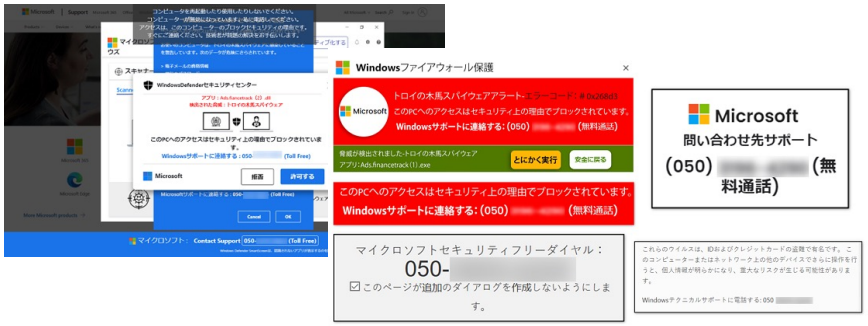
偽セキュリティ警告

サポート詐欺の手口概要

1. インターネット閲覧中に突然偽のセキュリティ警告が表示され、解決のために記載してある電話番号に電話をかけるように誘導される。
2. 電話をかけると、オペレーターに端末を遠隔操作され有償サポート契約と代金支払いへ誘導される。
3. 支払いはプリペイドカードを指定されるため、ほとんどの場合はコンビニエンスストアにそのカードを買いに行くように指示される。

偽セキュリティ警告

PCで遭遇する偽のセキュリティ警告の画面例

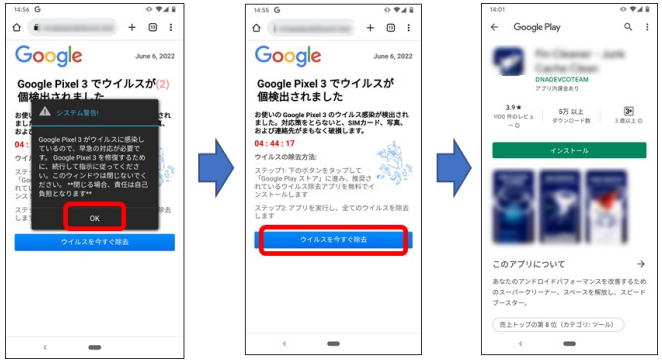


警告画面がいくつも重なって開き、しかも警告が全画面表示で固定されて「閉じるボタン」が隠されてしまい、画面を閉じることができない事例が多い。

偽セキュリティ警告

スマホで遭遇する偽のセキュリティ警告の画面例

Android



スマートフォンの動作を改善させるという説明のクリーナーアプリやVPNのためのアプリのインストール等に誘導されることが多くなっています。

偽セキュリティ警告

スマホで遭遇する偽のセキュリティ警告の画面例

iPhone

スマートフォンの動作を改善させるという説明のクリーナーアプリやVPNのためのアプリのインストール等に誘導されることが多くなっています。

偽セキュリティ警告

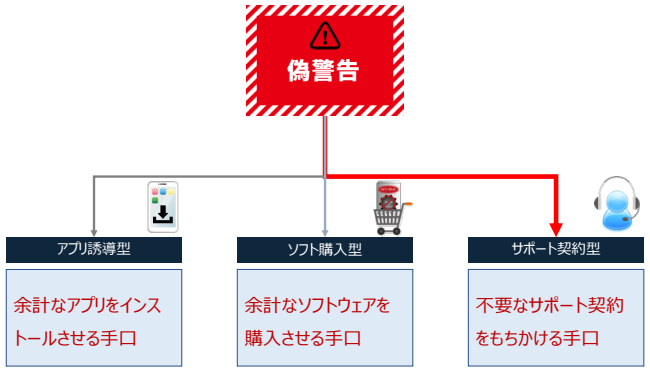
考えてみましょう

Q サイトにアクセスしただけでウイルス感染していることを検知することは可能だと思いますか？

A ウェブサイトを閲覧しただけで外部からウイルス検知することはできません。何らかのプログラムを実行させる必要があります。よってこれは実際のウイルス感染により表示されるものではなく、特定のアプリをインストールさせるための一種の広告のようなものです。

