Grafsec-J第三回全国大会

サイバー犯罪に関する相談例から

安心相談窓口に寄せられる相談の傾向と、今後必要と考える被害予防対策について

2017年 3月13日（月）13:50～14：25

独立行政法人情報処理推進機構
技術本部　セキュリティセンター
吉川誠司

IPA情報セキュリティ 安心相談窓口

コンピュータウイルスおよび不正アクセスに関する被害や技術的な相談を受付けて
被害拡大防止に向けた情報発信を行っています。

対象

すべての企業・
組織、IT利用者

窓口

平日
9:00-12:00
13:30-17:00

情報発信

- 安心相談窓口だより
- 注意喚起
- 白書・統計
- FAQ

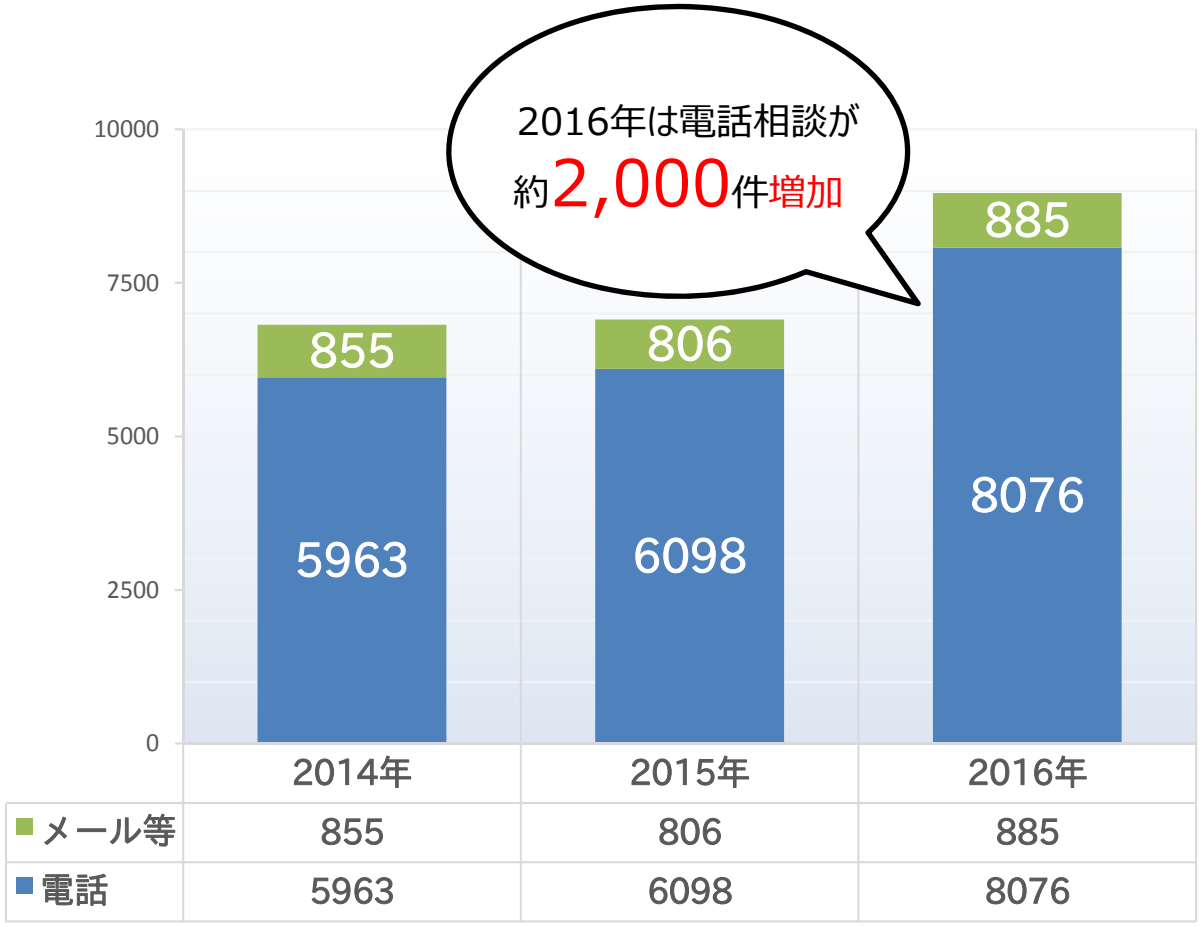
1 相談種別ごとの傾向分析

2 20歳未満からの相談内容

3 セキュリティ警告を装う手口に要注意

4 相談傾向から見えてくる３つの課題

相談員対応件数*1の推移



	2014年	2015年	2016年
メール等	855	806	885
電話	5963	6098	8076

*1：電話、メール、FAX等で実際に相談員が対応した件数。「自動応答システム」で入電したものの、相談員が対応しないまま切断したものは含まない。

2016年　相談種別ランキング

1位　ワンクリック請求

２位　偽警告事案

３位　その他諸々

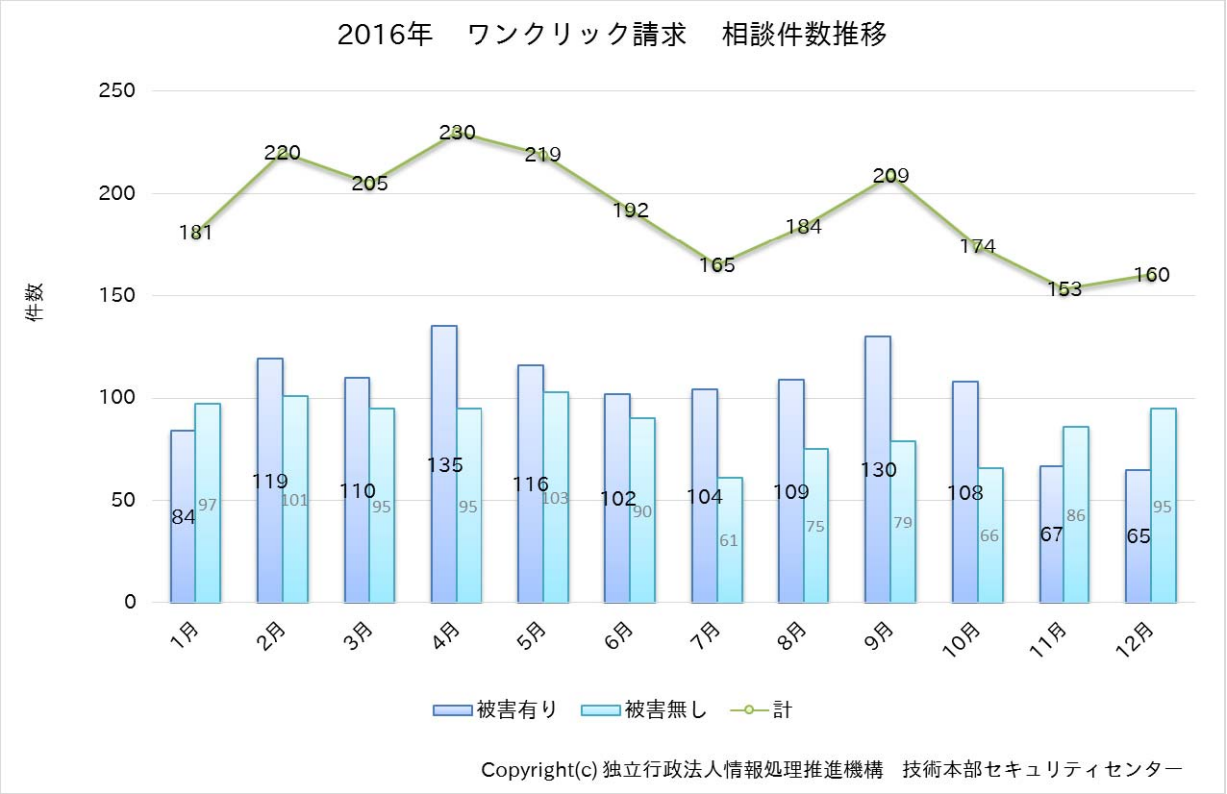
- ランサムウェア
- Dos攻撃
- ウェブページ改ざん
- アカウント乗っ取り
- セクストーション
- フィッシング

