MS&AD基礎研究所株式会社
MS&AD INSURANCE GROUP

2016 年 12 月 13 日

セキュリティ被害の実態

MS&AD 基礎研究所株式会社（社長 深澤 良彦）は、2016 年 11 月に、インターネット利用おいて何らかのセキュリティ上の脅威を経験した全国の 1,000 人（男性 500 人、女性 500 人）を対象に、「セキュリティ被害の実態」をテーマとする調査を実施しました。

本レポートでは、調査対象者が経験したセキュリティ上の脅威、その場合にとった行動、金銭被害を含む被害の形態・程度、日常の対策等について、調査で明らかになった最新の状況をご紹介します。

＜ 目　次 ＞

ご照会先	MS&AD 基礎研究所株式会社 遠藤・新納（ニイロ） http://www.msadri.jp/	電話：03-5371-6055 FAX：03-5371-6114 E メール：endo@msadri.jp

1. 調査概要

1.1 調査の目的

インターネットの利用に伴う架空請求に関する相談件数は、独立行政法人国民生活センターの集計によると 2010 年前後に一段落したものの、2012 年を境に再び増加し始めており、特にここ数年、スマートフォン経由でのトラブルに関する相談が急増している。

また、SNS は Facebook・Twitter・LINE という従来からの 3 大サイトに加え Instagram や SNOW といった新しい画像共有系 SNS の利用も若者を中心に拡大し、アクセスするデバイス環境、情報共有の場は以前にも増して著しい多様化が進んでいる。これに伴って、アカウントが乗っ取られ、金品を詐取される被害が増加している可能性がある。

加えて直近では、企業や医療機関を狙う標的型攻撃・ランサムウェアが猛威を振るっており、個人ユーザーへの影響も無視できない状況となっている。

こうした環境の中、個人のインターネット・ユーザーがどのような脅威にさらされ、どのような被害を実際に受けているかについて最新状況を把握し、対策の見直しに有用な情報を提供することを目的に本調査を実施し、被害の実態を種々の観点からとりまとめた。

1.2 調査方法

事前調査において、過去 3 年間くらいの間に以下の 9 つの「脅威」のうち 1 つ以上を経験した男女各 500 人、計 1,000 人を抽出し、その方々を対象にインターネットにより本調査を実施した。

- E メールでの架空請求
- 電話での架空請求
- アカウント乗っ取り（自分のアカウントが乗っ取られた）
- アカウント乗っ取り（乗っ取られた知人のアカウントから連絡が来た）
- 身代金型ウィルス（ランサムウェア）
- 従来型ウィルス（端末のロック、データの破壊等）
- フィッシング詐欺
- 迷惑メール（架空請求を除く）
- ワンクリック詐欺（請求）

アカウント乗っ取り／LINE、Facebook 等の登録アカウントが第三者より不正ログインされ、本人に成りすまして友人・知人にメッセージを送ったりして金品を騙し取る詐欺。

身代金型ウィルス（ランサムウェア）／PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに金銭の支払いを要求する不正プログラム。