偽セキュリティ警告

偽セキュリティ警告からの３つの手口



偽セキュリティ警告

不要なサポート契約を

もちかける手口

サポート契約型

偽セキュリティ警告　サポート契約型

サポート契約をもちかける

電話をかけると遠隔操作で診断と称する作業をし、
不安をあおって有償サポート契約をもちかける

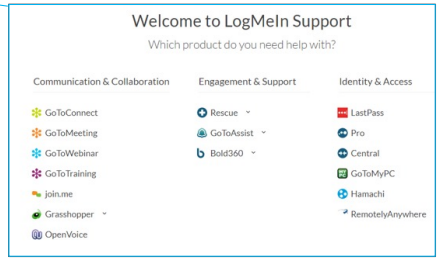
ベーシックプラン
¥X,XXX/3年
ゴールドプラン
¥X,XXX/5年
⋮

偽セキュリティ警告　サポート契約型

よく使われる遠隔操作ソフト

TeamViewer
AnyDesk
LogMeIn

最近はほとんどがLogMeIn系
遠隔操作される前に「www.support.me」と入力するように言われた場合はRescue
遠隔操作される前に「fastsupport.com」」と入力するように言われた場合はGoToAssist

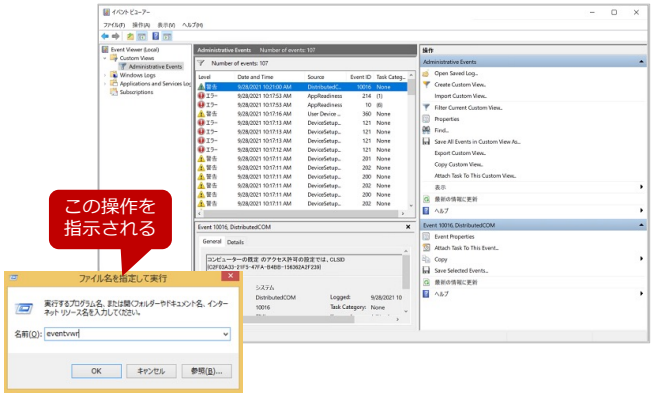


Rescue・・・・・・・・クライアント側にソフトのインストールが必要
GoToAssist・・・Webアプリケーション版はインストール不要

偽セキュリティ警告　サポート契約型

遠隔操作で何をしているか（事例）

（ファイル名を指定して実行）で「eventvwr」を実行した結果



偽セキュリティ警告　サポート契約型

次々支払わされたという相談例

電話すると、ウイルスを除去するためコンビニでGoogle Playカード５万円と１万円を購入して番号を知らせるようにという指示があり、そのようにしました。

すると「**グーグルがコロナで休業**のため別のカードを再度購入し番号を提示するように。」と言われる。

今度は「返金するために20万円のクレジットカードが必要だが、５万のビットキャシュカードを2枚購入して合計22万円にして、そこから６万引くと16万になるので、あと4万円の別のカードを購入して提示ください。１週間後に返金します。」と言われる。

言われたとおり入力すると、「入力ミスでブロックされたので、再度４万円の別のカードを購入するように。」と言われ、そこでおかしいと気づきました。

どうも詐欺にあったみたいです。合計26万だまし取られたようです。

偽セキュリティ警告　サポート契約型

契約を拒んだときの嫌がらせ-その１

画面反転攻撃

4万円分のGoogle Playカードを支払ったのに、また電話がかかってきて「3万円のセキュリティーを入れる必要がある。そうしないとパソコンが壊れる。」と脅し始めて喧嘩になった。挙句の果てに遠隔操作で画面を上下逆さにされて電源を切られた。
上下を直すために、Ctrl＋Alt＋↑を押したが直らなかった。
パソコンを再起動しても画面は逆さのままである。

偽セキュリティ警告　サポート契約型

契約を拒んだときの嫌がらせ-その２

起動ロック攻撃

ソフトでパソコン起動時のロックをかけ、解除用のパスワードを教えて欲しければ金を払えと要求する。

Windows OSが起動する前にロック画面が出るため、通常の方法で初期化することができない。

＜一例＞

偽セキュリティ警告　サポート契約型

「Lock My PC」でロックされたときの復旧方法

https://fspro.net/_service/lmpc-passrec/

「Lock My PC」の提供元による説明

1. パスワード入力欄に「999901111」を入力
   ※決してEnterやOKボタンを押さない
2. 回復数値が表示される
3. 回復数値をフォームに入力して「submit」を押すことで新しい回復パスワードをゲットできる。