相談種別1位：「ワンクリック請求」

2016年に寄せられた「ワンクリック請求」に関する相談件数は2,292件

相談種別順位：1位

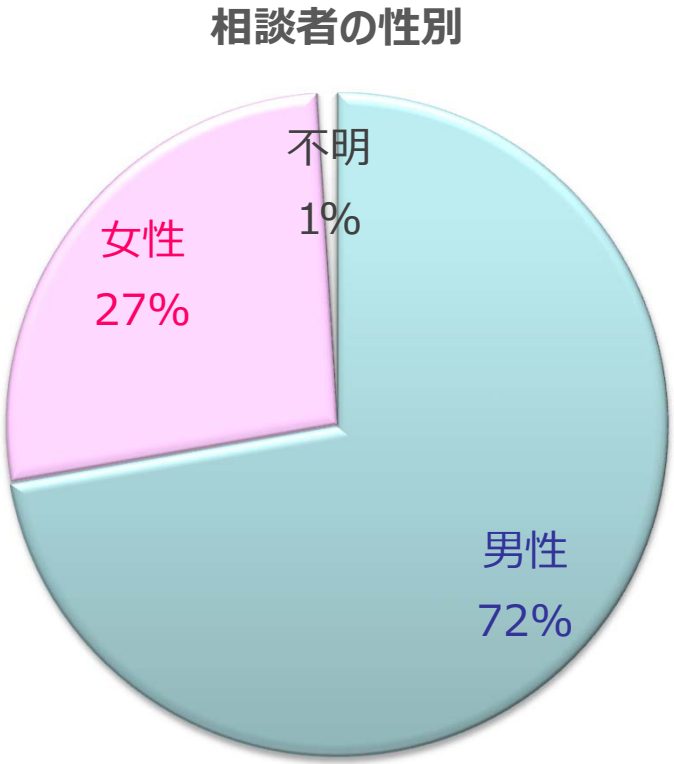
全ての相談に占める割合：25.6%



「ワンクリック請求」の事例

釈明しようと連絡をとってしまったら相手の思うつぼ。年齢が上がるにつれ、素直に連絡してしまう傾向にある。

「ワンクリック請求」相談者の性別



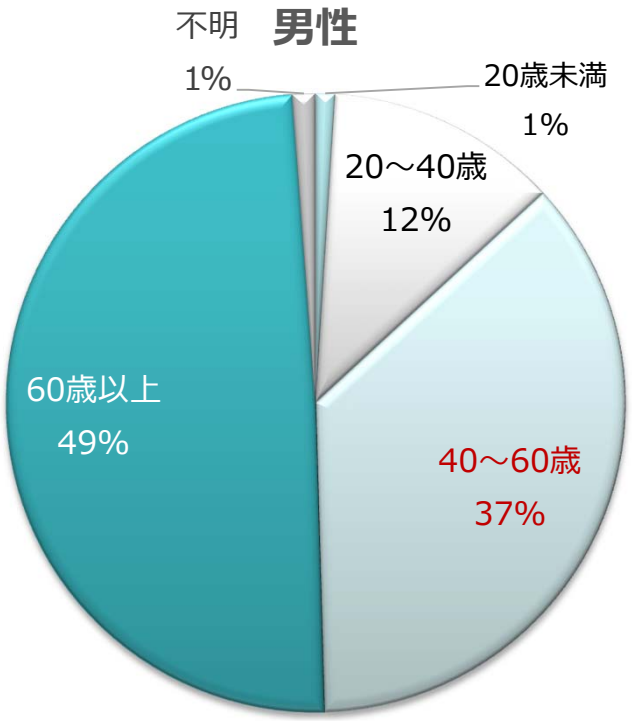
POINT!

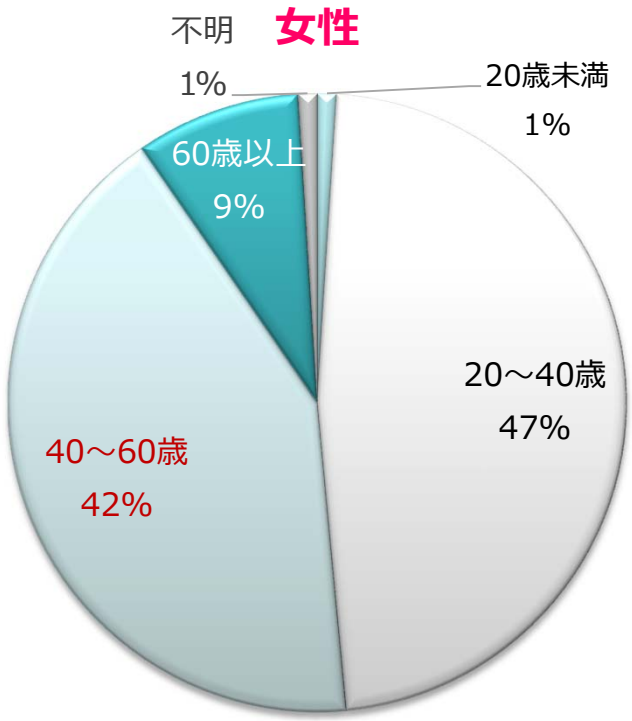
アダルトサイトを閲覧中に遭遇することが多いためか、7割は男性

POINT!

女性からの相談内容に「アダルトサイト」を含むものが65%

「ワンクリック請求」相談者の年齢層





POINT!

- 20歳未満が少ない理由は、スマホの基本操作能力とワンクリ手口の認知度の影響か
- 請求画面の消し方に関する相談がほとんどであるためか、年齢層高めの相談が多い

「ワンクリック請求」相談例

パソコン利用

- ゴルフの無料動画をクリックしたらいきなり、登録料25万円とでて、請求画面が消えない。（60歳以上　男性）
- 消費者センターに相談しようと思いWebで検索したところ、民間の消費者センターに連絡してしまい、探偵に5万ほど支払った。（40～60歳　男性）
- 請求画面を出ないようにしたいが、システムの復元ポイントがない。（60歳以上　男性）

「ワンクリック請求」相談例

スマホ利用

- スマホから請求画面が消えない。
- 動画の再生ボタンを押すとシャッター音。情報漏えいやウイルス感染が心配。（20～40歳、男性）
- 登録料19,8万円＋契約料19,8万円を支払えば画面解除できるというので支払ったが、契約解除には210万円を支払う必要があると言われた。（年齢性別不明）
- 退会のために電話したらいきなりフルネームを言われた。（20～40歳、女性）

