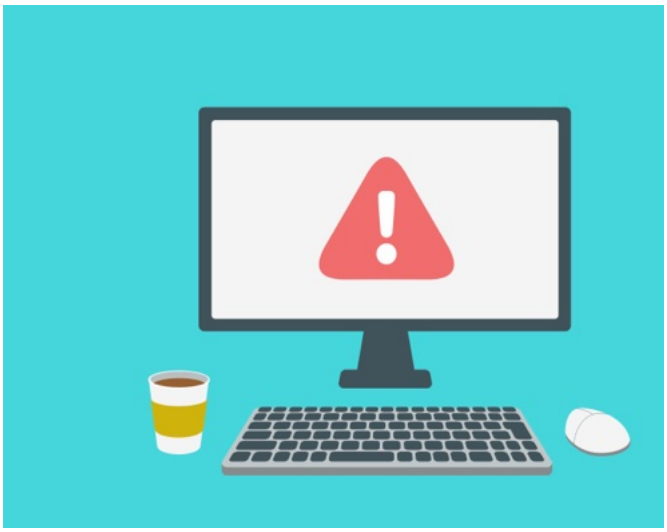
配布資料

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～



90分コース

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 2025」

https://www.ipa.go.jp/security/10threats/10threats2025.html

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

解説

2024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。

[ネットで起きている被害の分類]

1 不正アクセス

2 セクストーション

3 偽セキュリティ警告

4 詐欺

5 誹謗中傷

6 ディープフェイク

1 【不正アクセス】

企業の場合：

VPN機器から侵入してランサムウェアに感染させる手口が主流

個人の場合：

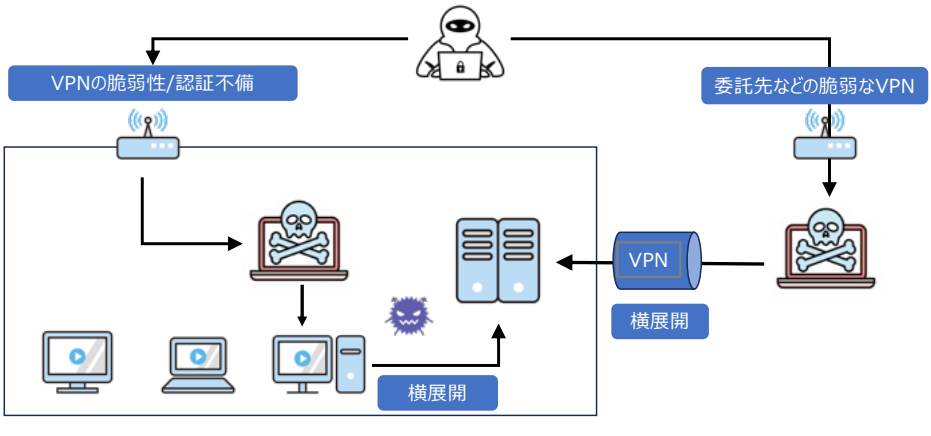
SMSを使ったフィッシングでログイン情報を詐取する手口が主流

ランサムウェア攻撃の変化 ～ダブルエクストーション

1 不正アクセス 企業編

ランサムウェア攻撃の変化

テレワーク等に利用されるVPN機器等の脆弱性や強度の弱い認証情報等を利用して侵入する手口が8割



ランサムウェア対策のポイント

① 感染の完全予防は不可避

→「感染しても怖くない」体制が必須

② バックアップは分離保管

→ クラウド上のバックアップデータも攻撃されるから。

1 不正アクセス 企業編

ランサムウェア対策のポイント

③ バックアップは万能ではない

→暗号化の恐喝には有効だが、データ公開の恐喝には効かない

④ データの暗号化（保存・転送）

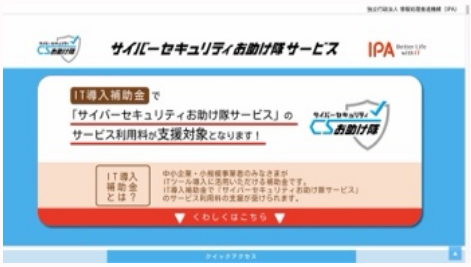
→ 万が一盗まれても、暗号化してあれば中身は読めません。

→ 標準機能のBitLocker（Windows）だけでは不十分。

1 不正アクセス 企業編

中小企業支援制度の活用

- IPA／サイバーセキュリティお助け隊
- 各種助成金など



初年度導入費用10万円～60万円程度でネットワーク監視と端末監視が可能

1 不正アクセス 個人編

SMSを使ったフィッシング

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

1 不正アクセス 個人編

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

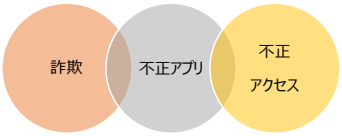
- 同様の偽不在通知の大量送信
- キャリア決済の悪用
- フリマなどのアカウントの無断作成
- Googleアカウントへの不正ログイン