偽セキュリティ警告　サポート契約型

「Lock My PC」でロックされたときの復旧方法

チェックをつけないとSUBMITボタンが押せない

偽セキュリティ警告　サポート契約型

パソコンをロックされたときの復旧方法

Windows10で起動に問題があってスタートメニューから通常の初期化ができない場合でも、対処の方法はある。

具体的な操作方法はパソコンメーカーのサポートに相談するよう勧めるのがよい。

偽セキュリティ警告　サポート契約型

山形県警察広報動画

LgMeInを使った手口の例ですが、この動画を観ることで 遠隔操作が開始されるまでの流れ、相手が遠隔操作中にどういった 説明をしているのか、コンビニにウェブマネーを買いに行かせる際のトークなど、最近の手口の詳細が分かります。

「サポート詐欺」にだまされないで！
（その１）警告画面に 表示された番号に電話をかけると
https://www.youtube.com/watch?v=sWftPO_l3r8

（その２）犯人がPCを遠隔操作する
https://www.youtube.com/watch?v=lElNtiVK-qU

（その３、最終）犯人が金銭を要求！
https://www.youtube.com/watch?v=NNEBT8ZAXL0

偽セキュリティ警告　サポート契約型

相談者が気にしていること-1

Q 遠隔操作で情報が盗られて悪用されないか？

A 判断に際しては下記のヒアリングが必要

①遠隔操作中に相手が何を見ていたか
②遠隔操作中に目を離していた時間がどれくらいあったか
③パソコンの中にどのような情報を保存していたか
④ブラウザにログインパスワードを保存しているサイトがあるか
⑤アカウントに不正ログインされていないか

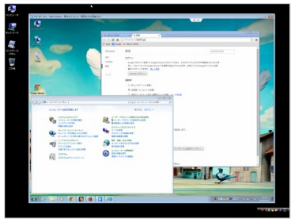
偽セキュリティ警告　サポート契約型

① 遠隔操作中に相手が何を見ていたか

遠隔操作中は、相手の操作内容が見える

遠隔操作される側

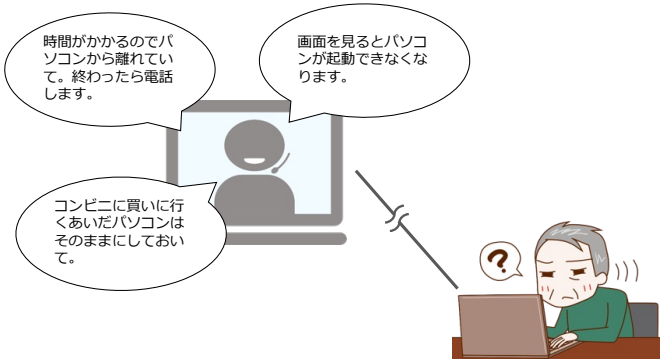
遠隔操作する側



偽セキュリティ警告　サポート契約型

②目を離していた時間がどれくらいあったか

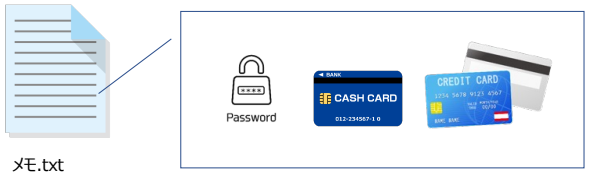
遠隔操作の内容を見せないための口実



偽セキュリティ警告　サポート契約型

③ パソコン内にパスワードやクレジットカード情報をメモしていなかったか

パソコンの中のメモ帳などに、平文でパスワードやクレジットカード番号、銀行口座番号、暗証番号などをメモしていた場合は、それらを見られた可能性がある。



メモ.txt

偽セキュリティ警告　サポート契約型

④ ブラウザにログインパスワードを保存していないか

ブラウザにサイトのパスワードを保存している場合は、それらも見られた可能性がある。

<ブラウザに保存してあるパスワードリストの表示方法>

Google Chrome	設定＞パスワード
Microsoft Edge	コントロールパネル＞ユーザーアカウント＞Web資格情報の管理
Internet explore	設定＞インターネットオプション＞コンテンツ＞オートコンプリート