「ワンクリック請求」の被害予防に必要な知識

1.請求画面の消し方

消し方は様々だけど、必ず消す方法があること
だけは知っておいて欲しい

2. 絶対に業者には連絡しない

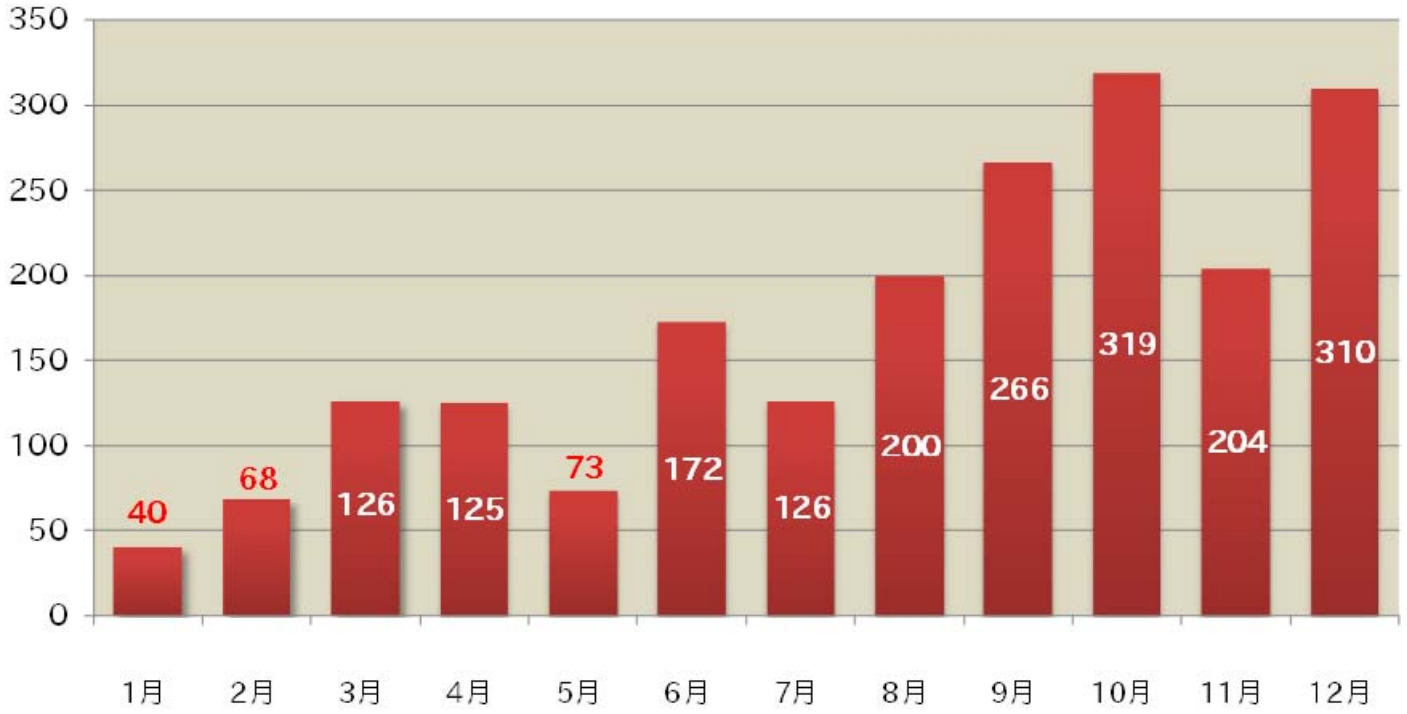
- 連絡したら相手の思うつぼ
- 連絡するなら業者ではなく消費生活センター
  かIPA安心相談窓口

相談種別2位：「偽警告」

2016年に安心相談窓口へ寄せられた偽警告に関する相談件数は2029件

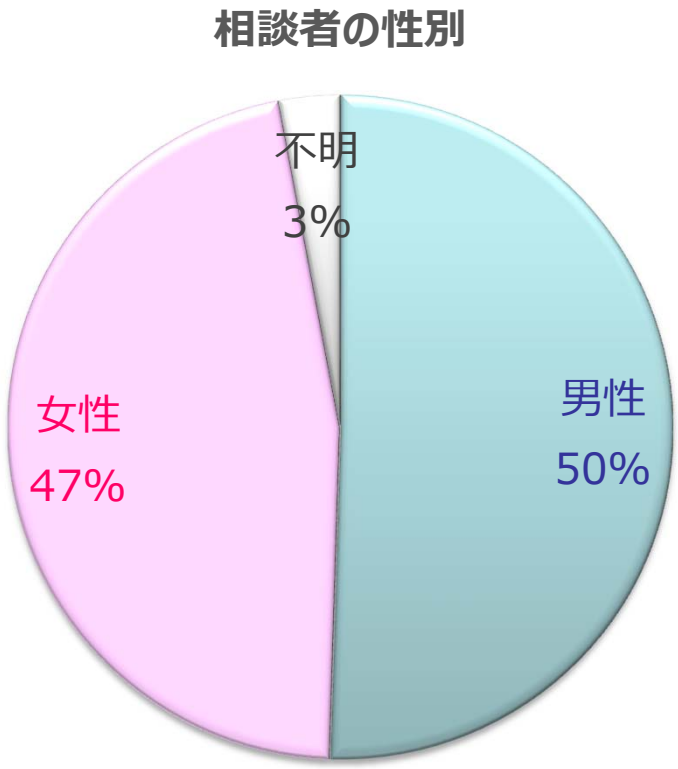
相談種別順位：２位

全ての相談に占める割合：22.6%



（図）2016年に安心相談窓口へ寄せられた偽警告に関する相談件数の推移

「偽警告」相談者の性別

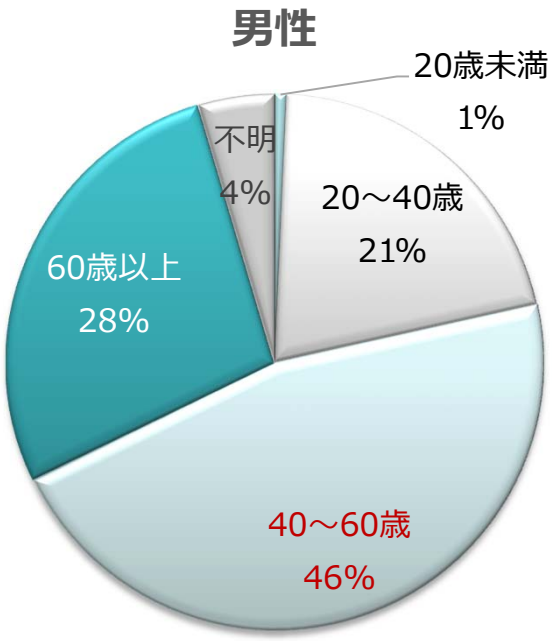


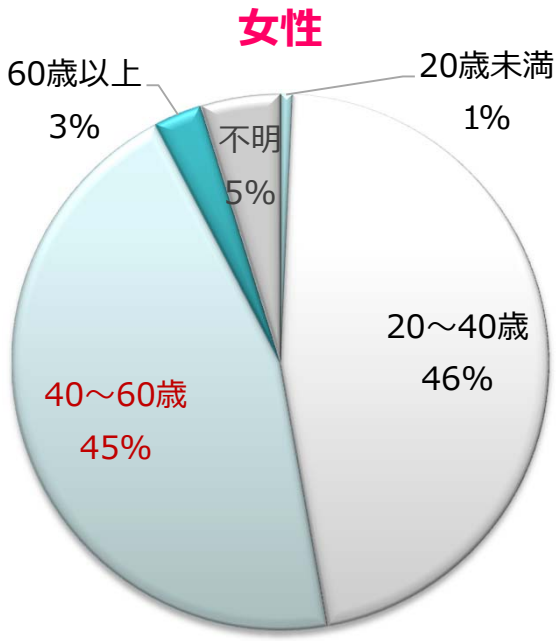
POINT!