フィッシング詐欺／正規の Web サイトやソーシャルメディアを装い、個人情報やクレジットカード情報を登録させることで情報を詐取する詐欺。

ワンクリック詐欺（請求）／メール内の URL や、Web 画面で表示されたアイコンをクリックするだけで、一方的に契約したことにさせて料金の支払いを求める詐欺。

1.3 調査対象者の属性

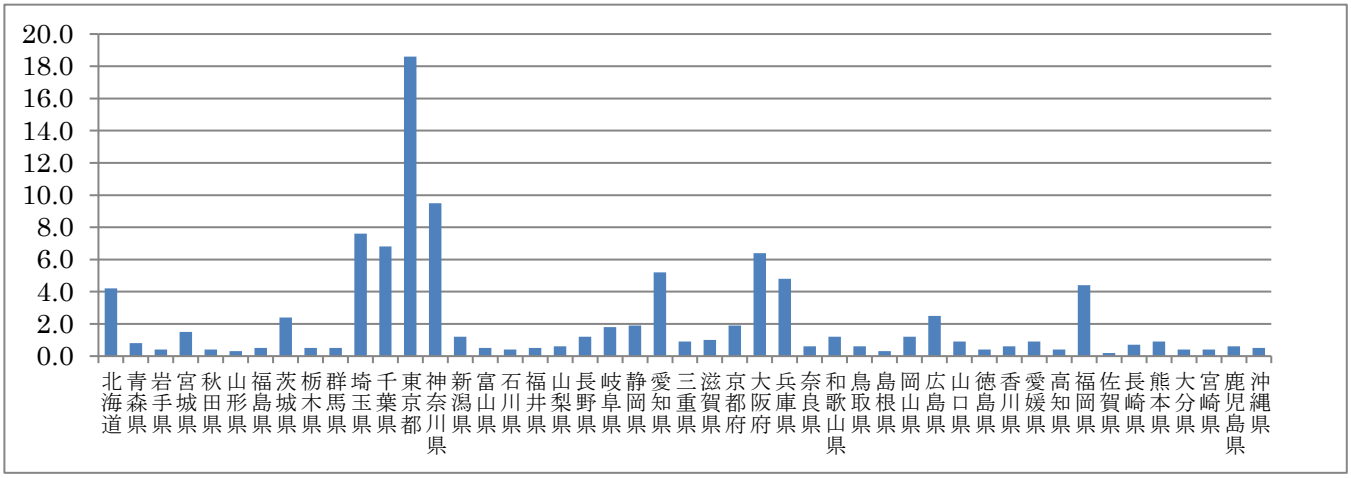
対象者 1,000 人の主な属性は次のとおりである。

(1) 年齢

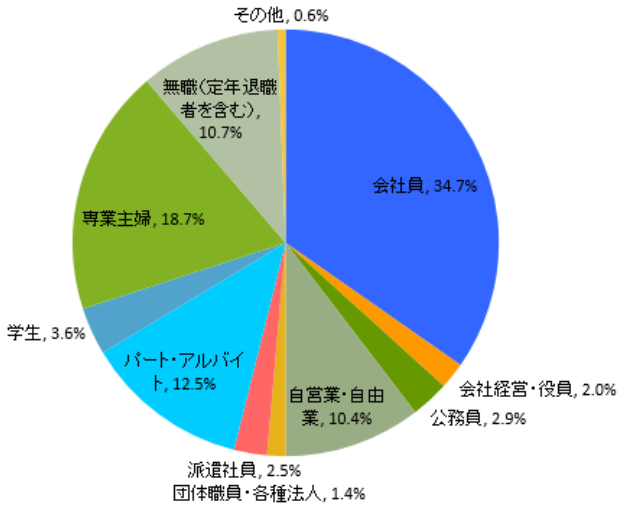
男女ともに 20 代・30 代・40 代・50 代・60 代の各年代で 100 人ずつとした。

（最若年 20 歳、最高齢 69 歳、平均 44.7 歳）

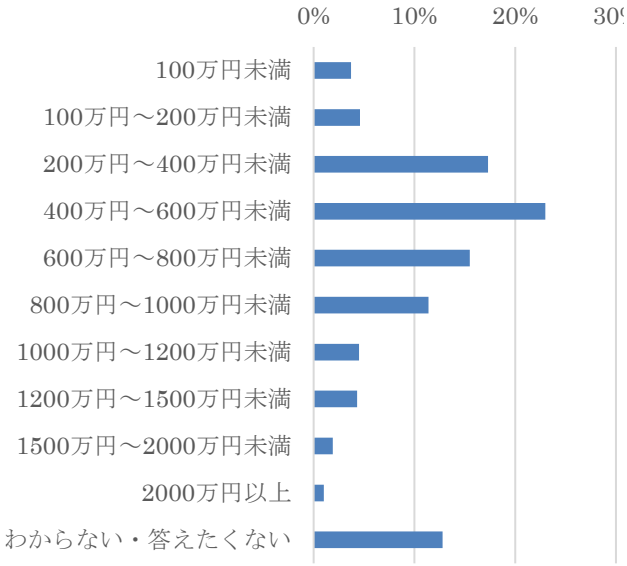
(2) 居住地域



(3) 職業



(4) 世帯年収



(5) 利用している端末・OS

スマホ（Android）	スマホ（iOS）	スマホ（Windows）	スマホ（その他／OS不明）	パソコン（Windows）	パソコン（Mac）	パソコン（その他／OS不明）	タブレット（Android）	タブレット（iOS）	タブレット（Windows）	タブレット（その他／OS不明）	スマホ以外の携帯電話
38.3%	30.5%	1.6%	0.8%	69.5%	7.5%	1.2%	9.9%	10.5%	3.3%	1.6%	22.5%

2. セキュリティ上の脅威の経験・被害発生の状況

脅威経験者（全対象者）のうち経験した脅威の内訳は、「Eメールでの架空請求」48.5%、「ワンクリック詐欺」29.0%、「アカウント乗っ取りI」（自分のアカウント）26.5%が高い。同じく脅威経験者のうち金銭的損失等の実被害にあった人の割合は「Eメールでの架空請求」18.5%、「アカウント乗っ取りI」17.4%、「従来型ウィルス」14.7%が高い。