偽セキュリティ警告　サポート契約型

Google Chromeのパスワード管理画面

偽セキュリティ警告　サポート契約型

⑤ アカウントに不正ログインされていないか

ブラウザにパスワードを保存していた場合は、遠隔操作中にブラウザを開いてサイトに不正ログインされた可能性がある。

それがGmailのようなウェブメールだった場合、メッセージが読まれたかもしれないし、そのメールアカウントを使って勝手に何かのサービスに登録しているかもしれない。

AmazonやAppleなどの場合、不正ログインされた上でAmazonギフト券やiTunesカードなどを勝手に買われてしまう可能性もある。

偽セキュリティ警告　サポート契約型

相談者が気にしていること- 2

Q 遠隔操作中にウイルスを仕掛けられてないだろうか？

A AdBlock Plusのような広告をブロックするソフトや、ccleanerといったよくわからないソフトをインストールしていく事例はあるが、あからさまにウイルスを仕込まれたという事例は確認していない。
ただ、何らかのソフトウェアをインストールされたことが確かな場合は、システムの復元または初期化をしておくのが安全。

偽セキュリティ警告　サポート契約型

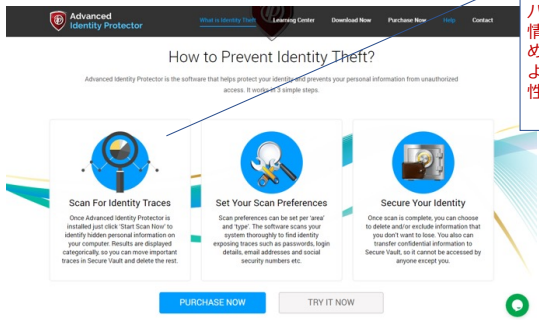
サポート契約をした場合によくインストールされているプログラム

Advanced Identity Protector	隠れた個人情報の洗い出しと保護を謳うソフト（詳細は後述）
OneSafe PC Cleaner	無料の診断ソフトを謳ってはいるが、最終的に有償版の購入を促される
GoTo Opener	遠隔サポートツール「LogMeIn」のトレーニング開始用ヘルパーアプリケーション
Go to Assist Customer	遠隔サポートツール「LogMeIn」のカスタマープログラム
Driver Updater	よく分からないソフト

偽セキュリティ警告　サポート契約型

サポート契約をした場合によくインストールされているソフト

Advanced Identity Protector



このソフトでスキャンすると、パソコン内に隠されている個人情報をカテゴリ別に表示するため、個人情報の保護目的というより悪用目的で入れている可能性がありそう。

偽セキュリティ警告　サポート契約型

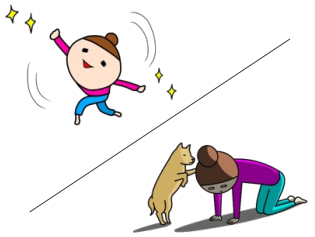
遠隔操作ソフト（アプリ）の動作や機能

遠隔操作する側からの操作		Windows PC	Android	iPhone
画面	画面表示をリアルタイムに見る	◎	◎	◎
	画面ロックを遠隔で解除	× ※1	× ※1	× ※2
遠隔操作	マウスやキーボード、スクリーンタッチの操作	◎	○ ※3	×
	アプリの起動	◎	◎	×
	新たなアプリのインストール	◎	◎	×
接続	操作を受ける側の許可なしに再接続可能	○ ※4	×	×
	再起動後に自動で再接続可能	○ ※4	×	×

※1　ロック解除のパスワードやPINが設定されている場合
※2　iPhoneの場合、画面ロック状態になった時点で遠隔操作アプリが終了します
※3　操作する側に表示された画面上でマウス操作することでタップ及びスワイプが可能
※4　遠隔操作をされる側であらかじめ設定が必要