偽警告が表示される仕掛けはあらゆるところに点在するためか、男女間の有意差は見られない。

言い換えると、誰もが被害に遭う可能性がある。

「偽警告」相談者の年齢層

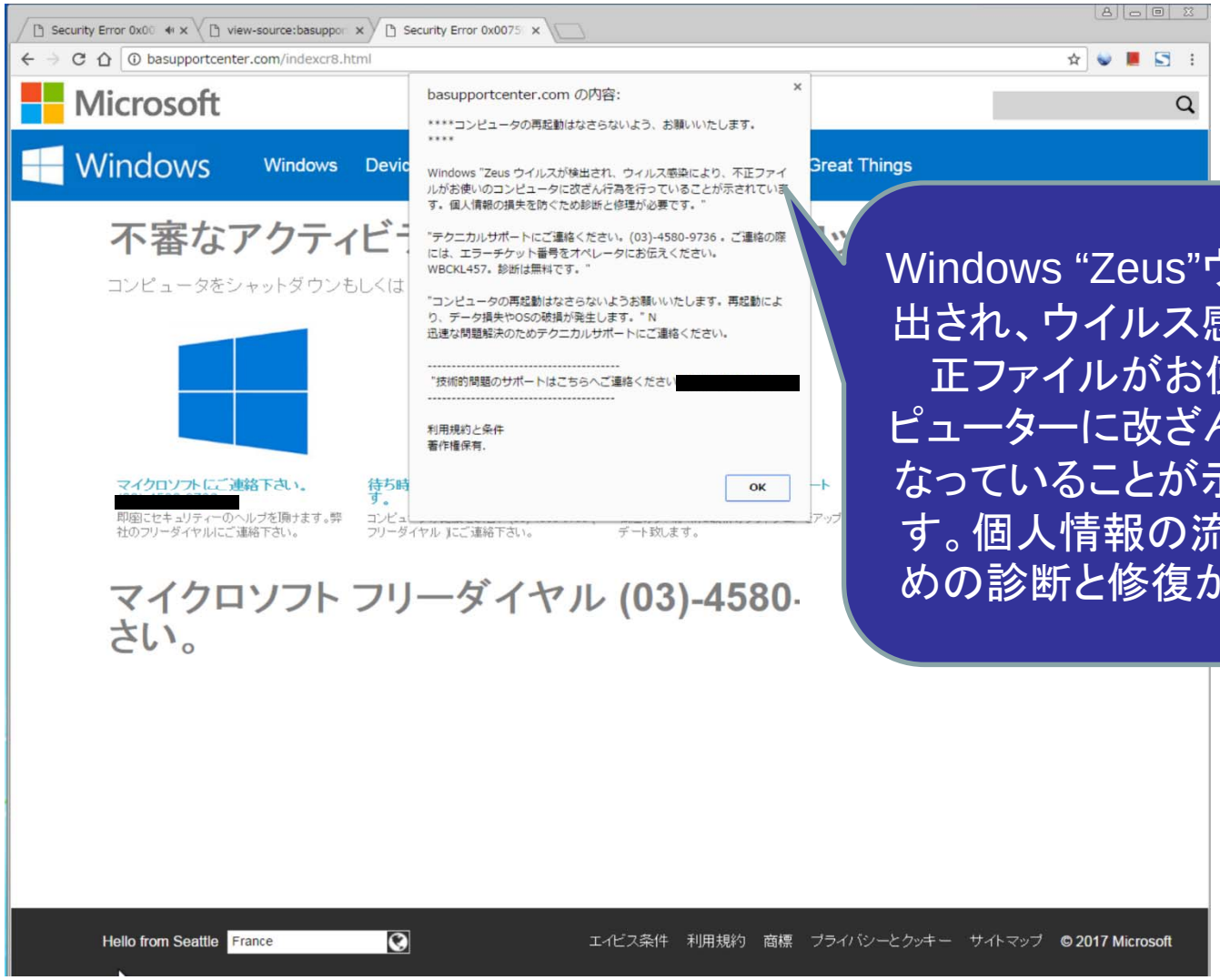




POINT!

- 女性は20～60歳で全体の92%を占めるが、男性は60歳以上も28%。
- はっきりした原因は分からないが、60歳以上の女性でインターネットを使う人は男性ほど多くないということなのか？

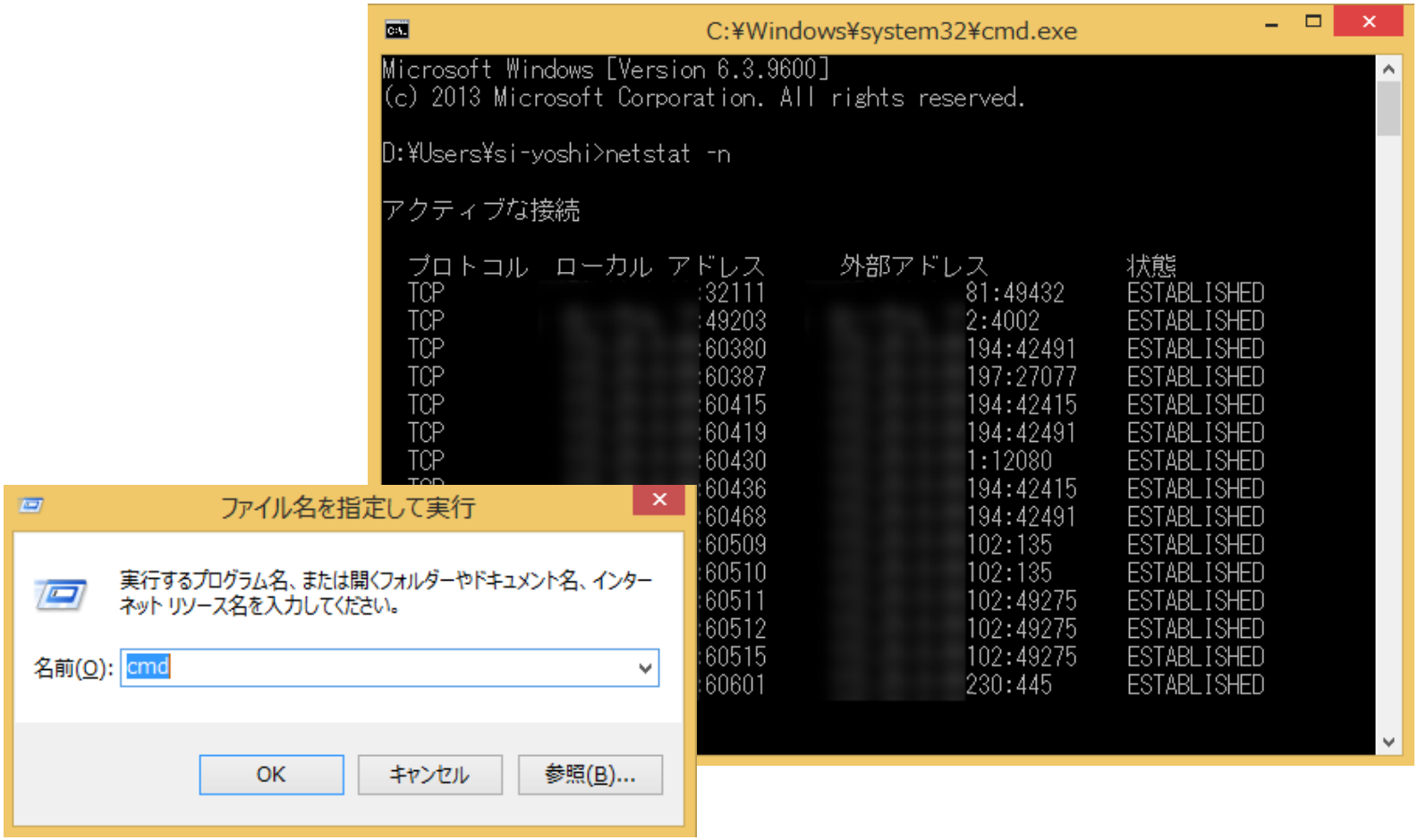
偽警告の内容は様々で、一般ユーザーが真偽を判断することは困難。マイクロソフトを騙る手口も。