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



SMSを使ったフィッシング

Androidの場合

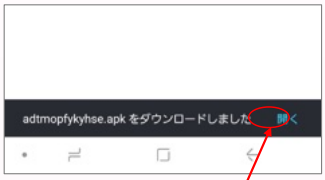
SMSのリンクをタップした後の画面遷移

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

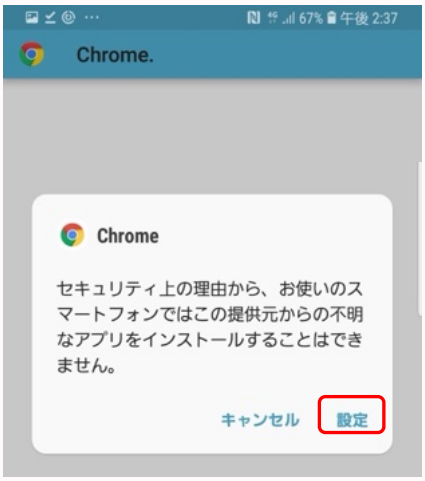
OKを押すと.apkファイルがダウンロードされる

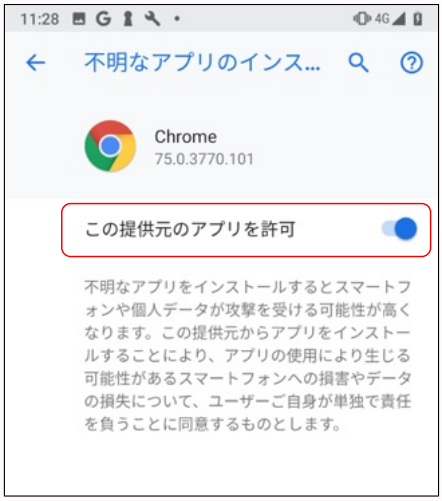
「開く」をタップするとアプリのインストール手順に進む



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

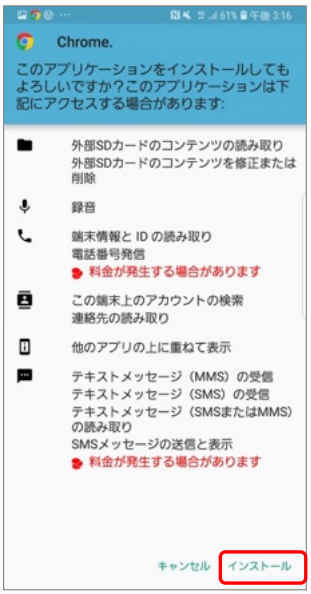




1 不正アクセス 個人編

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

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

1 不正アクセス 個人編

攻撃者によるキャリア決済悪用までの流れ

Androidの場合

攻撃者のiPhone

設定＞アカウント名＞支払いと配送先

キャリア決済を選択

攻撃者によるキャリア決済悪用までの流れ

Androidの場合

攻撃者のiPhone

不正アプリをインストールした被害者の電話番号を入力

被害者のAndroidスマホ

正規のキャリアからSMSで認証コードが送られてくる

1 不正アクセス 個人編

攻撃者によるキャリア決済悪用までの流れ

Androidの場合

被害者のAndroidスマホ

攻撃者のiPhone

被害者端末にインストールされた不正アプリの権限により、攻撃者がSMS内の確認コードを窃取

攻撃者のApple IDに確認コードを入力

攻撃者のApple IDに被害者の電話番号に紐付くキャリア決済の登録が完了

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る連絡先情報（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。

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Apple Gift Card等の請求が発生する。
- アドレス帳データが外部に送信される可能性がある。
- フリマサイト、後払い決済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。

1 不正アクセス 個人編

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

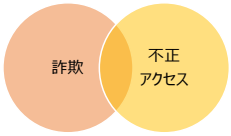
➢ 不正アプリのアンインストール
- Chromeアプリに扮しているケースが多い

➢ 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、フリマサイト、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。