3　うまい儲け話し

偽当選サイト



偽当選サイト

偽の当選画面例- 1

偽当選サイト

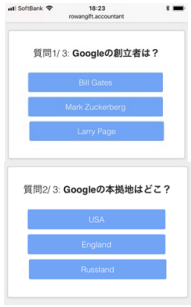
偽の当選画面例- 2

iPhoneでTOHOシネマズのサイトからチケットを購入したところ、同日夕方になり、右のポップアップメッセージが表示された。

偽当選サイト

クイズに答えた場合の流れ

簡単な質問が３つ出る



正解でも不正解でも同じ画面に行き着く

賞品を選択するとこの画面になる

偽当選サイト

クイズに答えた場合の流れ

購入画面ではクレカによる1ドルの決済が求められる

「129円で新しいiphone Xを入手」と書かれたページをスクロールすると支払いに関する記載が書かれてある

5日以内に解約手続きをとらないと90ユーロ相当の請求が定期的に来ることになる。

偽当選サイト

被害に遭った場合の対処

偽当選サイト経由でカード決済してしまった場合（パターンA）

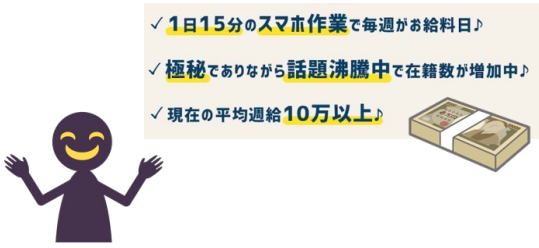
- クレジットカード会社に連絡する
- 相手方事業者の問い合わせフォーム、またはメールにて解約意思を伝える

アプリをインストールしてしまった場合（パターンB）

- サブスクリプション契約を解約する（具体的手順は参考資料）
- アプリはアンインストールする

3 うまい儲け話し

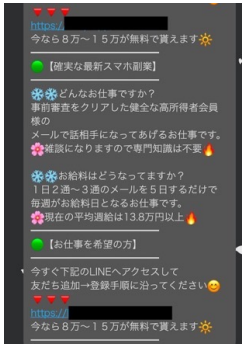
簡単に稼げるスマホ副業の罠



簡単に稼げるスマホ副業の罠

広告からのランディングページ

別のLINEアカウントへの友達登録を促される



「１日2～3通のメールをするだけで、メール開始より7日後にお給料が貰えます。」などの文言で副業への期待を膨らませ、メールアドレスの登録を要求してくる。

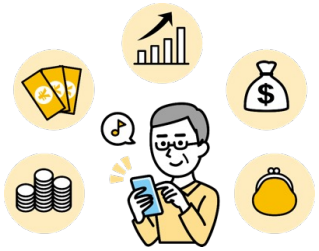
簡単に稼げるスマホ副業の罠

登録をするとどうなる？

四六時中、何十通もの副業紹介メッセージが送られてくるようになるが、どれも全く稼げない。

稼げるスペシャル副業の狙いは、オプトイン・アフィリエイトによる報酬稼ぎ

簡単に稼げるスマホ副業の罠

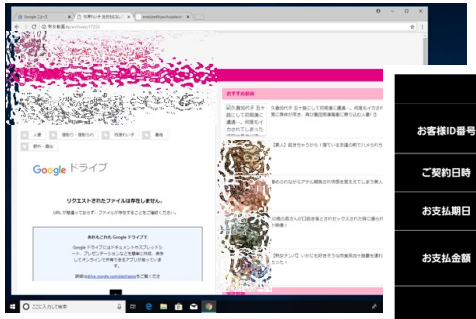


詐欺・脅迫

ワンクリック請求

ワンクリック請求

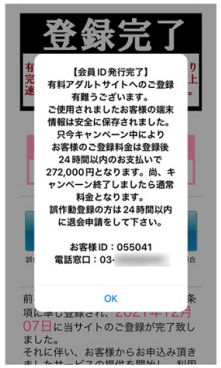
パソコン版のワンクリック請求の実例



「あたかも個人情報を取得したかのように表示される」
画面事例

ワンクリック請求

スマホ版のワンクリック請求の実例



ワンクリック請求

パソコンでの請求画面の消し方

■ 症状

- ☑ 画面を閉じても、暫くするとまた出てくる
- ☑ PCを再起動しても、また出てくる

いずれも**Yes**

不正なプログラムをインストールしてしまったことが原因

■ **システムの復元が必要**

システムの復元ができる条件
1. 「システムの保護」が有効になっている
2. 請求画面表示時点より前の「復元ポイント」が作成されている

いずれも**No**

単なるウェブページ

■ **ブラウザを閉じるのみ**

ブラウザを閉じるいくつかの方法（一例）
1. 【Alt】+【F4】でアクティブなウィンドーを閉じる
2. 【Ctrl】+【Alt】+【Delet】キーで[タスク マネージャー] を呼び出し、ブラウザを終了する