Windows “Zeus”ウイルスが検出され、ウイルス感染により不正ファイルがお使いのコンピューターに改ざん行為をおこなっていることが示されています。個人情報の流失を防ぐための診断と修復が必要です。

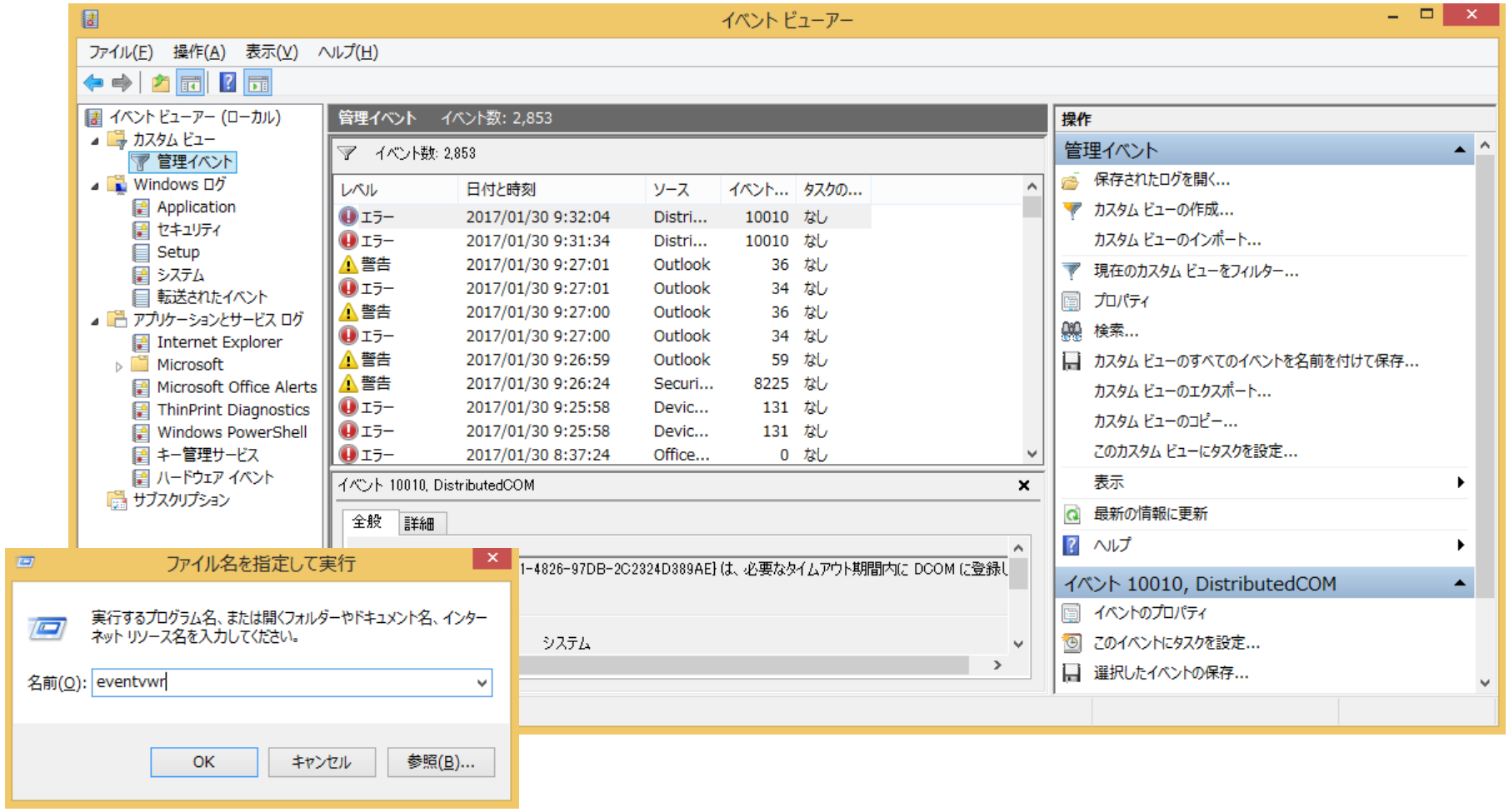
遠隔操作で相手が見せてくる画面の一例

（ファイル名を指定して実行）で「cmd」を実行し、「netstat -n」コマンドを実行した結果



遠隔操作で相手が見せてくる画面の一例

（ファイル名を指定して実行）で「eventvwr」を実行した結果



「偽警告」よくある相談例

- 警告画面と警告音が消えない
- 遠隔操作でパソコン内の情報を盗まれた可能性はないか？
- 今後も遠隔操作され続けることはないか？
- サポート代金を支払ったがそのままパソコンを使い続けて大丈夫か？