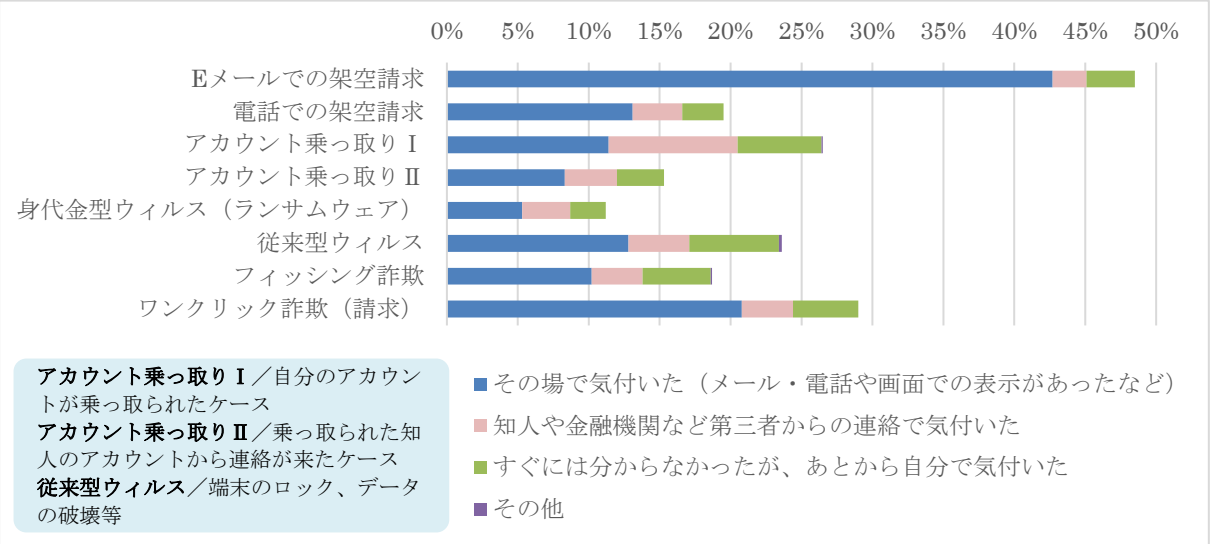
セキュリティ上の脅威は、大きく、①金品の詐取を目的としたもの、②端末やWebサイトの環境破壊（損害を与えること）を目的としたもの、③愉快犯、に分類できる。以下の分析では、①および②を対象とするため、先に挙げた9つの「脅威」のうち「迷惑メール（架空請求を除く）」以外の8つを取り上げる。

脅威経験者のうち、先に挙げた経験した脅威の割合および気付いたタイミングを示したのが図表2-1である。経験した脅威の割合が最も高いのは「Eメールでの架空請求」の48.5%であり、「ワンクリック詐欺」29.0%、「アカウント乗っ取りI」（自分のアカウントが乗っ取られた）26.5%が続く。

気付いたタイミングとしては、その場で表示が視認できる「Eメールでの架空請求」や「ワンクリック詐欺」の場合に、「その場で気付いた」の割合が高い。なお、「電話での架空請求」でもその割合が高いが、これは電話がかかってきた段階で架空請求であると気付く割合と推測される。

一方、「アカウント乗っ取りI」、「アカウント乗っ取りII」（乗っ取られた知人のアカウントから連絡が来た）、「身代金型ウィルス（ランサムウェア）」、「フィッシング詐欺」等の場合、その場では認識できず、犯人からのアプローチを含む「第三者からの連絡で気付いた」や「あとから自分で気付いた」が多くなっている。

＜図表2-1＞経験した脅威の割合と気付いたタイミング



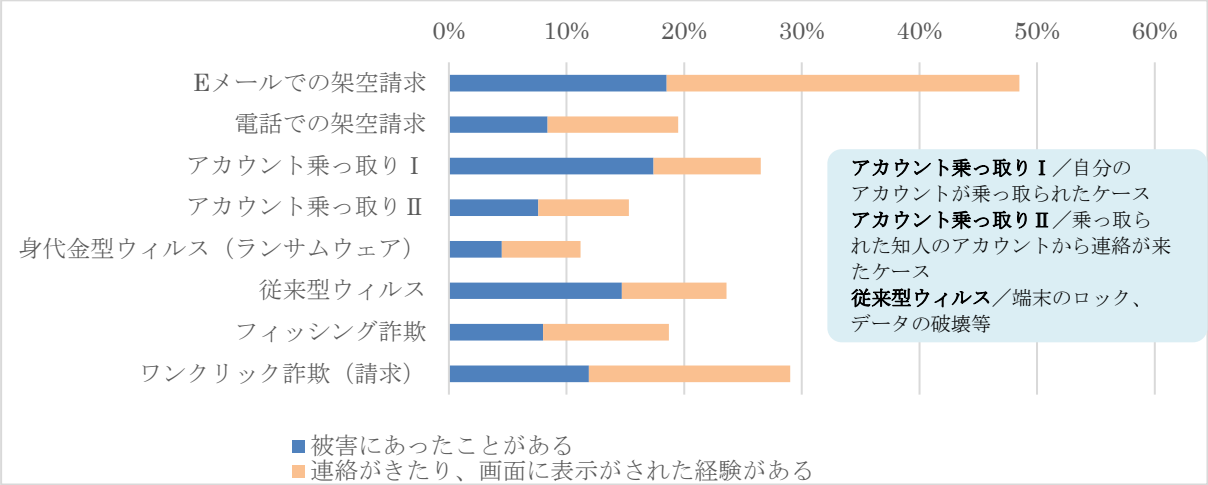
脅威経験者のうち金銭的損失や端末環境破壊等の実被害にあった人の割合を脅威の種類ごとに示したのが図表2-2である。