ワンクリック請求

スマホでの請求画面の消し方

基本的にブラウザの表示のみの手口となるため、

「タブを閉じる」、または**「閲覧履歴の消去」**

のみで対処可能。

ワンクリック請求

理解しておくべきポイント

1. サイトにアクセスしただけで個人情報はわかりません

IPアドレスや携帯の機種情報が知られたからといって住所や氏名を特定されることはありません。

2. 決して自分から業者に連絡してはいけません

支払いを免除するなどという理由で自宅や勤務先の情報を聞かれ、さらに取り立てがエスカレートするおそれがあります。

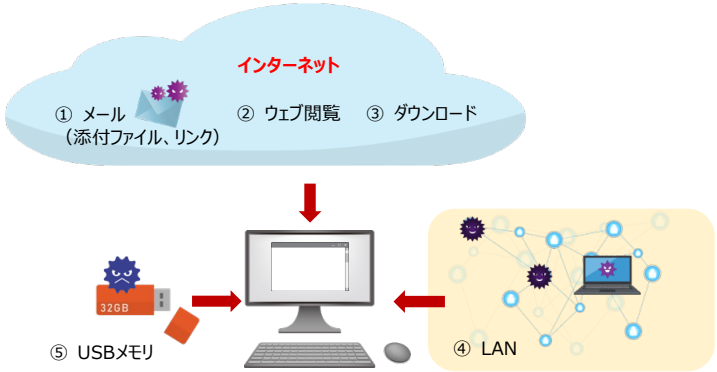
3. 登録完了画面は消すことができます

通常はパソコンを再起動すれば消えます。
消えない場合はシステムの復元で対処可能です。

金銭被害にあわないための
ウイルスに関する基礎知識

金銭被害にあわないためのウイルスに関する基礎知識

ウイルスの５大感染経路



拾ったUSBだったら、**道に落ちてる食べ物を拾い食い** してお腹を壊すような感染パターン

金銭被害にあわないためのウイルスに関する基礎知識

理解しておくべきポイント

1. 有線・無線による感染リスクの違いはありません。

同一Wi-Fiネットワーク上にある他の端末に感染が広がる場合もあるし、さらにそこからインターネット経由で他の端末（有線無線問わず）に感染が広がる場合もあります。

2. OSが異なれば感染することはありません。

Windows用のウイルスがAndroidに感染することや、
Android用のウイルスがiPhoneに感染することはありません。

3. 感染した際にネットワーク切断を行う理由

- 自己増殖タイプだった場合の感染拡大防止
- 感染端末からウイルスつきメールがばらまかれることの防止
- 外部のサーバーと不正な通信が行われることの防止

Androidを狙った不正アプリの主な種類

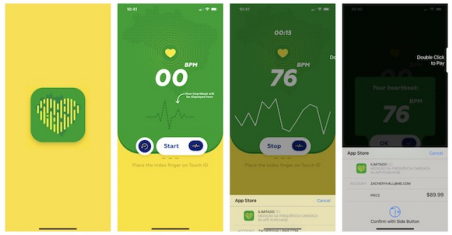
通称	主な機能
SPYWARE /スパイウェア	標的とする端末から、SMS、通話履歴、連絡先、位置情報、SD カードのファイル一覧のような個人情報を窃取する。
COINMINER /コインマイナー	感染端末の計算能力を盗用して仮想通貨を発掘する 。
FAKESPY /フェイクスパイ	端末にオンライン銀行アプリがないかを確認し、あった場合は偽アプリに置き換える。ない場合は偽アプリを感染端末に送り込む。 ※宅配便の不在通知SMSを利用した手口
BACKDOOR /バックドア	感染したモバイル端末が接続しているLANに攻撃の足掛かりを仕掛けるバックドア型アプリ
FRAUDBOT /フラウドボット	偽のアンケート調査ページを自動的にポップアップさせたり、広告の自動クリック機能を有する。

iOSとAndroidとのセキュリティリスクの違い

脅威の種類	iOS 改造していない前提	Android
不正アプリ	• アプリの入手先がApp Storeに限定されている。 • App Storeに載る前にすべてApple社が挙動面を厳格に審査しているため不正なアプリが混入する可能性が低い。	• 公式マーケット以外からもアプリのダウンロードが可能。 • Google Playに載る前に十分な挙動面での審査が行われないため不正なアプリが混入する可能性が比較的高い。
ワンクリックサイト 偽ショッピングサイトフィッシングサイト	OSの違いによる差はない 閲覧リスクを軽減するには別途、フィルタリングアプリや安全性の高いブラウザアプリが必要	