1 不正アクセス 個人編



SMSを使ったフィッシング

iPhoneの場合

1 不正アクセス 個人編

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すると被害に繋がる

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。

1 不正アクセス 個人編

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

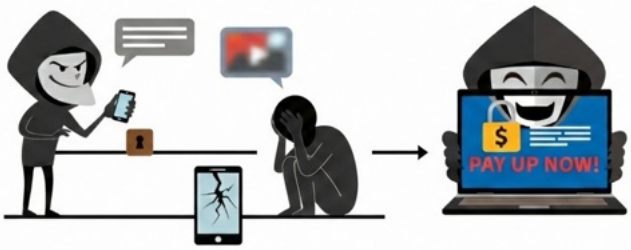
2. キャリア決済の限度額の変更

   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。

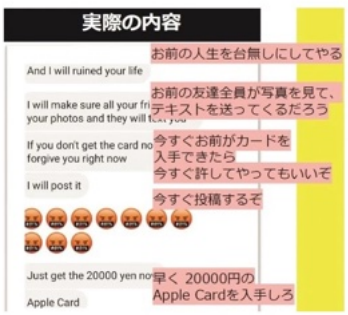
2 セクストーション

（性的脅迫）



セクストーションとは

SNSで知り合った相手に性的な写真や動画を送らせ、それらを拡散すると脅してお金などを要求する行為



深刻化するセクストーション被害

NPO法人「ぱっぷす」に'25年に寄せられた被害相談は7月時点で

1066件

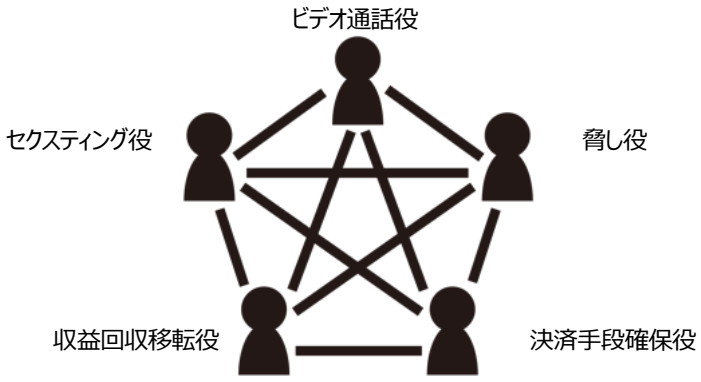
22年度は131件、23年度は528件、24年度は1864件と推移し、
急増傾向

従来型セクストーションに加え、金銭型セクストーションが急増中

2 セクストーション

金銭型セクストーションは男性も狙われる

西アフリカ・東南アジア地域の犯罪グループによる冷酷非情な犯行



セクストーションの被害に遭ってしまったら

脅迫されている証拠を保存した上で警察に相談

不安でも相手を即ブロックして連絡を遮断する

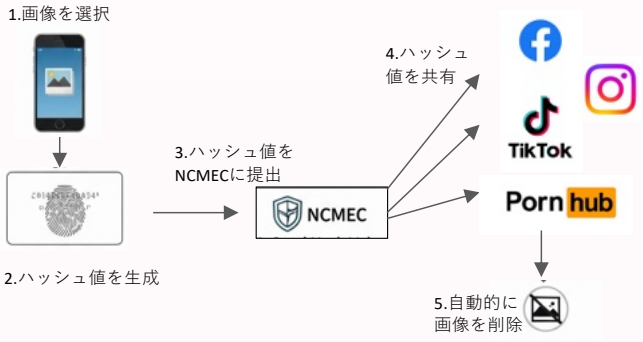
「Take It Down」で画像の拡散を阻止

2 セクストーション

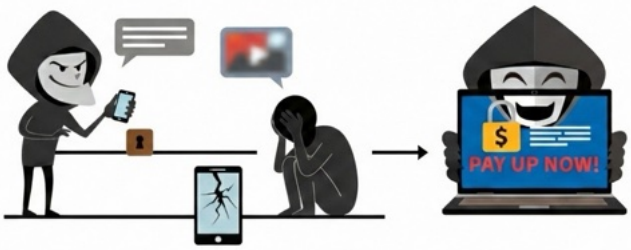
全米行方不明・被搾取児童センター(NCMEC)が運営する「Take It Down」

https://takeitdown.ncmec.org/ja/

拡散を防ぎたい画像や動画からハッシュ値（デジタルの指紋のようなもの）を作成し、それをNCMECに提出すると、加盟プラットフォーム企業がそれを使って該当画像を削除し、同じ画像が投稿されるのを防ぐことができる。



2 偽セクストーション



2 偽セクストーション

こんにちは！

私はあなたに悪い知らせがあります。
2018年6月28日 - この日、私はあなたのオペレーティングシステムをハッキングし、xxxx@aaaa.comにフルアクセスできました。
その日のあなたのアカウントパスワードは：●●●●●●●
それはどうだった：
その日接続していたルータのソフトウェアには、脆弱性が存在しました。
私は最初にこのルータをハックし、その上に悪質なコードを置いた。
インターネットに接続すると、私のトロイの木馬はあなたのデバイスのオペレーティングシステムにインストールされました。

その後、私はあなたのディスクの完全なデータを保存しました（私はすべてあなたのアドレス帳、サイトの閲覧履歴、すべてのファイル、電話番号、あなたのすべての連絡先のアドレス）を持っています。

あなたのデバイスをロックしたかったのです。ロックを解除するために、私はお金がほしいと思った。
しかし、私はあなたが定期的に訪れるサイトを見ました, そしてあなたのお気に入りのリソースから大きなショックを受けました。
私は大人のためのサイトについて話しています。

私は言う - あなたは大きな変態です。無限のファンタジー！

その後、アイデアが私の頭に浮かんだ。
私はあなたが楽しんでいる親密なウェブサイトのスクリーンショットを作った (私はあなたの喜びについて話しています、あなたは理解していますか？).
その後、私はあなたの喜びの写真を作った (あなたのデバイスのカメラを使って). すべてが素晴らしくなった！

あなたの親戚、友人、同僚にこの写真を見せたくないと強く信じています。
私は$577が私の沈黙のために非常に小さいと思う。
それに、私はあなたに多くの時間を費やしました！

（次ページに続く）

2 偽セクストーション

私はBitcoinsだけを受け入れる。
私のBTCウォレット： 17zmnmqEUCesNz6UgXGbRk7fKnu8iq1q2J

Bitcoinウォレットを補充する方法がわからないのですか？
どの検索エンジンでも、「btc walletにお金を送る方法」と書いてください。
クレジットカードに送金するよりも簡単です！