脅威経験者のうち実被害にあった人の割合は、上位から「Eメールでの架空請求」18.5%、「アカウント乗っ取りI」17.4%、「従来型ウィルス」14.7%、「ワンクリック詐欺」11.9%と続いている。

また、図表 2-2 では数値の表示はないが、それぞれの種類の脅威を経験した人のうち実被害にあった人の割合は、「アカウント乗っ取りI」65.7%と「従来型ウィルス」62.3%が高い。

「アカウント乗っ取りI」については、ショッピングサイトで乗っ取られたアカウントで商品を購入されたり、ポイントを勝手に交換されたりするという直接的な金銭被害が非常に多く、また、アカウントを土台として勝手に詐欺メールや広告メールを登録連絡先にばら巻かれる、といった被害も含まれている。

＜図表 2-2＞被害にあった人の割合



3. セキュリティ上の脅威を経験した場合の行動

3.1 行動パターンと金銭的被害

それぞれの種類の脅威経験者のうち要求に従い金銭を支払った人の割合は「電話での架空請求」18.9%、「アカウント乗っ取りII」18.3%、「身代金型ウィルス(ランサムウェア)」15.2%、「アカウント乗っ取りI」11.3%の順に高い。また、支払いに応じたのは、20代・30代の若年層の割合が圧倒的に高い。

脅威を経験した場合にどのような行動をとったかを示したのが図表 3-1 である。こうした場合に最も良い対処法は「何もせず無視する」ことであるとよく言われる。実際、「E メールでの架空請求」、「電話での架空請求」、「フィッシング詐欺」、「ワンクリック詐欺」を経験したユーザーでは、「特に何もせず無視をした」人の割合が高い。

しかし、「アカウント乗っ取りI」、「身代金型ウィルス(ランサムウェア)」、「従来型ウィルス」では、気付いた時点ですでに端末のロック等の被害が発生しているケースが多く、何らかのアクションを起こさざるを得ない実態にある。

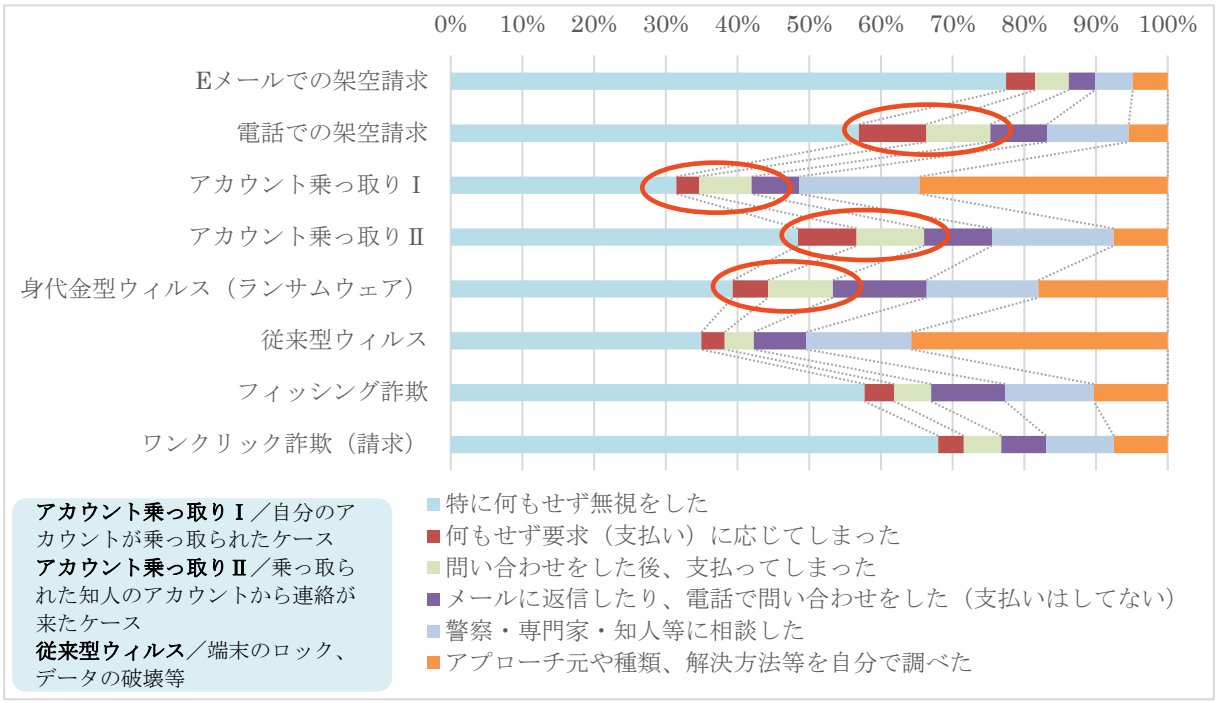
特に注目すべきは支払いに応じてしまったケースである。脅威を経験した人のうち、「何もせず要求(支払い)に応じてしまった」かまたは「問い合わせをした後、支払ってしまった」人の割合は、「電話での架空請求」18.9%、「アカウント乗っ取りII」18.3%、「身代金型ウィルス(ランサムウェア)」15.2%、「アカウント乗っ取りI」11.3%の順に多くなっている。