iPhoneでも油断は禁物
心拍数計測と見せかけ、Touch IDで約1万円を課金する詐欺アプリが出現　2018年12月

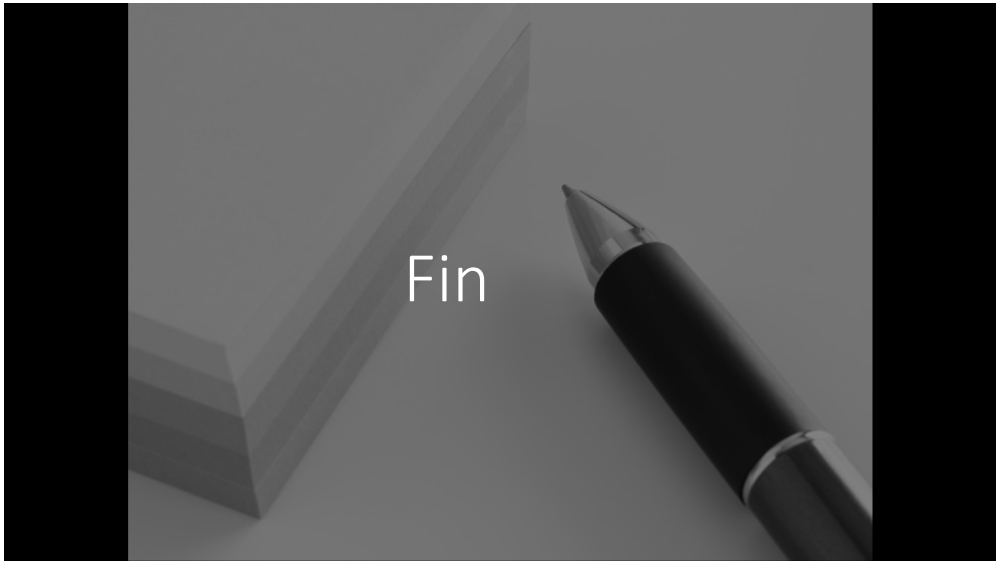
発見されたアプリ「Heart Rate Measurement」は、心拍数を計測するために人差し指をTouch IDに置くよう要求してきます。
ユーザーがTouch IDに指紋を登録した指を置くと、アプリ内課金が承認され、89.99ドル（約1万円）をだまし取られてしまいます。



Touch I認証をする段階で、画面の明るさを最低まで引き下げて白黒表示に変更するため、指紋認証をされていることに気付きにくい（画面右）

端末をウイルスから守るための3箇条

1. **OSやソフトウェアのバージョンを常に最新にする**
   脆弱性をついた攻撃対策として有効
2. **ウイルス対策ソフトを使用し、定義ファイルを自動更新する**
   ウイルス対策として有効
3. **アプリの入手は公式アプリマーケットから**
   スマホの不正アプリ対策として有効



質疑応答

参考資料

iPhone/Android共通

キャリア決済の上限設定方法

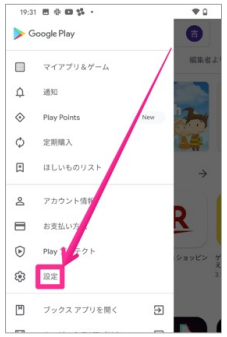
ドコモ	「dメニュー」→「マイメニュー」→「継続課金一覧／ご利用履歴【決済サービスご利用明細　（spモード決済・ドコモ ケータイ払い／dケータイ払いプラス）】」→「ネットワーク暗証番号を入力」→「電話料金合算払い【限度額設定変更】」
au	[auスマートパスTOPからログイン]→[au IDトップ]→[右上のMENU]→[利用限度額の変更]
ソフトバンク	パソコンからMy SoftBankへアクセスし、画面上部の「安心・便利サービス」→「ソフトバンクまとめて支払い」→「設定を変更する」→「ご利用可能額の設定」をクリックして希望の上限額を設定する。