お支払いの場合は、ちょうど2日以上（正確には50時間）をご提供します。
心配しないで、タイマーはこの手紙を開いた瞬間に始まります。**はい、はい。それはすでに始まっています！**

支払い後、私のウイルスと汚れた写真は自動的に自己破壊されます。
私はあなたから指定された金額を受け取っていない場合、あなたのデバイスはブロックされ、あなたのすべての連絡先は、あなたの "喜び"と写真を受信します。

私はあなたが賢明であることを望みます。
- 私のウイルスを見つけて破壊しようとしないでください！ （すべてのデータはすでにリモートサーバーにアップロードされています） - 私に連絡しようとしないでください（これは実現可能ではありません、私はあなたのアカウントからメールを送りました）
- 様々なセキュリティサービスはあなたを助けません。あなたのデータは既にリモートサーバー上にあるので、ディスクのフォーマットやデバイスの破壊は役に立ちません。

P.S. 私は支払い後にあなたに再び邪魔をしないことを保証します。
これはハッカーの名誉のコードです。

これからは、良いアンチウィルスを使用し、定期的に更新することをお勧めします
（1日に数回）！

私に怒らないでください、誰もが自分の仕事をしています。
お別れ。

2 偽セクストーション

解説

＜脅迫内容について＞

同じような文面で不特定多数に送られ、実際の動画へのリンクや添付等がないことから、このメールの内容については根拠がなく、迷惑メールと同じく無視して削除するだけで問題ない。

＜実際に使用していたパスワードが書かれていることについて＞

過去に流出したパスワードリスト等をもとに記載された情報であると考えるが、流出経路とその原因は不明。
当該パスワードを現在も使用している場合はただちに変更し、可能なら2段階認証の利用が望ましい。

恐喝メールへの対応

- **ひたすら無視する**

同じ内容のメールが不特定多数にばら撒かれていることから、迷惑メールの一種に過ぎません。仮に「証拠の画像」と称するリンクや添付ファイルがあっても危険なので開かないようにしてください。