これら 4 種類の脅威を経験し、支払いに応じたケースにつき、男女別・年齢層別の割合を示したのが図

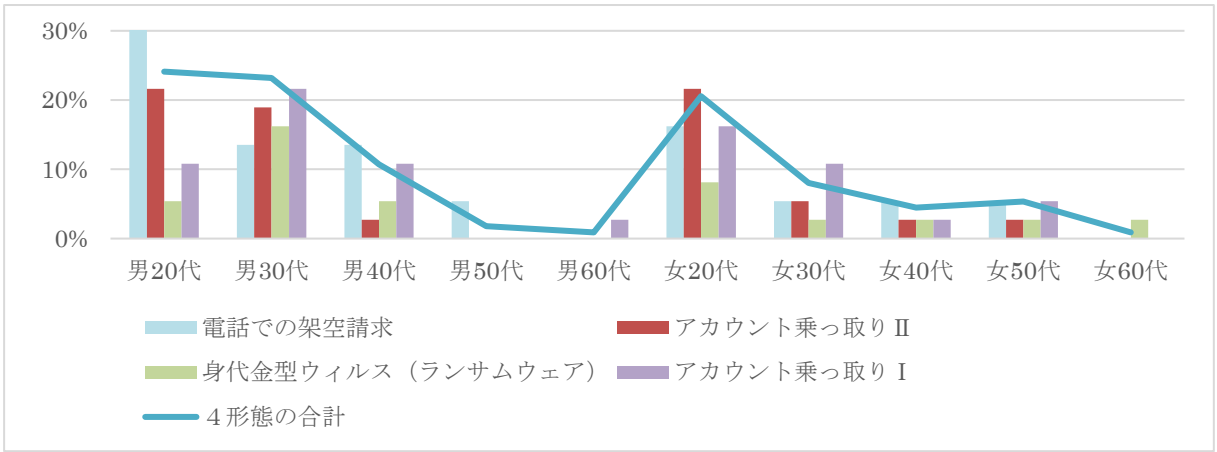
表 3-2 である。支払いに応じた人の割合は、20 代・30 代の若年層で圧倒的に高く、逆に 50 代・60 代では非常に低くなっている。若年層に金銭被害が多い理由は、フリーコメント欄を読み解く限り、「そもそもネット上での活動範囲が広く、また無警戒にバナーやリンクをクリックする傾向が強い」ためと言えそうである。

なお、支払いに応じたケースを地域別に見ると、最も割合が高いのは中国・四国の 27.3%、最も低いのは北海道の 12.5%であった。巷間取りざたされる「関西人は電話による架空請求を撃退し、被害には遭わない。」という傾向は、少なくとも近畿（滋賀、京都、大阪、兵庫、奈良、和歌山）というくくりでは顕著には表れなかった。