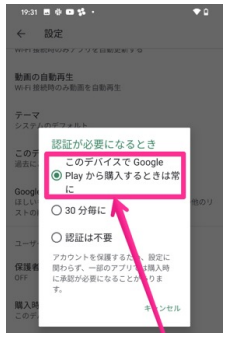
参考資料

Android

アプリ内課金を制限する方法（1）

Google Playストアの設定で、購入時に認証を必要としておく

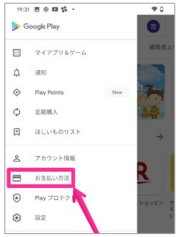




参考資料

Android　アプリ内課金を制限する方法（2）

Google Playの支払い方法を「Google Play の残高」または
「Google Play ギフトカード」にしておく



Google　Playヘルプ：お支払い方法の追加、削除、編集
https://support.google.com/googleplay/answer/4646404

参考資料

Android　Google Play アプリで定期購入を解約する方法

重要: アプリをアンインストールしても、定期購入は解約されません。

1. Android デバイスで、Google Play の定期購入 にアクセスします。
2. 解約する定期購入を選択します。
3. [**定期購入を解約**] をタップします。
4. 画面上の手順に沿って操作します。

ヒント: 定期購入しているアプリが Google Play から削除された場合、今後の定期購入は解約されます。過去の定期購入の払い戻しは行われません。ただし、この記事または Google Play の払い戻しポリシーで指定されているとおり、一部例外があります。

Google　Playヘルプ：お支払い方法の追加、削除、編集
https://support.google.com/googleplay/answer/7018481

参考資料

iPhone　アプリ内課金を制限する方法（1）

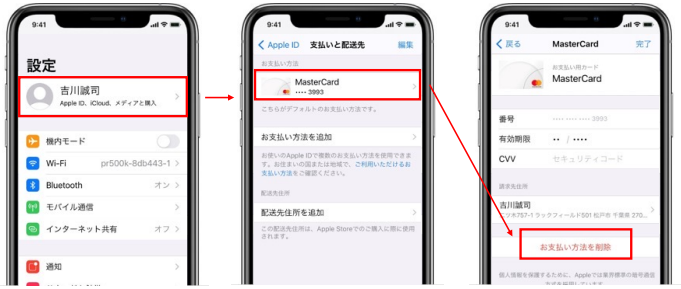
「スクリーンタイム」でアプリ内課金を不許可にする

Apple：App Store での App 内課金を防ぐ
https://support.apple.com/ja-jp/HT204396

参考資料

iPhone　アプリ内課金を制限する方法（2）

Apple IDの支払い方法を登録しておかない。またはデビッドカードにしておく。

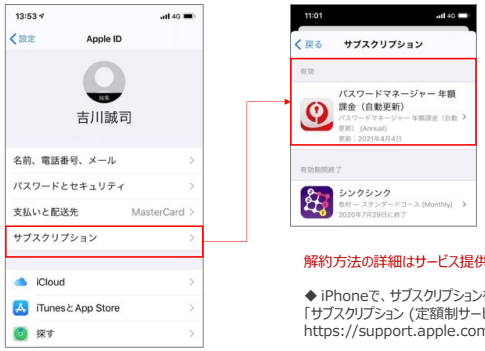


参考資料

iPhone

サブスクリプションの確認方法

設定 ＞ 名前＞ サブスクリプション



解約方法の詳細はサービス提供者のヘルプページ参照

◆ iPhoneで、サブスクリプションを解約する
「サブスクリプション（定額制サービスの登録）を表示・変更・解約する」
https://support.apple.com/ja-jp/HT202039

参考資料

主な相談機関

ジャンル	名称	URL
海外事業者との契約トラブル	越境消費者センター（CCJ）	https://www.ccj.kokusen.go.jp/
フィッシング詐欺	フィッシング対策協議会	https://www.antiphishing.jp/consumer/rep_phishing.html
インターネットや無線サービス	TCA相談窓口	https://www.tca.or.jp/consult/leaflet02.pdf
子供のネットトラブル	こたエール	https://www.tokyohelpdesk.metro.tokyo.lg.jp/
情報セキュリティ	IPA情報セキュリティ安心相談窓口	https://www.ipa.go.jp/security/anshin/about.html
迷惑メール	迷惑メール相談センター	https://www.dekyo.or.jp/soudan/index.html
銀行	全国銀行協会相談室	https://www.zenginkyo.or.jp/adr/about/
仮想通貨	日本暗号資産取引業協会	https://jvcea.or.jp/contact/form-contact/