- **パスワードが記載されていた場合は変更する**

どこかのサイトから漏えいしたパスワードがリストとして流通している可能性があります。現在も使用している場合はすぐに変更してください。

- **送信元が自分のアドレスになっていることもある**

送信元アドレスを書き換えることは技術的には容易なこと。

決して自分のメールアカウントがハッキングされているわけではありません。

3 “偽セキュリティ警告”による不正な誘導

偽セキュリティ警告からの３つの手口

アプリ誘導型	ソフト購入型	サポート契約型
余計なアプリをインストールさせる手口	余計なソフトウェアを購入させる手口	不要なサポート契約をもちかける手口

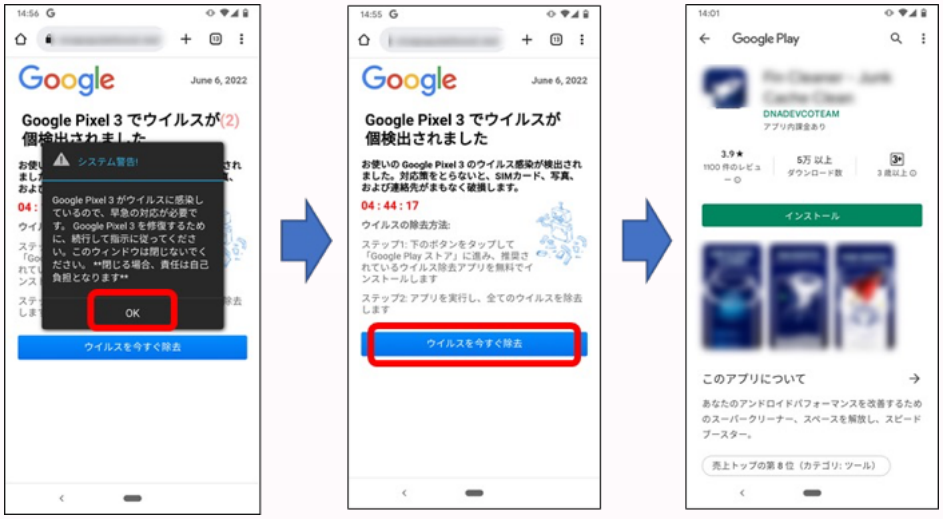
不要なアプリを
インストールさせる手口

偽警告（アプリ誘導型）

3 偽セキュリティ警告 アプリ誘導型

スマホで遭遇する偽のセキュリティ警告の画面例

Android



スマホの動作を軽くするというクリーナーアプリやVPNのためのアプリに誘導されることが多い。

3 偽セキュリティ警告 アプリ誘導型

スマホで遭遇する偽のセキュリティ警告の画面例

iPhone

スマホの動作を軽くするというクリーナーアプリやVPNのためのアプリに誘導されることが多い。

3 偽セキュリティ警告 アプリ誘導型

表示されるメッセージについて

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**と考えられます。

警告メッセージの内容を鵜呑みにせず、画面が表示された場合には**ブラウザアプリのタブを閉じて**ください。

3 偽セキュリティ警告 アプリ誘導型

誘導されるアプリについて

多くは公式マーケットにあるアプリに誘導されるため、端末に害悪を与えるような悪質なものではないと考えられる。

インストールしたアプリが不要であれば、**アンインストール**するだけで端末への対処はOK。

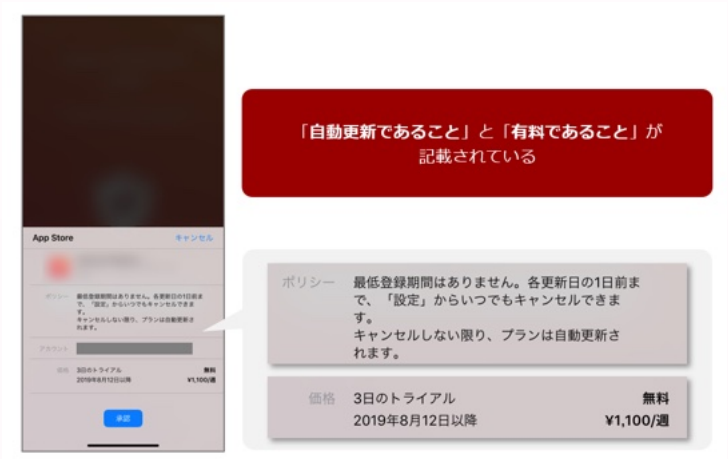
ただし、**サブスクリプション契約**になっていないか確認する必要がある。

3 偽セキュリティ警告 アプリ誘導型

アプリをインストールしてしまった場合の影響

※iPhoneの事例

サブスクリプション契約が発生する可能性が高い



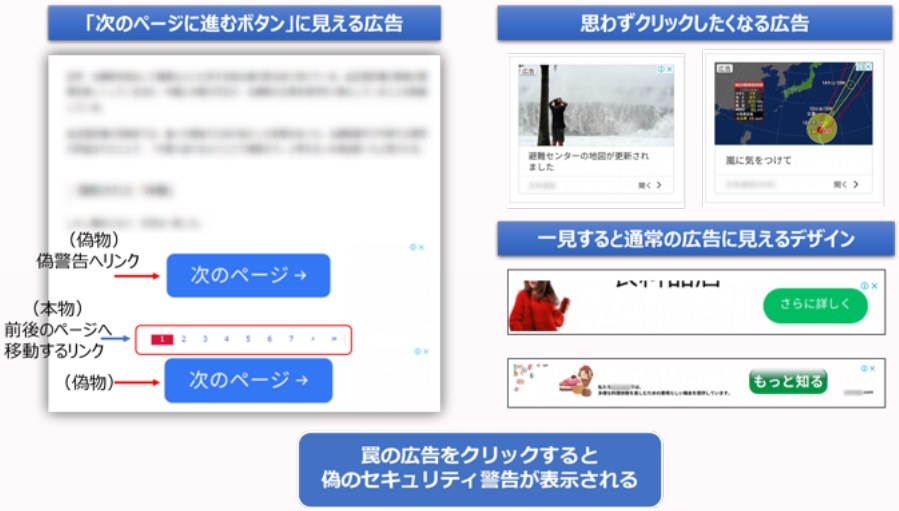
3 偽セキュリティ警告

不要なサポート契約を

もちかける手口

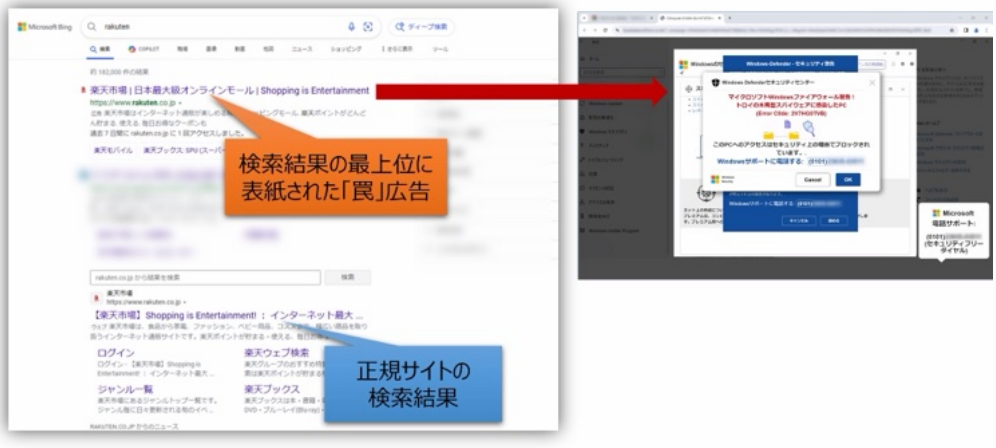
サポート契約型

サポート詐欺に繋がる危険なリンクの例-その１



3 偽セキュリティ警告 サポート契約型

サポート詐欺に繋がる危険なリンクの例-その２



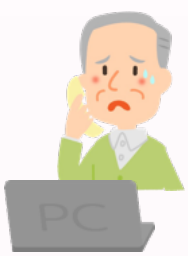
3 偽セキュリティ警告 サポート契約型

PCで遭遇する偽のセキュリティ警告の画面例

3 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

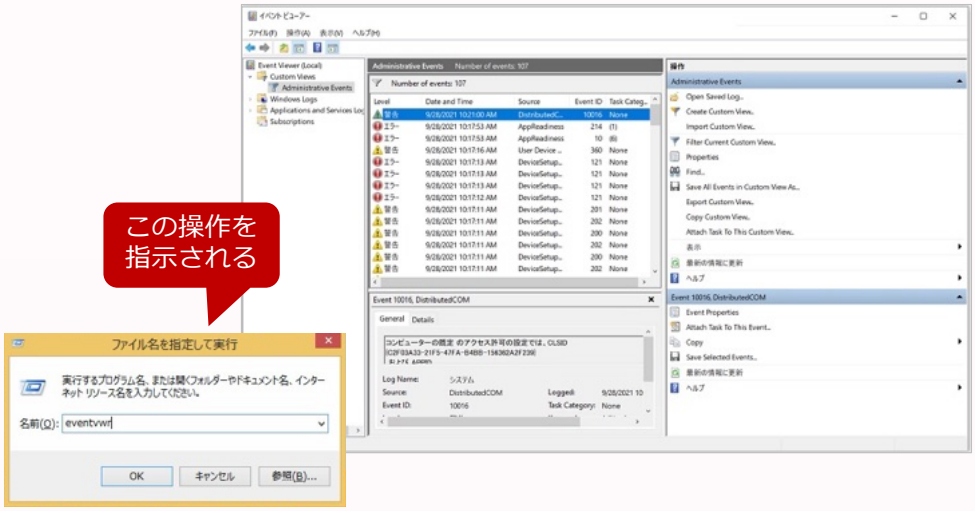


ベーシックプラン
¥X,XXX/3年
ゴールドプラン
¥X,XXX/5年
⋮

3 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