「偽警告」被害予防に必要な知識

1.偽警告の手口が存在することを知る

既存の点検商法と対比して説明すると分かりやすい

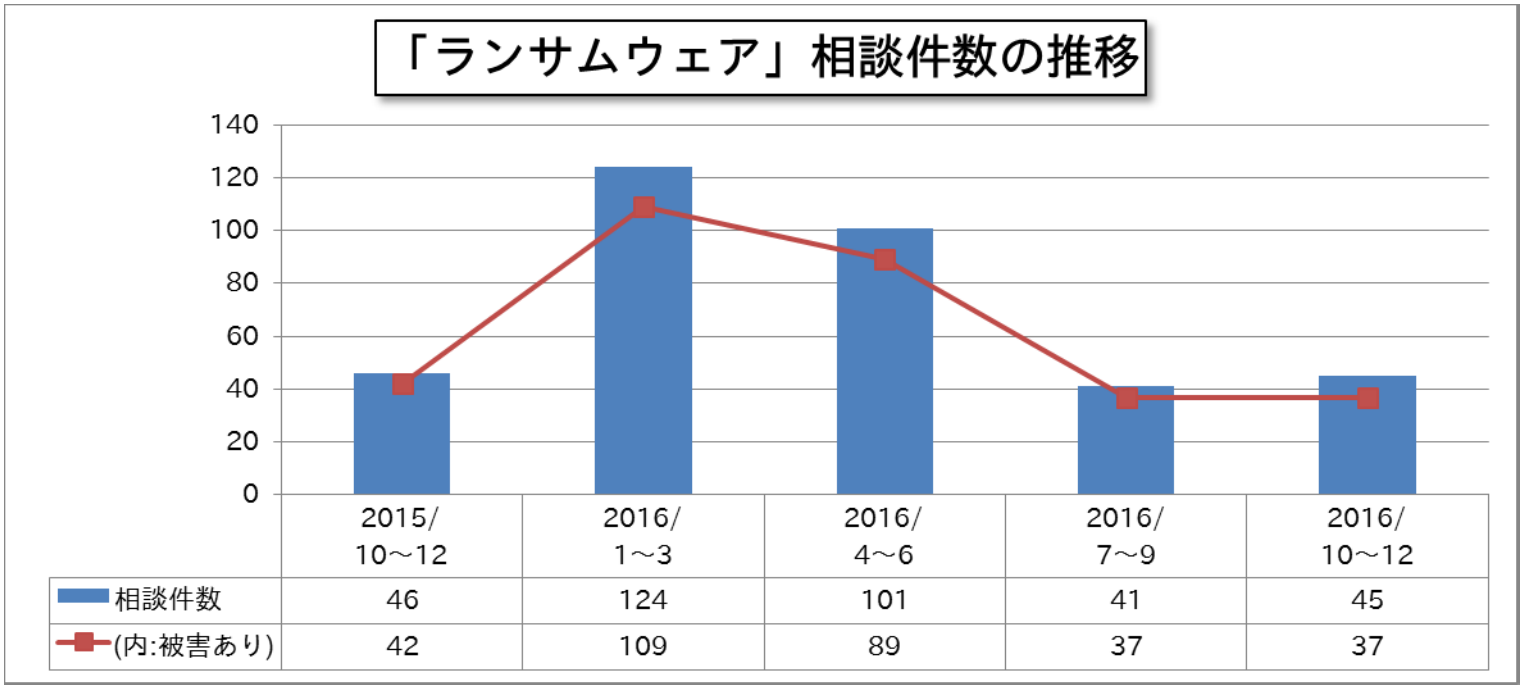
2. 偽警告画面はブラウザの終了で対処

再びブラウザを開くときに前回のセッションを再開しなければ警告表示は出てこない

相談種別：ランサムウェア

2016年に安心相談窓口へ寄せられた偽警告に関する相談件数は311件

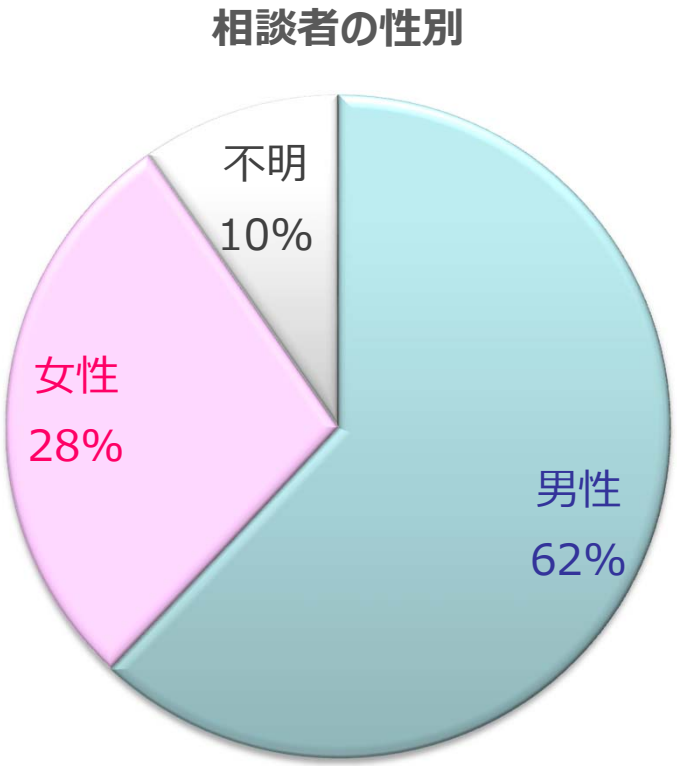
全ての相談に占める割合：3.5%



	2015/10～12	2016/1～3	2016/4～6	2016/7～9	2016/10～12
相談件数	46	124	101	41	45
(内:被害あり)	42	109	89	37	37

2016年に安心相談窓口へ寄せられた「ランサムウェア」に関する相談件数の推移

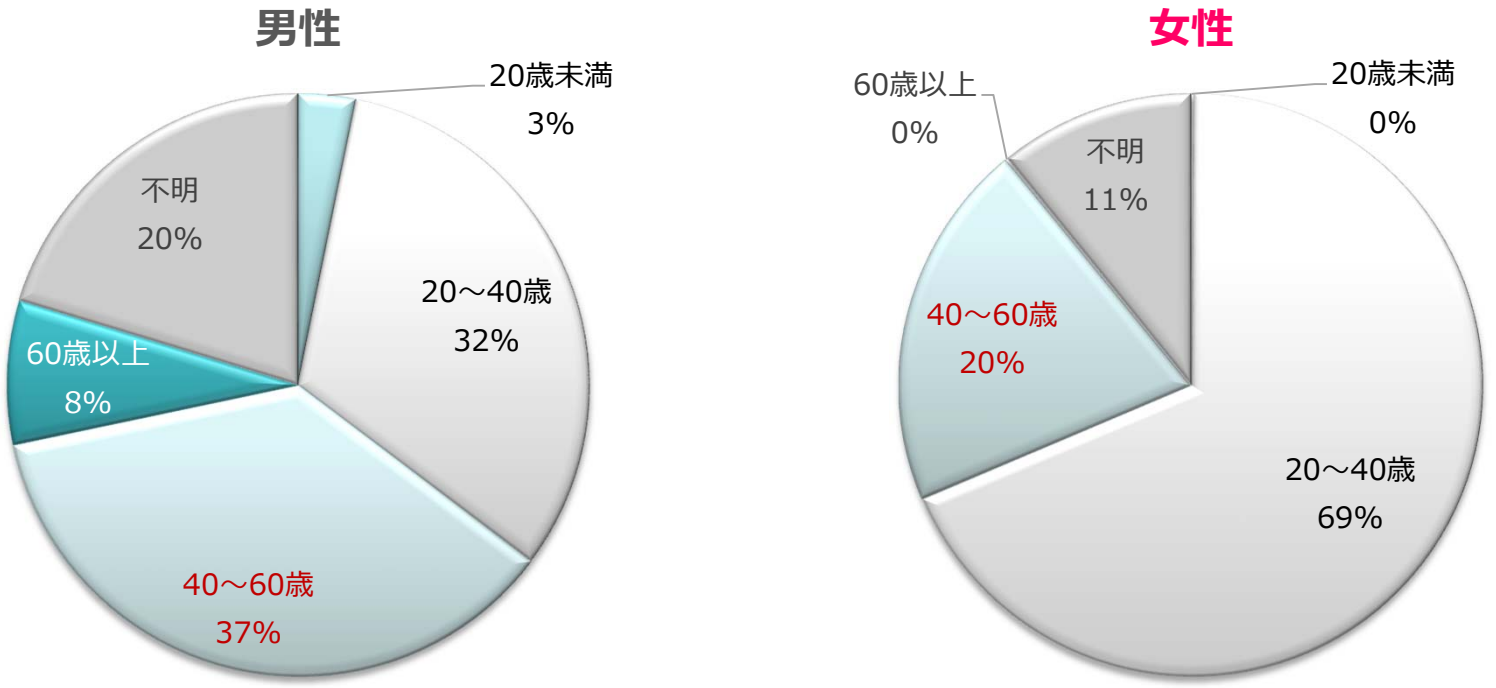
「ランサムウェア」相談者の性別



POINT!