＜図表 3-1＞脅威を経験した場合の行動



＜図表 3-2＞支払いに応じたケースの男女別・年齢層別割合



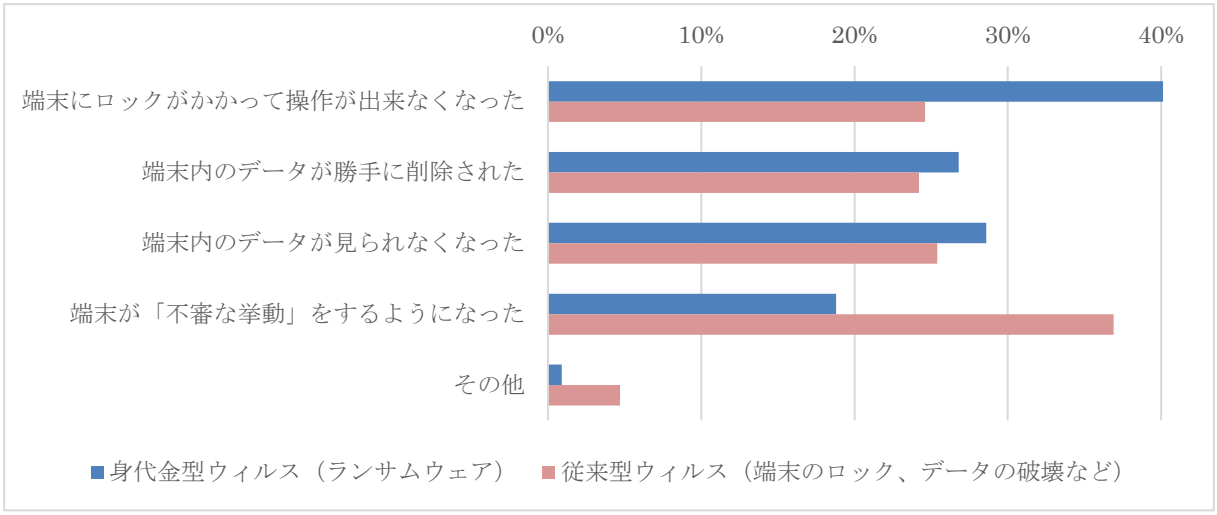
3.2 ウィルスによる被害の形態と事後対処

身代金型・従来型の両ウィルスについては、前者が端末・データの操作を制限する動きがメインであるのに対し、後者は端末の不審な挙動に繋がるケースが多い。
また、事後対処で自ら復旧する割合は男性が女性の1.7倍、第三者に委ねる割合は女性が男性の2.3倍である。

「身代金型ウィルス（ランサムウェア）」と「従来型ウィルス」を経験した場合の実被害の形態は図表 3-3 のとおりである。「身代金型ウィルス（ランサムウェア）」の場合、典型的な被害形態である「端末にロックがかかって操作が出来なくなった」、「端末内のデータが勝手に削除された」、「端末内のデータが見られなくなった」のいずれかに該当した割合は同被害数の 84%に及んだ。

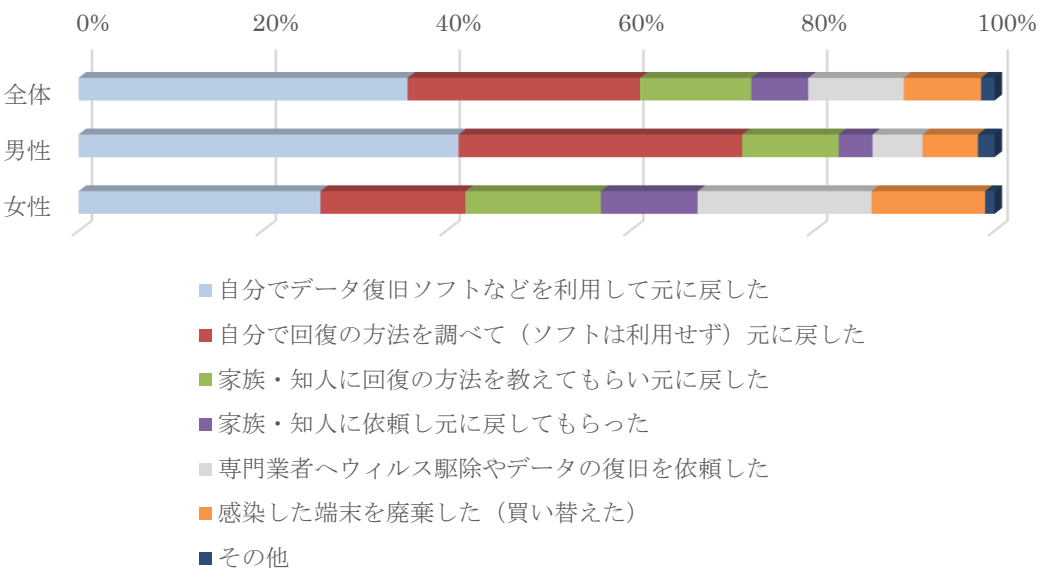
一方、「従来型ウィルス」の場合、動作が極端に遅くなる、通信量が増大する、電源が勝手に落ちる、覚えのないアプリがインストールされるといった、端末の「不審な挙動」が起こるケースが被害経験者のうち 36.9%と最も多い。