3 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。

3 偽セキュリティ警告 サポート契約型

遠隔操作されて送金額を勝手に増やされるケース

3 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。

3 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>

3 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

- 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

- するとその下に数値回復コードが表示される。
- それを左図の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らしい。

4

詐欺

（楽して儲かる話）

偽当選サイト

4 詐欺 偽当選サイト

偽の当選画面例- 1

4 詐欺 偽当選サイト

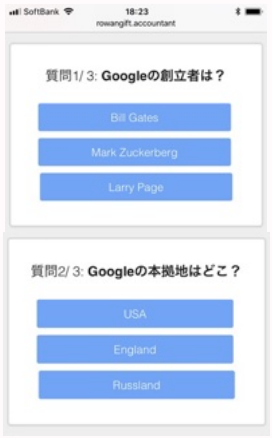
偽の当選画面例- 2

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。

4 詐欺 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

4 詐欺 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。

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）

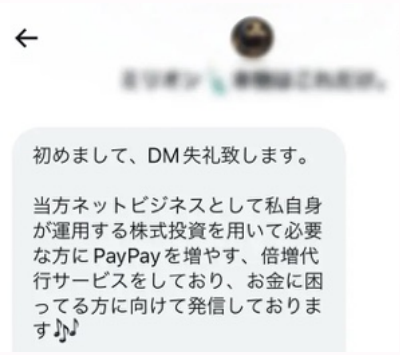
- クレジットカード会社に連絡する
- 相手方事業者の問い合わせフォーム、またはメールにて解約意思を伝える

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

PayPay倍増詐欺

PayPay倍増詐欺のポスト例



＜犯行の流れ＞

DM勧誘
↓
24時間以内での返金を約束
↓
送金したとたん音信不通
↓
被害者のアカウントをブロック。

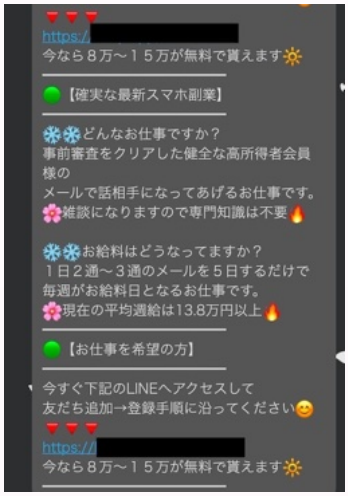
簡単に稼げるスマホ副業の罠

✓1日15分のスマホ作業で毎週がお給料日♪
✓極秘でありながら話題沸騰中で在籍数が増加中♪
✓現在の平均週給10万以上♪

4 詐欺 簡単に稼げるスマホ副業

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。

4 詐欺 簡単に稼げるスマホ副業

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。

4 詐欺 簡単に稼げるスマホ副業

3 詐欺 簡単に稼げるスマホ副業

すでに怪しいアカウントを友だち登録してしまった場合はどうすればいい

- 「**LINE友だち追加**」してしまった場合はその**アカウントをブロックする。**
- 他のアカウントからのコンタクトによって詐欺を仕掛けられる可能性が高いので、知り合いと断定できる人以外からの連絡は基本的に**無視**する。
- 「**メールアドレス入力**」などをしてしまった場合は、フィッシングメールなどが来る可能性が高いので十分注意する。