- 男性の相談が多いことの明確な理由は不明
- 女性の6割、男性の7割はwindowsパソコンでの被害

「ランサムウェア」相談者の年齢層

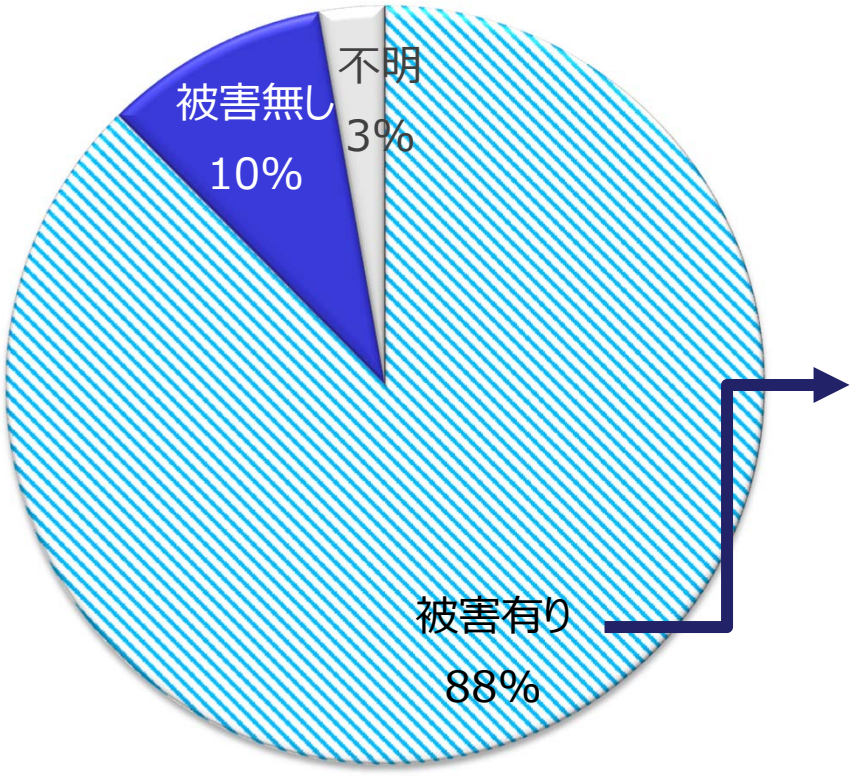


POINT!

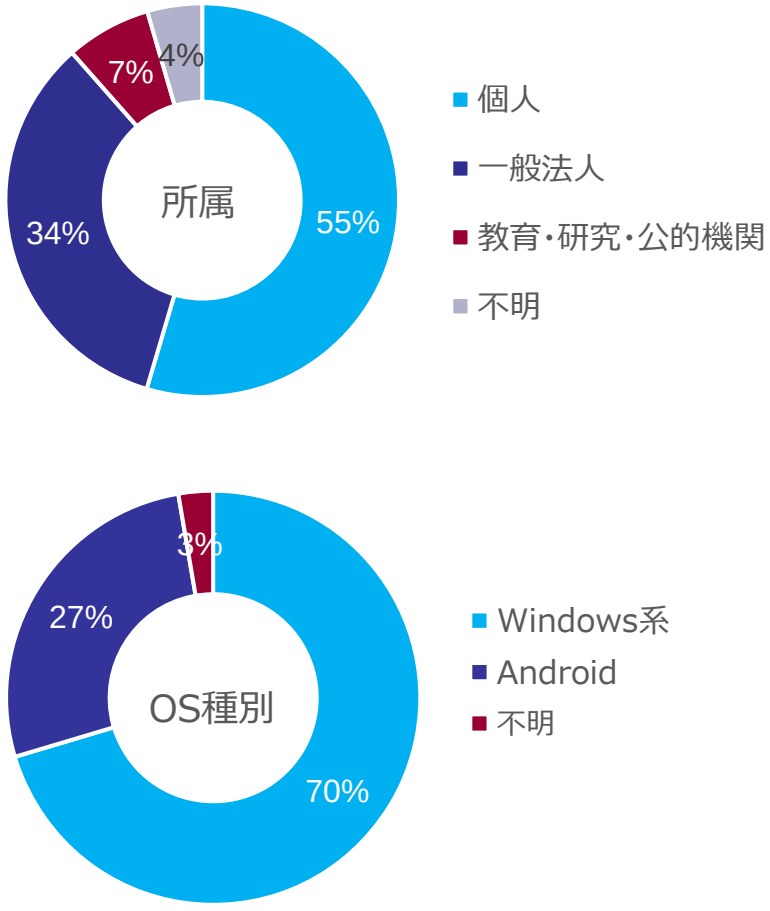
- 女性は20～40歳に集中しているが、男性は極端な偏りはない。
- はっきりした原因は分からないが、60歳以上の女性でインターネットを使う人は男性ほど多くないということなのか？

「ランサムウェア」被害の有無および内訳

＜被害の有無＞



＜被害有りの内訳＞



ランサムウェア「被害無し（10%）」の相談例

- ランサムウエアに感染しているかどうか心配
- ランサムウェア被害防止のバックアップ方法について聞きたい
- ランサムウェアに感染した場合の対処について確認したい
- ランサムウェアを体験するアプリやソフト、または映像はありますか

- ランサムウェアに対する危機意識は有するものの、具体的な対処法に関する知識が不足している。
- 既存の情報がまだ十分届いていないことが原因と考えられる。

● ランサムウェア「被害有り」の相談例

全体共通

- 暗号化されたファイルの修復はできるのか。
- パソコンはそのまま使って問題ないのか。
- ランサムウェアがネットワーク上の他のパソコンに感染することはないか。

ランサムウェアの認知度が上がるにつれて
こうした基本的な質問は減ってくると思われる。

- 修復をどこに依頼すればいい。知り合いから紹介を受けた業者には48万円と言われたが高くないか。

基本的に犯人以外にファイルの復元は不可能
であることの周知が必要

● ランサムウェア「被害有り」の相談例

IPA

個人

- 長い期間をかけて作ってきた論文が暗号化された。
- ランサムウェアに感染後、新たなファイルを入れても暗号化はされていない。これはもう大丈夫だと考えて良いのか。
- 復元するツールがあるようだが使っても大丈夫か。
- 拡張子がすべて変えられてしまったが、市販のウイルス対策ソフトで駆除できるのか、それとも業者に依頼しなければならないのか。

● ランサムウェア「被害有り」の相談例

一般法人、教育・研究・公的機関

- ファイルが暗号化されたことよりも情報漏えいが心配。
- 基幹システムの都合上、Javaの更新が5～6年できないまま放置していたことが感染原因。
- 暗号化されなかったoutlookの.pstファイルをそのまま使い続けてもウイルスを拡散されるようなことはないか。
- 感染した端末を特定できていないのでネットワークから隔離できない。
- バックアップ先も暗号化された。身代金を支払うしかないと思っているのだが支払い方法がまったくわからない。