＜図表 3-3＞ウィルスによる被害の形態



ウィルスに感染した場合の対処は図表 3-4 のとおりで、自分で復旧した割合は全体で 61.1%（男性 72.3%、女性 42.1%）、専門業者・知人等の支援により復旧した割合は全体で 28.8%（男性 19.6%、女性 44.1%）となっている。

＜図表 3-4＞ウィルスに感染した場合の対処



4. 金銭的被害の実態

それぞれの脅威を経験し、さらに金銭的被害を受けた人のうち、5万円以上の被害比率が最も高いのは「身代金型ウィルス（ランサムウェア）」（35.3%）、5万円までの少額被害の比率が最も高いのは「フィッシング詐欺」（44.5%）である。
こうした要求型の脅威では、個人として支払う可能性の高い金額レベルに要求を設定している傾向があると考えられる。

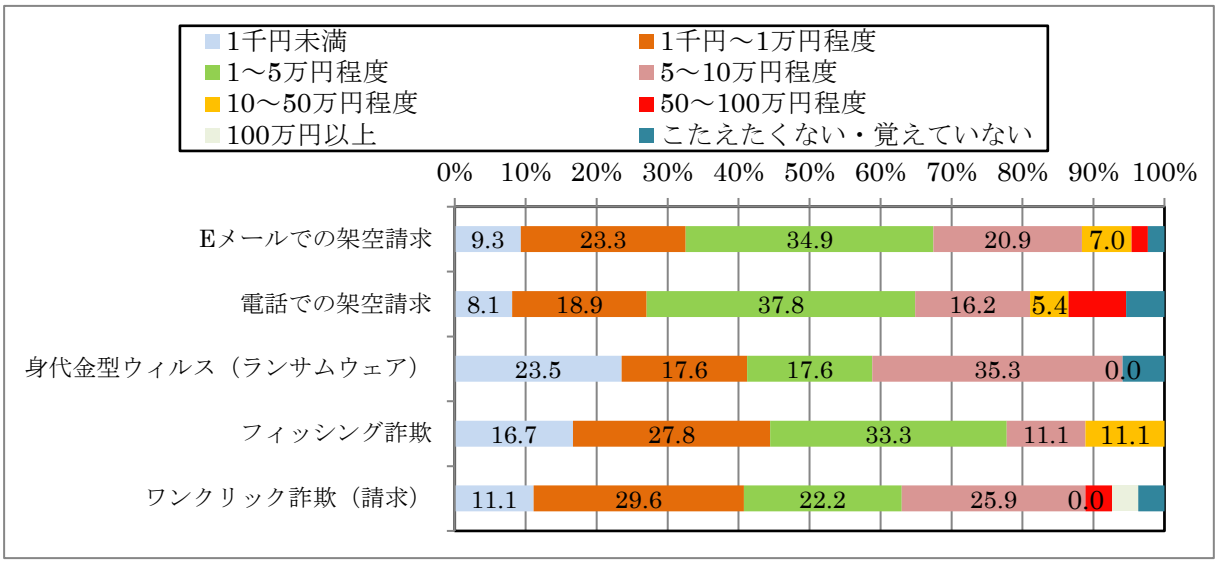
要求に応じて金銭を支払った場合（前記 3.1 参照）、その被害金額はどれくらいであったかについて、図表 4-1 にまとめた。

5 万円以上の支払比率が最も高いのは「身代金型ウィルス（ランサムウェア）」で、金銭的被害経験者のうち 35.3%のユーザーが 5～10 万円の支払要求に応じている。また、10 万円以上では「電話による架空請求」13.5%、「フィッシング詐欺」11.1%が高く、50 万以上では「電話による架空請求」8.1%、「ワンクリック詐欺」7.4%が高い。なお、「ワンクリック詐欺」には、100 万円以上の支払い事例が 1 件含まれている。

少額被害については、1万円程度まで・5 万円程度までのカテゴリーで共に「フィッシング詐欺」の割合が最も高い。フィッシング詐欺については金融機関口座やクレジットカード情報を狙いダミーサイトに誘導して ID・パスワードを盗み取る、というイメージが強く、図表 4-2 のとおりこれらの被害比率も高い。もっとも、近年では SNS や大手IT企業の運営するインターネットサービスのアカウント情報を詐取し、アプリを購入したり、不正にサービスを利用したりするケースも増加してきている。