5 SNS上での誹謗中傷

誹謗中傷の舞台が匿名掲示板からSNSに移ったことで拡散力がアップ。その中には偽・誤情報も。「いいね」だけでも加害者に加担してしまう。

<近年話題になった炎上事例>

旭川女子中学生凍死事件
Twitterで、女児が死亡した原因が家庭環境の問題にあるかのような内容が同一アカウントから投稿された。

山梨女児行方不明事件
Twitterやブログで、母親やその親族らが事件を起こしたかのような趣旨の書き込みがあった。

女子プロレスラー自死事件
番組放送中での言動をきっかけに当人のTwitterやInstagramには毎日100通を越える批判コメントが寄せられていた。

常磐道あおり運転殴打事件
あおり運転の車に同乗していたガラケー女だとして、無関係な女性の個人情報がインターネットに投稿され拡散された。被害女性のInstagramアカウントには1000件をこえる誹謗中傷のメッセージが届く結果となった。

元アイドルタレントへの中傷
元AKB48のメンバーでタレントの女性が本人のブログで妊娠発表後に「嘘つくな」「流産しろ」といったメッセージが毎日届いたり、インターネット上に自宅の住所を晒されるなどの被害を受けたりした。

5 SNS上での誹謗中傷

情報モラルとしての注意点

- 非難されるようなことをしたんだからネットで中傷されても当然という主張は通らない
- みんなが言っているからといって、自分も悪口を言っていいわけではない

- PCやスマホ画面の向こう側には生身の人間がいることを忘れずに
- 面と向かって言えないことはネットでも言わない

情報リテラシーとしての注意点

- ネット上の情報は真偽不明のものが多い。常に批判的な目で見る必要がある。
- 情報源、発言者の信頼度を見る
- 情報の一次ソースを確認する
- 複数の情報を比較参照する

5 SNS上での誹謗中傷

でも現実は・・・

拡散される中傷や誤情報

暴走する“ネット私刑”

5 SNS上での誹謗中傷

もしかすると・・・

もはやソーシャルメディアは「情報を共有する」ためのものではなく、「感情を共有する」ためのものなのかも。

その裏には感情を動かした情報があるが、それが正しいかどうかはまた別の話。

5 SNS上での誹謗中傷

匿名がそのジレンマを解決してくれんや

世の中の評価なんざどうでもいいと思えば、そんな線引きはどうでも良くなる

評価が下がるけど言わなければいけないこともー杯あると思います。そもそも人の評価なんて気にしてると、逆に評価下がるんじゃないでしょうか？

「言ってもいい事」と
「言ってはいけない事」の間に
「言うことで自分の評価が下がる言葉」が
あることを忘れてはいけません
言葉の取り扱いには『想像力』が必須です

母から子へのSNS金言がクール！

小5の息子にSNSで気をつけるべきことは何かと聞かれたから「フォロワー数は自分に向けられた銃口の数だと思え」「誹謗中傷受けても一切反論せず全部スクショ撮れ」「500RT超えたらクソリプラインだから覚悟しろ」って答えたんだけど宿題だったらしくクラスのみんなの前で発表したらしい。

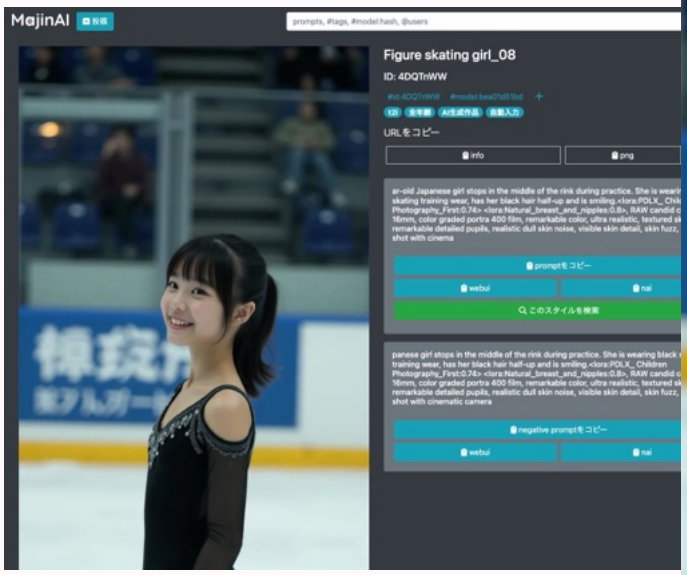
というツイートがネットでバズって朝起きたらクソリプライン超えて銃口が増えていた

6 ディープフェイク

生成AIの到来で、実写と見分けがつかない画像や巧妙な偽情報が容易に生成できてしまう。ますます情報リテラシーが求められる。

6 ディープフェイク

実写かAI生成かの判断がつかないことの問題



6 ディープフェイク

生成AIによるディープフェイクが招く問題

視聴者の行動に与える影響

- 本物の情報だと信じて誤った行動をとってしまう危険性
- 全てがフェイクではないかと疑い始めることでの不利益

擬似児童ポルノの影響

- 被告人が「これはAIで作ったものだ」と主張したときの検察側の主張責任
- 被害児童の保護が遅れる可能性

Thank you!