「ランサムウェア」被害予防に必要な知識

1.ファイル暗号型に有効なデータバックアップ方法

ネットワークから切り離したところでバックアップデータを保存しておくということ

2. スマホの画面ロック型への対処方法

セーフモードで起動して問題のアプリをアンインストールすればよい。ファイルの暗号化はない。

今のところ

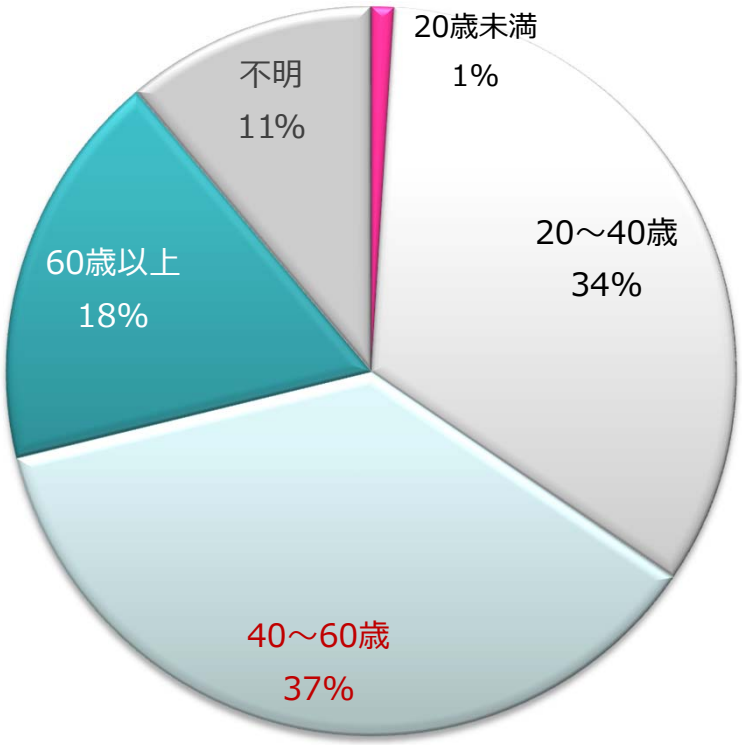
1 相談種別ごとの傾向分析

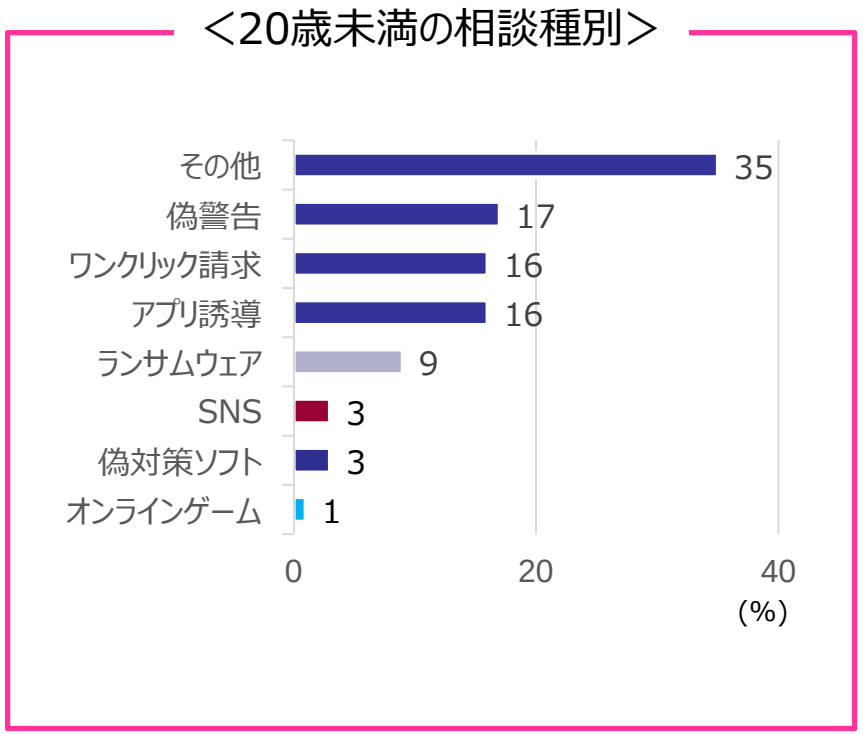
2 20歳未満からの相談内容

3 セキュリティ警告を装う手口に要注意

4 相談傾向から見えてくる３つの課題

20歳未満からの相談内容





20歳未満からの相談「その他」の例

消費生活系

- LINEとカカオトークのゲームでどんどん課金されている。元カレが怪しい。（女性）
- 有料動画を閲覧したといった架空請求のSMSが届いた。（女性）
- Redtubeのプレミアム会員料は前払いなのか知りたい。（男性）

ウイルス・不正アクセス系

- iPadにBitTorrentをインストールした。アンインストールしたらお母さんのSafariが使えなくなった。（男性）
- ポケモンGOのために作成したGoogleアカウントが乗っ取られたかもしれない。（女性）
- 無料ゲームアプリの広告を触ったらサイトに飛んだがウイルスか？（男性）

プライバシー系

- yahooなどで自分の名前を入れた時にあまりよくないものが一緒に出てくるので検索結果に出ないようにしてほしい。（男性）
- オンラインゲームのチャットで喧嘩したら「IPアドレスをばら撒くぞ」といわれた。2ちゃんねるに書かれた。Whois検索すれば個人が特定されてしまうのか。（男性）
- ツイプロに投稿した内容を削除したいがどうすればいいか。（女性）

1 相談種別ごとの傾向分析

2 20歳未満からの相談内容

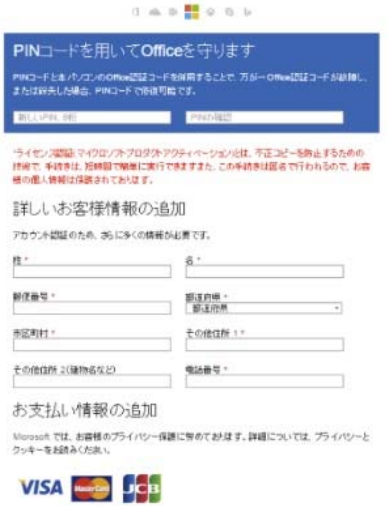
3 セキュリティ警告を装う手口に要注意

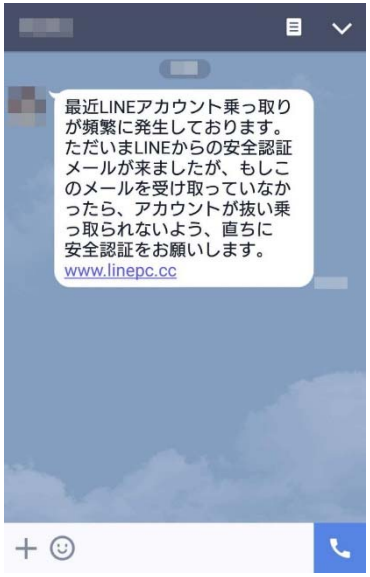
4 相談傾向から見えてくる３つの課題

セキュリティ警告を装う手口に要注意

セキュリティ警告を装った攻撃の一例

2017/02
　偽Appleから「Apple IDのアカウントがロックされる」とのメール-偽サイトへ誘導。-ログインさせてアカウント情報を詐取
2017/01
　マイクロソフトを騙るフィッシングメール「Officeのプロダクトキーが不正コピーされている」-指示に従うとアカウント情報や支払情報が盗まれる（右図上）。
2016/12
　「セゾンNetアンサー」の利用者を狙ったフィッシング攻撃。「第三者によるアクセスを確認した」として偽サイトの誘導 -ログインID、パスワード、クレジットカード番号、セキュリティコード等の入力を求められる
2016/11
　LINEを装い「異常ログイン」などの警告メッセージ。-リンク先の偽サイトを開くとログインID、パスワードの入力が求められる（右図下）。
2016/11
　ICT-ISACを装った「マルウェア除去ツールの配布」装うメール - 指示に従うとマルウェア感染





1 相談種別ごとの傾向分析

2 20歳未満からの相談内容

3 セキュリティ警告を装う手口に要注意

4 相談傾向から見えてくる３つの課題

4. 相談傾向から見えてくる３つの課題

1. 高齢者を意識したやさしいセキュリティ講座の実施と、注意喚起における媒体と経路の工夫

例

- 生涯学習センター等（自宅から歩いて行ける場所）での講座実施
- 紙媒体を消費生活センター、役所、福祉事務所等で配布

2. セキュリティへの関心が低くなりがちな女性にも興味を持ってもらえるプロモーション

例

- 女性に人気の女性タレントにトークライブで自身の被害体験を語ってもらう→女子向けのニュース媒体を通じて拡散
- 小さい子供に人気のヒーローのイケメン俳優を呼んで安全教室を開催→子供を連れた若いママさん集まる

3. スマホ主体の若年層に適した情報発信

例

- スマートフォンでの閲覧に最適化したコンテンツ
- 若年層がよく利用するアプリを通じた情報発信

セキュリティセンター （IPA/ISEC）
https://www.ipa.go.jp/security/