以上のような要求型の脅威の場合、犯罪者側も個人が相手であることを認識の上、無謀な金額ではなく、支払い可能性の高い金額レベルを設定しているように思われる。

＜図表 4-1＞被害に遭った金額



＜図表 4-2＞フィッシング詐欺での被害形態

	自分でデータ復旧ソフトなどを利用して元に戻した	自分で回復の方法を調べて（ソフトは利用せず）元に戻した	家族・知人に回復の方法を教えてもらい元に戻した	家族・知人に依頼し元に戻してもらった	専門業者へウィルス駆除やデータの復旧を依頼した	感染した端末を廃棄した（買い替えた）	その他
全体	35.8%	25.3%	12.1%	6.2%	10.5%	8.6%	1.6%
男性	41.4%	30.9%	10.5%	3.7%	5.6%	6.2%	1.9%
女性	26.3%	15.8%	14.7%	10.5%	18.9%	12.6%	1.1%

5. セキュリティ対策状況

最も浸透している対策は「セキュリティソフト・アプリ使用」で、利用している端末の種類毎では、パソコン82.5%、スマホ50.6%、タブレット47.6%の導入率である。

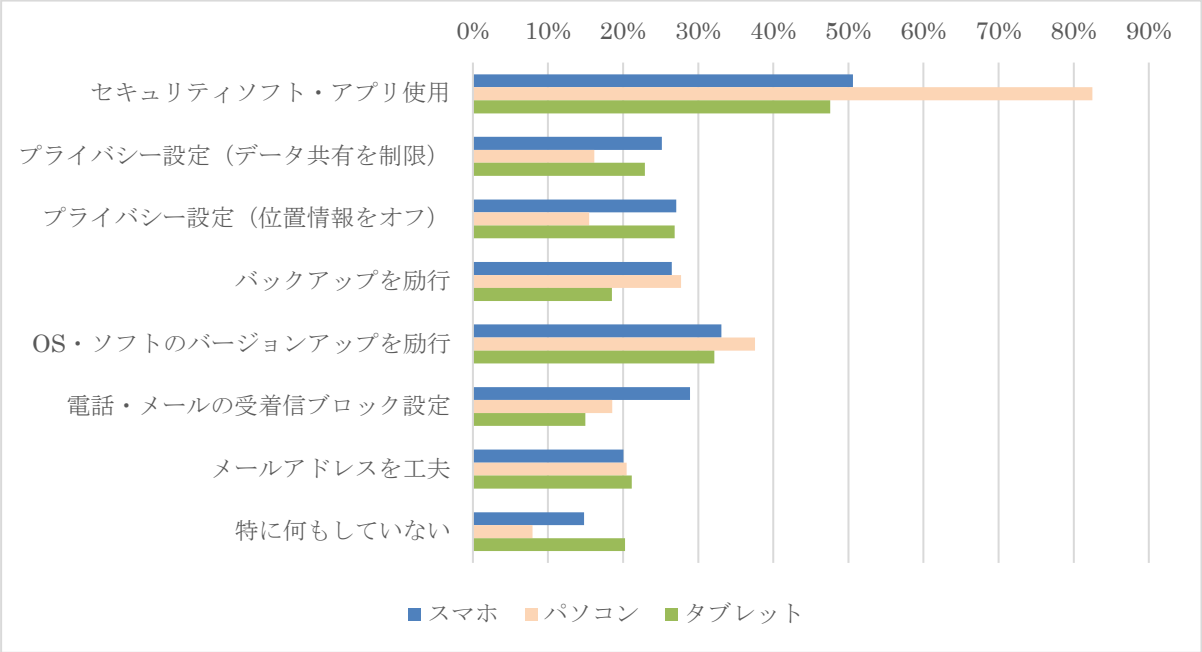
対象者が日常行っているセキュリティ対策の概況は図表 5-1 のとおりである。

最も浸透している対策はパソコンにおける「セキュリティソフト・アプリ使用」で、パソコン利用者の 82.5%が導入している。これを世代別に見ると、男女ともに 30 代～60 代は総じて高い導入率であるが、これも男女ともに 20 代の導入率が一番低くなっており（男性 76.6%、女性 57.1%）、有料ソフト・アプリへの投資意向が反映していると見られる。

また、パソコンでの「バックアップの励行」、「OS・ソフトのバージョンアップの励行」も男女ともに 20 代の実施率が一番低く、中高年層は総じて実施率が高い。

一方、ある程度のデジタルリテラシーを必要とする「プライバシー設定」（スマホ）は、意外にも若年層に極端に偏ることもなく、全年代で均等に利用されている。

＜図表 5-1＞利用端末でのセキュリティ対策



設問で対象とした上記対策の他にも、ID・パスワードの使い回しをせず一定期間に更新する、メールの添付ファイル・リンクの URL を不用意に開かない、二段階認証を利用するといった対策も現実的対応として有効である。

また、直近では宅配業者を装ったメールによるセキュリティ被害が増えている等、時期によって犯罪の手口に一定の傾向があるケースも多く、これらの情報への感度を高くしておくことも必要である。

以上