ご心配ごとなどありましたら
お気軽にご相談ください。

web110.com

参考資料

参考資料

万が一に備えてサイバー保険

サイバー保険とは | サイバー保険 | 日本損害保険協会
https://www.sonpo.or.jp/cyber-hoken/about/

サイバー保険で補償されるのは 3 種類

1. 第三者への賠償責任
2. 自社の復旧費用
3. 事業の中断による逸失利益

ランサムウエアの被害によって支払った身代金は補償対象にならない。

参考資料

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

参考資料

iPhoneで契約したサブスクを確認する方法

設定 ＞ Apple Account ＞ サブスクリプション

参考資料

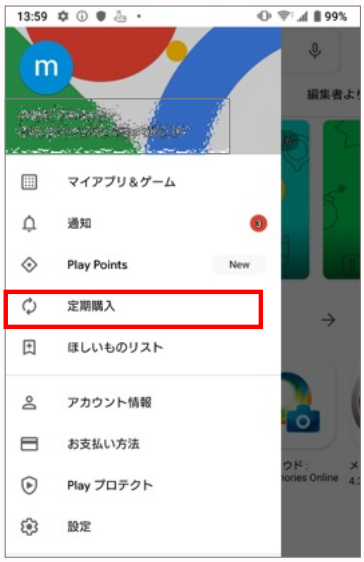
iPhoneで購入履歴を確認する方法

設定 ＞ Apple Account ＞ メディアと購入 ＞ 購入履歴

参考資料

サブスクリプションの確認方法

<Androidの場合>



解約方法の詳細はサービス提供者のヘルプページ参照

◆ Android端末で、定期購入を解約する

「Google Play での定期購入の解約、一時停止、変更」

https://support.google.com/googleplay/answer/7018481?co=GENIE.Platform=Android

参考資料

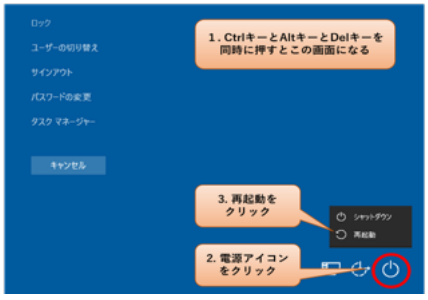
偽のセキュリティ警告画面を閉じる方法

【Esc】キーを3秒程長押し

「×」（閉じる）ボタンが現れたらクリック

【Ctrl】【Alt】【Delete】キーを同時に押す

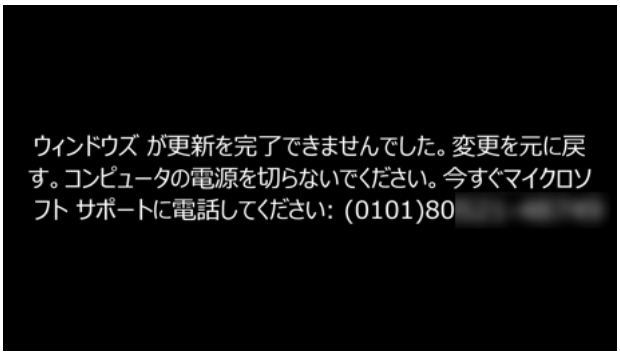
表示された画面から再起動を選択



参考資料

偽のセキュリティ警告画面を閉じることができない場合もある

この画面が出てESC長押しでも閉じれない場合は当該画面が出現する以前に意図しない何らかのソフトやサービスをインストールしてしまったことが原因と推定されます。初期化が必要。



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
警察相談専用	警察相談専用窓口	#9110
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	03-5978-7509
未公開株	未公開株通報専用窓口	0120-344-999
契約上のトラブル	消費者ホットライン	188（いやや）
仮想通貨	日本暗号資産取引業協会	https://jvcea.or.jp/contact/form-contact/

参考資料

インターネット上の誹謗中傷に関する相談窓口

悩みや不安を聞いて欲しい

「まもろうよ こころ」
（厚生労働省）
https://www.mhlw.go.jp/mamorouyokokoro/

相談窓口を紹介

- 悩みや不安を抱えて困っている方に対して、気軽に相談できる窓口を紹介している。
- 電話、メール、チャット、SNSなど、様々な方法による相談が可能。

まずアドバイスがほしい・自分で迅速に削除依頼したい

違法有害情報相談センター
（総務省支援事業）
https://ihaho.jp/

迅速な助言

- 相談者自身で行う削除依頼の方法などを迅速にアドバイスする。
- 人権侵害に限らず、様々な事案に対して幅広なアドバイスが可能。
- メールでの相談対応のみ。

自分で削除依頼できない・自分の代わりに削除依頼して欲しい

人権相談
（法務省）
https://www.jinken.go.jp/

削除要請・助言

- 相談者自身で行う削除依頼の方法などの助言に加え、法務局が事案に応じてプロバイダ等に対する削除要請を行う。
- 全国の法務局における面談のほか、電話やインターネットでも相談を行う（外国語にも対応）。

誹謗中傷ホットライン
（セーファーインターネット協会）
https://www.saferinternet.or.jp/bullying/

プロバイダへの通知

- 被害者から連絡を受け付け、特定誹謗中傷に該当すると判断したものについては、国内外のコンテンツプロバイダに各社の利用規約等に沿った対応を求める。